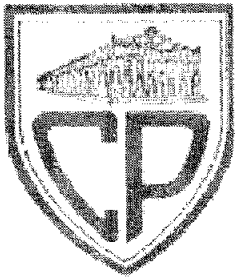
328348



COLEGIO PARTENÓN, S. C.

INC. U.N.A.M. 3283

ELEMENTOS DE SEGURIDAD EN INFORMÁTICA

T E S I S

QUE PARA OBTENER EL TITULO DE:
LICENCIADO EN INFORMÁTICA
P R E S E N T A:
GONZÁLEZ TRUJILLO LUIS MAURICIO

ASESOR: LIC. DAVID MONROY RODRÍGUEZ

MÉXICO, D. F. SEPTIEMBRE 2005

M352142

Universidad Nacional Autónoma de México
UNAM
Biblioteca Central
Dirección General de Bibliotecas de la UNAM

UNAM – Dirección General de Bibliotecas
Tesis Digitales
Restricciones de uso

DERECHOS RESERVADOS ©
PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

Todo el material contenido en esta tesis esta protegido por la Ley Federal del Derecho de Autor (LFDA) de los Estados Unidos Mexicanos (México).

El uso de imágenes, fragmentos de videos, y demás material que sea objeto de protección de los derechos de autor, será exclusivamente para fines educativos e informativos y deberá citar la fuente donde la obtuvo mencionando el autor o autores. Cualquier uso distinto como el lucro, reproducción, edición o modificación, será perseguido y sancionado por el respectivo titular de los Derechos de Autor.

¡MIL GRACIAS¡

A DIOS POR LA FUERZA, A MI MAMA ESTA TESIS ES TUYA, POR TI Y PARA MI, SIN TI NO LO HUBIESE LOGRADO, POR TUS DESVELOS, PREOCUPACIONES Y ESFUERZO.

A MI PAPA Y MIS HERMANOS POR SU COOPERACIÓN Y CONFIANZA, NO IMPORTA SER EL ULTIMO.

A MI BRUJITA BONITA (MARA) TU ERES PARTE DE ESTO, POR AYUDARME, AGUANTARME Y DARME FUERZAS, POR QUE TE AMO Y SIEMPRE SEREMOS M & M.

AL PARTENON, POR HACER DE MI SUEÑO UNA REALIDAD NUNCA LO OLVIDARE.

AL PROF. MONROY, POR GUIARME, Y A TODOS MIS MAESTROS Y PERSONAL ADMINISTRATIVO QUE DE UNA U OTRA MANERA INFLUYERON EN MI, SIEMPRE PARA BIEN, AUNQUE NO LO PAREZCA.

A MIS AMIGOS ANJFB, QUE ME QUIEREN Y SON CORRESPONDIDOS, A MIS OTROS COMPAÑEROS Y A LOS QUE ME ODIAN, PERO SIEMPRE SE QUEDARAN CON LA GANAS DE ESTAR CONMIGO Y SER COMO YO...TAMBIÉN

Y COMO DICE EL REFRÁN MAS VALE TARDE QUE NUNCA Y ESPERO QUE TODO EN MI VIDA FUTURA, SEA COMO HASTA AHORA CON SALUD, SIENDO FELIZ Y DANDO GRACIAS POR LO QUE TENGO.

"ELEMENTOS DE SEGURIDAD EN INFORMÁTICA"

ÍNDICE

- **INTRODUCCIÓN** 3

- **PLANTEAMIENTO DEL PROBLEMA** 9

- **HIPÓTESIS AFIRMATIVAS** 12

- **JUSTIFICACIÓN DEL TEMA** 15

- **CAPITULO 1 SEGURIDAD LÓGICA** 18

1.1 Controles de Acceso 18
1.2 Identificación y Autentificación 19
Roles 21
Transacciones 21
1.3 Limitaciones a los servicios 22
1.4 Criptografía 22
Listas de Control de Accesos 24
1.5 Limites sobre la interfase de usuario 24
1.6 Administración 25
1.6.1 Administración del Personal y Usuarios 25
1.7 Niveles de Seguridad informática 26
Nivel D 26
1.7.1 Nivel C1: Protección Discrecional 26
1.7.2 Nivel C2: Protección de Acceso Controlado 27
1.7.3 Nivel B1: Seguridad Etiquetada 27
1.7.4 Nivel B2: Protección Estructurada 28
1.7.5 Nivel B3: Dominios de Seguridad 28
1.7.6 Nivel A: Protección Verificada 28

- **CAPITULO 2 DELITOS INFORMÁTICOS** 32

2.1 La información y el delito 32
2.2 Tipos de delitos informáticos 36
2.3 Delincuente y Victima 37

CAPITULO 3 AMENAZAS HUMANAS 41

3.1 Carta de Presentación 41
3.2 Definición de Hacker 45
3.3 Definición de Crackers 45
3.4 Definición de Phreakers 46
3.5 Definición de Carding Trashing 47
3.6 Desafíos de un Hacker 48
3.7 Habilidades básicas en un Hacker 48
3.8 ¿Cómo lo hacen? 49
3.9 La ética del Hacker 49
3.10 Manifiesto Hacker 50
3.11 Otros habitantes del Ciberespacio 51
Gurus 51
Lamers o Script Kidders 51
3.12 Personal (Insiders) 51
3.13 Personal Interno 52
3.14 Ex Empleado 52
3.15 Curiosos 53
3.16 Terroristas 53
3.17 Intrusos remunerados 53
3.18 Recomendaciones 53

CAPITULO 4 AMENAZAS LÓGICAS 58

4.1 Acceso, Uso y Autorización 58
4.2 Detección de intrusos 59
4.3 Identificación de las amenazas 61
4.4 Tipos de ataque 61
4.5 Trashing (cartoneo) 62
Ataques de monitorización 62
4.6 Shoulder Surfing 62
4.7 Decoy (señuelos) 63
4.8 Scanning (busqueda) 63
4.8.1 T C P Connect Scanning 63
4.8.2 T C P SYN Scanning 64
4.8.3 T C P FIN Scanning Stealth Port Scanning 65
4.8.4 Fragmentation Scanning 66
4.9 Eavesdropping Packet Sniffing 66
4.10 Snooping Downloading 67
4.11 Ataques de Autentificacion 67
4.11.1 Spoofing Looping 67
4.11.2 Web Spoofing 68
4.11.3 IP Splicing Hijacking 68
4.11.4 Utilización de BackDoors 69

4.11.5 Utilización de Exploits 70
4.11.6 Obtención de Passwords 70
4.11.7 Uso de Diccionarios 70
4.12 Denial of Service (D o S) 71
4.12.1 Jamming o Flooding 72
4.12.2 Syn Flood 72
4.12.3 Connection Flood 74
4.12.4 Net Flood 74
4.12.5 Land Attack 75
4.12.6 Smurf o Broadcast Store 75
4.12.7 OOB, Supernuke o Winnuke 77
4.12.8 Teardrop I y IINewtearBonk-Boink 77
4.12.9 E - Mail Bombing y Spamming 77
4.13 Ataques de Modificación Daño - Tampering o Data Diddling 78
4.13.1 Borrado de Huellas 78
4.13.2 Ataques Mediante Java Applets 79
4.13.3 Ataques Mediante JavaScript y VBScript 79
4.13.4 Ataques Mediante ActiveX 79
4.13.5 Vulnerabilidades en los Navegadores 80
4.14 Errores de Diseño, Implementación y Operación 81
4.15 Implementación de estas Técnicas 81
4.16 ¿Cómo defenderse de estos Ataques? 82
4.17 Creación y difusión de Virus 83
4.18 Virus Informáticos vs. virus Biológicos 83
4.19 Origen 84
4.20 Los números Hablan 86
4.21 Descripción de un Virus 88
4.21.1 Riesgos de Infección 89
4.21.2 Técnicas de Propagación 89
4.21.3 Incubación 90
4.22 Tipos de Virus 91
4.22.1 Archivos Ejecutables (Virus Exe Vir) 91
4.22.2 Virus en el Sector de Arranque (Virus ACSO Anterior a la carga del SO) 92
4.22.3 Virus Residente 92
4.22.4 Macro Virus 92
4.22.5 Virus de Mail 93
4.22.6 Virus de Sabotaje 93
4.22.7 Hoax, los Virus Fantasmas 93
4.22.8 Virus de Applets Java y Controles Active X 94
4.22.9 Reproductores Gusanos 94
4.22.10 Caballos de Troya 94
4.22.11 Bombas Lógicas 94
4.22.12 Cookies 95
4.22.13 Sniffers 95

4.23 Modelo de Virus Informático 95
4.24 Tipos de Daños Ocasionados por los Virus 96
4.25 Los Autores 97
4.26 Programa Antivirus 97
4.27 Modelo de un Antivirus 99
4.28 Utilización de los Antivirus 100
4.29 Aspectos Jurídicos sobre Virus Informáticos 100
4.30 Consejos 101

CAPITULO 5 FIREWALLS Y SEGURIDAD EN INTERNET 105

5.1 Beneficios de un firewall en Internet 106
5.2 Limitaciones de un firewall 107
5.3 Conexión circunvecina al firewall de Internet 108
Herramientas del hacker 109
5.4 Recolección de información 109
5.5 Sondeo del sistema para debilitar la seguridad 110
5.6 Acceso a sistemas protegidos 111
5.7 Bases para el diseño decisivo del firewall 111
5.8 Políticas del firewall 111
5.9 Política interna de la seguridad 112
5.10 Costo del firewall 112
5.11 Componentes del sistema firewall 113
5.12 Edificando obstáculos: ruteador filtra-paquetes 115
5.12.1 Servicio dependiente del filtrado 116
5.12.2 Servicio independiente del filtrado 116
5.12.3 Agresiones Originadas Por El Direccionamiento IP 116
5.12.4 Agresiones Originadas En El Ruteador 117
5.12.5 Agresiones Por Fragmentación 117
5.12.6 Beneficios del ruteador filtra-paquetes 117
5.12.7 Limitaciones del ruteador filtra-paquetes 117
5.12.8 Gateways a nivel-aplicación 118
5.12.9 Servidor de defensa 119
5.12.10 Sistema de seguridad por el Gateway a nivel-aplicación 120
5.12.11 Beneficios del gateway a nivel-aplicación 121
5.12.12 Limitaciones del gateway a nivel-aplicación 122
5.12.13 Gateway a nivel-circuito 122
5.12.14 La operación de una conexión típica Telnet a través de un Gateway a Nivel-circuito 122

CAPITULO 6 REDES 125

6.1 Seguridad física 126
6.2 Seguridad Perimetral 126
6.3 Monitorear constantemente la red 127

6.4 Mantener las computadoras al día 127
6.5 Protección de datos en los medios digitales 127
6.6 Las cláusulas de información 128
6.7 Respecto a la colocación de Cookies 129
6.8 Respecto a la finalidad de los datos recogidos 129
6.9 Respecto a las cesiones y la finalidad de la cesión 130
6.10 Síntomas para detectar un virus 130
6.11 Objetivos de las redes 130
6.12 Estructuras 132
6.13 Tecnologías de transmisión 133
6.14 Modelo Cliente / Servidor 134
Tecnología de objetos 134
6.15 Sistemas abiertos 134
6.16 El modelo OSI 135
6.16.1 Transmisión de Datos en el Modelo OSI 136
6.17 Protocolos de red 138
6.17.1 NETBIOS – NETBEUI – NWLINK – WINS 139
6.17.2 TCP / IP 139
6.17.3 Las capas del modelo TCP / IP 139
6.17.4 Funcionamiento 141
6.17.5 Comparación con el modelo OSI 141
6.18 Nivel físico del modelo TCP / IP "ARP" Y "RARP" 141
6.19 Nivel de datos del modelo TCP / IP "SLIP" 142
6.19.1 PPP 142
6.20 Nivel de red del modelo TCP / IP "IPXSPX" 143
6.20.1 IP 143
DNS Nombre de Dominio 144
6.20.2 Puertos 145
APPLE TALK 145
6.21 Nivel de transporte del modelo TCP/IP "TCP" 145
6.22 UDP 148
6.23 Nivel de aplicación del modelo TCP/IP "ICMP" Y "FTP" 148
6.24 HTTP 149
6.25 SMTP 150
6.26 POP 151
6.27 MIME 151
NNTP 151
SNMP 152
6.28 Estructura básica de la Web 152
6.29 Servicios de Internet 152
6.30 TELNET 153
6.31 IRC 153
6.32 USE NET 154
6.33 FINGER 155
6.34 WHO IS 155

- **CONCLUSIÓN** 158

- **GLOSARIO DE TÉRMINOS** 164

- **APÉNDICE "FIGURAS Y TABLAS"** 181

- **BIBLIOGRAFÍA** 184

INTRODUCCIÓN

INTRODUCCIÓN

"Ser lo que soy, no es nada sin la Seguridad". Sin duda W. Shakespeare, tenía un concepto más evolucionado de la seguridad que sus contemporáneos del siglo XV y quizás también que algunos de los nuestros.

La meta es ambiciosa. La seguridad como materia académica no existe, y es considerada por los "estudiosos" como una herramienta dentro del ámbito en que se la estudia:

Estudios de riesgo, prevención de crímenes y pérdidas, etc.

Muchos sostienen que es una teoría tan amplia, compleja y abstracta como la pobreza, la belleza o el amor; y ni siquiera arriesgan su definición.

El amplio desarrollo de las nuevas tecnologías informáticas está ofreciendo un nuevo campo de acción a conductas antisociales y delictivas manifestadas en formas antes imposibles de imaginar, ofreciendo la posibilidad de cometer delitos tradicionales en formas no tradicionales.

El motivo de la presente es desarrollar un estudio de los elementos de la Seguridad en Informática, que continuamente se pone sobre el tapete y en realidad se conoce muy poco;

Se suele manejar con el amarillismo de los medios no especializados, dificultando esto su accionar y colocando en tela de juicio el arduo trabajo de los especialistas.

También intentaré brindar un plan de estrategias y metodologías, que sin bien no brindan la solución total (como muchos prometen), podrá cubrir parte del "agujero" que hoy se presenta al hablar de Seguridad Informática.

La mayoría del mundo informático desconoce la magnitud del problema con el que se enfrenta y, generalmente no se invierte ni el capital humano ni económico necesarios para prevenir, principalmente, el daño y/o pérdida de la información que, en última instancia es el Conocimiento con que se cuenta.

Paradójicamente, en el mundo informático, existe una demanda constante y muy importante que está esperando a que alguien los atienda.

La "Seguridad" es una necesidad básica. Estando interesada en la prevención de la vida y las posesiones, y es tan antigua como ella.

Los rimeros conceptos de seguridad se evidencian en los inicios de la escritura con los Sumerios (3000 AC) o el Hammurabi (2000 AC). También la Biblia, Homero, Cicerón, Cesar han sido autores de obras en donde aparecen ciertos rasgos de la seguridad en la guerra y el gobierno.

Los descubrimientos arqueológicos marcan, sin duda, las más importantes pruebas de seguridad de los antiguos: las pirámides egipcias, el palacio de Sargon, el templo Karnak en el valle del Nilo; el dios egipcio Anubi representado con una llave en su mano, etc.

Se sabe que los primitivos, para evitar amenazas, reaccionaban con los mismos métodos defensivos de los animales: luchando o huyendo (fight or flight), para eliminar o evitar la causa.

Así la pugna por la vida se convertía en una parte esencial y los conceptos de alertar, evitar, detectar, alarmar y reaccionar ya eran manejados por ellos.
Como todo concepto, la Seguridad se ha desarrollado y ha seguido una evolución dentro de las organizaciones sociales. La sociedad se conformó en familias, y esto se convirtió en un elemento limitante par huir. Se tuvieron que concebir nuevas estrategias de intimidación y disuasión para convencer al atacante que las pérdidas eran inaceptables contra las posibles ganancias.

La primera evidencia de una cultura y organización en seguridad "madura" aparece en los documentos de la Roma Imperial y Republicana.

El próximo paso de la Seguridad fue la especialización. Así nace la Seguridad Externa (aquella que se preocupa por la amenaza de entes externos hacia la organización); y la Seguridad Interna (aquella preocupada por las amenazas de nuestra organización con la organización misma). De estas dos se pueden desprender la Seguridad Privada y Pública al aparecer el estado y depositar su confianza en unidades armadas.

Desde el siglo XVIII, los descubrimientos científicos y el conocimiento resultante de la imprenta han contribuido a la cultura de la seguridad. Los principios de probabilidad, predicción y reducción de fallos y pérdidas han traído nueva luz a los sistemas de seguridad.

La seguridad moderna se originó con al Revolución Industrial para combatir los delitos y movimientos laborales, tan comunes en aquella época. Finalmente, un teórico y pionero del Management, Henry Fayol en 1919 identifica la Seguridad como una de las funciones empresariales, luego de la técnica, comercial, financiera, contable y directiva.

Al definir el objetivo de la Seguridad Fayol dice: "...salvaguardar propiedades y personas contra el robo, fuego, inundación contrarrestar huelgas y felonías, y de forma amplia todos los disturbios sociales que puedan poner en peligro el progreso e incluso la vida del negocio. Es, generalmente hablando, todas las medidas para conferir la requerida paz y tranquilidad (Peace of Mind) al personal".

Las medidas de seguridad a las que se refiere Fayol, sólo se restringían a los exclusivamente físicos de la instalación, ya que el mayor activo era justamente ese: los equipos, ni siquiera el empleado. Con la aparición de los "cerebros electrónicos", esta mentalidad se mantuvo, porque ¿Quien sería capaz de entender estos complicados aparatos como para poner en peligro la integridad de los datos por ellos utilizados?.

Hoy, la seguridad, desde el punto de vista legislativo, está en manos de los políticos, a quienes les toca decidir sobre su importancia, los delitos en que se pueden incurrir, y el respectivo castigo, si correspondiera. Este proceso ha conseguido importantes logros en las áreas de prevención del crimen, terrorismo y riesgo más que en el pensamiento general sobre Seguridad.

En cambio desde el punto de vista técnico, la seguridad está en manos de la dirección de las organizaciones y, en última instancia, en cada uno de nosotros y en nuestro grado de concientización respecto a la importancia de la información y el conocimiento en este nuevo milenio.

Es en este proceso en donde se aprecia que no se ha añadido ningún nuevo concepto a los ya conocidos en la antigüedad; los actuales sólo son perfeccionamientos de aquellos: llaves, cerraduras, cajas fuerte, puertas blindadas, trampas, vigilancia, etc.

Conceptos como Seguridad son "borrosos" o su definición se maneja con cierto grado de incertidumbre teniendo distinto significando para distintas personas. Esto tiene la peligrosa consecuencia de que la función de seguridad puede ser frecuentemente etiquetada como inadecuada o negligente, haciendo imposible a los responsables justificar sus técnicas ante reclamos basados en ambigüedades de conceptos y definiciones.

"La Seguridad es hoy día una profesión compleja con funciones especializadas".

Para dar una respuesta satisfactoria es necesario eliminar la incertidumbre y distinguir entre la seguridad filosófica y la operacional o práctica.

Como se sabe los problemas nunca se resuelven: la energía del problema no desaparece, sólo se transforma y la "solución" estará dada por su transformación en problemas diferentes, más pequeños y aceptables. Por ejemplo: la implementación de un sistema informático puede solucionar el problema de velocidad de procesamiento pero abrirá problemas como el de personal sobrante o reciclable. Estos, a su vez, descontentos pueden generar un problema de seguridad interno.

"La seguridad en un problema de antagonismo y competencia. Si no existe un competidor-amenaza el problema no es de seguridad".

En el plano social, comercial e industrial hemos evolucionado técnica y científicamente desde una era primitiva agrícola a una era postmoderna tecnológica, pero utilizando los mismos principios (e inclusos inferiores) a la época de las cavernas en el ambiente virtual:

Establecer el valor de la información es algo totalmente relativo, pues constituye un recurso que, en muchos casos, no se valora adecuadamente debido a su intangibilidad, cosa que no ocurre con los equipos, las aplicaciones y la documentación.

Existe Información que debe o puede ser pública: puede ser visualizada por cualquier persona (por ejemplo índice de analfabetismo en un país); y aquella que debe ser privada: sólo puede ser visualizada por un grupo selecto de personas que trabaja con ella (por ejemplo antecedentes médicos). En esta última debemos maximizar nuestros esfuerzos para preservarla de ese modo reconociendo las siguientes características en la Información:

1. Es Crítica: es indispensable para garantizar la continuidad operativa.
2. Es Valiosa: es un Activo con valor en sí misma.
3. Es Sensitiva: debe ser conocida por las personas que la procesan y sólo por ellas.

La Integridad de la Información es la característica que hace que su contenido permanezca inalterado a menos que sea modificado por personal autorizado, y esta modificación sea registrada para posteriores controles o auditorias. Una falla de integridad puede estar dada por anomalías en el hardware, software, virus informáticos y/o modificación por personas que se infiltran en el sistema.

La Disponibilidad u Operatividad de la Información es su capacidad de estar siempre disponible para ser procesada por las personas autorizadas. Esto requiere que la misma se mantenga correctamente almacenada con el hardware y el software funcionando perfectamente y que se respeten los formatos para su recuperación en forma satisfactoria.

La Privacidad o Confidencialidad de la Información es la necesidad de que la misma sólo sea conocida por personas autorizadas. En casos de falta de confidencialidad, la Información puede provocar severos daños a su dueño (por ejemplo conocer antecedentes médicos de una persona) o volverse obsoleta (por ejemplo: los planes de desarrollo de un producto que se "filtran" a una empresa competidora, facilitarán a esta última desarrollar un producto de características semejantes).

El Control sobre la información permite asegurar que sólo los usuarios autorizados pueden decidir cuando y como permitir el acceso a la misma.

La Autenticidad permite definir que la información requerida es válida y utilizable en tiempo, forma y distribución. Esta propiedad también permite asegurar el origen de la información, validando el emisor de la misma, para evitar suplantación de identidades.

Luego, el Daño es el resultado de la amenaza; aunque esto es sólo la mitad del problema. El daño también es el resultado de la no acción, o acción defectuosa, del protector. El daño puede producirse porque el protector no supo identificar adecuadamente la amenaza y, si lo hizo, se impusieron criterios comerciales por encima de los de seguridad. De allí que se deriven responsabilidades para la amenaza (por supuesto) pero también para la figura del protector.

Luego, el protector será el encargado de detectar cada una de las Vulnerabilidades (debilidades) del sistema que pueden ser explotadas y empleadas, por la amenaza, para comprometerlo. También será el encargado de aplicar las Contramedidas (técnicas de protección) adecuadas.

La Seguridad indicara el índice en que un Sistema Informático está libre de todo peligro, daño o riesgo. Esta característica es muy difícil de conseguir (según los especialistas imposible) en un 100% por lo que sólo se habla de Fiabilidad y se la define como "La probabilidad de que un sistema se comporte tal y como se espera de él"; y se habla de Sistema Fiable en vez de sistema seguro.

Luego para garantizar que un sistema sea fiable se deberá garantizar las características ya mencionadas de Integridad, Operatividad, Privacidad, Control y Autenticidad. Se deberá conocer "qué es lo que queremos proteger", "de quién lo queremos proteger", "cómo se puede lograr esto técnicamente"; para luego concluir con la formulación de estrategias adecuadas de seguridad tendientes a la disminución (¿anulación?) de los riesgos.

Comprender y conocer de seguridad ayudará a llevar a cabo análisis sobre los Riesgos, las Vulnerabilidades, Amenazas y Contramedidas; evaluar las ventajas o desventajas de la situación; a decidir medidas técnicas y tácticas metodológicas, físicas, e informáticas, en base de las necesidades de seguridad.

Es importante remarcar que cada unas de estas técnicas parten de la premisa de que no existe el 100% de seguridad esperado o deseable en estas circunstancias (por ejemplo: al cruzar la calle ¿estamos 100% seguros que nada nos pasará?).

PLANTEAMIENTO DEL PROBLEMA

PLANTEAMIENTO DEL PROBLEMA

1. ¿CUÁLES SON LOS FACTORES QUE DETERMINAN LA SEGURIDAD EN INFORMÁTICA?

2. ¿POR QUE ES IMPORTANTE TENER UN CONOCIMIENTO BÁSICO DE LA SEGURIDAD INFORMÁTICA?

HIPÓTESIS AFIRMATIVAS

HIPÓTESIS AFIRMATIVAS

1. LOS FABRICANTES DE SOFTWARE INCURREN EN DEFICIENCIAS TECNOLÓGICAS EN SUS PRODUCTOS.

2. LA FALTA DE PROFESIONALIZACIÓN DE LOS RESPONSABLES EN EL ÁREA DE INFORMÁTICA ES UN FACTOR DETERMINANTE EN LA CARENCIA DE SEGURIDAD EN DICHA ÁREA.

3. LA INFRAESTRUCTURA CON LA QUE CUENTA LA MAYORÍA DE LAS ÁREAS EN INFORMÁTICA, ES OBSOLETA O NO ESTÁN A LA VANGUARDIA TECNOLÓGICA PARA GARANTIZAR SU SEGURIDAD.

JUSTIFICACIÓN DEL TEMA

JUSTIFICACIÓN DEL TEMA

Los graduados de la licenciatura en informática deben tener los conocimientos y habilidades para asumir la responsabilidad y garantizar la seguridad del área de informática; Es por ello que asumí el reto de investigar el tema al que se hace alusión, con esto intentare dar un enfoque general de como podemos cuidar desde una computadora hasta un complejo sistema, y de acuerdo a lo que he observado y analizado, en la realidad estamos lejos de llegar a tener una cultura de Seguridad Informática, por lo que el tema podrá servir como base para informarse sobre este complejo problema y que de una u otra manera podamos hacer frente al entorno en el que vivimos,

En la actualidad uno de los problemas fundamentales para los lideres y responsables del las unidades de informática de las empresas es lograr obtener recursos para asegurar los activos digitales, seguidamente se exponen las razones fundamentales que justifican la ejecución de un proyecto de consultoría de seguridad informática para la plataforma de cualquier organización.

Adicionalmente, pretender cumplir con las metas diarias sin la utilización de los servicios de cómputo disponibles en el mercado para cualquier industria, resultaría imposible, por lo que es imprescindible crecer de forma organizada y segura, así como resguardar la información y servicios existentes.

Es importante destacar que aun cuando pueda mencionar algunos de los objetivos que alcanzaremos con la ejecución del proyecto, esencialmente el simple hecho de incrementar la cultura organizacional respecto a la seguridad informática genera una cantidad de objetivos adicionales que se estarían cumpliendo como consecuencia del desarrollo de una evaluación de seguridad.

El desarrollo de este tipo de proyectos en términos generales mejoraría rápida y efectivamente los niveles de calidad en la prestación de los servicios ofrecidos por la organización a nuestros clientes internos y externos, no solamente desde el punto de vista de mejora del rendimiento, sino también asegurando la información, su integridad, y confiabilidad y dedicando los recursos para lo que están planificados.

Uno de los principales problemas que afrontamos diariamente en nuestras organizaciones es la inexistencia de una política de seguridad informática bien definida y documentada; Entonces, este es el punto de partida para cualquier iniciativa al respecto, pero ¿Cómo aplicar políticas sin una evaluación profunda de la situación de la empresa, las herramientas que soportan la información, la determinación del nivel de conciencia de nuestros usuarios, sin conocer realmente que activo de información es más importante proteger o resguardar para la organización.

Definitivamente la labor es compleja y la responsabilidad inmensa, asegurar nuestra información es una actividad continua y necesaria.

CAPITULO 1

SEGURIDAD LÓGICA

CAPITULO 1

SEGURIDAD LÓGICA

1. SEGURIDAD LÓGICA

Nuestro sistema puede verse afectado contra la información por él almacenada y procesada.

El activo más importante que se posee es la información, y por lo tanto deben existir técnicas, que la aseguren. Estas técnicas las brinda la Seguridad Lógica.

Es decir que la Seguridad Lógica consiste en la "aplicación de barreras y procedimientos que resguarden el acceso a los datos y sólo se permita acceder a ellos a las personas autorizadas para hacerlo."

Existe un viejo dicho en la seguridad informática que dicta que "todo lo que no está permitido debe estar prohibido" y esto es lo que debe asegurar la Seguridad Lógica.

Los objetivos que se plantean serán:

1. Restringir el acceso a los programas y archivos.
2. Asegurar que los operadores puedan trabajar sin una supervisión minuciosa y no puedan modificar los programas ni los archivos que no correspondan.
3. Asegurar que se estén utilizados los datos, archivos y programas correctos en y por el procedimiento correcto.
4. Que la información transmitida sea recibida sólo por el destinatario al cual ha sido enviada y no a otro.
5. Que la información recibida sea la misma que ha sido transmitida.
6. Que existan sistemas alternativos secundarios de transmisión entre diferentes puntos.
7. Que se disponga de pasos alternativos de emergencia para la transmisión de información.

1.1 CONTROLES DE ACCESO

Estos controles pueden implementarse en el Sistema Operativo, sobre los sistemas de aplicación, en bases de datos, en un paquete específico de seguridad o en cualquier otro utilitario.

Constituyen una importante ayuda para proteger al sistema operativo de la red, al sistema de aplicación y demás software de la utilización o modificaciones no autorizadas; para mantener la integridad de la información (restringiendo la cantidad de usuarios y procesos con acceso permitido) y para resguardar la información confidencial de accesos no autorizados.

Asimismo, es conveniente tener en cuenta otras consideraciones referidas a la seguridad lógica, como por ejemplo las relacionadas al procedimiento que se lleva a cabo para determinar si corresponde un permiso de acceso (solicitado por un usuario) a un determinado recurso.

Al respecto, el National Institute for Standars and Technology (NIST) ha resumido los siguientes estándares de seguridad que se refieren a los requisitos mínimos de seguridad en cualquier sistema;

1.2 IDENTIFICACIÓN Y AUTENTIFICACIÓN

Es la primera línea de defensa para la mayoría de los sistemas computarizados, permitiendo prevenir el ingreso de personas no autorizadas. Es la base para la mayor parte de los controles de acceso y para el seguimiento de las actividades de los usuarios.

Se denomina Identificación al momento en que el usuario se da a conocer en el sistema; y Autenticación a la verificación que realiza el sistema sobre esta identificación.

Al igual que se consideró para la seguridad física, y basada en ella, existen cuatro tipos de técnicas que permiten realizar la autenticación de la identidad del usuario, las cuales pueden ser utilizadas individualmente o combinadas:

1. Algo que solamente el individuo conoce: por ejemplo una clave secreta de acceso o password, una clave criptográfica, un número de identificación personal o PIN, etc.
2. Algo que la persona posee: por ejemplo una tarjeta magnética.
3. Algo que el individuo es y que lo identifica unívocamente: por ejemplo las huellas digitales o la voz.
4. Algo que el individuo es capaz de hacer: por ejemplo los patrones de escritura.

Para cada una de estas técnicas vale lo mencionado en el caso de la seguridad física en cuanto a sus ventajas y desventajas. Se destaca que en los dos primeros casos enunciados, es frecuente que las claves sean olvidadas o que las tarjetas o dispositivos se pierdan, mientras que por otro lado, los controles de autenticación biométricos serían los más apropiados y fáciles de administrar, resultando ser también, los más costosos por lo dificultosos de su implementación eficiente.

Desde el punto de vista de la eficiencia, es conveniente que los usuarios sean identificados y autenticados solamente una vez, pudiendo acceder a partir de allí, a todas las aplicaciones y datos a los que su perfil les permita, tanto en sistemas locales como en sistemas a los que deba acceder en forma remota. Esto se denomina "single login" o sincronización de passwords.

Una de las posibles técnicas para implementar esta única identificación de usuarios sería la utilización de un servidor de autenticaciones sobre el cual los usuarios se identifican, y que se encarga luego de autenticar al usuario sobre los restantes equipos a los que éste pueda acceder.

Este servidor de autenticaciones no debe ser necesariamente un equipo independiente y puede tener sus funciones distribuidas tanto geográfica como lógicamente, de acuerdo con los requerimientos de carga de tareas.

La Seguridad Informática se basa, en gran medida, en la efectiva administración de los permisos de acceso a los recursos informáticos, basados en la identificación, autenticación y autorización de accesos. Esta administración abarca:

1. Proceso de solicitud, establecimiento, manejo, seguimiento y cierre de las cuentas de usuarios. Es necesario considerar que la solicitud de habilitación de un permiso de acceso para un usuario determinado, debe provenir de su superior y, de acuerdo con sus requerimientos específicos de acceso, debe generarse el perfil en el sistema de seguridad, en el sistema operativo o en la aplicación según corresponda.
2. Además, la identificación de los usuarios debe definirse de acuerdo con una norma homogénea para toda la organización.
3. Revisiones periódicas sobre la administración de las cuentas y los permisos de acceso establecidos. Las mismas deben encararse desde el punto de vista del sistema operativo, y aplicación por aplicación, pudiendo ser llevadas a cabo por personal de auditoria o por la gerencia propietaria del sistema; siempre sobre la base de que cada usuario disponga del mínimo permiso que requiera de acuerdo con sus funciones.
4. Las revisiones deben orientarse a verificar la adecuación de los permisos de acceso de cada individuo de acuerdo con sus necesidades operativas, la actividad de las cuentas de usuarios o la autorización de cada habilitación de acceso. Para esto, deben analizarse las cuentas en busca de períodos de inactividad o cualquier otro aspecto anormal que permita una redefinición de la necesidad de acceso.
5. Detección de actividades no autorizadas. Además de realizar auditorias o efectuar el seguimiento de los registros de transacciones (pistas), existen otras medidas que ayudan a detectar la ocurrencia de actividades no autorizadas. Algunas de ellas se basan en evitar la dependencia hacia personas determinadas, estableciendo la obligatoriedad de tomar vacaciones o efectuando rotaciones periódicas a las funciones asignadas a cada una.
6. Nuevas consideraciones relacionadas con cambios en la asignación de funciones del empleado. Para implementar la rotación de funciones, o en caso de reasignar funciones por ausencias temporales de algunos empleados, es necesario considerar la importancia de mantener actualizados los permisos de acceso.
7. Procedimientos a tener en cuenta en caso de desvinculaciones de personal con la organización, llevadas a cabo en forma amistosa o no. Los despidos del personal de sistemas presentan altos riesgos ya que en general se trata de empleados con capacidad para modificar aplicaciones o la configuración del sistema, dejando "bombas lógicas" o destruyendo sistemas o recursos informáticos. No obstante, el personal de otras áreas usuarias de los sistemas también puede causar daños, por ejemplo, introduciendo información errónea a las aplicaciones intencionalmente.

Para evitar estas situaciones, es recomendable anular los permisos de acceso a las personas que se desvincularán de la organización, lo antes posible. En caso de despido, el permiso de acceso debería anularse previamente a la notificación de la persona sobre la situación.

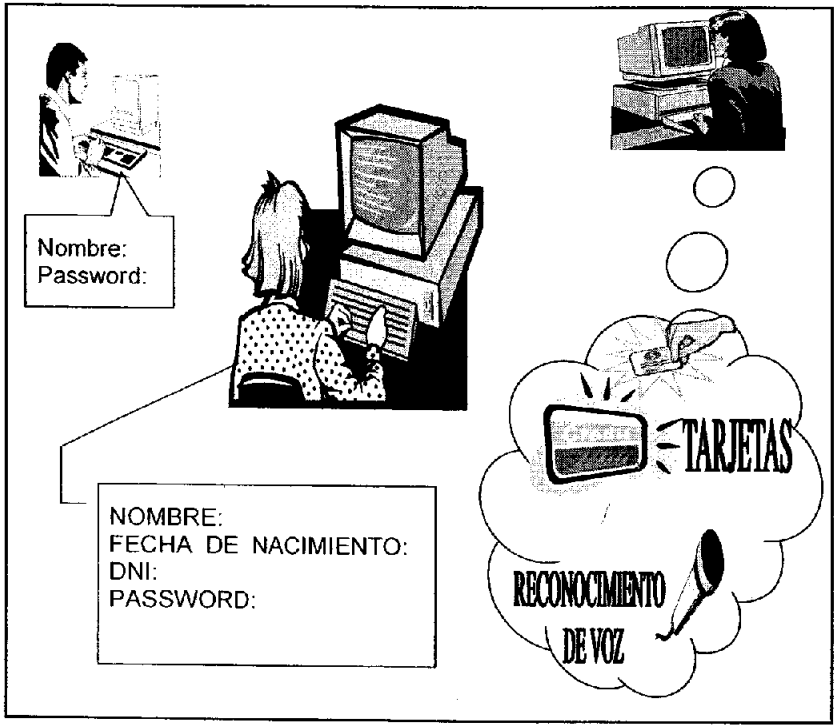


FIG. 1 EJEMPLO DE CONTRASEÑAS

ROLES

El acceso a la información también puede controlarse a través de la función o rol del usuario que requiere dicho acceso. Algunos ejemplos de roles serían los siguientes: programador, líder de proyecto, gerente de un área usuaria, administrador del sistema, etc. En este caso los derechos de acceso pueden agruparse de acuerdo con el rol de los usuarios.

TRANSACCIONES

También pueden implementarse controles a través de las transacciones, por ejemplo solicitando una clave al requerir el procesamiento de una transacción determinada.

1.3 LIMITACIONES A LOS SERVICIOS

Estos controles se refieren a las restricciones que dependen de parámetros propios de la utilización de la aplicación o preestablecidos por el administrador del sistema. Un ejemplo podría ser que en la organización se disponga de licencias para la utilización simultánea de un equipo o de varios equipos y así mismo tener el control sobre ellos.

Se podrá, por años, seguir creando sistemas altamente seguros, pero en última instancia cada uno de ellos se romperá por este eslabón: la elección de passwords débiles.

Es mi deseo que después de la lectura del presente quede la idea útil de usar passwords seguras ya que aquí radican entre el 90% y 99% de los problemas de seguridad planteados.

Sincronización de passwords: consiste en permitir que un usuario acceda con la misma password a diferentes sistemas interrelacionados y, su actualización automática en todos ellos en caso de ser modificada. Podría pensarse que esta es una característica negativa para la seguridad de un sistema, ya que una vez descubierta la clave de un usuario, se podría tener acceso a los múltiples sistemas a los que tiene acceso dicho usuario.

Sin embargo, estudios hechos muestran que las personas normalmente suelen manejar un solo password para todos los sitios a los que tengan acceso, y que si se los fuerza a elegir diferentes passwords tienden a guardarlas escritas para no olvidarlas, lo cual significa un riesgo aún mayor. Para implementar la sincronización de passwords entre sistemas es necesario que todos ellos tengan un alto nivel de seguridad.

1.4 CRIPTOGRAFÍA

Desde que el hombre ha necesitado comunicarse con los demás ha tenido la necesidad de que algunos de sus mensajes solo fueran conocidos por las personas a quien estaban destinados. La necesidad de poder enviar mensajes de forma que solo fueran entendidos por los destinatarios hizo que se crearan sistemas de cifrado, de forma que un mensaje después de un proceso de transformación, lo que llamamos cifrado, solo pudiera ser leído siguiendo un proceso de descifrado. Las civilizaciones mas antiguas (egipcia, mesopotámica, china..) ya usaban esos métodos.

Uno de los primeros métodos de encriptado que está documentado es atribuido a Julio Cesar, que se basaba en la sustitución de las letras de un documento por la tercera letra que le correspondiese en el alfabeto. Así la A se convertía en una D, la B en E ...

Con el tiempo y debido principalmente a su uso militar, los sistemas criptográficos fueron avanzando en complejidad, hasta llegar a nuestros días donde la informática ha entrado en nuestras vidas y la necesidad de seguridad al realizar nuestras operaciones aumenta.

Como funciona

La palabra criptología proviene de las palabras griegas Kryto y logos y significa estudio de lo oculto. Una rama de la criptología es la criptografía, que se ocupa del cifrado de mensajes. Esta se basa en que el emisor emite un mensaje en claro, que es tratado mediante un cifrador con la ayuda de una clave, para crear un texto cifrado. Este texto cifrado, por medio del canal de comunicación establecido, llega al descifrador que convierte el texto cifrado, apoyándose en otra clave, para obtener el texto en claro original. Las dos claves implicadas en el proceso de cifrado/descifrado pueden ser o no iguales dependiendo del sistema de cifrado utilizado.

La información encriptada solamente puede ser desencriptada por quienes posean la clave apropiada. La encriptación puede proveer de una potente medida de control de acceso.

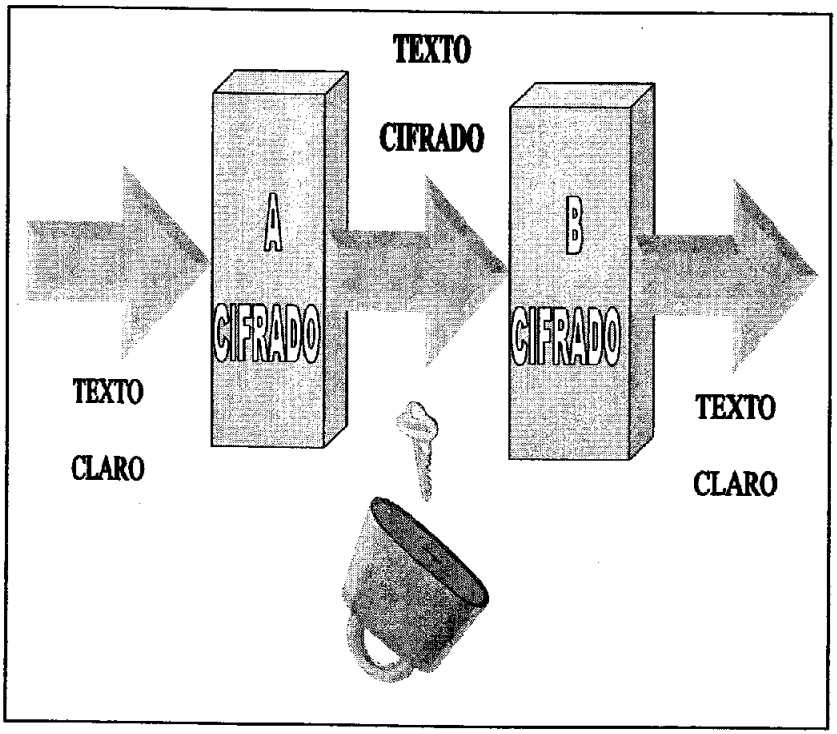


FIG. 2 EJEMPLO DE ENCRIPTACIÓN

LISTAS DE CONTROL DE ACCESOS

Se refiere a un registro donde se encuentran los nombres de los usuarios que obtuvieron el permiso de acceso a un determinado recurso del sistema, así como la modalidad de acceso permitido. Este tipo de listas varían considerablemente en su capacidad y flexibilidad.

1.5 LÍMITES SOBRE LA INTERFASE DE USUARIO

Esto límites, generalmente, son utilizados en conjunto con las listas de control de accesos y restringen a los usuarios a funciones específicas. Básicamente pueden ser de tres tipos: menús, vistas sobre la base de datos y límites físicos sobre la interfase de usuario. Por ejemplo los cajeros automáticos donde el usuario sólo puede ejecutar ciertas funciones presionando teclas específicas.

La política de seguridad que se desarrolle respecto a la seguridad lógica debe guiar a las decisiones referidas a la determinación de los controles de accesos y especificando las consideraciones necesarias para el establecimiento de perfiles de usuarios.

La definición de los permisos de acceso requiere determinar cual será el nivel de seguridad necesario sobre los datos, por lo que es imprescindible clasificar la información, determinando el riesgo que produciría una eventual exposición de la misma a usuarios no autorizados.

Así los diversos niveles de la información requerirán diferentes medidas y niveles de seguridad.

Para empezar la implementación, es conveniente comenzar definiendo las medidas de seguridad sobre la información más sensible o las aplicaciones más críticas, y avanzar de acuerdo a un orden de prioridad descendiente, establecido alrededor de las aplicaciones.

Una vez clasificados los datos, deberán establecerse las medidas de seguridad para cada uno de los niveles.

Un programa específico para la administración de los usuarios informáticos desarrollado sobre la base de las consideraciones expuestas, puede constituir un compromiso vacío, si no existe una conciencia de la seguridad organizacional por parte de todos los empleados.

Esta conciencia de la seguridad puede alcanzarse mediante el ejemplo del personal directivo en el cumplimiento de las políticas y el establecimiento de compromisos firmados por el personal, donde se especifique la responsabilidad de cada uno.

Pero además de este compromiso debe existir una concientización por parte de la administración hacia el personal en donde se remarque la importancia de la información y

las consecuencias posibles de su pérdida o apropiación de la misma por agentes extraños a la organización.

1.6 ADMINISTRACIÓN

Toda vez que se establecieron los controles de acceso sobre los sistemas y la aplicación, es necesario realizar una eficiente administración de estas medidas de seguridad, lo que involucra la implementación, seguimientos, pruebas y modificaciones sobre los accesos de los usuarios de los sistemas.

La política de seguridad que se desarrolle debe guiar a las decisiones referidas a la determinación de los controles de acceso y especificando las condiciones necesarias para el establecimiento de perfiles de usuarios.

La definición de los permisos de acceso requiere determinar cual será el nivel de seguridad necesario sobre los datos, por lo que es imprescindible clasificar la información, determinando el riesgo que produciría una eventual exposición de la misma a usuarios no autorizados.

Así los diversos niveles de la información

1.6.1 ADMINISTRACIÓN DEL PERSONAL Y USUARIOS

Organización del Personal

Este proceso lleva generalmente cuatro pasos:

1. Definición de puestos: debe contemplarse la máxima separación de funciones posibles y el otorgamiento del mínimo permiso de acceso requerido por cada puesto para la ejecución de las tareas asignadas.
2. Determinación de la sensibilidad del puesto: para esto es necesario determinar si la función requiere permisos riesgosos que le permitan alterar procesos, perpetrar fraudes o visualizar información confidencial.
3. Elección de la persona para cada puesto: requiere considerar los requerimientos de experiencia y conocimientos técnicos necesarios para cada puesto. Asimismo, para los puestos definidos como críticos puede requerirse una verificación de los antecedentes personales.
4. Entrenamiento inicial y continuo del empleado: cuando la persona seleccionada ingresa a la organización, además de sus responsabilidades individuales para la ejecución de las tares que se asignen, deben comunicárseles las políticas organizacionales, haciendo hincapié en la política de seguridad. El individuo debe conocer las disposiciones organizacionales, su responsabilidad en cuanto a la seguridad informática y lo que se espera de él.

Esta capacitación debe orientarse a incrementar la conciencia de la necesidad de proteger los recursos informáticos y a entrenar a los usuarios en la utilización de los sistemas y

equipos para que ellos puedan llevar a cabo sus funciones en forma segura, minimizando la ocurrencia de errores (principal riesgo relativo a la tecnología informática).

Sólo cuando los usuarios están capacitados y tienen una conciencia formada respecto de la seguridad pueden asumir su responsabilidad individual. Para esto, el ejemplo de la gerencia constituye la base fundamental para que el entrenamiento sea efectivo: el personal debe sentir que la seguridad es un elemento prioritario dentro de la organización.

1.7 NIVELES DE SEGURIDAD INFORMÁTICA

El estándar de niveles de seguridad mas utilizado internacionalmente es el TCSEC Orange Book, desarrollado en 1983 de acuerdo a las normas de seguridad en computadoras del Departamento de Defensa de los Estados Unidos.

Los niveles describen diferentes tipos de seguridad del Sistema Operativo y se enumeran desde el mínimo grado de seguridad al máximo.

Estos niveles han sido la base de desarrollo de estándares europeos (ITSEC/ITSEM) y luego internacionales (ISO/IEC).

Cabe aclarar que cada nivel requiere todos los niveles definidos anteriormente: así el subnivel B2 abarca los subniveles B1, C2, C1 y el D.

NIVEL D

Este nivel contiene sólo una división y está reservada para sistemas que han sido evaluados y no cumplen con ninguna especificación de seguridad. Sin sistemas no confiables, no hay protección para el hardware, el sistema operativo es inestable y no hay autentificación con respecto a los usuarios y sus derechos en el acceso a la información. Los sistemas operativos que responden a este nivel son MS-DOS y System 7.0 de Macintosh.

1.7.1 NIVEL C1: PROTECCIÓN DISCRECIONAL

Se requiere identificación de usuarios que permite el acceso a distinta información. Cada usuario puede manejar su información privada y se hace la distinción entre los usuarios y el administrador del sistema, quien tiene control total de acceso./

Muchas de las tareas cotidianas de administración del sistema sólo pueden ser realizadas por este "súper usuario"; quien tiene gran responsabilidad en la seguridad del mismo. Con la actual descentralización de los sistemas de cómputos, no es raro que en una organización encontremos dos o tres personas cumpliendo este rol. Esto es un problema, pues no hay forma de distinguir entre los cambios que hizo cada usuario.

A continuación se enumeran los requerimientos mínimos que debe cumplir la clase C1:

- Acceso de control discrecional: distinción entre usuarios y recursos. Se podrán definir grupos de usuarios (con los mismos privilegios) y grupos de objetos (archivos, directorios, disco) sobre los cuales podrán actuar usuarios o grupos de ellos.

- Identificación y Autentificación: se requiere que un usuario se identifique antes de comenzar a ejecutar acciones sobre el sistema. El dato de un usuario no podrá ser accedido por un usuario sin autorización o identificación.

1.7.2 NIVEL C2: PROTECCIÓN DE ACCESO CONTROLADO

Este subnivel fue diseñado para solucionar las debilidades del C1. Cuenta con características adicionales que crean un ambiente de acceso controlado. Se debe llevar una auditoria de accesos e intentos fallidos de acceso a objetos. Tiene la capacidad de restringir aún más el que los usuarios ejecuten ciertos comandos o tengan acceso a ciertos archivos, permitir o denegar datos a usuarios en concreto, con base no sólo en los permisos, sino también en los niveles de autorización.

Requiere que se audite el sistema. Esta auditoria es utilizada para llevar registros de todas las acciones relacionadas con la seguridad, como las actividades efectuadas por el administrador del sistema y sus usuarios. La auditoria requiere de autenticación adicional para estar seguros de que la persona que ejecuta el comando es quien dice ser. Su mayor desventaja reside en los recursos adicionales requeridos por el procesador y el subsistema de discos.

Los usuarios de un sistema C2 tienen la autorización para realizar algunas tareas de administración del sistema sin necesidad de ser administradores. Permite llevar mejor cuenta de las tareas relacionadas con la administración del sistema, ya que es cada usuario quien ejecuta el trabajo y no el administrador del sistema.

1.7.3 NIVEL B1: SEGURIDAD ETIQUETADA

Este subnivel, es el primero de los tres con que cuenta el nivel B. Soporta seguridad multinivel, como la secreta y ultrasecreta. Se establece que el dueño del archivo no puede modificar los permisos de un objeto que está bajo control de acceso obligatorio. A cada objeto del sistema (usuario, dato, etc.) se le asigna una etiqueta, con un nivel de seguridad jerárquico (alto secreto, secreto, reservado, etc.) y con unas categorías (contabilidad, nóminas, ventas, etc.).

Cada usuario que accede a un objeto debe poseer un permiso expreso para hacerlo y viceversa. Es decir que cada usuario tiene sus objetos asociados. También se establecen controles para limitar la propagación de derecho de accesos a los distintos objetos.

1.7.4 NIVEL B2: PROTECCIÓN ESTRUCTURADA

Requiere que se etiquete cada objeto de nivel superior por ser padre de un objeto inferior. La Protección Estructurada es la primera que empieza a referirse al problema de un objeto a un nivel mas elevado de seguridad en comunicación con otro objeto a un nivel inferior. Así, un disco rígido será etiquetado por almacenar archivos que son accedidos por distintos usuarios.

El sistema es capaz de alertar a los usuarios si sus condiciones de accesibilidad y seguridad son modificadas; y el administrador es el encargado de fijar los canales de almacenamiento y ancho de banda a utilizar por los demás usuarios.

1.7.5 NIVEL B3: DOMINIOS DE SEGURIDAD

Refuerza a los dominios con la instalación de hardware: por ejemplo el hardware de administración de memoria se usa para proteger el dominio de seguridad de acceso no autorizado a la modificación de objetos de diferentes dominios de seguridad. Existe un monitor de referencia que recibe las peticiones de acceso de cada usuario y las permite o las deniega según las políticas de acceso que se hayan definido.

Todas las estructuras de seguridad deben ser lo suficientemente pequeñas como para permitir análisis y tests ante posibles violaciones. Este nivel requiere que la terminal del usuario se conecte al sistema por medio de una conexión segura.

Además, cada usuario tiene asignado los lugares y objetos a los que puede acceder.

1.7.6 NIVEL A: PROTECCIÓN VERIFICADA

Es el nivel más elevado, incluye un proceso de diseño, control y verificación, mediante métodos formales (matemáticos) para asegurar todos los procesos que realiza un usuario sobre el sistema.

Para llegar a este nivel de seguridad, todos los componentes de los niveles inferiores deben incluirse. El diseño requiere ser verificado de forma matemática y también se deben realizar análisis de canales encubiertos y de distribución confiable. El software y el hardware son protegidos para evitar infiltraciones ante traslados o movimientos del equipamiento.

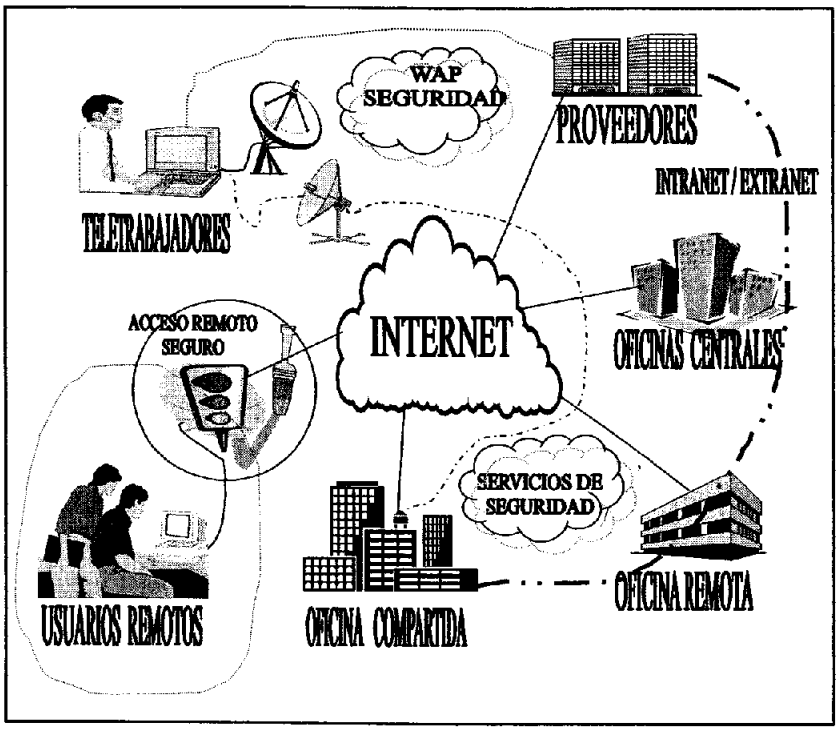


FIG. 3 FORMAS DE PROTECCIÓN

CAPITULO 2

DELITOS INFORMÁTICOS

CAPITULO 2

DELITOS INFORMÁTICOS

2. DELITOS INFORMÁTICOS

Ya he dejado en claro la importancia de la información en el mundo altamente tecnificado de hoy. También se ha dejado en claro cada uno de los riesgos "Naturales" con los que se enfrenta nuestro conocimiento y la forma de enfrentarlos.

El desarrollo de la tecnología informática ha abierto las puertas a nuevas posibilidades de delincuencia antes impensables. La cuantía de los perjuicios así ocasionados es a menudo muy superior a la usual en la delincuencia tradicional y también son mucho más elevadas las posibilidades de que no lleguen a descubrirse o castigarse.

Es propósito de los capítulos siguientes disertar sobre los riesgos "No naturales"; es decir los que se encuadran en el marco del delito. Para ello deberemos dejar en claro, nuevamente, algunos aspectos.

2.1 LA INFORMACIÓN Y EL DELITO

El delito informático implica actividades criminales que los países han tratado de encuadrar en figuras típicas de carácter tradicional, tales como robos, hurtos, fraudes, falsificaciones, perjuicios, estafas, sabotajes. Sin embargo, debe destacarse que el uso de las técnicas informáticas han creado nuevas posibilidades del uso indebido de las computadoras lo que ha creado la necesidad de regulación por parte del derecho.

Se considera que no existe una definición formal y universal de delito informático pero se han formulado conceptos respondiendo a realidades nacionales concretas: "no es labor fácil dar un concepto sobre delitos informáticos, en razón de que su misma denominación alude a una situación muy especial, ya que para hablar de "delitos" en el sentido de acciones típicas, es decir tipificadas o contempladas en textos jurídicos penales, se requiere que la expresión "delitos informáticos" esté consignada en los códigos penales, lo cual en nuestro país, al igual que en otros muchos no han sido objeto de tipificación aún".

En 1983, la Organización e Cooperación y Desarrollo Económico (OCDE) inicio un estudio de las posibilidades de aplicar y armonizar en el plano internacional las leyes penales a fin e luchar contra el problema del uso indebido de los programas computacionales.

En 1992 la Asociación Internacional de Derecho Penal, durante el coloquio celebrado en Wurzburgo (Alemania), adoptó diversas recomendaciones respecto a los delitos informáticos, entre ellas que, en la medida que el Derecho Penal no sea suficiente, deberá promoverse la modificación de la definición de los delitos existentes o la creación de otros nuevos, si no basta con la adopción de otras medidas como por ejemplo el "principio de subsidiariedad".

Se entiende Delito como: "acción penada por las leyes por realizarse en perjuicio de algo o alguien, o por ser contraria a lo establecido por aquéllas".

Finalmente la OCDE publicó un estudio sobre delitos informáticos y el análisis de la normativa jurídica en donde se reseñan las normas legislativas vigentes y se define Delito Informático como "cualquier comportamiento antijurídico, no ético o no autorizado, relacionado con el procesado automático de datos y/o transmisiones de datos".

"Los delitos informáticos se realizan necesariamente con la ayuda de los sistemas informáticos, pero tienen como objeto del injusto la información en sí misma".

Adicionalmente, la OCDE elaboró un conjunto de normas para la seguridad de los sistemas de información, con la intención de ofrecer las bases para que los distintos países pudieran erigir un marco de seguridad para los sistemas informáticos.

1. En esta delincuencia se trata con especialistas capaces de efectuar el crimen y borrar toda huella de los hechos, resultando, muchas veces, imposible de deducir como es como se realizó dicho delito. La Informática reúne características que la convierten en un medio idóneo para la comisión de nuevos tipos de delitos que en gran parte del mundo ni siquiera han podido ser catalogados.
2. La legislación sobre sistemas informáticos debería perseguir acercarse lo más posible a los distintos medios de protección ya existentes, pero creando una nueva regulación basada en los aspectos del objeto a proteger: la información.

En este punto debe hacerse un punto y notar lo siguiente:

No es la computadora la que atenta contra el hombre, es el hombre el que encontró una nueva herramienta, quizás la más poderosa hasta el momento, para delinquir.

No es la computadora la que afecta nuestra vida privada, sino el aprovechamiento que hacen ciertos individuos de los datos que ellas contienen.

La humanidad no está frente al peligro de la informática sino frente a individuos sin escrúpulos con aspiraciones de obtener el poder que significa el conocimiento.

Por eso la amenaza futura será directamente proporcional a los adelantos de las tecnologías informáticas.

La protección de los sistemas informáticos puede abordarse desde distintos perspectivas: civil, comercial o administrativa.

Lo que se deberá intentar es que ninguna de ellas sea excluyente con las demás y, todo lo contrario, lograr una protección global desde los distintos sectores para alcanzar cierta eficiencia en la defensa de estos sistemas informáticos.

Se clasifica a los delitos informáticos en base a dos criterios:

1. Como instrumento o medio: se tienen a las conductas criminales que se valen de las computadoras como método, medio o símbolo en la comisión del ilícito.

Ejemplos:

- Falsificación de documentos vía computarizada: tarjetas de créditos, cheques, etc.
- Variación de la situación contable.
- Planeamiento y simulación de delitos convencionales como robo, homicidio y fraude.
- Alteración el funcionamiento normal de un sistema mediante la introducción de código extraño al mismo: virus, bombas lógicas, etc.
- Intervención de líneas de comunicación de datos o teleprocesos.

2. Como fin u objetivo: se enmarcan las conductas criminales que van dirigidas en contra de la computadora, accesorios o programas como entidad física.

Ejemplos:

- Instrucciones que producen un bloqueo parcial o total del sistema.
- Destrucción de programas por cualquier método.
- Atentado físico contra la computadora, sus accesorios o sus medios de comunicación.
- Secuestro de soportes magnéticos con información valiosa, para ser utilizada con fines delictivos.

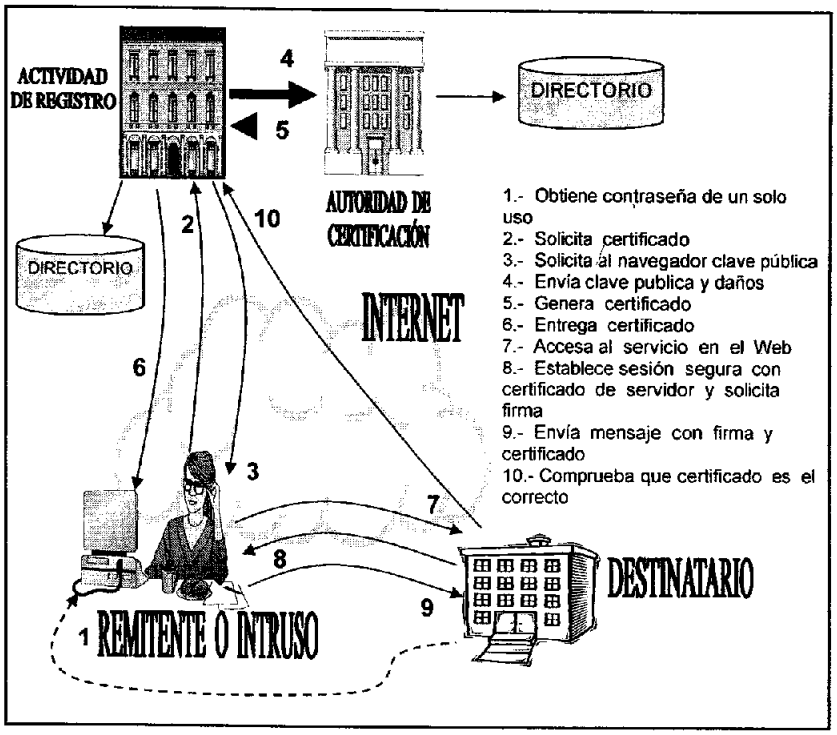


FIG. 4 EJEMPLO DE INTROMISIÓN

Podemos sostener que las acciones delictivas informáticas presentan las siguiente características:

1. Sólo una determinada cantidad de personas (con conocimientos técnicos por encima de lo normal) pueden llegar a cometerlos.
2. Son conductas criminales del tipo "cuello blanco": no de acuerdo al interés protegido (como en los delitos convencionales) sino de acuerdo al sujeto que los comete. Generalmente este sujeto tiene cierto status socioeconómico y la comisión del delito no puede explicarse por pobreza, carencia de recursos, baja educación, poca inteligencia, ni por inestabilidad emocional.
3. Son acciones ocupacionales, ya que generalmente se realizan cuando el sujeto atacado se encuentra trabajando.
4. Son acciones de oportunidad, ya que se aprovecha una ocasión creada por el atacante.
5. Provocan pérdidas económicas.
6. Ofrecen posibilidades de tiempo y espacio.

7. Son muchos los casos y pocas las denuncias, y todo ello por la falta de regulación y por miedo al descrédito de la organización atacada.
8. Presentan grandes dificultades para su comprobación, por su carácter técnico.
9. Tienden a proliferar, por lo se requiere su urgente regulación legal.

Por otra parte se presenta la siguiente clasificación de "delitos electrónicos"

1. Como Método: conductas criminales en donde los individuos utilizan métodos electrónicos para llegar a un resultado ilícito.
2. Como Medio: conductas criminales en donde para realizar un delito utilizan una computadora como medio o símbolo.
3. Como Fin: conductas criminales dirigidas contra la entidad física del objeto o máquina electrónica o su material con objeto de dañarla.

2.2 TIPOS DE DELITOS INFORMÁTICOS

La Organización de Naciones Unidas (ONU) reconocen los siguientes tipos de delitos informáticos:

- Fraude en el campo de la informática.
- Falsificación en materia informática.
- Sabotaje informático y daños a datos computarizados o programas informáticos.
- Acceso no autorizado.
- Intercepción sin autorización.
- Reproducción no autorizada de un programa informático protegido.
- Espionaje informático.
- Uso no autorizado de una computadora.
- Tráfico de claves informáticas obtenidas por medio ilícito.
- Distribución de virus o programas delictivos.

2.3 DELINCUENTE Y VICTIMA

SUJETO ACTIVO

Se llama así a las personas que cometen los delitos informáticos. Son aquellas que poseen ciertas características que no presentan el denominador común de los delincuentes, esto es, los sujetos activos tienen habilidades para el manejo de los sistemas informáticos y generalmente por su situación laboral se encuentran en lugares estratégicos donde se maneja información de carácter sensible, o bien son hábiles en el uso de los sistemas informatizados, aún cuando, en muchos de los casos, no desarrollen actividades laborales que faciliten la comisión de este tipo de delitos.

Con el tiempo se ha podido comprobar que los autores de los delitos informáticos son muy diversos y que lo que los diferencia entre sí es la naturaleza de los delitos cometidos. De esta forma, la persona que "entra" en un sistema informático sin intenciones delictivas es muy diferente del empleado de una institución financiera que desvía fondos de las cuentas de sus clientes.

El nivel típico de aptitudes del delincuente informático es tema de controversia ya que para algunos el nivel de aptitudes no es indicador de delincuencia informática en tanto que otros aducen que los posibles delincuentes informáticos son personas listas, decididas, motivadas y dispuestas a aceptar un reto tecnológico, características que pudieran encontrarse en un empleado del sector de procesamiento de datos.

Sin embargo, teniendo en cuenta las características ya mencionadas de las personas que cometen los delitos informáticos, estudiosos en la materia los han catalogado como delitos de "cuello blanco" término introducido por primera vez por el criminólogo norteamericano Edwin Sutherland en el año de 1943.

La "cifra negra" es muy alta; no es fácil descubrirlos ni sancionarlos, en razón del poder económico de quienes lo cometen, pero los daños económicos son altísimos; existe una gran indiferencia de la opinión pública sobre los daños ocasionados a la sociedad.

Legislar la instigación al delito cometido a través de la computadora. Adherimos, por nuestra parte, a los postulados de la ONU sobre los delitos informáticos, con el fin de unificar la legislación internacional que regule la problemática de la cibernética y su utilización tan generalizada en el mundo

Desde la Criminología debemos señalar que el anonimato, sumado a la inexistencia de una norma que tipifique los delitos señalados, son un factor criminal que favorece la multiplicación de autores que utilicen los medios electrónicos para cometer delitos a sabiendas que no serán alcanzados por la ley.

No solo debe pensarse en la forma de castigo, sino algo mucho más importante como lograr probar el delito. Este sigue siendo el principal inconveniente a la hora de legislar por el carácter intangible de la información.

"Al final, la gente se dará cuenta de que no tiene ningún sentido escribir leyes específicas para la tecnología. El fraude es el fraude, se realice mediante el correo postal, el teléfono o Internet. Un delito no es más o menos delito si se utilizó criptografía (...). Y el chantaje no es mejor o peor si se utilizaron virus informáticos o fotos comprometedoras, a la antigua usanza. Las buenas leyes son escritas para ser independientes de la tecnología. En un mundo donde la tecnología avanza mucho más deprisa que las sesiones del Congreso, eso es lo único que puede funcionar hoy en día. Mejores y más rápidos mecanismos de legislación, juicios y sentencias...quizás algún día".

CAPITULO 3

AMENAZAS HUMANAS

CAPITULO 3

AMENAZAS HUMANAS

3. AMENAZAS HUMANAS

Este capítulo trata sobre cada uno de los personajes que pueden ser potenciales atacantes de nuestro sistema: el mundo under y el personal perteneciente a la organización.

En el presente sólo se tratará de exponer el perfil de la persona encargada de una de las principales, (publicitariamente), si bien no la mayor amenaza que asechan nuestro sistema informático; para luego sí entrar en las formas de ataques propiamente dichos.

3.1 CARTA DE PRESENTACIÓN

"Hola, soy Cybor. Probablemente no me conozcan. Tampoco pretendo salir en la prensa. Eso no me importa, sin embargo si hay otras cosas que me interesan mas que mi identidad. Por ejemplo, me interesan las aperturas de sistemas cifrados. Pero eso es algo que nadie te enseña. Eso tienes que aprenderlo por ti mismo. También me interesa que todos sepáis quienes somos y que no estamos solos en este peculiar mundo. Me interesa que sepan que no todos los Hackers somos iguales. También me interesa saber que la palabra Hacker tiene un significado muy curioso. En un articulo reciente se publicó que se nos conocían como piratas informáticos; es probable, pero creo que están tremendamente equivocados.

Quiero reivindicar mi posición. Pero lo cierto es que cada vez que hablan de nosotros es para decir que hemos reventado el ordenador de tal multinacional con grandes perdidas o que hemos robado cierta información. Estas cosas suceden, y particularmente tengo que decir que estas cosas están al alcance de otros personajes más peligrosos que nosotros. En nuestro mundo habitan los Crackers y los Phreackers... para la mayoría todos somos iguales y todos somos piratas informáticos. Pero quiero ir por pasos. ¿Que te parece saber de donde procede la palabra Hacker?.

En el origen de esta palabra esta el término Hack algo así como golpear con un hacha en inglés que se usaba como forma familiar para describir como los técnicos telefónicos arreglaban las cajas defectuosas, asestándoles un golpe seco... Quien hacia esto era un Hacker. Otra historia relata como los primeros ordenadores grandes y defectuosos, se fallaban continuamente. Los que las manejaban se devanaban los sesos creando rutas para aumentar la velocidad y cosas parecidas. Estas cosas se denominaban Hacks y a los que lo hacían se les llamaban Hackers. Otra denominación se le hacia a aquel experto en cualquier campo que disfrutaba modificando el orden de funcionamiento del aparato. De esta forma siempre superaba las limitaciones y esto le producía una alta satisfacción. A estas personas también se les llamaban Hackers.

Pero pronto surgieron otros acrónimos como Crackers. Fue inventado por los propios Hackers para diferenciar a aquel que fisgaba en un ordenador con aquel que creaba un virus dañino o copiaba un software. Así, frente a un ordenador ajeno un Hacker y un Cracker no son la misma cosa.

Por otro lado en algunas ocasiones un Hacker es muy útil porque siempre detecta un agujero en cualquier programa nuevo... El Cracker aprovecharía este error para entrar en el programa y copiarlo.

Aparte del Cracking existen otras formas de vandalismo tecnológico. Así, el Phreacking, por ejemplo es la manipulación de las redes telefónicas para no pagar las llamadas. El Carding se refiere al uso ilegal de las tarjetas de crédito. Y el Trashing consiste en rastrear la basura o residuos de los sistemas informáticos en busca de información como contraseñas.

Pero, volviendo a los Hackers. ¿Cómo son?. ¿Qué aspecto tienen?. Cuando alguien oye mencionar la palabra Hacker rápidamente se le viene a la cabeza un adolescente ojeroso, con los ojos inyectados en sangre que ha pasado las últimas 24 horas delante del ordenador. Esta imagen esta estereotipada. No es así. Un Hacker puede ser cualquier estudiante de informática o electrónica, que sale con los amigos y que tiene novia.

Un Hacker es una persona normal como tu. Los Hackers son casi siempre gente joven. Quizás somos los que más nos interesamos por la tecnología. Un Hacker normalmente despierta el gusanillo a temprana edad. Y no se hace de la noche a la mañana. Cuando logra serlo después de realizar un Hack, se busca un apodo y no da la cara por cuestión de seguridad... Normalmente al final de todo somos contratados por empresas importantes para ayudarles en su trabajo. Y otra cosa que hacemos es contar como funciona la tecnología que se nos oculta. Este método se llama enseñar y creo que no es nada malo.
De modo que si un Hacker escribe un libro es porque tiene algo que enseñar y nada más... Y sobre todo quiero que quede buena constancia de lo que somos.

Cybor, Bangkok Diciembre del 02 Maine"

Se mueven en una delgada e indefinida barrera que separa lo legal de lo ilegal. Las instituciones y las multinacionales del software les temen, la policía los persigue y hay quien los busca para contratarlos. Se pasean libremente por las mayores computadoras y redes del mundo sin que ellas tengan secretos.

Como expresa Cybor, hay quienes los llama piratas y delincuentes. Ellos reivindican su situación e intentan aclarar las diferencias entre los distintos clanes del Underground asegurando que sus acciones se rigen por un código ético.

Alguien aseguró que el que no usa su PC para escribir cartas, lleva un hacker dentro.
Esta afirmación es una falacia si entendemos como hacker a un pirata informático; o quizás después de aclarar lo que significa este término, el resultado sea que existan mayores cuestionamientos que respuestas pero, sin duda, estos serán de una índole radicalmente distinta a la planteada hasta ahora.

"La policía quiere creer que todos los hackers son ladrones. Es una acción tortuosa y casi insoportable por parte del sistema judicial, poner a la gente en la cárcel, simplemente porque quieren aprender cosas que les esta prohibido saber...".

La familia es grande, y el término más conocido es hacker. Pero, ¿qué son?, ¿quiénes son?, ¿qué persiguen?, ¿existen?, ¿cuántos son?, ¿dónde están?...

Los años han hecho que esta palabra sea prácticamente intraducible, dando esto diversos resultados negativos y casi siempre acusadores sobre la persona que realiza hacking.

Actualmente el término acepta, según la "jergón" (Jerga Hacker) hasta siete definiciones y variados orígenes de la palabra. En el presente se maneja la etimología más ampliamente aceptada en el Underground digital.

La palabra inglesa "hack" literalmente significa "golpear" o "hachear" y proviene de los tiempos en que los técnicos en telefonía "arreglaban" algunas máquinas con un golpe seco y certero: es decir que estos técnicos eran "Hackers" y se dedicaban a "hachear" máquinas.

Estos inocentes golpes no parecen tener nada en común con las fechorías que hoy se les atribuyen. Estos hackers tampoco parecen ser el estereotipo formado en la actualidad de ellos: un chico con gruesos lentes, con acné y ojeroso por estar todo el día delante de su computadora, vagando por Internet tratando de esconder su último golpe y gastando cifras astronómicas en cuentas de teléfono que pagará su vecino, alguien en otro continente o nadie.

Estudiemos historia y veamos los puntos en común que hacen que un técnico en telefonía sea hacker al igual que un chico curioso; y hace que cada uno de nosotros sea un pirata al fotocopiar un libro o copiar el último procesador de palabras del mercado.

En el MIT (Massachussets Institute of Technology) existen diferentes grupos con intereses especiales, fraternidades y similares que cada año intentan reclutar a los nuevos estudiantes para sus filas. En el otoño de 1958, durante su primera semana en el MIT, Peter Samson, que siempre había estado fascinado por los trenes y en especial por los metros, fue a ver la espectacular maqueta que el TMRC (Tech Model Railroad Club) tenía instalada en el Edificio 20 del Instituto, y se quedó inmediatamente prendado de la parte técnica de la instalación.

En el TMRC existían dos facciones claramente diferenciadas: aquellos que se encargaban de construir los modelos de los trenes, edificios y paisajes que formaban la parte visible de la instalación y; el Subcomité de Señales y Energía que tenía a su cargo el diseño, mantenimiento y mejora de "el sistema", todo aquello que quedaba bajo los tableros, hacía funcionar los trenes y que permitía controlarlos. El TMRC daba una llave de sus instalaciones a sus miembros cuando estos acumulaban 40 horas de trabajo en las instalaciones, y Samson obtuvo la suya en un fin de semana.

Los miembros del Subcomité de Señales y Energía no se limitaban a trabajar en las instalaciones del TMRC, sino que no era extraño encontrarlos a altas horas de la madrugada recorriendo edificios y túneles de servicio intentando averiguar cómo funcionaba el complejo sistema telefónico del MIT, sistema que llegaron a conocer mejor que quienes lo habían instalado.

En la primavera de 1959, se dictaba el primer curso de programación al que se podían apuntar alumnos en su primer año. Samson y otros miembros del TMRC estaban en él (...).

Fue en aquel entonces, cuando un antiguo miembro del TMRC y entonces profesor del MIT hizo una visita al club y le preguntó a los miembros del Subcomité de Señales y Energía si les apetecería usar el TX-0. Este era uno de las primeras computadoras que funcionaban con transistores en lugar de con lámparas de vacío.

El TX-0 no usaba tarjetas sino que disponía de un teclado en el que el propio usuario tecleaba sus programas, que quedaban codificados en una cinta perforada que luego se introducía en el ordenador. El programa era entonces ejecutado, y si algo iba mal, el mismo usuario se podía sentar en la consola del TX-0 e intentar corregir el problema directamente usando una serie de interruptores y controles.

Dado que sólo se disponía un equivalente a 9 KB de memoria, era fundamental optimizar al máximo los programas que se hacían, por lo que una de las obsesiones fundamentales de los que lo usaban y se consideraban hábiles era hacer los programas tan pequeños como fuera posible, eliminando alguna instrucción aquí y allá, o creando formas ingeniosas de hacer las cosas. A estos apaños ingeniosos se les llamaba "hacks" y de ahí es de dónde viene el término "Hacker", denominación que uno recibía de sus compañeros (...).

De esta historia podemos obtener el perfil principal:

Un hacker es a todas luces, alguien con profundos conocimientos sobre la tecnología.

Tiene ansias de saberlo todo, de obtener conocimiento.

Le gusta (apasiona) la investigación.

Disfruta del reto intelectual y de rodear las limitaciones en forma creativa.

Busca la forma de comprender las características del sistema estudiado, aprovechar sus posibilidades y por último modificarlo y observar los resultados.

Dicen NO a la sociedad de la información y SI a la sociedad informada.

Recolectar y filtrar información útil e interesante y construir páginas Web o documentos como FAQs y ponerlos a disposición de los demás.

Ayudar a mantener en funcionamiento la infraestructura. La cultura hacker funciona gracias al trabajo voluntario.

Los administradores de listas de correo, moderadores de foros de discusión y sitios donde se archivan grandes cantidades de software, desarrolladores de RFCs y otros estándares técnicos gozan de mucho respeto, porque se sabe que estos son trabajos consumidores de tiempo y no tan "divertidos", llevar adelante este trabajo demuestra mucha dedicación.

Hacer algo por la cultura hacker en sí misma. Esta cultura no tiene líderes exactamente, pero tiene héroes culturales, historiadores tribales y voceros. La búsqueda visible de esa clase de fama es peligrosa, por lo que la modestia es siempre recomendada.

3.2 DEFINICIÓN DE HACKER

Un Hacker es una persona que está siempre en una continua búsqueda de información, vive para aprender y todo para él es un reto; no existen barreras, y lucha por la difusión libre de información (Free Information), distribución de software sin costo y la globalización de la comunicación.

El concepto de hacker, generalmente es confundido erróneamente con los mitos que existen acerca de este tema:

Un hacker es pirata. Esto no es así ya que los piratas comercian con la información que obtienen, entre otras cosas, y un verdadero hacker solo obtiene esa información para su uso personal.

Un hacker es el que entra en los sistemas ajenos y se dedica a destruir la información almacenada en ellos. El error consiste en que el que destruye información y sistemas ajenos, no es el hacker sino el Cracker.

Pero entonces veamos que sí es un Hacker

1. Un verdadero Hacker es curioso y paciente. Si no fuera así terminarían por hartarse en el intento de entrar en el mismo sistema una y otra vez, abandonando el objetivo.

2. Un verdadero Hacker no se mete en el sistema para borrarlo todo o para vender lo que consiga. Quiere aprender y satisfacer su curiosidad. Esa es la única finalidad de introducirse en el sistema. Buscan dentro de un lugar en el que nunca han estado, exploran todos los pequeños rincones de un mundo diferente del que ya conocen y que les aburre. ¿Porqué destruir algo y perderse el placer de decir a los demás que hemos estado en un lugar donde ellos no han estado?.

3.3 DEFINICIÓN DE CRACKERS

Los Crackers, en realidad, son hackers cuyas intenciones van más allá de la investigación. Es una persona que tiene fines maliciosos o de venganza, quiere demostrar sus habilidades pero de la manera equivocada o simplemente personas que hacen daño solo por diversión.

Los hackers opinan de ellos que son "... Hackers mediocres, no demasiados brillantes, que buscan violar (literalmente "break") un sistema".

3.4 DEFINICIÓN DE PHREAKERS

Otro personaje en el Underground es el conocido como Phreaker. El Phreaking, es la actividad por medio de la cual algunas personas con ciertos conocimientos y herramientas de hardware y software, pueden engañar a las compañías telefónicas para que éstas no cobren las llamadas que se hacen.

La realidad indica que lo Phreakers son Cracker de las redes de comunicación. Personas con amplios (a veces mayor que el de los mismo empleados de las compañías telefónicas) conocimientos en telefonía.

Se dice que el Phreaking es el antecesor del Hacking ya que es mucho más antiguo.

Comenzó en los albores de la década de los '60 cuando un tal Mark Bernay descubrió como aprovechar un error de seguridad de Bell (LA COMPAÑÍA TELEFÓNICA) basaba en la utilización de los mecanismos para la realización de llamadas gratuitas. Lo que Bernay descubrió, fue que dentro de Bell existían unos números de prueba que servían para que los operarios comprobaran las conexiones.

Hasta aquí todos eran simples adolescentes que hacían llamadas gratuitas a sus padres en otro estado.

La situación cambió cuando se descubrió que MamaBell (como suele llamarse a Bell) era un universo sin explorar y al que se le podría sacar más partido que el de unas simples llamadas. Se comenzaron a utilizar ciertos aparatos electrónicos, los cuales son conocidos como "Boxes" (cajas). La primera fue la "Blue Box" que fue hallada en 1961 en el Washington State College, y era un aparato con una carcasa metálica que estaba conectada al teléfono. Estas Boxes lo que hacían era usar el nuevo sistema de Bell (los tonos) para redirigir las llamadas. Cuando se marcaba un número, Bell lo identificaba como una combinación de notas musicales que eran creadas por seis tonos maestros, los cuales eran los que controlaban Bell y por lo tanto eran secretos (al menos eso pretendían y creían los directivos de Bell).

El cómo los Phreakers llegaron a enterarse del funcionamiento de estos tonos fue algo muy simple: Bell, orgullosa de su nuevo sistema, lo publicó detalladamente en revistas que iban dirigidas única y exclusivamente a los operarios de la compañía telefónica. Lo que sucedió es que no cayeron en la cuenta de que todo suscriptor de esa revista recibió también en su casa un ejemplar que narraba el funcionamiento del nuevo sistema.

Al poco tiempo hubo en la calle variaciones de la Blue Box inicial que fueron llamadas Red Box y Black Box, la cuales permitían realizar llamadas gratis desde teléfonos públicos.

Las Blue Boxes no solo servían para realizar llamadas gratuitas, sino que proporcionaban a sus usuarios los mismos privilegios que los operadores de Bell.

Lo realmente curioso, y desastroso para Bell, es que algunas personas eran capaces de silbar 2600 ciclos (lo cual significa que la línea está preparada para recibir una llamada) de forma completamente natural.

El primer Phreaker que utilizó este método fue Joe Engressia, quien era ciego. A los 8 años, y por azar, silbó por el auricular de su teléfono cuando escuchaba un mensaje pregrabado y la llamada se cortó. Realizo esto varias veces y en todas se le cortaba. La razón es un fenómeno llamado Talk-Off, que consiste en que cuando alguien silba y alcanza casualmente los 2600 Hz, la llamada se corta, como si fuera una Blue Box orgánica.

Joe aprendió como potenciar su habilidad para silbar 2600 Hz y ya con 20 años era capaz de producir los 2600 Hz con su boca y silbar los tonos del número con el que quería conectarse.

Otro Phreaker que utilizaba el método de Engressia, fue John Draper, más conocido por Capitán Crunch, que creo un silbato que regalaban con la marca de cereales Capitán Crunch, el cual, podría utilizarse como instrumento para hacer Phreaking. Draper hacia algo parecido a lo que hacia Joe Engressia: soplaba su silbato y la línea se quedaba libre.

Muchos Phreackers evolucionaron mas tarde al Hacking, como es el caso del pionero Mark Bernay, que bajo el nick de The Midnight Skulker (El Vigilante de Medianoche) se rió de todos los fallos de seguridad de muchas empresas.

Hoy, el Hacking y el Phreacking viven en perfecta armonía y en pleno auge con las nuevas tecnologías existentes. Es difícil delimitar el terreno de cada uno, ya que un hacker necesitara, tarde o temprano, hacer Phreacking si desea utilizar la línea telefónica mucho tiempo en forma gratuita y; de la misma forma un Phreaker necesitará del Hacking si desea conocer en profundidad cualquier sistema de comunicaciones.

3.5 DEFINICIÓN DE CARDING TRASHING

Entre las personas que dedicaban sus esfuerzos a romper la seguridad como reto intelectual hubo un grupo (con no tan buenas intenciones) que trabajaba para conseguir una tarjeta de crédito ajena. Así nació:

1. El Carding, es el uso (o generación) ilegitimo de las tarjetas de crédito (o sus números), pertenecientes a otras personas con el fin de obtener los bienes realizando fraude con ellas. Se relaciona mucho con el Hacking y el Cracking, mediante los cuales se consiguen los números de las tarjetas.

2. El Trashing, que consiste en rastrear en las papeleras en busca de información, contraseñas o directorios.

3.6 DESAFÍOS DE UN HACKER

1. El mundo está lleno de problemas fascinantes que esperan ser resueltos.

2. El esfuerzo requiere motivación. Los atletas exitosos obtienen su motivación a partir de una clase de placer físico que surge de trabajar su cuerpo, al forzarse a sí mismos más allá de sus propios límites físicos. De manera similar, un hacker siente un estremecimiento de tipo primitivo cuando resuelve un problema, agudiza sus habilidades, y ejercita su inteligencia.

3. Nadie debería tener que resolver un problema dos veces.

4. Los cerebros creativos son un recurso valioso y limitado. No deben desperdiciarse reinventando la rueda cuando hay tantos y tan fascinantes problemas nuevos esperando por allí.

5. Lo aburrido y lo rutinario es malo.

6. Los hackers (y las personas creativas en general) no deberían ser sometidas a trabajos rutinarios, porque cuando esto sucede significa que no están resolviendo nuevos problemas.

7. La libertad es buena.

8. Los hackers son naturalmente anti-autoritaristas. Cualquiera que le pueda dar órdenes, puede hacer que deba dejar de resolver ese problema con el cual está fascinado.

9. La actitud no es sustituto para la competencia.

10. Tener la actitud para ser hacker no alcanza, como tampoco alcanza para transformarse en un atleta campeón o en estrella del rock. Para transformarse en hacker necesitará inteligencia, práctica, dedicación, y trabajo pesado. Por lo tanto, debe respetar la competencia en todas sus formas.

3.7 HABILIDADES BÁSICAS EN UN HACKER.

El conjunto de habilidades cambia lentamente a lo largo del tiempo a medida que la tecnología crea nuevas tecnologías y descarta otras por obsoletas. Por ejemplo, hace tiempo, se incluía la programación en lenguaje de máquina y Assembler, y no se hablaba de HTML.

Un buen hacker incluye las siguientes reglas en su itinerario:

1. Aprender a programar. Esta es, por supuesto, la habilidad fundamental del hacker. Se deberá aprender como pensar en los problemas de programación de una manera general, independiente de cualquier lenguaje. Se debe llegar al punto en el cual se pueda aprender un lenguaje nuevo en días, relacionando lo que está en el manual con lo que ya sabe de antes. Se debe aprender varios lenguajes muy diferentes entre sí. Es una habilidad compleja y la mayoría de los mejores hackers lo hacen de forma autodidacta.

2. Aprender Unix. El paso más importante es obtener un Unix libre, instalarlo en una máquina personal, y hacerlo funcionar. Si bien se puede aprender a usar Internet sin saber Unix, nunca se podrá ser hacker en Internet sin conocerlo. Por este motivo, la cultura hacker actual está centrada fuertemente en Unix.

3.8 ¿CÓMO LO HACEN?

Quizás esta sea la pregunta más escuchada cuando se habla de hackers y los ataques por ellos perpetrados.

Para contestarla debemos ser conscientes de cada una las características de los hackers entre las que se destacan la paciencia y la perseverancia ante el desafío planteado. Será común ver a algunos de ellos fisgonear durante meses a la victima para luego recién intentar un ataque que además de efectivo debe ser invisible.

En capítulos posteriores se analizarán las técnicas (si bien no las herramientas específicas) por ellos utilizadas para perpetrar un ataque, así como también las utilizadas por los expertos en seguridad a la hora de descubrir y tirar por tierra las ambiciones hackers.

3.9 LA ÉTICA DEL HACKER

Desde el principio los hackers desarrollaron un código de ética o una serie de principios que eran tomados como un acuerdo implícito y no como algo escrito o fijo:

I. El acceso a las computadoras debe ser ilimitado y total.

II. El acceso a la información debe ser libre y gratuito.

III. Desconfíen de la autoridad, promuevan la descentralización.

IV. Los hackers deben ser juzgados por su habilidad, no por criterios absurdos como títulos, edad, raza o posición social.

V. Se puede crear arte y belleza en una computadora.

VI. Las computadoras pueden cambiar tu vida para mejor.

Así también se desarrollaron algunos "Mandamientos" en los cuales se basa un hacker a la hora de actuar sobre los sistemas que ataca:

I. Nunca destroces nada intencionadamente en la PC que estés hackeando.

II. Modifica solo los ficheros que hagan falta para evitar tu detección y asegurar tu acceso futuro al sistema.

III. Nunca dejes tus datos reales, tu nombre o tu teléfono en ningún sistema, por muy seguro que creas que es.

IV. Ten cuidado a quien le pasas información. A ser posible no pases nada a nadie que no conozcas su voz, número de teléfono y nombre real.

V. Nunca dejes tus datos personales en un BBS, si no conoces al SysOp, déjale un mensaje con la lista de gente que pueda responder por ti.

VI. Nunca hackees en computadoras del gobierno. El gobierno puede permitirse gastar fondos en buscarte, mientras que las universidades y las empresas particulares no.

VII. No uses Blue Box a menos que no tengas un PAD local o número gratuito al que conectarte, si se abusa de la Blue Box, puedes ser cazado.

VIII. No dejes en mucha información del sistema que estas hackeando. Di sencillamente "estoy trabajando en ..." pero no digas a quien pertenece, ni el número de teléfono, dirección, etc.

IX. No te preocupes en preguntar, nadie te contestara. Piensa que por responderte a una pregunta, pueden cazarte a ti, al que te contesta o a ambos.

X. Punto final. Hasta que no estés realmente hackeando, no sabrás que es...

3.10 MANIFIESTO HACKER

En los principios, un grupo hackers llamado Legión of Doom, dirigido por The Mentor, quería demostrar hasta donde era capaz de llegar. Para ello modificaron la página principal el sitio Web de la NASA, durante media hora, con el siguiente "manifiesto":

(...) "Hoy he hecho un descubrimiento. He encontrado una computadora. Esperen, esto es lo mejor. La computadora hacía lo que yo quería. Si cometía un error era porque yo me equivocaba.

No porque yo no le gustara... Y entonces ocurrió... una puerta se abrió al mundo, surcando la línea telefónica igual que la heroína surca las venas del adicto, el impulso eléctrico te envía a un refugio a salvo de las incompetencias del día a día... la BBS ha sido encontrada. Es... es a donde pertenezco.

Conozco a todo el mundo aquí, incluso sin haberlos visto antes, sin haber hablado con ellos y puede que a algunos no vuelva a verlos jamás... Os conozco a todos... Éste es nuestro mundo... el mundo del electrón y el conmutador, la belleza del baudio. Hacemos uso de un servicio ya existente sin pagar por lo que podría ser gratis si no estuviera en manos de unos glotones aprovechados, y tú nos llamas a nosotros criminales. Nosotros exploramos... y tú nos llamas criminales. Existimos sin color de piel, sin nacionalidad, sin inclinaciones religiosas... y tú nos llamas criminales.

Tú que construyes bombas atómicas, tú que haces la guerra, tú asesino, nos engañas y mientes intentando hacernos creer que es por nuestro propio bien, sin embargo somos criminales. Si, soy un criminal. Mi crimen es la curiosidad. Mi crimen es juzgar a la gente por que lo que ellos dicen y piensan, no por como ellos aparentan ser exteriormente. Mi crimen es ser más inteligente que tú, algo por lo que nunca me perdonarás." (...)

3.11 OTROS HABITANTES DEL CIBERESPACIO

GURÚS

Son considerados los maestros y los encargados de "formar" a los futuros hackers. Generalmente no están activos pero son identificados y reconocidos por la importancia de sus hackeos, de los cuales sólo enseñan las técnicas básicas.

LAMERS O SCRIPT KIDDERS

Son aficionados jactanciosos. Prueban todos los programas (con el título "como ser un hacker en 21 días") que llegan a sus manos. Generalmente son los responsables de soltar virus para darse fama al menos por unos instantes y con eso sentir la gloria y el poder en sus manos.

3.12 PERSONAL (INSIDERS)

Hasta aquí se ha presentado al personal como víctima de atacantes externos; sin embargo, de los robos, sabotajes o accidentes relacionados con los sistemas informáticos, el 70% (APROXIMADAMENTE), son causados por el propio personal de la organización propietaria de dichos sistemas ("Inside Factor").

Hablando de los Insiders podemos explica que de acuerdo a las investigaciones hechas "desde mitad de 1996 hasta el 2000 la mayoría de las empresas tuvieron por lo menos dos casos de intrusiones pero del 2000 en adelante se han registrado siete, de las cuales 5 fueron intrusos internos o ex empleados".

Esto es realmente preocupante, ya que, una persona que trabaje con el administrador, el programador o el encargado de una máquina conoce perfectamente el sistema, sus puntos fuertes y débiles; de manera que un ataque realizado por esa persona podrá ser más directo, difícil de detectar y más efectivo que el que un atacante externo pueda realizar.

Existen diversos estudios que tratan sobre los motivos que llevan a una persona a cometer delitos informáticos contra su organización, pero sean cuales sean, estos motivos existen y deben prevenirse y evitarse. Suele decirse que todos tenemos un precio (dinero, chantaje, factores psicológicos, etc.), por lo que nos pueden arrastrar a robar y vender información o simplemente proporcionar acceso a terceros.

Como ya se ha mencionado los ataques pueden ser del tipo pasivos o activos, y el personal realiza ambos indistintamente dependiendo de la situación concreta. Dentro de este espectro podemos encontrar:

3.13 PERSONAL INTERNO

Las amenazas a la seguridad de un sistema, provenientes del personal del propio sistema informático, rara vez es tomada en cuenta porque se supone un ámbito de confianza muchas veces inexistente. Generalmente estos ataques son accidentes por desconocimiento o inexistencia de las normas básicas de seguridad; pero también pueden ser del tipo intencional.

Es de destacar que un simple electricista puede ser más dañino que el más peligroso de los piratas informáticos, ya que un corte de energía puede causar un desastre en los datos del sistema. Al evaluar la situación, se verá que aquí el daño no es intencionado pero ello no esta en discusión; el daño existió y esto es lo que compete a la seguridad informática.

3.14 EX EMPLEADO

Este grupo puede estar especialmente interesado en violar la seguridad de nuestra empresa, sobre todo aquellos que han sido despedidos y no han quedado conformes; o bien aquellos que han renunciado para pasar a trabajar en la competencia. Generalmente se trata de personas descontentas con la organización que conocen a la perfección la estructura del sistema y tienen los conocimientos necesarios como para causar cualquier tipo de daño; También han existido casos donde el ex empleado deja Bombas Lógicas que "explotan" tiempo después de marcharse.

3.15 CURIOSOS

Suelen ser los atacantes más habituales del sistema. Son personas que tienen un alto interés en las nuevas tecnologías, pero aún no tienen los conocimientos ni experiencia básicos para considerarlos hackers o crackers.

En la mayoría de los casos son estudiantes intentando penetrar los servidores de su facultad o empleados consiguiendo privilegios para obtener información para él vedada.

Generalmente no se trata de ataques de daño pero afectan el entorno de fiabilidad con confiabilidad generado en un sistema.

3.16 TERRORISTAS

Bajo esta definición se engloba a cualquier persona que ataca el sistema para causar daño de cualquier índole en él; y no sólo a la persona que coloca bombas o quema automóviles.

Son ejemplos concretos de este tipo, ataque de modificación de los datos de clientes entre empresa competidoras, o de servidores que albergan páginas Web, bases de datos entre partidos políticos contrarios, etc.

3.17 INTRUSOS REMUNERADOS

Este es, sin duda, el grupo de atacantes más peligroso, aunque también el menos habitual. Se trata de Crackers o piratas con grandes conocimientos y experiencia, pagados por una tercera parte para robar "secretos" (código fuente de programas, bases de datos de clientes, información confidencial de satélites, diseño de un nuevo producto, etc.) o simplemente para dañar, de alguna manera la imagen de la entidad atacada.

Suele darse, sólo, en grandes multinacionales donde la competencia puede darse el lujo de un gran gasto para realizar este tipo de contratos y contar con los medios necesarios para realizar el ataque.

3.18 RECOMENDACIONES

Una norma básica, sería verificar cada aspirante a ser nuevo empleado; aunque tampoco debemos olvidar que el hecho de que alguien entre "limpio" a la organización no implica que vaya a seguir así durante el tiempo que trabaje en la misma, y mucho menos cuando abandone su trabajo.

Para minimizar el daño que un atacante interno puede causar se pueden seguir estos principios fundamentales:

Necesidad de conocimiento (Need to Know): comúnmente llamado mínimo privilegio.

Cada usuario debe tener el mínimo privilegio que necesite para desempeñar correctamente su función, es decir, que sólo se le debe permitir que sepa lo necesario para realizar su trabajo.

Conocimiento parcial (dual control): las actividades más delicadas dentro de la organización deben ser realizadas por dos personas competentes, de forma que si uno comete un error en las políticas de seguridad el otro pueda subsanarlo. Esto también es aplicable al caso de que si uno abandona la organización el otro pueda seguir operando el sistema mientras se realiza el reemplazo de la persona que se retiró.

Rotación de funciones: la mayor amenaza del conocimiento parcial de tareas es la complicidad de dos responsables, de forma tal, que se pueda ocultar sendas violaciones a la seguridad. Para evitar el problema, una norma común es rotar (dentro de ciertos límites) a las personas a lo largo de diferentes responsabilidades, para establecer una vigilancia mutua.

Separación de funciones: es necesario que definan y separen correctamente las funciones de cada persona, de forma que alguien cuya tarea es velar por la seguridad del sistema no posea la capacidad para violarla sin que nadie se percate de ello.

Cancelación inmediata de cuenta: cuando un empleado abandona la organización se debe cancelar inmediatamente el acceso a sus antiguos recursos y cambiar las claves que el usuario conocía.
Quizás este último punto sea el más difícil de implementar debido a la gran cantidad de usuarios que se deben informar de los nuevos accesos y de la movilidad de alguno de ellos.

En estos puntos se encuentran las mayores vulnerabilidades de un sistema ya que, por ejemplo, suelen encontrarse cuentas de usuario que hace años que no se utilizan, y por ende tampoco se han cambiado sus passwords.

Si bien estas normas pueden aplicarse a las organizaciones, no podrán hacerlo en instituciones como una universidad, donde la mayoría de los atacantes son alumnos y no podrá verificarse los antecedentes de miles de alumnos (y tampoco ético prohibir su acceso por ser estos dudosos). De esta forma, en las redes de Investigación y Desarrollo (I+D) de acceso público debemos ceñirnos a otros mecanismos de control y casi siempre se opta por las sanciones a todos aquellos que utilicen el centro para cometer delitos informáticos.

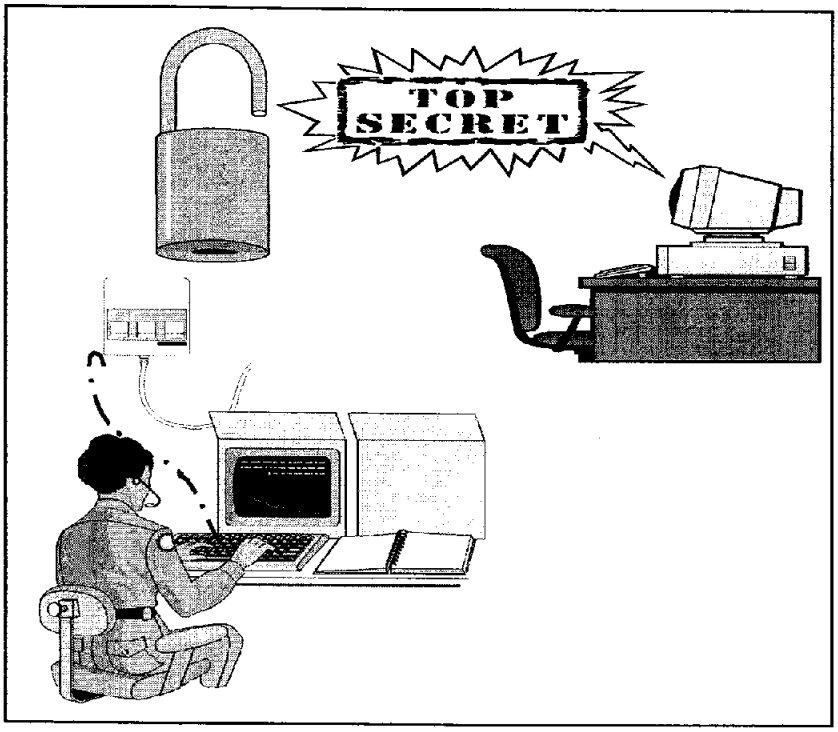


FIG. 5 EJEMPLO DE ROBO DE INFORMACIÓN

CAPITULO 4

AMENAZAS LÓGICAS

CAPITULO 4

AMENAZAS LÓGICAS

4. AMENAZAS LÓGICAS

La Entropía es una magnitud termodinámica que cuantifica el grado de desorden de un sistema; y según las leyes físicas todo sistema tiende a su máxima entropía. Si extrapolamos este concepto a la Seguridad resultaría que todo sistema tiende a su máxima inseguridad. Este principio supone decir:

Los protocolos de comunicación utilizados carecen, en su mayoría, de seguridad o esta ha sido implementada, tiempo después de su creación, en forma de "parche".

Existen agujeros de seguridad en los sistemas operativos.

Existen agujeros de seguridad en las aplicaciones.

Existen errores en las configuraciones de los sistemas.

Los usuarios carecen de información respecto al tema.

Todo sistema es inseguro.

Esta lista podría seguir extendiéndose a medida que se evalúen mayor cantidad de elementos de un Sistema Informático.

4.1 ACCESO, USO Y AUTORIZACIÓN

La identificación de estas palabras es muy importante ya que el uso de algunas implica un uso desapropiado de las otras.

Específicamente "Acceso" y "Hacer Uso" no son el mismo concepto cuando se estudian desde el punto de vista de un usuario y de un intruso. Por ejemplo:

Cuando un usuario tiene acceso autorizado, implica que tiene autorizado el uso de un recurso.

Cuando un atacante tiene acceso desautorizado está haciendo uso desautorizado del sistema.

Pero, cuando un atacante hace uso desautorizado de un sistema, esto implica que el acceso fue autorizado (simulación de usuario).

Luego un Ataque será un intento de acceso, o uso desautorizado de un recurso, sea satisfactorio o no. Un Incidente envuelve un conjunto de ataques que pueden ser distinguidos de otro grupo por las características del mismo (grado, similitud, técnicas utilizadas, tiempos, etc.).

4.2 DETECCIÓN DE INTRUSOS

A finales de 2003, Dan Farmer (creador de una de las herramientas más útiles en la detección de intrusos: SATAN) realizó un estudio sobre seguridad analizando 2,203 sistemas de sitios en Internet. Los sistemas objeto del estudio fueron Web Sites orientados al comercio y con contenidos específicos, además de un conjunto de sistemas informáticos aleatorios con los que realizar comparaciones.

El estudio se realizó empleando técnicas sencillas y no intrusivas. Se dividieron los problemas potenciales de seguridad en dos grupos: rojos (red) y amarillos (yellow). Los problemas del grupo rojo son los más serios y suponen que el sistema está abierto a un atacante potencial, es decir, posee problemas de seguridad conocidos en disposición de ser explotados. Así por ejemplo, un problema de seguridad del grupo rojo es un equipo que tiene el servicio de FTP anónimo mal configurado.

Los problemas de seguridad del grupo amarillo son menos serios pero también reseñables. Implican que el problema detectado no compromete inmediatamente al sistema pero puede causarle serios daños o bien, que es necesario realizar tests más intrusivos para determinar si existe o no un problema del grupo rojo.

La siguiente tabla resume los sistemas evaluados, el número de equipos en cada categoría y los porcentajes de vulnerabilidad para cada uno. Aunque los resultados son límites superiores, no dejan de ser... escandalosos.

TIPO DE SITIO	# TOTAL DE SITIOS TESTEADOS	% TOTAL VULNERABLES	% YELLOW	% RED
BANCOS	660	8.34	32.73	35.61
CRÉDITOS	274	51.10	30.66	20.44
SITIOS FEDERALES USA	47	61.70	23.40	38.30
NOTICIAS	312	69.55	30.77	38.78
SEXO	451	66.08	40.58	25.50
TOTALES	**1,734**	**64.93**	**33.85**	**31.08**
GRUPO ALEATORIO	**469**	**33.05**	**15.78**	**17.27**

TABLA 1 Porcentaje de Vulnerabilidades por tipo de sitio.
Fuente: http://www.trouble.org/survey

Como puede observarse, cerca de los dos tercios de los sistemas analizados tenían serios problemas de seguridad y se destaca que casi un tercio de ellos podían ser atacados con un mínimo esfuerzo.

4.3 IDENTIFICACIÓN DE LAS AMENAZAS

La identificación de amenazas requiere conocer los tipos de ataques, el tipo de acceso, la forma operacional y los objetivos del atacante.

Las consecuencias de los ataques se podrían clasificar en:

Data Corruption: la información que no contenía defectos pasa a tenerlos.

Denial of Service (DoS): servicios que deberían estar disponibles no lo están.

Leakage: los datos llegan a destinos a los que no deberían llegar.

Desde 1990 hasta nuestros días, el CERT viene desarrollando una serie de estadísticas que demuestran que cada día se registran más ataques informáticos, y estos son cada vez más sofisticados, automáticos y difíciles de rastrear.

Los administradores tienen cada vez mayor conciencia respecto de la seguridad de sus sistemas y arreglan por sí mismos las deficiencias detectadas. A esto hay que añadir las nuevas herramientas de seguridad disponibles en el mercado.

Los "Advisories" (documentos explicativos) sobre los nuevos agujeros de seguridad detectados y la forma de solucionarlos, lanzados por el CERT, han dado sus frutos.

4.4 TIPOS DE ATAQUE

A continuación se expondrán diferentes tipos de ataques perpetrados, principalmente, por Hackers. Estos ataques pueden ser realizados sobre cualquier tipo de red, sistema operativo, usando diferentes protocolos, etc.

En los primeros tiempos, los ataques involucraban poca sofisticación técnica. Los Insiders (operadores, programadores, data entrys) utilizaban sus permisos para alterar archivos o registros. Los Outsiders ingresaban a la red simplemente averiguando una password válida.

A través de los años se han desarrollado formas cada vez más sofisticadas de ataque para explotar "agujeros" en el diseño, configuración y operación de los sistemas.

Son muchos los autores que describen con detalle las técnicas y las clasifican de acuerdo a diferentes características de las mismas. Ante la diversificación de clasificaciones de amenazas y la inminente aparición de nuevas técnicas, para la realización del presente los ataques serán clasificados y categorizados según la experiencia y conocimiento de cada caso.

Otra lista de términos asociada con los ataques puede ser la siguiente

Trojan horses, Fraud networks, Fictitious people, Infrastructure observation, e-mail overflow, Time bombs, Get a job, Protection limit poke, Infrastructure interference, Human engineering, Bribes, Dumpster diving, Sympathetic vibration Password, guessing Packet, insertion, Data diddling, Computer viruses, Invalid values on calls, Van Eck bugging, Packet watching, Login spoofing, Data diddling, Wiretapping, Combined attacks, e-mail spoofing, Scanning Dumpster, diving, Eavesdropping, Denial-of-service, Harassment, Masquerading Software, piracy, Data copying, Degradation of service, Traffic analysis, Trap doors, Covert channels, Viruses and worms, Session hijacking, Timing attacks, Tunneling, Trojan horses, IP spoofing, Logic bombs, Salamis, Password sniffing, Excess privileges.

Al describirlos no se pretende dar una guía exacta ni las especificaciones técnicas necesarias para su uso. Sólo se pretende dar una idea de la cantidad y variabilidad de los mismos, así como que su adaptación (y aparición de nuevos) continúa paralela a la creación de nuevas tecnologías.

4.5 TRASHING (CARTONEO)

Generalmente, un usuario anota su login y password en un papelito y luego, cuando lo recuerda, lo arroja a la basura. Este procedimiento por más inocente que parezca es el que puede aprovechar un atacante para hacerse de una llave para entrar el sistema... "nada se destruye, todo se transforma".

El Trashing puede ser físico (como el caso descrito) o lógico, como analizar buffers de impresora y memoria, bloques de discos, etc.

El Trashing físico suele ser común en organizaciones que no disponen de alta confidencialidad, como colegios y universidades.

ATAQUES DE MONITORIZACIÓN

Este tipo de ataque se realiza para observar a la victima y su sistema, con el objetivo de obtener información, establecer sus vulnerabilidades y posibles formas de acceso futuro.

4.6 SHOULDER SURFING

Consiste en espiar físicamente a los usuarios para obtener el login y su password correspondiente. El Surfing explota el error de los usuarios de dejar su login y password anotadas cerca de la computadora (generalmente en post-it adheridos al monitor o teclado).

Cualquier intruso puede pasar por ahí, verlos y memorizarlos para su posterior uso. Otra técnica relacionada al surfing es aquella mediante la cual se ve, por encima del hombro, al usuario cuando teclea su nombre y password.

4.7 DECOY (SEÑUELOS)

Los Decoy son programas diseñados con la misma interfase que otro original. En ellos se imita la solicitud de un logeo y el usuario desprevenido lo hace. Luego, el programa guardará esta información y dejará paso a las actividades normales del sistema. La información recopilada será utilizada por el atacante para futuras "visitas".

Una técnica semejante es aquella que, mediante un programa se guardan todas las teclas presionadas durante una sesión. Luego solo hará falta estudiar el archivo generado para conocer nombres de usuarios y claves.

4.8 SCANNING (BÚSQUEDA)

El Scaneo, como método de descubrir canales de comunicación susceptibles de ser explotados, lleva en uso mucho tiempo. La idea es recorrer (scanear) tantos puertos de escucha como sea posible, y guardar información de aquellos que sean receptivos o de utilidad para cada necesidad en particular. Muchas utilidades de auditoria también se basan en este paradigma.

El Scaneo de puertos pertenece a la Seguridad Informática desde que era utilizado en los sistemas de telefonía. Dado que actualmente existen millones de números de teléfono a los que se pueden acceder con una simple llamada, la solución lógica (para encontrar números que puedan interesar) es intentar conectarlos a todos.

La idea básica es simple: llamar a un número y si el módem devuelve un mensaje de conectado, grabar el número. En otro caso, la computadora cuelga el teléfono y llama al siguiente número.

Scanear puertos implica las mismas técnicas de fuerza bruta. Se envía una serie de paquetes para varios protocolos y se deduce que servicios están "escuchando" por las respuestas recibidas o no recibidas.

Existen diversos tipos de Scanning según las técnicas, puertos y protocolos explotados:

4.8.1 T C P Connect Scanning

Esta es la forma básica del scaneo de puertos TCP. Si el puerto está escuchando, devolverá una respuesta de éxito; cualquier otro caso significará que el puerto no está abierto o que no se puede establecer conexión con él.

Las ventajas que caracterizan esta técnica es que no necesita de privilegios especiales y su gran velocidad.

Su principal desventaja es que este método es fácilmente detectable por el administrador del sistema. Se verá un gran número de conexiones y mensajes de error para los servicios en los que se ha conseguido conectar la máquina, que lanza el scanner, y también se verá su inmediata desconexión.

4.8.2 T C P SYN Scanning

Cuando dos procesos establecen una comunicación usan el modelo Cliente/Servidor para establecerla. La aplicación del Servidor "escucha" todo lo que ingresa por los puertos.

La identificación del Servidor se efectúa a través de la dirección IP del sistema en el que se ejecuta y del número de puerto del que depende para la conexión. El Cliente establece la conexión con el Servidor a través del puerto disponible para luego intercambiar datos.

La información de control de llamada HandShake (saludo) se intercambia entre el Cliente y el Servidor para establecer un dialogo antes de transmitir datos. Los "paquetes" o segmentos TCP tienen banderas que indican el estado del mismo.

El protocolo TCP de Internet, sobre el que se basa la mayoría de los servicios (incluyendo el correo electrónico, el Web y el IRC) implica esta conexión entre dos máquinas.

El establecimiento de dicha conexión se realiza mediante lo que se llama Three-Way Handshake ("conexión en tres pasos") ya que intercambian tres segmentos.

1. El programa Cliente (C) pide conexión al Servidor (S) enviándole un segmento SYN. Este segmento le dice a S que C desea establecer una conexión.

2. S (si está abierto y escuchando) al recibir este segmento SYN (activa el indicador) y envía una autentificación ACK de manera de acuse de recibo a C. Si S está cerrado envía un indicador RST.

3. C entonces ACKea (autentifica) a S. Ahora ya puede tener lugar la transferencia de datos.

Cuando las aplicaciones conectadas terminan la transferencia, realizaran otra negociación a tres bandas con segmentos FIN en vez SYN.

La técnica TCP SYN Scanning, implementa un scaneo de "media-apertura", dado que nunca se abre una sesión TCP completa.

Se envía un paquete SYN (como si se fuera a usar una conexión real) y se espera por la respuesta. Al recibir un SYN/ACK se envía, inmediatamente, un RST para terminar la conexión y se registra este puerto como abierto.

La principal ventaja de esta técnica de escaneo es que pocos sitios están preparados para registrarlos. La desventaja es que en algunos sistemas Unix, se necesitan privilegios de administrador para construir estos paquetes SYN.

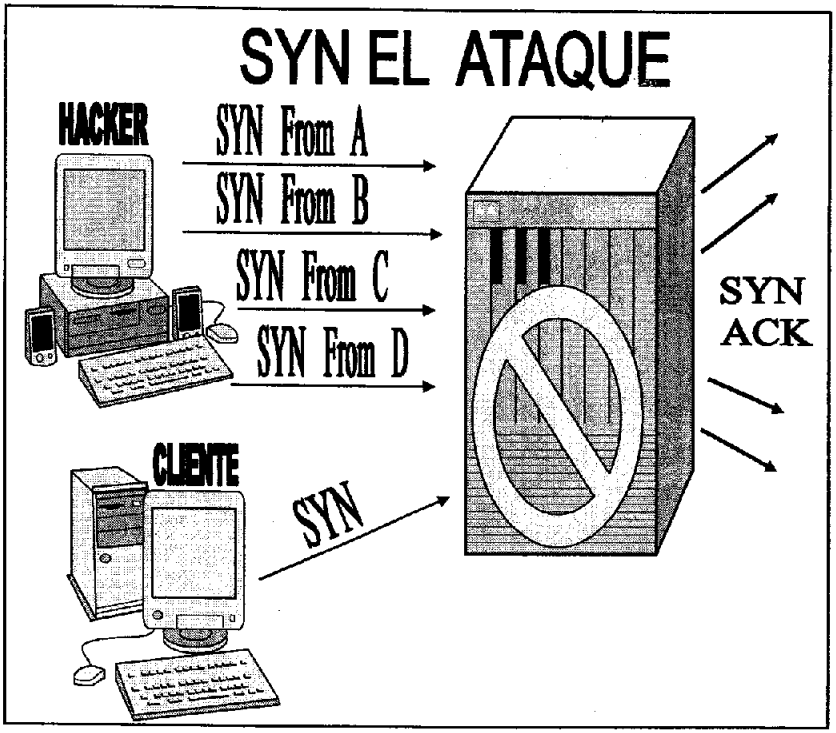


FIG. 6 TIPO DE ATAQUE SYN

4.8.3 T C P FIN Scanning Stealth Port Scanning

Hay veces en que incluso el scaneo SYN no es lo suficientemente "clandestino" o limpio. Algunos sistemas (Firewalls y filtros de paquetes) monitorizan la red en busca de paquetes SYN a puertos restringidos.

Para subsanar este inconveniente los paquetes FIN, en cambio, podrían ser capaces de pasar sin ser advertidos. Este tipo de Scaneo está basado en la idea de que los puertos cerrados tienden a responder a los paquetes FIN con el RST correspondiente. Los puertos abiertos, en cambio, suelen ignorar el paquete en cuestión.

Este es un comportamiento correcto del protocolo TCP, aunque algunos sistemas, entre los que se hallan los de Microsoft, no cumplen con este requerimiento, enviando paquetes RST siempre, independientemente de si el puerto está abierto o cerrado. Como resultado, no son vulnerables a este tipo de scaneo. Sin embargo, es posible realizarlo en otros sistemas UNIX.

Este último es un ejemplo en el que se puede apreciar que algunas vulnerabilidades se presentan en las aplicación de tecnologías (en este caso el protocolo TCP nacido en los años ´70) y no sobre sus implementaciones. Es más, se observa que una implementación incorrecta (la de Microsoft) soluciona el problema.

"Muchos de los problemas globales de vulnerabilidades son inherentes al diseño original de algunos protocolos".

4.8.4 Fragmentation Scanning

Esta no es una nueva técnica de scaneo como tal, sino una modificación de las interiores. En lugar de enviar paquetes completos de sondeo, los mismos se particionan en un par de pequeños fragmentos IP. Así, se logra partir una cabecera IP en distintos paquetes para hacerlo más difícil de monitorizar por los filtros que pudieran estar ejecutándose en la máquina objetivo.

Sin embargo, algunas implementaciones de estas técnicas tienen problemas con la gestión de este tipo de paquetes tan pequeños, causando una caída de rendimiento en el sistema del intruso o en el de la víctima. Problemas de esta índole convierte en detectables a este tipo de ataque.

4.9 EAVESDROPPING PACKET SINFFING

Muchas redes son vulnerables al Eavesdropping, o a la pasiva intercepción (sin modificación) del tráfico de red.

Esto se realiza con Packet Sniffers, los cuales son programas que monitorean los paquetes que circulan por la red. Los Sniffers pueden ser colocados tanto en una estación de trabajo conectada a la red, como a un equipo Router o a un Gateway de Internet, y esto puede ser realizado por un usuario con legítimo acceso, o por un intruso que ha ingresado por otras vías.

Cada maquina conectada a la red (mediante una placa con una dirección única) verifica la dirección destino de los paquetes TCP. Si estas direcciones son iguales asume que el paquete enviado es para ella, caso contrario libera el paquete para que otras placas lo analicen.

Un Sniffers consiste en colocar a la placa de red en un modo llamado promiscuo, el cual desactiva el filtro de verificación de direcciones y por lo tanto todos los paquetes enviados a la red llegan a esta placa (computadora donde está instalado el Sniffer).

Inicialmente este tipo de software, era únicamente utilizado por los administradores de redes locales, aunque con el tiempo llegó a convertirse en una herramienta muy usada por los intrusos.

Actualmente existen Sniffers para capturar cualquier tipo de información específica. Por ejemplo passwords de un recurso compartido o de acceso a una cuenta, que generalmente viajan sin encriptar al ingresar a sistemas de acceso remoto. También son utilizados para capturar números de tarjetas de crédito y direcciones de e-mails entrantes y salientes. El análisis de tráfico puede ser utilizado también para determinar relaciones entre organizaciones e individuos.

Para realizar estas funciones se analizan las tramas de un segmento de red, y presentan al usuario sólo las que interesan.

Normalmente, los buenos Sniffers, no se pueden detectar, aunque la inmensa mayoría, y debido a que están demasiado relacionados con el protocolo TCP/IP, si pueden ser detectados con algunos trucos.

4.10 SNOOPING DOWNLOADING

Los ataques de esta categoría tienen el mismo objetivo que el Sniffing: obtener la información sin modificarla.

Sin embargo los métodos son diferentes. Aquí, además de interceptar el tráfico de red, el atacante ingresa a los documentos, mensajes de correo electrónico y otra información guardada, realizando en la mayoría de los casos un downloading (copia de documentos) de esa información a su propia computadora, para luego hacer un análisis exhaustivo de la misma.

El Snooping puede ser realizado por simple curiosidad, pero también es realizado con fines de espionaje y robo de información o software. Los casos mas resonantes de este tipo de ataques fueron: el robo de un archivo con mas de 1700 números de tarjetas de crédito desde una compañía de música mundialmente famosa, y la difusión ilegal de reportes oficiales reservados de las Naciones Unidas, acerca de la violación de derechos humanos en algunos países europeos en estado de guerra.

4.11 ATAQUES DE AUTENTIFICACIÓN

Este tipo de ataque tiene como objetivo engañar al sistema de la víctima para ingresar al mismo. Generalmente este engaño se realiza tomando las sesiones ya establecidas por la víctima u obteniendo su nombre de usuario y password.

4.11.1 SPOOFING LOOPING

Spoofing puede traducirse como "hacerse pasar por otro" y el objetivo de esta técnica, justamente, es actuar en nombre de otros usuarios, usualmente para realizar tareas de Snooping o Tampering (ver Ataques de Modificación y Daño).

Una forma común de Spoofing es conseguir el nombre y password de un usuario legítimo para, una vez ingresado al sistema, tomar acciones en nombre de él.

El intruso usualmente utiliza un sistema para obtener información e ingresar en otro, y luego utiliza este para entrar en otro, y así sucesivamente. Este proceso, llamado Looping, tiene la finalidad de "evaporar" la identificación y la ubicación del atacante.

El camino tomado desde el origen hasta el destino puede tener muchas estaciones, que exceden obviamente los límites de un país.

4.11.2 WEB SPOOFING

En el caso Web Spoofing el atacante crea un sitio Web completo (falso) similar al que la víctima desea entrar. Los accesos a este sitio están dirigidos por el atacante, permitiéndole monitorear todas las acciones de la víctima, desde sus datos hasta las passwords, números de tarjeta de créditos, etc.

El atacante también es libre de modificar cualquier dato que se esté transmitiendo entre el servidor original y la víctima o viceversa.

4.11.3 IP SPLICING HIJACKING

Se produce cuando un atacante consigue interceptar una sesión ya establecida. El atacante espera a que la victima se identifique ante el sistema y tras ello le suplanta como usuario autorizado.

Para entender el procedimiento supongamos la siguiente situación:

IP Cliente : IP 195.1.1.1
IP Servidor: IP 195.1.1.2
IP Atacante: IP 195.1.1.3

1. El cliente establece una conexión con su servidor enviando un paquete que contendrá la dirección origen, destino, número de secuencia (para luego armar el paquete) y un número de autentificación utilizado por el servidor para "reconocer" el paquete siguiente en la secuencia. Supongamos que este paquete contiene:

IP Origen : 195.1.1.1 Puerto 1025
IP Destino: 195.1.1.2 Puerto 23
SEQ = 3DF45ADA (el primero es al azar)
ACK = F454FDF5
Datos: Solicitud

2. El servidor, luego de recibir el primer paquete contesta al cliente con paquete

Echo (recibido).
IP Origen : 195.1.1.2 Puerto 1025
IP Destino: 195.1.1.1 Puerto 23
SEQ = F454FDF5 (ACK enviado por el cliente)
ACK = 3DF454E4
Datos: Recepción OK (Echo)

3. El cliente envía un paquete ACK al servidor, sin datos, en donde le comunica lo "perfecto" de la comunicación.

IP Origen : 195.1.1.1 Puerto 1025
IP Destino: 195.1.1.2 Puerto 23
SEQ = 3DF454E4 (ACK enviado por el servidor)
ACK = F454FDFF
Datos: Confirmación de Recepción (ACK)

4. El atacante que ha visto, mediante un Sniffer, los paquete que circularon por la red calcula el número de secuencia siguiente: el actual + tamaño del campo de datos. Para calcular el tamaño de este campo:

1° Paquete ACK Cliente = F454FDF5
2° Paquete ACK Cliente = F454FDFF
Tamaño del campo datos = F454FDFF F454FDF5 = 0A

5. Hecho esto el atacante envía un paquete con la siguiente aspecto:

IP Origen : IP 195.1.1.1 (IP del Cliente por el atacante)
IP Destino: IP 195.1.1.2 (IP del Servidor)
SEQ = 3DF454E4 (Ultimo ACK enviado por el Cliente)
ACK = F454FE09 (F454FDFF + 0A)

El servidor al recibir estos datos no detectará el cambio de origen ya que los campos que ha recibido como secuencia y ACK son los que esperaba recibir. El cliente, a su vez, quedará esperando datos como si su conexión estuviera colgada y el atacante podrá seguir enviando datos mediante el procedimiento descrito.

4.11.4 UTILIZACIÓN DE BACK DOORS

Las puertas traseras son trozos de código en un programa que permiten a quien las conoce saltarse los métodos usuales de autentificación para realizar ciertas tareas.

Habitualmente son insertados por los programadores del sistema para agilizar la tarea de probar código durante la fase de desarrollo.

Esta situación se convierte en una falla de seguridad si se mantiene, involuntaria o intencionalmente, una vez terminado el producto ya que cualquiera que conozca el agujero o lo encuentre en su código podrá saltarse los mecanismos de control normales.

4.11.5 UTILIZACIÓN DE EXPLOITS

Es muy frecuente ingresar a un sistema explotando agujeros en los algoritmos de encriptación utilizados, en la administración de las claves por parte la empresa, o simplemente encontrando un error en los programas utilizados.

Los programas para explotar estos "agujeros" reciben el nombre de Exploits y lo que realizan es aprovechar la debilidad, fallo o error hallado en el sistema (hardware o software) para ingresar al mismo.

Nuevos Exploits (explotando nuevos errores en los sistemas) se publican cada día por lo que mantenerse informado de los mismos y de las herramientas para combatirlos es de vital importancia.

4.11.6 OBTENCIÓN DE PASSWORDS

Este método comprende la obtención por "Fuerza Bruta" de aquellas claves que permiten ingresar a los sistemas, aplicaciones, cuentas, etc. atacados.
Muchas passwords de acceso son obtenidas fácilmente porque involucran el nombre u otro dato familiar del usuario y, además, esta nunca (o rara vez) se cambia. En esta caso el ataque se simplifica e involucra algún tiempo de prueba y error. Otras veces se realizan ataques sistemáticos (incluso con varias computadoras a la vez) con la ayuda de programas especiales y "diccionarios" que prueban millones de posibles claves hasta encontrar la password correcta.

4.11.7 USO DE DICCIONARIOS

Los Diccionarios son archivos con millones de palabras, las cuales pueden ser posibles passwords de los usuarios. Este archivo es utilizado para descubrir dicha password en pruebas de fuerza bruta.

El programa encargado de probar cada una de las palabras encripta cada una de ellas, mediante el algoritmo utilizado por el sistema atacado, y compara la palabra encriptada contra el archivo de passwords del sistema atacado (previamente obtenido). Si coinciden se ha encontrado la clave de acceso al sistema, mediante el usuario correspondiente a la clave hallada.

Actualmente es posible encontrar diccionarios de gran tamaño orientados, incluso, a un área específico de acuerdo al tipo de organización que se este atacando.

En la siguiente tabla podemos observar el tiempo de búsqueda de una clave de acuerdo a su longitud y tipo de caracteres utilizados. La velocidad de búsqueda se supone en 100,000 passwords por segundo, aunque este número suele ser mucho mayor dependiendo del programa utilizado.

CANTIDAD DE CARACTERES	26 LETRAS MINÚSCULAS	36 LETRAS Y DÍGITOS	52 MAYÚSCULAS Y MINÚSCULAS	96 TODOS LOS CARACTERES
6	51 minutos	6 horas	2.3 días	3 meses
7	22.3 horas	9 días	4 meses	24 años
8	24 días	10.5 meses	17 años	2,288 años
9	21 meses	32.6 años	890 años	219,601 años
10	45 años	1,160 años	45,840 años	21,081,075 años

TABLA 2 Cantidad de claves generadas según el número de caracteres empleado Fuente: SCHNEIER Bruce. Applied Cryptography. Editorial John Wiley & Sons.

Aquí puede observarse la importancia de la utilización de passwords con al menos 8 caracteres de longitud y combinando todos los caracteres disponibles.

4.12 DENIAL OF SERVICE (D ó S)

Los protocolos existentes actualmente fueron diseñados para ser empleados en una comunidad abierta y con una relación de confianza mutua. La realidad indica que es más fácil desorganizar el funcionamiento de un sistema que acceder al mismo; así los ataques de Negación de Servicio tienen como objetivo saturar los recursos de la víctima de forma tal que se inhabilita los servicios brindados por la misma.

Más allá del simple hecho de bloquear los servicios del cliente, existen algunas razones importantes por las cuales este tipo de ataques pueden ser útiles a un atacante:

1. Se ha instalado un troyano y se necesita que la víctima reinicie la máquina para que surta efecto.

2. Se necesita cubrir inmediatamente sus acciones o un uso abusivo de CPU. Para ello provoca un "crash" del sistema, generando así la sensación de que ha sido algo pasajero y raro.

3. El intruso cree que actúa bien al dejar fuera de servicio algún sitio Web que le disgusta. Este accionar es común en sitios pornográficos, religiosos o de abuso de menores.

4. El administrador del sistema quiere comprobar que sus instalaciones no son vulnerables a este tipo de ataques.

5. El administrador del sistema tiene un proceso que no puede "matar" en su servidor y, debido a este, no puede acceder al sistema. Para ello, lanza contra sí mismo un ataque D ó S deteniendo los servicios.

4.12.1 JAMMING O FLOODING

Este tipo de ataques desactivan o saturan los recursos del sistema. Por ejemplo, un atacante puede consumir toda la memoria o espacio en disco disponible, así como enviar tanto tráfico a la red que nadie más pueda utilizarla.

Aquí el atacante satura el sistema con mensajes que requieren establecer conexión. Sin embargo, en vez de proveer la dirección IP del emisor, el mensaje contiene falsas direcciones IP usando Spoofing y Looping. El sistema responde al mensaje, pero como no recibe respuesta, acumula buffers con información de las conexiones abiertas, no dejando lugar a las conexiones legítimas.

Muchos ISPs (proveedores de Internet) han sufrido bajas temporales del servicio por ataques que explotan el protocolo TCP. Muchos Hosts de Internet han sido dados de baja por el "ping de la muerte" (una versión-trampa del comando ping).

Mientras que el ping normal simplemente verifica si un sistema esta enlazado a la red, el ping de la muerte causa el bloqueo instantáneo del equipo. Esta vulnerabilidad ha sido ampliamente utilizada en el pasado pero, aún hoy pueden encontrarse sistemas vulnerables.

Otra acción común es la de enviar millares de e-mails sin sentido a todos los usuarios posibles en forma continua, saturando los sistemas destinos.

4.12.2 SYN FLOOD

Como ya se explicó en el TCP SYN Scanning el protocolo TCP se basa en una conexión en tres pasos. Pero, si el paso final no llega a establecerse, la conexión permanece en un estado denominado "semiabierto".

El SYN Flood es el más famoso de los ataques del tipo Denial of Service, publicado por primera vez en la revista under Phrack; y se basa en un "saludo" incompleto entre los dos hosts.

El Cliente envía un paquete SYN pero no responde al paquete ACK ocasionando que la pila TCP/IP espere cierta cantidad de tiempo a que el Host hostil responda antes de cerrar la conexión. Si se crean muchas peticiones incompletas de conexión (no se responde a ninguna), el Servidor estará inactivo mucho tiempo esperando respuesta. Esto ocasiona la lentitud en los demás servicios.

SYN Flood aprovecha la mala implementación del protocolo TCP, funcionando de la siguiente manera:

Se envía al destino, una serie de paquetes TCP con el bit SYN activado, (petición de conexión) desde una dirección IP Spoofeada. Esta última debe ser inexistente para que el destino no pueda completar el saludo con el cliente.

Aquí radica el fallo de TCP: ICMP reporta que el cliente es inexistente, pero TCP ignora el mensaje y sigue intentando terminar el saludo con el cliente de forma continua.

Cuando se realiza un Ping a una maquina, esta tiene que procesarlo. Y aunque se trate de un proceso sencillo, (no es mas que ver la dirección de origen y enviarle un paquete Reply), siempre consume recursos del sistema. Si no es un Ping, sino que son varios a la vez, la máquina se vuelve mas lenta... si lo que se recibe son miles de solicitudes, puede que el equipo deje de responder (Flood).

Es obligatorio que la IP origen sea inexistente, ya que sino el objetivo, logrará responderle al cliente con un SYN/ACK, y como esa IP no pidió ninguna conexión, le va a responder al objetivo con un RST, y el ataque no tendrá efecto.

El problema es que muchos sistemas operativos tienen un límite muy bajo en el número de conexiones "semiabiertas" que pueden manejar en un momento determinado (5 a 30). Si se supera ese límite, el servidor sencillamente dejará de responder a las nuevas peticiones de conexión que le vayan llegando. Las conexiones "semiabiertas" van caducando tras un tiempo, liberando "huecos" para nuevas conexiones, pero mientras el atacante mantenga el SYN Flood, la probabilidad de que una conexión recién liberada sea capturada por un nuevo SYN malicioso es muy alta.

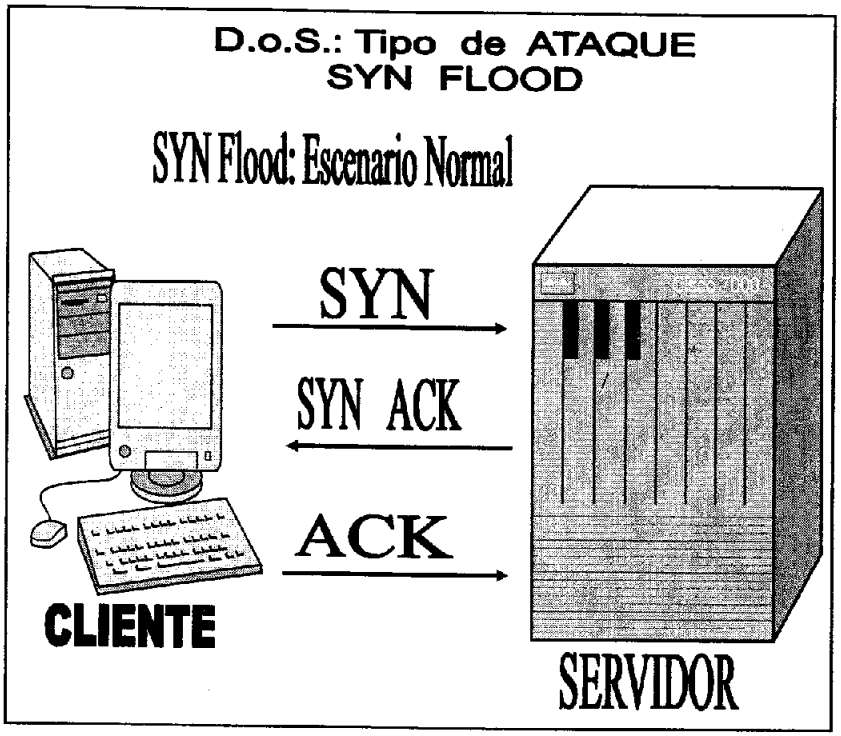


FIG. 7 TIPO DE ATAQUE SYN FLOOD

4.12.3 CONNECTION FLOOD

La mayoría de las empresas que brindan servicios de Internet (ISP) tienen un límite máximo en el número de conexiones simultaneas. Una vez que se alcanza ese límite, no se admitirán conexiones nuevas. Así, por ejemplo, un servidor Web puede tener, por ejemplo, capacidad para atender a mil usuarios simultáneos. Si un atacante establece mil conexiones y no realiza ninguna petición sobre ellas, monopolizará la capacidad del servidor. Las conexiones van caducando por inactividad poco a poco, pero el atacante sólo necesita intentar nuevas conexiones, (como ocurre con el caso del SYN Flood) para mantener fuera de servicio el servidor.

4.12.4 NET FLOOD

En estos casos, la red víctima no puede hacer nada. Aunque filtre el tráfico en sus sistemas, sus líneas estarán saturadas con tráfico malicioso, incapacitándolas para cursar tráfico útil.

Un ejemplo habitual es el de un teléfono: si alguien quiere molestar, sólo tiene que llamar, de forma continua.
Si se descuelga el teléfono (para que deje de molestar), tampoco se puede recibir llamadas de otras personas. Este problema es habitual, por ejemplo, cuando alguien intenta mandar un fax empleando el número de voz: el fax insiste durante horas, sin que el usuario llamado pueda hacer nada al respecto.

En el caso de Net Flooding ocurre algo similar. El atacante envía tantos paquetes de solicitud de conexión que las conexiones auténticas simplemente no pueden competir.

En casos así el primer paso a realizar es el ponerse en contacto con el Proveedor del servicio para que intente determinar la fuente del ataque y, como medida provisional, filtre el ataque en su extremo de la línea.

El siguiente paso consiste en localizar las fuentes del ataque e informar a sus administradores, ya que seguramente se estarán usando sus recursos sin su conocimiento y consentimiento. Si el atacante emplea IP Spoofing, el rastreo puede ser casi imposible, ya que en muchos casos la fuente del ataque es, a su vez, víctima y el origen último puede ser prácticamente imposible de determinar (Looping).

4.12.5 LAND ATTACK

Este ataque consiste en un Bug (error) en la implementación de la pila TCP/IP de las plataformas Windows. El ataque consiste en mandar a algún puerto abierto de un servidor (generalmente al NetBIOS 113 o 139) un paquete, maliciosamente construido, con la dirección y puerto origen igual que la dirección y puerto destino.

Por ejemplo se envían un mensaje desde la dirección 10.0.0.1:139 hacia ella misma. El resultado obtenido es que luego de cierta cantidad de mensajes enviados - recibidos la máquina termina colgándose.

Existen ciertas variantes a este método consistente, por ejemplo, en enviar el mensaje a una dirección específica sin especificar el puerto.

4.12.6 SMURF O BROADCAST STORE

Este ataque es bastante simple y a su vez devastador. Consiste en recolectar una serie de direcciones BroadCast para, a continuación, mandar una petición ICMP (simulando un Ping) a cada una de ellas en serie, varias veces, falsificando la dirección IP de origen máquina víctima).

Este paquete maliciosamente manipulado, será repetido en difusión (Broadcast), y cientos ó miles de hosts mandarán una respuesta a la víctima cuya dirección IP figura en el paquete ICMP.

Suponiendo que se considere una red de tipo C la dirección de BroadCast sería .255; por lo que el "simple" envío de un paquete se convierte en un efecto multiplicador devastador.

Desgraciadamente la víctima no puede hacer nada para evitarlo. La solución está en manos de los administradores de red, los cuales deben configurar adecuadamente sus Routers para filtrar los paquetes ICMP de petición indeseados (Broadcast); o bien configurar sus máquinas para que no respondan a dichos paquetes. Es decir, que lo que se parchea son las máquinas/redes que puedan actuar de intermediarias (inocentes) en el ataque y no la máquina víctima.

También se podría evitar el ataque si el Router/Firewall de salida del atacante estuviera convenientemente configurado para evitar Spoofing. Esto se haría filtrando todos los paquetes de salida que tuvieran una dirección de origen que no perteneciera a la red interna.

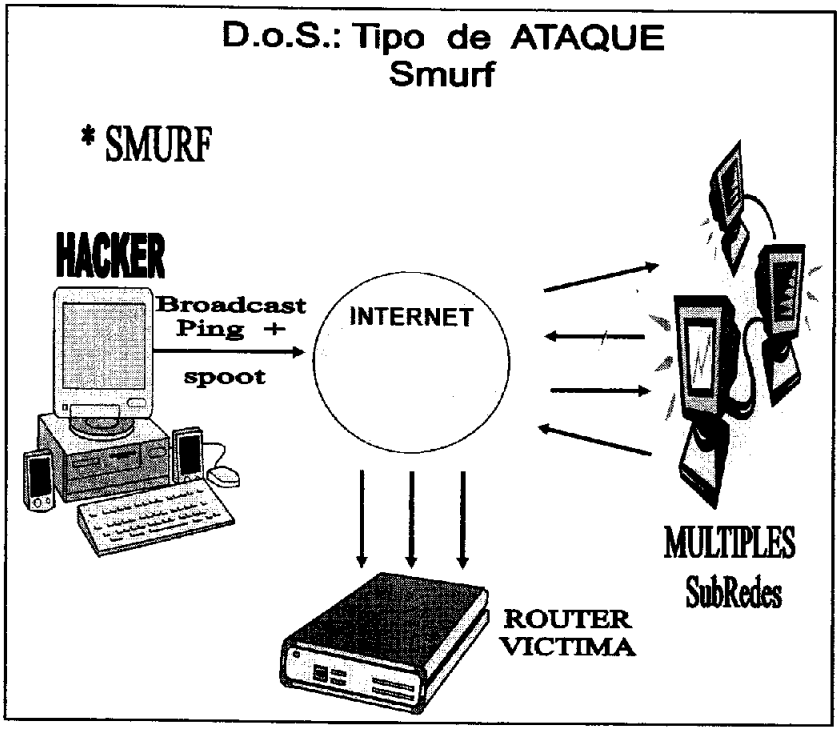


FIG. 8 TIPO DE ATAQUE Smurf

4.12.7 OOB, SUPERNUKE O WINNUKE

Un ataque característico, y quizás el más común, de los equipos con Windows es el Nuke, que hace que los equipos que escuchan por el puerto NetBIOS sobre TCP/UDP 137 a 139, queden fuera de servicio, o disminuyan su rendimiento al enviarle paquetes UDP manipulados.
Generalmente se envían fragmentos de paquetes Out Of Band, que la máquina víctima detecta como inválidos pasando a un estado inestable. OOB es el término normal, pero realmente consiste en configurar el BIT Urgente (URG) en los indicadores del encabezamiento TCP, lo que significa que este BIT es válido.

Este ataque puede prevenirse instalando los parches adecuados suministrado por el fabricante del sistema operativo afectado. Un filtro efectivo debería garantizar la detección de una inundación de bits Urgentes.

4.12.8 TEARDROP I y II NEWTEAR BONK - BOINK

Al igual que el Supernuke, los ataques Teardrop I y Teardrop II afectan a fragmentos de paquetes. Algunas implementaciones de colas IP no vuelven a armar correctamente los fragmentos que se superponen, haciendo que el sistema se cuelgue. Windows NT 4.0 de Microsoft es especialmente vulnerable a este ataque. Aunque existen Patchs (parches) que pueden aplicarse para solucionar el problema, muchas organizaciones no lo hacen, y las consecuencias pueden ser devastadoras.

Los ataques tipo Teardrop son especialmente peligrosos ya que existen multitud de implementaciones (algunas de ellas forman paquetes), que explotan esta debilidad. Las más conocidas son aquellas con el nombre Newtear, Bonk y Boink.

4.12.9 E - Mail Bombing Spamming

El E-mail Bombing consiste en enviar muchas veces un mensaje idéntico a una misma dirección, saturando asi el Mailbox del destinatario.

El Spamming, en cambio se refiere a enviar un E-mail a miles de usuarios, hayan estos solicitados el mensaje o no. Es muy utilizado por las empresas para publicitar sus productos.

El Spamming esta siendo actualmente tratado por las leyes europeas (principalmente España) como una violación de los derechos de privacidad del usuario.

4.13 ATAQUES DE MODIFICACIÓN DAÑO TAMPERING O DATA DIDDLING

Esta categoría se refiere a la modificación desautorizada de los datos o el software instalado en el sistema víctima, incluyendo borrado de archivos. Son particularmente serios cuando el que lo realiza ha obtenido derechos de administrador o Supervisor, con la capacidad de disparar cualquier comando y por ende alterar o borrar cualquier información que puede incluso terminar en la baja total del sistema.

Aún así, si no hubo intenciones de "bajar" el sistema por parte del atacante; el administrador posiblemente necesite darlo de baja por horas o días hasta chequear y tratar de recuperar aquella información que ha sido alterada o borrada.

Como siempre, esto puede ser realizado por Insiders o Outsiders, generalmente con el propósito de fraude o de dejar fuera de servicio a un competidor.

Son innumerables los casos de este tipo: empleados bancarios (o externos) que crean falsas cuentas para derivar fondos de otras cuentas, estudiantes que modifican calificaciones de exámenes, o contribuyentes que pagan para que se les anule una deuda impositiva.

Múltiples Web Sites han sido víctimas del cambio en sus páginas por imágenes (o manifiestos) terroristas o humorísticos, como el ataque de The Mentor, ya visto, a la NASA;

Otras veces se reemplazan versiones de software por otros con el mismo nombre pero que incorporan código malicioso (virus, troyanos, etc.).

4.13.1 BORRADO DE HUELLAS

El borrado de huellas es una de las tareas mas importantes que debe realizar el intruso después de ingresar en un sistema, ya que, si se detecta su ingreso, el administrador buscará como conseguir "tapar el hueco" de seguridad, evitar ataques futuros e incluso rastrear al atacante.

Las Huellas son todas las tareas que realizó el intruso en el sistema y por lo general son almacenadas en Logs (archivo que guarda la información de lo que se realiza en el sistema) por el sistema operativo.

Los archivos Logs son una de la principales herramientas (y el principal enemigo del atacante) con las que cuenta un administrador para conocer los detalles de las tareas realizadas en el sistema y la detección de intrusos.

4.13.2 ATAQUES MEDIANTE JAVA APPLETS

Java es un lenguaje de programación interpretado, desarrollado inicialmente por la empresa SUN. Su mayor popularidad la merece por su alto grado de seguridad.
Los más usados navegadores actuales, implementan Máquinas Virtuales Java (MVJ) para ser capaces de ejecutar programas (Applets) de Java.

Estos Applets, al fin y al cabo, no son más que código ejecutable y como tal, susceptible de ser manipulado por intrusos. Sin embargo, partiendo del diseño, Java siempre ha pensado en la seguridad del sistema. Las restricciones a las que somete a los Applets son de tal envergadura (imposibilidad de trabajar con archivos a no ser que el usuario especifique lo contrario, imposibilidad de acceso a zonas de memoria y disco directamente, firma digital, etc.) que es muy difícil lanzar ataques. Sin embargo, existe un grupo de expertos especializados en descubrir fallas de seguridad en las implementaciones de las MVJ.

4.13.3 ATAQUES CON JAVA SCRIPT Y VBSCRIPT

Java Script (de la empresa Netscape) y VBScript (de Microsoft) son dos lenguajes usados por los diseñadores de sitios Web para evitar el uso de Java. Los programas realizados son interpretados por el navegador.

Aunque los fallos son mucho más numerosos en versiones antiguas de Java Script, actualmente se utilizan para explotar vulnerabilidades específicas de navegadores y servidores de correo ya que no se realiza ninguna evaluación sobre si el código.

4.13.4 ATAQUES MEDIANTE ACTIVE X

ActiveX es una de las tecnologías más potentes que ha desarrollado Microsoft.

Mediante ActiveX es posible reutilizar código, descargar código totalmente funcional de un sitio remoto, etc. Esta tecnología es considerada la respuesta de Microsoft a Java.

ActiveX soluciona los problemas de seguridad mediante certificados y firmas digitales.

Una Autoridad Certificadora (AC) expende un certificado que acompaña a los controles activos y a una firma digital del programador.

Cuando un usuario descarga una página con un control, se le preguntará si confía en la AC que expendió el certificado y/o en el control ActiveX. Si el usuario acepta el control, éste puede pasar a ejecutarse sin ningún tipo de restricciones (sólo las propias que tenga el usuario en el sistema operativo). Es decir, la responsabilidad de la seguridad del sistema se

deja en manos del usuario, ya sea este un experto cibernauta consciente de los riesgos que puede acarrear la acción o un perfecto novato en la materia.

Esta última característica es el mayor punto débil de los controles ActiveX ya que la mayoría de los usuarios aceptan el certificado sin siquiera leerlo, pudiendo ser esta la fuente de un ataque con un control dañino.

La filosofía ActiveX es que las Autoridades de Certificación se fían de la palabra del programador del control. Es decir, el programador se compromete a firmar un documento que asegura que el control no es nocivo. Evidentemente siempre hay programadores con pocos escrúpulos o con ganas de experimentar.

Así, un conocido grupo de hackers alemanes (Computers Chaos Club), desarrolló un control ActiveX maligno que modificaba el programa de Gestión Bancaria Personal Quicken95 de tal manera que si un usuario aceptaba el control, éste realizaba la tarea que supuestamente tenía que hacer y además modificaba el Quicken, para que la próxima vez que la víctima se conectara a su banco, se iniciara automáticamente una transferencia a una cuenta del grupo alemán .

Otro control ActiveX muy especialmente "malévolo" es aquel que manipula el código de ciertos exploradores, para que éste no solicite confirmación al usuario a la hora de descargar otro control activo de la Web. Es decir, deja totalmente descubierto, el sistema de la víctima, a ataques con tecnología ActiveX.

4.13.5 VULNERABILIDADES EN LOS NAVEGADORES

Generalmente los navegadores no fallan por fallos intrínsecos, sino que fallan las tecnologías que implementan, aunque en este punto analizaremos realmente fallos intrínsecos de los navegadores, como pueden ser los "Buffer Overflow".

Los "Buffer Overflow" consisten en explotar una debilidad relacionada con los buffers que la aplicación usa para almacenar las entradas de usuario. Por ejemplo, cuando el usuario escribe una dirección en formato URL ésta se guarda en un buffer para luego procesarla. Si no se realizan las oportunas operaciones de comprobación, un usuario podría manipular estas direcciones.

Los protocolo usado puede ser HTTP, pero también otros menos conocidos, internos de cada explorador, como el "res:" o el "mk:". Precisamente existen fallos de seguridad del tipo "Buffer Overflow" en la implementación de estos dos protocolos.

Además la reciente aparición (octubre de 2000) de vulnerabilidades del tipo Transversal en el servidor Web Internet Information Server de la empresa Microsoft, explotando fallas en la traducción de caracteres Unicode, puso de manifiesto cuan fácil puede resultar explotar una cadena no validada. Por ejemplo:

www.servidor.com/_vti_bin/..%c0%af../..%c0%af../..%c0%af../winnt/system32/cmd.exe?/c+dir+c:\

Devuelve el directorio de la unidad c: del servidor deseado. Para poder lanzar este tipo de ataques hay que tener un buen conocimiento de lenguaje ensamblador y de la estructura interna de la memoria del sistema operativo utilizado o bien, leer la documentación de sitios Web donde explican estas fallas.

También se puede citar el fallo de seguridad descubierto por Cybersnot Industries relativo a los archivos ".lnk" y ".url" de Windows 95 y NT respectivamente. Algunas versiones de Microsoft Internet Explorer podían ser utilizadas para ejecutar la aplicación que se deseara siempre que existiera en la computadora de la víctima (por ejemplo el tan conocido y temido format.com).

Para más información relacionada con los ataques intrínsecos a los navegadores, se aconsejan las páginas no oficiales de seguridad tanto en Internet Explorer como en Netscape Communicator.

4.14 ERRORES DE DISEÑO, IMPLEMENTACIÓN Y OPERACIÓN

Muchos sistemas están expuestos a "agujeros" de seguridad que son explotados para acceder a archivos, obtener privilegios o realizar sabotaje. Estas vulnerabilidades ocurren por variadas razones, y miles de "puertas invisibles" son descubiertas cada día en sistemas operativos, aplicaciones de software, protocolos de red, browsers de Internet, correo electrónico y todas clase de servicios informáticos disponibles.

Los Sistemas operativos abiertos (como UNIX y LINUX) tienen agujeros mas conocidos y controlados que aquellos que existen en sistemas operativos cerrados (como Windows).

La importancia y ventaja del código abierto radica en miles de usuarios analizan dicho código en busca de posibles bugs y ayudan a obtener soluciones en forma inmediata.

Constantemente se encuentran en Internet avisos de nuevos descubrimientos de problemas de seguridad, herramientas de Hacking y Exploits que los explotan, por lo que hoy también se hace indispensable contar con productos que conocen esas debilidades, puedan diagnosticarlas y actualizar el programa afectado con el parche adecuado.

4.15 IMPLEMENTACIÓN DE ESTAS TÉCNICAS

A lo largo de mi investigación he recopilado distinto tipos de programas que son la aplicación de las distintas técnicas enumeradas anteriormente. La mayoría de las mismos son encontrados fácilmente en Internet en versiones ejecutables, y de otros se encuentra el código fuente, generalmente en lenguaje C y Java.

Cada una de las técnicas explicadas pueden ser utilizadas por un intruso en un ataque.

A continuación se intentarán establecer el orden de utilización de las mismas, pero siempre remarcando que un ataque insume mucha paciencia, imaginación acumulación de conocimientos y experiencia dada, en la mayoría de los casos por prueba y error.

1. Identificación del problema (víctima): en esta etapa se recopila toda la información posible de la víctima. Cuanta más información se acumule, más exacto y preciso será el ataque, más fácil será eliminar las evidencias y más difícil será su rastreo.

2. Exploración del sistema víctima elegido: en esta etapa se recopila información sobre los sistemas activos de la víctima, cuales son los más vulnerables y cuales se encuentran disponibles. Es importante remarcar que si la victima parece apropiada en la etapa de Identificación, no significa que esto resulte así en esta segunda etapa.

3. Enumeración: en esta etapa se identificaran las cuentas activas y los recursos compartidos mal protegidos. La diferencia con las etapas anteriores es que aquí se establece una conexión activa a los sistemas y la realización de consultas dirigidas.

Estas intrusiones pueden (y deberían) ser registradas, por el administrador del sistema, o al menos detectadas para luego ser bloqueadas.

4. Intrusión propiamente dicha: en esta etapa el intruso conoce perfectamente el sistema y sus debilidades y comienza a realizar las tareas que lo llevaron a trabajar, en muchas ocasiones, durante meses.

Contrariamente a lo que se piensa, los sistemas son difíciles de penetrar si están bien administrados y configurados. Ocasionalmente los defectos propios de la arquitectura de los sistemas proporciona un fácil acceso, pero esto puede ser, en la mayoría de los casos, subsanado aplicando las soluciones halladas.

4.16 ¿CÓMO DEFENDERSE DE ESTOS ATAQUES?

La mayoría de los ataques mencionados se basan en fallos de diseño inherentes a Internet (y sus protocolos) y a los sistemas operativos utilizados, por lo que no son "solucionables" en un plazo breve de tiempo.

La solución inmediata en cada caso es mantenerse informado sobre todos los tipos de ataques existentes y las actualizaciones que permanentemente lanzan las empresas desarrolladoras de software, principalmente de sistemas operativos.

Las siguientes son medidas preventivas. Medidas que toda red y administrador deben conocer y desplegar cuanto antes:

1. Mantener las máquinas actualizadas y seguras físicamente
2. Mantener personal especializado en cuestiones de seguridad (o subcontratarlo).

3. Aunque una máquina no contenga información valiosa, hay que tener en cuenta que puede resultar útil para un atacante, a la hora de ser empleada en un DoS coordinado o para ocultar su verdadera dirección.
4. No permitir el tráfico "broadcast" desde fuera de nuestra red. De esta forma evitamos ser empleados como "multiplicadores" durante un ataque Smurf.
5. Filtrar el tráfico IP Spoof.
6. Auditorias de seguridad y sistemas de detección.
7. Mantenerse informado constantemente sobre cada unas de las vulnerabilidades encontradas y parches lanzados. Para esto es recomendable estar suscripto a listas que brinden este servicio de información.
8. Por último, pero quizás lo más importante, la capacitación continua del usuario.

4.17 CREACIÓN Y DIFUSIÓN DE VIRUS

Quizás uno de los temas más famosos y sobre los que más mitos e historias fantásticas se corren en el ámbito informático sean los Virus.

Pero como siempre en esta obscura realidad existe una parte que es cierta y otra que no lo es tanto. Para aclarar este enigma veamos porque se eligió la palabra Virus (del latín Veneno) y que son realmente estos "parásitos"

4.18 VIRUS INFORMÁTICOS vs. VIRUS BIOLÓGICOS

Un análisis comparativo de analogías y diferencias entre las dos "especies", muestra que las similitudes entre ambos son poco menos que asombrosas. Para notarlas ante todo debemos saber con exactitud que es un Virus Informático y que es un Virus Biológico.

Virus Informático (VI): Pequeño programa, invisible para el usuario (no detectable por el sistema operativo) y de actuar específico y subrepticio, cuyo código incluye información suficiente y necesaria para que, utilizando los mecanismos de ejecución que le ofrecen otros programas a través del microprocesador, puedan reproducirse formando réplicas de sí mismos (completas, en forma discreta, en un archivo, disco u computadora distinta a la que ocupa), susceptibles de mutar; resultando de dicho proceso la modificación, alteración y/o destrucción de los programas, información y/o hardware afectados (en forma lógica).

"Un virus responde al modelo DAS: Dañino, Auto replicante y Furtivo".

Virus Biológico (VB): Fragmentos de ADN o ARN cubiertos de una capa proteica. Se reproducen solo en el interior de células vivas, para lo cual toman el control de sus enzimas y metabolismo. Sin esto son tan inertes como cualquier otra macromolécula.

Algunas analogías entre ambos son:

1. Los VB están compuestos por ácidos nucleicos que contienen información (programa dañino o VI) suficiente y necesaria para que utilizando los ácidos de la célula huésped (programa infectado por los VI) puedan reproducirse a sí mismos.
2. Los VB no poseen metabolismo propio, por lo tanto no manifiestan actividad fuera del huésped. Esto también sucede en los VI, por ejemplo, si se apaga la máquina o si el virus se encuentra en un disquete que esta dentro de un cajón.
3. El tamaño de un VB es relativamente pequeño en comparación con las células que infectan. Con los VI sucede lo mismo. Tanto los VB como los VI causan un daño sobre el huésped.
4. Ambos virus inician su actividad en forma oculta y sin conocimiento de su huésped, y suelen hacerse evidentes luego de que el daño ya es demasiado alto como para corregirse.
5. La finalidad de un VB (según la ciencia) es la reproducción y eventual destrucción del huésped como consecuencia. La de los VI pueden ser muchos los motivos de su creación (por parte de su autor), pero también terminan destruyendo o modificando de alguna manera a su huésped.
6. Ambos virus contienen la información necesaria para su replicación y eventual destrucción. La diferencia radica en la forma de contener esta información: en los VB es un código genético y en los VI es código binario.
7. El soporte de la información también es compartida por ambos "organismos". En los VB el soporte lo brinda el ADN o ARN (soporte orgánico). En los VI el soporte es un medio magnético (inorgánico).
8. Ambos tipos de virus son propagados de diversa formas (y raramente en todas ellas). En el caso de los VB su medio de propagación es el aire, agua, contacto directo, etc. Los VI pueden propagarse introduciendo un disquete infectado en una computadora sana (y ejecutando la zona infectada); o viceversa de RAM infectada a un disquete sano; o directamente aprovechando un flujo de electrones: MODEM, Red, etc.
9. En ambos casos sucede que la reproducción es de tipo replicativo del original y cuya exactitud dependerá de la existencia de mutaciones o no.
10. Ambas entidades cumplen con el patrón de epidemiología médica.
11. El origen de una entidad generalmente es desconocido, pero lo que se sabe con exactitud es que los VI son producidos por seres humanos y que los VB son entidades de origen biológico y últimamente de origen humano (armas biológicas).

Son, sin dudas, muchas más las analogías que pueden encontrarse haciendo un análisis más exhaustivo de ambas entidades, pero que trascenderían los límites de este informe. La idea es solamente dejar bien en claro que no existe ningún extraño, oscuro o sobrenatural motivo que dé explicación a un VI. Simplemente es un programa más, que cualquiera de nosotros sería capaz de concebir... con las herramientas e intenciones apropiadas del caso.

4.19 ORIGEN

Los orígenes de los VI se puede establecer al observar investigaciones sobre Inteligencia y Vida Artificial. Estos conceptos fueron desarrollados por John Von Neuman hacia 1950 estableciendo por primera vez la idea de programas autorreplicables.

Luego, en 1960 en los laboratorios de Bell se desarrollaron juegos (programas) que "luchaban" entre sí con el objetivo de lograr el mayor espacio de memoria posible.
Estos programas llamados Core Wars hacían uso de técnicas de ataque, defensa, ocultamiento y reproducción que luego adoptaron los VI.

En 1970, John Shoch y Jon Hupp elaboraron, en el Palo Alto Research Center (PARC) de Xerox, programas autorreplicables que servían para controlar la salud de las redes informáticas. Días después de su lanzamiento el programa se propago en todas las máquinas y sus múltiples (miles) copias de sí mismo colapsaron la red. Cabe aclarar que el fin de estos programas era, en un principio, solo experimental y sin fines maléficos.

En los años 80 nacen los primeros VI propiamente dichos y en 1983 se establece una definición para los mismos. En 1985 infectaban el MSDOS y en 1986 ya eran destructivos (Brain, Vienna, Viernes 13, etc.). Estos utilizaban disquetes para su propagación y dependían totalmente de la ignorancia del público que hacia copias indiscriminadas de los mismos.

En palabras del Dr. Fred Cohen. "El 3 noviembre de 1983, el primer virus fue concebido como un experimento para ser presentado en un seminario semanal de Seguridad Informática. El concepto fue introducido por el autor y el nombre "virus" fue dado por Len Adleman. Después de ocho horas de trabajo sobre un VAX 11/750 ejecutando UNIX, el primer virus estuvo listo para la demostración. En esa semana fueron obtenidos los permisos y cinco experimentos fueron realizados. El 10 de noviembre el virus fue mostrado. La infección inicial fue realizada en "vd" (un programa que mostraba la estructura de archivos de UNIX gráficamente) e introducido a los usuarios vía un BBS (...)."

De aquí quizás provenga la ¿leyenda? en donde se sugiere que los VI surgieron como una medida de seguridad de compañías de desarrollo de software para disuadir a los usuario de la adquisición de software ilegal. Esta versión no ha sido demostrada ni desmentida, pero el tiempo ha demostrado que los verdaderos perjudicados son las mismas compañías acusadas en su momento.

El 2 de noviembre de 1988 se produce el primer ataque masivo a una red (ARPAnet, precursora de Internet). El método utilizado para su autorreplicación era el correo electrónico y en tres horas el gusano se hizo conocer en todo EE.UU. La erradicación de este gusano costó un millón de dólares y demostró qué podía hacer un programa autorreplicable fuera de control.

El autor, Robert Morris (hijo de uno de los programadores de Core Wars), graduado de Harvard de 23 años reconoció su error y lo calificó de "fallo catastrófico", ya que su idea no era hacer que los ordenadores se volvieran lentos.

En este mismo año, como consecuencia de lo acontecido y de la concientización, por parte de la industria informática, de la necesidad de defender los sistemas informáticos, aparecen los primeros programas antivirus.

En 1991 aparecen los primeros Kits para la construcción de virus, lo que facilitó su creación e hizo aumentar su número a mayor velocidad. El primero fue el VCL (Virus Creation Laboratory), creado por Nowhere Man.

En 1992 nace el virus Michelangelo (basado en el Stoned), y aunque es un virus no especialmente destructivo, la prensa lo "vendió" como una grave amenaza mundial.

Algunos fabricantes de antivirus, aseguraron que cinco millones de computadoras se verían afectadas por el virus.

El número no pasó de cinco mil. Pese a ello, la noticia provocó una alarma injustificada entre los usuarios de computadoras personales, aunque en cierto modo también sirvió para concientizar a estos mismos usuarios de la necesidad de estar alerta frente a los virus, que ya habían dejado definitivamente de ser una curiosidad científica para pasar a convertirse en una plaga peligrosa.

A partir de aquí, los virus alcanzaron notoriedad y son perfeccionados día a día mediante técnicas de programación poco comunes. Su proliferación se debió, principalmente, al crecimiento de las redes y a los medios para compartir información.

4.20 LOS NÚMEROS HABLAN

A mediados de los noventa se produjeron enormes cambios en el mundo de la informática personal que llegan hasta nuestros días y que dispararon el número de virus en circulación hasta límites insospechados. Si a finales de 1994 el número de virus, según la International Computer Security Association (ICSA), rondaba los cuatro mil, en los siguientes cinco años esa cifra se multiplicó por diez, y promete seguir aumentando.

Cientos de virus son descubiertos mes a mes (de 6 a 20 por día), y técnicas más complejas se desarrollan a una velocidad muy importante a medida que el avance tecnológico permite la creación de nuevas puertas de entrada.

La NCSA es el principal organismo dedicado al seguimiento del fenómeno de los virus en todo el mundo. Según sus informes, en Estados Unidos más del 99% de las grandes y medianas empresas han sufrido la infección por virus en alguno de sus computadoras. Sólo un 0.67% asegura no haberse encontrado nunca con un virus.

Se calcula que, en término medio, se infectan 40,6% computadoras al año. La proporción de infecciones anuales ha crecido ampliamente, ya que en 1996 este índice era sólo del 12%.

Existen virus adscritos a programa y también a documentos, los conocidos como Macrovirus. Estos últimos, concretamente los que utilizan documentos de MS-Word para la infección comenzaron su propagación en 1995, cuando Microsoft lanza su nueva versión de este popular procesador de texto.

Aprovechando esta innovación tecnológica (las macros), han aparecido más de 1,900 virus diferentes, registrados y catalogados, que utilizan este medio para infectar los documentos. Tal ha sido su crecimiento y extensión, que los principales responsables de la lucha antivirus llegaron a recomendar que no se enviaran ni se aceptaran documentos de MS Word enviados por Internet, lo que suponía una fuerte limitación al uso del correo electrónico.

Entre los diez virus más importantes de 1997, cuatro eran macros de Word. Según la NCSA, si sólo un 30% de todos las PCs del mundo utilizaran un antivirus actualizado y activo de forma permanente, se cortaría las cadena de contagio y se acabaría con el fenómeno de los virus en todo el mundo.
Sin embargo, no todos los usuarios, bien sean de carácter empresarial o doméstico, son conscientes del riesgo que corren. Hace un tiempo bastaba con chequear los nuevos programas o archivos que se introducían en la computadora, teniendo especial cuidado con el software pirateado (principal forma de contagio) y con los disquetes usados provenientes de otras personas. De alguna manera, las vías de transmisión eran menores y estaban más controladas.

Pero con Internet, las posibilidades de infección se han multiplicado con creces.

Desde el 17 al 31 de julio del año 2000 la empresa antivirus Panda Software y otras organizaciones montaron la Primera Campaña Nacional Antivirus Informáticos, el propósito de la campaña era ofrecer al usuario la posibilidad de búsqueda de virus en su sistema (en forma online) y desinfección del mismo.

Al finalizar la campaña, se obtuvieron 516.122 visitas al sitio y se eliminaron 348,195 virus. Las vías de infección informadas fueron el 56% vía e-mail, el 31% vía disquete y el 5% vía CD-ROM.

A nivel mundial, en el ámbito de las medianas y grandes empresas, históricamente, la mayor causa de pérdidas de información fue el sabotaje, seguido por los virus informáticos y por último por otras causas como fallas e impericias. Durante 1993 y 1994 las pérdidas por virus superaron las ocasionadas por sabotaje, pero a partir de 1995 el sabotaje volvió a ocupar el primer lugar debido a la utilización de virus específicos.

Según la NCSA en 1995 el volumen de pérdidas causadas en los Estados Unidos por VI era similar al de las pérdidas por Hacking y alcanzaban los U$S 1,000 millones. En 1996 las pérdidas por VI, aumentaron en mayor proporción que las causadas por intrusos informáticos alcanzando los U$S 5,000 millones y U$S 6,000 millones respectivamente.

4.21 DESCRIPCIÓN DE UN VIRUS

Si bien un VI es un ataque de tipo Tampering, difiere de este porque puede ser ingresado al sistema por un dispositivo externo (diskettes) o a través de la red (e-mails u otros protocolos) sin intervención directa del atacante.

Dado que el virus tiene como característica propia su autoreproducción, no necesita de mucha ayuda para propagarse rápidamente.

Existen distintos tipos de virus, como aquellos que infectan archivos ejecutables (.exe, .com., .dll, etc.), los sectores de Boot y la Tabla de Partición de los discos.

Actualmente los que causan mayores problemas son los macro-virus y scriptvirus, que están ocultos en simples documentos, planillas de cálculo, correo electrónico y aplicaciones que utiliza cualquier usuario de PC.

La difusión se potencia con la posibilidad de su transmisión de un continente a otro a través de cualquier red o Internet. Y además son multiplataforma, es decir, no dependen de un sistema operativo en particular, ya que un documento puede ser procesado tanto en Windows 95/98/NT/2000/XP, como en una Macintosh u otras.

Los virus son la principal amenaza en la red. Estos programas de extensión relativamente pequeña, son programas capaces de autorreplicarse o copiarse a sí mismos. Internet aporta lo que se podría decir una vía rápida de infección de este tipo de programas dañinos.

Antes, la distribución de los virus era una tarea lenta ya que sólo se contagiaban a través de disquetes. Las tres vías de propagación más ampliamente conocidas son: un attach de correo electrónico, un trasvase FTP y un download desde una página Web.

Poseen unas particularidades que los hacen perfectamente reconocibles por la forma en que trabajan; el virus nace en el ordenador del creador como subprograma ejecutable, después se suelta en la red o se copia dentro de un programa comercial de gran difusión para asegurar un contagio rápido y masivo.

Tras la fase de creación vienen las más importantes a cumplir de forma automática e independiente del control del creador del virus. El proceso consta de contagio, incubación, replicación y ataque.

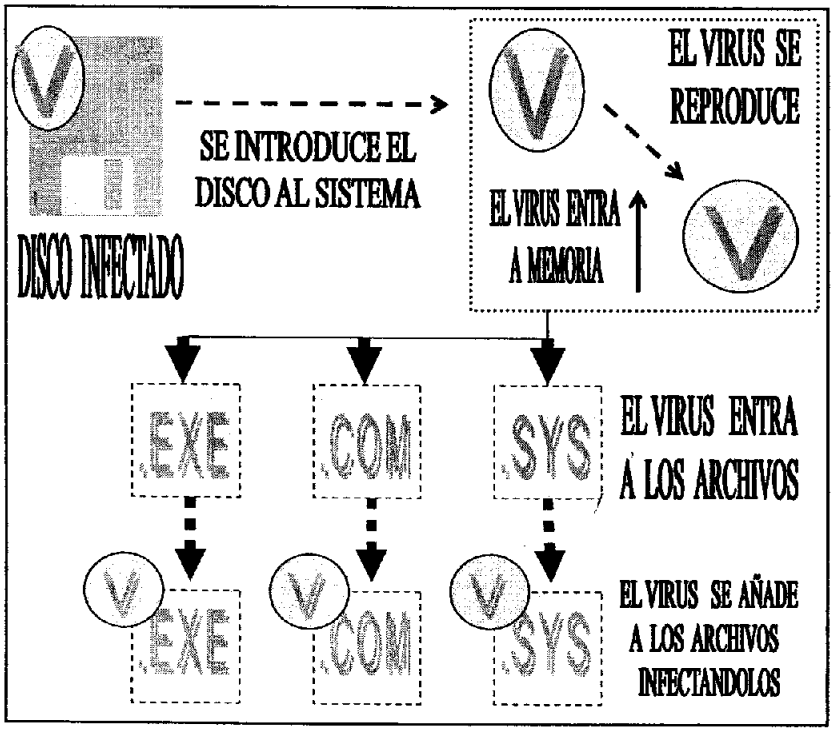


FIG. 9 EJEMPLO DE INTRODUCCIÓN DE UN VIRUS

4.21.1 RIESGOS DE INFECCIÓN.

Los primeros riesgos de infección de cualquier virus son, sin lugar a dudas, poner nuestra máquina a disposición de Internet. En cualquier rincón de ella podemos encontrar un nuevo virus o uno ya conocido, que incluso puede entrar por vía correo electrónico. Otro tipo de infección está a través de los CDs que se regalan en las revistas de informática e incluso la infección nos llega a través del disquete de un amigo, pero puestas así las cosas, uno bien podría decir que lo mejor sería tener la computadora apagada.

4.21.2 TÉCNICAS DE PROPAGACIÓN

Actualmente las técnicas utilizadas por los virus para logra su propagación y subsistencia son muy variadas y existen aquellos que utilizan varias de ellas para lograrlo.

1. Disquetes y otros medios removibles. A la posibilidad de que un disquete contenga un archivo infectado se une el peligro de que integre un virus de sector de arranque (Boot).

En este segundo caso, y si el usuario lo deja en la disquetera, infectará el ordenador cuando lo encienda, ya que el sistema intentará arrancar desde el disquete.

2. Correo electrónico: el usuario no necesita hacer nada para recibir mensajes que, en muchos casos ni siquiera ha solicitado y que pueden llegar de cualquier lugar del mundo. Los mensajes de correo electrónico pueden incluir archivos, documentos o cualquier objeto ActiveX Java infectado que, al ejecutarse, contagian la computadora del usuario. En las últimas generaciones de virus se envían e-Mail sin mensajes pero con archivos adjuntos (virus) que al abrirlos proceden a su ejecución y posterior infección del sistema atacado.

Estos virus poseen una gran velocidad de propagación ya que se envían automáticamente a los contactos de la libreta de direcciones del sistema infectado.

3. IRC o Chat: las aplicaciones de mensajería instantánea (ICQ, AOL Instant Messenger, etc.) o Internet Relay Chat (IRC), proporcionan un medio de comunicación anónimo, rápido, eficiente, cómodo y barato. Sin embargo, también son peligrosas, ya que los entornos de Chat ofrecen, por regla general, facilidades para la transmisión de archivos, que conllevan un gran riesgo en un entorno de red.

4. Páginas Web y transferencia de archivos vía FTP: los archivos que se descargan de Internet pueden estar infectados, y pueden provocar acciones dañinas en el sistema en el que se ejecutan.

5. Grupos de noticias: sus mensajes e información (archivos) pueden estar infectados y, por lo tanto, contagiar al equipo del usuario que participe en ellos.

4.21.3 INCUBACIÓN.

Normalmente los virus se crean de formas específicas que atienden a una serie de instrucciones programadas como el esconderse y reproducirse mientras se cumplen unas opciones concretas predeterminadas por el creador del virus. Así, el virus permanece escondido reproduciéndose en espera de activarse cuando se cumplan esas condiciones.

Así, el virus permanece escondido reproduciéndose en espera de activarse cuando se cumplan las condiciones determinadas por el creador. Este proceso puede ser muy rápido en algunos casos, y bastante rápido en otros, según el tipo de virus.

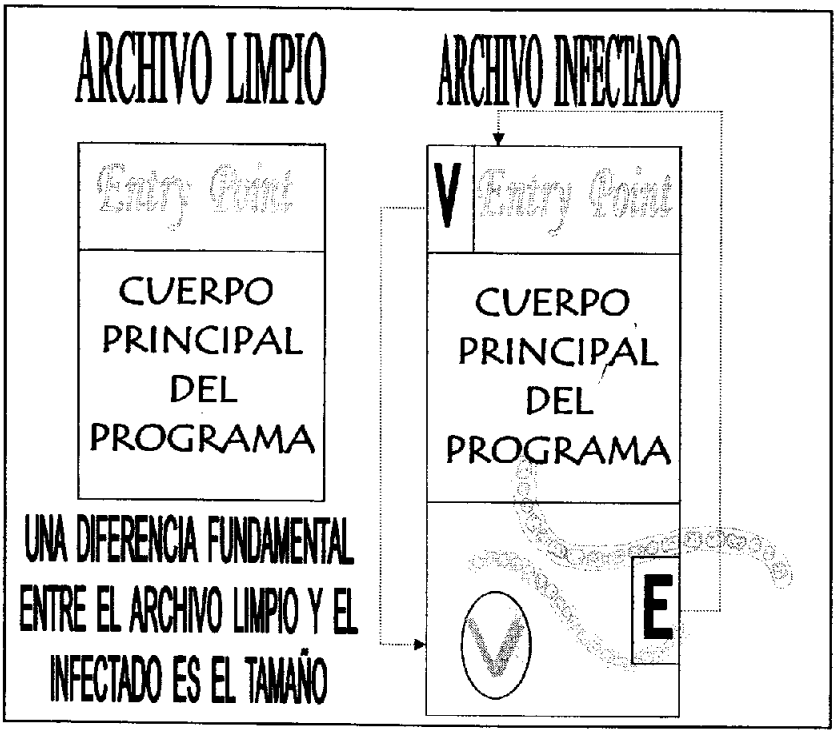


FIG. 10 EJEMPLO DE ARCHIVO INFECTADO

4.22 TIPOS DE VIRUS

Un virus puede causar daño lógico (generalmente) o físico (bajo ciertas circunstancias y por repetición) de la computadora infectada y nadie en su sano juicio deseará ejecutarlo. Para evitar la intervención del usuario los creadores de virus debieron inventar técnicas de las cuales valerse para que su "programa" pudiera ejecutarse. Estas son diversas y algunas de lo más ingeniosas.

4.22.1 Archivos Ejecutables (virus Exe Vir)

El virus se adosa a un archivo ejecutable y desvía el flujo de ejecución a su código, para luego retornar al huésped y ejecutar las acciones esperadas por el usuario. Al realizarse esta acción el usuario no se percata de lo sucedido. Una vez que el virus es ejecutado se aloja en memoria y puede infectar otros archivos ejecutables que sean abiertos en esa máquina.

En este momento su dispersión se realiza en sistema de 16 bits (DOS) y de 32 bits (Windows) indistintamente, atacando programas .com, .exe, .dll, .sys, .pif, etc, según el sistema infectado.

Ejemplos: Chernovil, Darth Vader, PHX

4.22.2 Virus en el Sector de Arranque (Virus ACSO Anterior a la Carga del SO)

En los primeros 512 bytes de un disquete formateado se encuentran las rutinas necesarias para la carga y reconocimiento de dicho disquete. Entre ellas se encuentra la función invocada si no se encuentra el Sistema Operativo. Es decir que estos 512 bytes se ejecutan cada vez que se intenta arrancar (bootear) desde un disquete (o si se dejó olvidado uno en la unidad y el orden de booteo de la PC es A: y luego C:). Luego, esta área es el objetivo de un virus de booteo.

Se guarda la zona de booteo original en otro sector del disco (generalmente uno muy cercano o los más altos). Luego el virus carga la antigua zona de booteo. Al arrancar el disquete se ejecuta el virus (que obligatoriamente debe tener 512 bytes o menos) quedando residente en memoria; luego ejecuta la zona de booteo original, salvada anteriormente. Una vez más el usuario no se percata de lo sucedido ya que la zona de booteo se ejecuta iniciando el sistema operativo (si existiera) o informando la falta del mismo.

Ejemplo: 512, Stoned, Michelangelo, Diablo.

4.22.3 Virus Residente

Como ya se mencionó, un virus puede residir en memoria. El objetivo de esta acción es controlar los accesos a disco realizados por el usuario y el Sistema Operativo. Cada vez que se produce un acceso, el virus verifica si el disco o archivo objetivo al que se accede, está infectado y si no lo está procede a almacenar su propio código en el mismo. Este código se almacenará en un archivo, tabla de partición, o en el sector de booteo, dependiendo del tipo de virus que se trate.

Ejemplos: 512, Avispa, Michelangelo, DIR II.

4.22.4 Macro Virus

Estos virus infectan archivos de información generados por aplicaciones de oficina que cuentan con lenguajes de programación de macros. Últimamente son los más expandidos, ya que todos los usuarios necesitan hacer intercambio de documentos para realizar su trabajo. Los primeros antecedentes de ellos fueron con las macros de Lotus 123 que ya eran lo suficientemente poderosas como permitir este tipo de implementación.

Pero los primeros de difusión masiva fueron desarrollados a principios de los '90 para el procesador de texto Microsoft Word, ya que este cuenta con el lenguaje de programación Word Basic.

Su principal punto fuerte fue que terminaron con un paradigma de la seguridad informática: "los únicos archivos que pueden infectarse son los ejecutables" y todas las tecnologías antivirus sucumbieron ante este nuevo ataque.

Su funcionamiento consiste en que si una aplicación abre un archivo infectado, la aplicación (o parte de ella) se infecta y cada vez que se genera un nuevo archivo o se modifique uno existente contendrá el macro-virus.

Ejemplos:

De Microsoft Word: CAP I, CAP II, Concept, Wazzu.
De Microsoft Excel: Laroux.
De Lotus Amipro: GreenStripe

4.22.5 Virus de Mail

El "último grito de la tecnología" en cuestión de virus. Su modo de actuar, al igual que los anteriores, se basa en la confianza excesiva por parte del usuario: a este le llega vía mail un mensaje con un archivo comprimido (.ZIP por ejemplo), el usuario lo descomprime y al terminar esta acción, el contenido (virus ejecutable) del archivo se ejecuta y comienza el daño.

Este tipo de virus tomó relevancia estos últimos años con al explosión masiva de Internet y últimamente con el virus Melissa y I Love You. Generalmente estos virus se auto envían a algunas de las direcciones de la libreta. Cada vez que uno de estos usuarios recibe el supuesto mensaje no sospecha y lo abre, ocurriendo el mismo reenvío y la posterior saturación de los servidores al existir millones de mensajes enviados.

4.22.6 Virus de Sabotaje

Son virus construidos para sabotear un sistema o entorno específico. Requieren de conocimientos de programación pero también una acción de inteligencia que provea información sobre el objetivo y sus sistemas.

4.22.7 Hoax, los Virus Fantasmas

El auge del correo electrónico generó la posibilidad de transmitir mensajes de alerta de seguridad. Así comenzaron a circular mensajes de distinta índole (virus, cadenas solidarias, beneficios, catástrofes, etc.) de casos inexistentes. Los objetivo de estas alertas pueden causar alarma, la pérdida de tiempo, el robo de direcciones de correo y la saturación de los servidores con las consecuentes pérdidas de dinero que esto ocasiona.

4.22.8 Virus de Applets Java y Controles Active X

Si bien, como ya se comentó, estas dos tecnologías han sido desarrolladas teniendo como meta principal la seguridad, la práctica demuestra que es posible programar virus sobre ellas. Este tipo de virus se copian y se ejecutan a sí mismos mientras el usuario mantiene una conexión a Internet.

4.22.9 Reproductores Gusanos

Son programas que se reproducen constantemente hasta agotar totalmente los recursos del sistema huésped y/o recopilar información relevante para enviarla a un equipo al cual su creador tiene acceso.

4.22.10 CABALLOS DE TROYA

De la misma forma que el antiguo caballo de Troya de la mitología griega escondía en su interior algo que los troyanos desconocía, y que tenía una función muy diferente a la que ellos podían imaginar; un Caballo de Troya es un programa que aparentemente realiza una función útil pero además realiza una operación que el usuario desconoce y que generalmente beneficia al autor del troyano o daña el sistema huésped.

Si bien este tipo de programas NO cumplen con la condición de autoreproducción de los virus, encuadran perfectamente en la características de programa dañino.

Consisten en introducir dentro de un programa una rutina o conjunto de instrucciones, no autorizadas y que la persona que lo ejecuta no conoce, para que dicho programa actúe de una forma diferente a como estaba previsto.

Los ejemplos más conocidos de troyanos son el Back Office y el Net Bus que, si bien no fueron desarrollados con ese fin, son una poderosa arma para tomar el control de la computadora infectada. Estos programas pueden ser utilizados para la administración total del sistema atacado por parte de un tercero, con los mismos permisos y restricciones que el usuario de la misma.

4.22.11 Bombas lógicas.

Son una de las buenas ganancias del Cracker malicioso, están especialmente diseñadas para hacer daño. Pueden realizar dos funciones: la de crear un subprograma que se active después de un tiempo llenando la memoria del ordenador y la de colapsar nuestro correo electrónico.

En la primera referencia, el subprograma se instala en nuestro ordenador después de ser bajado junto a un mensaje de correo electrónico. Se incuba sin crear ninguna copia de sí mismo a la espera de reunir las condiciones oportunas, tras ese período de espera el programa se activa y se auto replica para dañar nuestro sistema.

Para llevar a cabo la segunda función alguien envía una bomba lógica por correo electrónico (estos virus también se conocen con el nombre de Mailbombing), que es un mismo mensaje enviado miles de veces hasta colapsar nuestro sistema. Los antivirus no están preparados para detectar este tipo de virus, pero existen programas que pueden filtrar la información repetida (firewall).

4.22.12 Cookies

En principio un cookie es una partición de texto que se escribe en nuestro disco duro cuando visitamos una Web. Esta información identifica entre otras cosas desde el lugar que visitamos, hasta el tiempo que nuestro navegador los emplea para recordar buena parte de la Web la próxima vez que la visitemos. Así, es habitual vernos sorprendidos cuando visitamos una Web de hacking y nada más acceder a ella, muestra un mensaje en el cual se detalla la versión de navegador que empleamos, fecha, hora, y hasta la última página Web visitada.

Esto es posible gracias a estos microprogramas Cookies que lo mismo que se escriben en nuestro disco duro, escribimos en otros discos duros, o pueden ser leídos por programas específicos. A través de los Cookies se nos pueden colar virus de macro o incluso Troyanos, por ello los navegadores más populares nos permiten configurar la opción de eliminar estos Cookies de nuestro disco duro o evitar que se escriban.

4.22.13 SNIFFERS

Su misión es fisgonear la red en busca de claves o puertos abiertos. Los Sniffers actúan con otros programas revienta claves. También existen escaneadores espías en busca de puertos libres o sistemas en busca de número de tarjetas de créditos. Después estos datos son reventados por medio de la fuerza bruta, basándose en un diccionario electrónico.

4.23 MODELO DE VIRUS INFORMÁTICO

Un virus está compuesto por su propio entorno, dentro del cual pueden distinguirse tres módulos principales:

1. Módulo de Reproducción: es el encargado de manejar las rutinas de parasitación de entidades ejecutables con el fin de que el virus pueda ejecutarse subrepticiamente, permitiendo su transferencia a otras computadoras.

2. Módulo de Ataque: Es el que maneja las rutinas de daño adicional al virus. Esta rutina puede existir o no y generalmente se activa cuando el sistema cumple alguna condición. Por ejemplo el virus Chernovil se activa cada vez que el reloj del sistema alcanza el 26 de cada mes.

3. Módulo de Defensa: Este módulo, también optativo, tiene la misión de proteger al virus. Sus rutinas tienden a evitar acciones que faciliten o provoquen la detección o remoción del virus.

4.24 TIPOS DE DAÑOS OCASIONADOS POR LOS VIRUS

Los virus informáticos no afectan (en su gran mayoría) directamente el hardware sino a través de los programas que lo controlan; en ocasiones no contienen código nocivo, o bien, únicamente causan daño al reproducirse y utilizar recursos escasos como el espacio en el disco rígido, tiempo de procesamiento, memoria, etc. En general los daños que pueden causar los virus se refieren a hacer que el sistema se detenga, borrado de archivos, comportamiento erróneo de la pantalla, despliegue de mensajes, desorden en los datos del disco, aumento del tamaño de los archivos ejecutables o reducción de la memoria total.

Para realizar la siguiente clasificación se ha tenido en cuenta que el daño es una acción de la computadora, no deseada por el usuario:

a. Daño Implícito: es el conjunto de todas las acciones dañinas para el sistema que el virus realiza para asegurar su accionar y propagación. Aquí se debe considerar el entorno en el que se desenvuelve el virus ya que el consumo de ciclos de reloj en un medio delicado (como un aparato biomédico) puede causar un gran daño.

b. Daño Explícito: es el que produce la rutina de daño del virus.

Con respecto al modo y cantidad de daño, encontramos:

a. Daños triviales: daños que no ocasionan ninguna pérdida grave de funcionalidad del sistema y que originan una pequeña molestia al usuario. Deshacerse del virus implica, generalmente, muy poco tiempo.

b. Daños menores: daños que ocasionan una pérdida de la funcionalidad de las aplicaciones que poseemos. En el peor de los casos se tendrá que reinstalar las aplicaciones afectadas.

c. Daños moderados: los daños que el virus provoca son formatear el disco rígido o sobrescribir parte del mismo. Para solucionar esto se deberá utilizar la última copia de seguridad que se ha hecho y reinstalar el sistema operativo.

d. Daños mayores: algunos virus pueden, dada su alta velocidad de infección y su alta capacidad de pasar desapercibidos, lograr que el día que se detecta su presencia tener las copias de seguridad también infectadas. Puede que se llegue a encontrar una copia de seguridad no infectada, pero será tan antigua que se haya perdido una gran cantidad de archivos que fueron creados con posterioridad.

e. Daños severos: los daños severos son hechos cuando un virus realiza cambios mínimos, graduales y progresivos. No se sabe cuando los datos son correctos o han cambiado, pues no hay unos indicios claros de cuando se ha infectado el sistema.

f. Daños ilimitados: el virus "abre puertas" del sistema a personas no autorizadas. El daño no lo ocasiona el virus, sino esa tercera persona que, gracias a él, puede entrar en el sistema.

4.25 LOS AUTORES

Tras su alias (nic), los creadores de virus sostienen que persiguen un fin educacional para ilustrar las flaquezas de los sistemas a los que atacan. Pero... ¿es necesario crear un problema para mostrar otro?.

La creación de virus no es ilegal, y probablemente no debería serlo: cualquiera es dueño de crear un virus siempre y cuando lo guarde para sí. Infectar a otras computadoras sin el consentimiento de sus usuarios es inaceptable, esto sí es un delito y debería ser penado, como ya lo es un algunos países. Inglaterra pudo condenar a ¡18 meses! de prisión al autor de SMEG. Sin embargo, el autor del virus Loverletter no fue sentenciado porque la legislación vigente en Filipinas (su país de origen) no era adecuada en el momento del arresto.

Existen otros casos en que el creador es recompensado con una oferta de trabajo millonaria por parte de multinacionales. Este, y no las condenas, es el mensaje que reciben miles de jóvenes para empezar o continuar desarrollando virus y esto se transforma en una "actividad de moda", lejos de la informática ética sobre la cual deberían ser educados.

4.26 PROGRAMA ANTIVIRUS

Un antivirus es una gran base de datos con la huella digital de todos los virus conocidos para identificarlos y también con las pautas que más contienen los virus. Los fabricantes de antivirus avanzan tecnológicamente casi en la misma medida que lo hacen los creadores de virus. Esto sirve para combatirlos, aunque no para prevenir la creación e infección de otros nuevos.

Actualmente existen técnicas, conocidas como heurísticas, que brindan una forma de "adelantarse" a los nuevos virus. Con esta técnica el antivirus es capaz de analizar archivos y documentos y detectar actividades sospechosas.

Esta posibilidad puede ser explotada gracias a que de los 620 nuevos virus diarios, sólo aparecen unos cinco totalmente novedosos al año.

Debe tenerse en cuenta que:

Un programa antivirus forma parte del sistema y por lo tanto funcionará correctamente si es adecuado y está bien configurado.

No será eficaz el 100% de los casos, no existe la protección total y definitiva.

Las funciones presentes en un antivirus son:

1. Detección: se debe poder afirmar la presencia y/o accionar de un VI en una computadora. Adicionalmente puede brindar módulos de identificación, erradicación del virus o eliminación de la entidad infectada.

2. Identificación de un virus: existen diversas técnicas para realizar esta acción:

a. Scanning: técnica que consiste en revisar el código de los archivos (fundamentalmente archivos ejecutables y de documentos) en busca de pequeñas porciones de código que puedan pertenecer a un virus (sus huellas digitales). Estas porciones están almacenadas en una base de datos del antivirus. Su principal ventaja reside en la rápida y exacta que resulta la identificación del virus. En los primeros tiempos (cuando los virus no eran tantos ni su dispersión era tan rápida), esta técnica fue eficaz, luego se comenzaron a notar sus deficiencias. El primer punto desfavorable es que brinda una solución a posteriori y es necesario que el virus alcance un grado de dispersión considerable para que llegue a mano de los investigadores y estos lo incorporen a su base de datos (este proceso puede demorar desde uno a tres meses). Este modelo reactivo jamás constituirá una solución definitiva.

b. Heurística: búsqueda de acciones potencialmente dañinas perteneciente a un virus informático. Esta técnica no identifica de manera certera el virus, sino que rastrea rutinas de alteración de información y zonas generalmente no controlada por el usuario (MBR, Boot Sector, FAT, y otras). Su principal ventaja reside en que es capaz de detectar virus que no han sido agregados a las base de datos de los antivirus (técnica proactiva). Su desventaja radica en que puede "sospechar" de demasiadas cosas y el usuario debe ser medianamente capaz de identificar falsas alarmas.

3. Chequeadores de Integridad: Consiste en monitorear las actividades de la PC señalando si algún proceso intenta modificar sectores críticos de la misma. Su ventaja reside en la prevención aunque muchas veces pueden ser vulnerados por los virus y ser desactivados por ellos, haciendo que el usuario se crea protegido, no siendo así.

Es importante diferencia los términos detectar: determinación de la presencia de un virus e identificar: determinación de qué virus fue el detectado. Lo importante es la detección del virus y luego, si es posible, su identificación y erradicación.

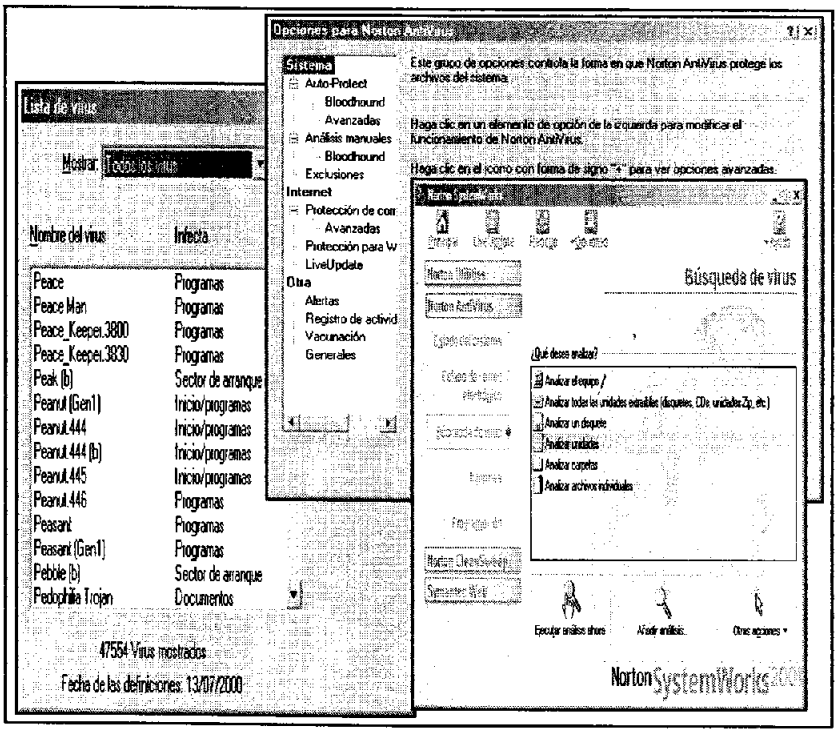


FIG. 11 EJEMPLO DE PROGRAMA ANTIVIRUS (Copyright Norton Antivirus by Symantec)

4.27 MODELO DE UN ANTIVIRUS

Un antivirus puede estar constituido por dos módulos principales y cada uno de ellos contener otros módulos.

Módulo de Control: Este módulo posee la técnica de Verificación de Integridad que posibilita el registro de posibles cambios en los zonas y archivos considerados de riesgo.

Módulo de Respuesta: La función de "Alarma" se encuentra en todos los antivirus y consiste en detener la ejecución de todos lo programas e informar al usuario de la posible existencia de un virus. La mayoría ofrecen la posibilidad de su erradicación si la identificación a sido positiva.

4.28 UTILIZACIÓN DE LOS ANTIVIRUS

Como ya se ha descrito un VI es un programa y, como tal se ejecuta, ocupa un espacio en memoria y realiza las tareas para las que ha sido programado. En el caso de instalarse un antivirus en una computadora infectada, es probable que este también sea infectado y su funcionamiento deje de ser confiable. Por lo tanto si se sospecha de la infección de una computadora, nunca deben realizarse operaciones de instalación o desinfección desde la misma. El procedimiento adecuado sería reiniciar el sistema y proceder a la limpieza desde un sistema limpio y seguro.

La mayoría de los antivirus ofrecen la opción de reparación de los archivos dañados.

Puede considerarse este procedimiento o la de recuperar el/los archivos perdidos desde una copia de seguridad segura.

4.29 ASPECTOS JURÍDICOS SOBRE VIRUS INFORMÁTICOS

El análisis de la responsabilidad derivada de la difusión de un virus merece especial atención en estos momentos en que el uso de la redes telemáticas permite un mayor alcance de sus efectos. Prueba de ello tenemos en la reciente difusión por correo electrónico del antes mencionado virus "I Love you".

Para analizar los diferentes supuestos que generan responsabilidad, debemos tener en cuenta los canales de difusión que contribuyen a potenciar el efecto pirámide en el que los virus basan su efectividad. En todos ellos es aplicable el régimen de la responsabilidad extracontractual establecida en el Código Civil que obliga a reparar los daños a quien, por acción u omisión, causa un perjuicio a otro, interviniendo la culpa o negligencia.

La mera creación de un virus puede obedecer a una intención distinta a la puesta en circulación. Cabe recordar aquí la diferencia que hacen los Hackers entre el creador de un virus y el diseminador del mismo.

En cuanto a la puesta en circulación es difícil obtener una identificación plena del responsable de la misma. Aunque en el caso de redes telemáticas es posible encontrar rastros de la primera aparición del virus, es posible alterar esa información. En cualquier caso, la responsabilidad de la persona que inicia la cadena de efectos nocivos de un virus, planificando la difusión intencionada del mismo a través de un medio está clara, pues el daño es perfectamente previsible (aunque no su magnitud) y seguro.

En cuanto a la introducción intencionada en un sistema específico, por su tipificación como delito de daños, los actos de sabotaje informático pueden generar responsabilidad civil y penal. Pueden tener su origen en personas del interior de la empresa que por un motivo como, por ejemplo, la ruptura de la relación laboral, deciden causar un daño, o en personas del exterior de la empresa, que acceden al sistema informático por medios telemáticos, por ejemplo. En ambos casos se cumplen los requisitos para reclamar una indemnización.

La difusión de un virus entre usuarios de sistemas informáticos puede ser debida a una conducta negligente o la difusión de virus no catalogados. La diligencia debida en el tratamiento de la información obliga a realizar copias de seguridad y a instalar sistemas de detección de virus. En el caso de archivos que se envían a otros usuarios, la ausencia de control previo puede ser calificado como negligente, puesto que el riesgo de destrucción de datos se está traspasando a terceros y ello podía haberse evitado de una manera sencilla y económica. Pero también puede alegarse que el usuario receptor del archivo afectado podría haber evitado el daño pasando el correspondiente antivirus, a lo que cabe replicar que este trámite se obvió por tratarse de un remitente que ofrecía confianza.

Por último, en algunos países en donde se han tratado Leyes de Propiedad Intelectual, se establece la exclusión de los VI de las creaciones protegidas por el derecho de autor. El objetivo de este precepto es facilitar las actividades de análisis necesarias para la creación de un antivirus, aunque esto resulta innecesario por la sencilla razón de que el creador de un virus no acostumbra a reclamar la titularidad del mismo de forma pública.

4.30 CONSEJOS

Aunque existe una relativa concientización, generalmente no se toman todas las precauciones necesarias para anular el peligro. No basta con tener un antivirus, sino que éste hay que actualizarlo periódicamente para contemplar los nuevos virus que van apareciendo.

Además de poseer la cualidad de chequeo manual, detección y eliminación, debe ser sobre todo capaz de actuar como vacuna o filtro, impidiendo la entrada de los nuevos virus que aparecen cada día. De esta forma, aunque al usuario se le olvide pasar el antivirus, sabe que al menos existe una protección automática. La mayoría de los antivirus que se comercializan poseen estas características.

En la Campaña Nacional Antivirus Informáticos se proponen 15 consejos para evitar el contagio de virus. A continuación se resumen todas ellas:

I. Instalar un buen antivirus para la detección y eliminación de nuevos virus. Además es necesario actualizarlo frecuentemente. Como ya se ha explicado la efectividad de un programa antivirus reside, en gran medida, en su capacidad de actualización (preferentemente diaria).

II. Comprobar que el antivirus elegido incluye soporte técnico, resolución urgente de nuevos virus y servicios de alerta, bien a través de correo electrónico, por teléfono o fax.

III. Asegurarse que el antivirus esté siempre activo vigilando constantemente todas las operaciones realizadas en el sistema.

IV. Verificar, antes de abrir, cada nuevo mensaje de correo electrónico recibido. Este medio es el medio de transmisión preferido por los diseminadores de virus. Cualquier correo puede contener virus, aunque no este acompañado de archivos adjuntos. Además no es necesario ejecutar el archivo adjunto de un mensaje de correo para ser infectado, en algunos sistemas basta únicamente con abrir el mensaje. Para prevenir esto, lo mejor es verificar los mensajes inesperados o que provengan de una fuente poco habitual.

V. Evitar la descarga de programas de lugares no seguros o pocos fiables de Internet. Muchas páginas Web permiten la descarga de programas y archivos cabiendo la posibilidad que estos archivos estén infectados. Son sitios seguros aquellos que muestran una información clara acerca de su actividad y los productos o servicios que ofrecen.

VI. Rechazar archivos que no se hayan solicitado cuando se esté en chats o grupos de noticias. Hay que tener especial cuidado y aceptar sólo lo que llegue de un remitente conocido y de confianza.

VII. Analizar siempre con un buen antivirus los disquetes que entran y salen de la computadora. Si se utilizan disquetes propios en otros lugares es aconsejable protegerlos contra escritura.

VIII. Retirar los disquetes de las disqueteras al apagar o reiniciar la computadora. Esta tarea es para evitar que se activen los virus de arranque.

IX. Analizar el contenido de los archivos comprimidos. El antivirus deberá de contar con una funcionalidad que permita detectar el mayor número de formatos comprimidos posibles. Además, antes de abrir uno de estos archivos, es aconsejable guardarlos en carpetas temporales.

X. Mantenerse alerta ante acciones sospechosas de posibles virus. Hay varios síntomas que pueden delatar la presencia de nuevos virus: aumento del tamaño de los archivos, aviso de macros en documentos, ralentización en ciertos procesos, etc. Como mejor solución a estas sospechas de posibles infecciones, se debe recurrir al servicio de resolución urgente de nuevos virus de la compañía antivirus.

XI. Añadir las opciones de seguridad de las aplicaciones que se utilizan normalmente en la política de protección antivirus, ya que los programas informáticos más utilizados se convierten, precisamente por esta razón, en blanco de los autores de virus.

XII. Realizar copias de seguridad frecuentes y periódicas de la información más importante. Esta es una muy buena forma de minimizar el impacto de un virus. De esta manera, una pérdida de datos, causada por un virus, puede ser superada mediante la restauración de la última copia.

XIII. Ante la gran cantidad de información recibida por diferentes medios, es aconsejable contrastar estos datos con la información completa, actualizada y experta difundida por determinadas compañías y organismos confiables.

XIV. A la hora de instalar nuevos programas, el riesgo de infección es menor (aunque no nulo) si se trata de software legal. Si el software ha llegado de fuentes piratas nadie puede asegurar que esté libre de virus.

XV. Exigir a los fabricantes de software, proveedores de acceso a Internet y editores de publicaciones, que se impliquen en la lucha contra los virus. En la lucha contra los virus es precisa la participación de todos los agentes implicados en el sector informático para minimizar el problema de las infecciones provocadas.

CAPITULO 5

FIREWALLS Y SEGURIDAD EN INTERNET

CAPITULO 5

FIREWALLS Y SEGURIDAD EN INTERNET

5. FIREWALLS Y SEGURIDAD EN INTERNET

La seguridad ha sido el principal concerniente a tratar cuando una organización desea conectar su red privada al Internet. Sin tomar en cuenta el tipo de negocios, se ha incrementado el numero de usuarios de redes privadas por la demanda del acceso a los servicios de Internet tal es el caso del World Wide Web (WWW), Internet Mail (e-mail), Telnet, y File Transfer Protocol (FTP). Adicionalmente los corporativos buscan las ventajas que ofrecen las paginas en el WWW y los servidores FTP de acceso publico en el Internet.

Los administradores de red tienen que incrementar todo lo concerniente a la seguridad de sus sistemas, debido a que se expone la organización privada de sus datos así como la infraestructura de sus red a los Expertos de Internet (*Internet Crakers*). Para superar estos temores y proveer el nivel de protección requerida, la organización necesita seguir una política de seguridad para prevenir el acceso no-autorizado de usuarios a los recursos propios de la red privada, y protegerse contra la exportación privada de información.

Todavía, aun si una organización no esta conectada al Internet, esta debería establecer una política de seguridad interna para administrar el acceso de usuarios a porciones de red y proteger sensitivamente la información secreta.

Firewall: Un Firewall en Internet es un sistema o grupo de sistemas que impone una política de seguridad entre la organización de red privada y el Internet. El firewall determina cual de los servicios de red pueden ser accesados dentro de esta por los que están fuera, es decir quien puede entrar para utilizar los recursos de red pertenecientes a la organización. Para que un firewall sea efectivo, todo trafico de información a través del Internet deberá pasar a través del mismo donde podrá ser inspeccionada la información. El firewall podrá únicamente autorizar el paso del trafico, y el mismo podrá ser inmune a la penetración. desafortunadamente, este sistema no puede ofrecer protección alguna una vez que el agresor lo traspasa o permanece entorno a este.

La Política De Seguridad Crea Un Perímetro De Defensa, esto es importante, ya que debemos de notar que un firewall de Internet no es justamente un ruteador, un servidor de defensa, o una combinación de elementos que proveen seguridad para la red. El firewall es parte de una política de seguridad completa que crea un perímetro de defensa diseñada para proteger las fuentes de información. Esta política de seguridad podrá incluir publicaciones con las guías de ayuda donde se informe a los usuarios de sus responsabilidades, normas de acceso a la red, política de servicios en la red, política de autenticidad en acceso remoto o local a usuarios propios de la red, normas de dial-in y dial-out, reglas de encriptación de datos y discos, normas de protección de virus, y entrenamiento. Todos los puntos potenciales de ataque en la red podrán ser protegidos con el mismo nivel de seguridad. Un firewall de Internet sin una política de seguridad comprensiva es como poner una puerta de acero en una tienda.

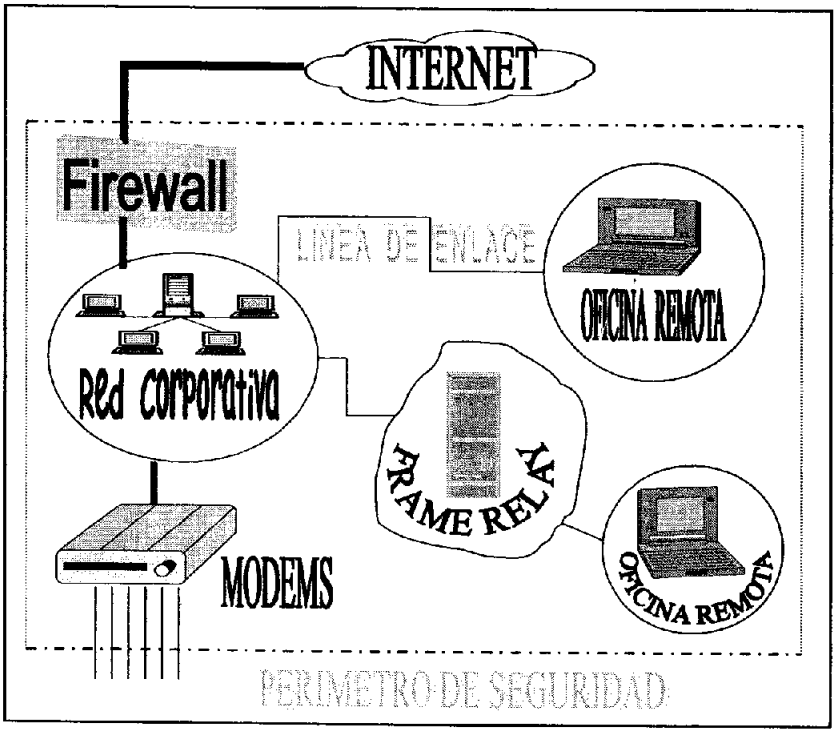


FIG. 12 EJEMPLO DE FIREWALL

5.1 BENEFICIOS DE UN FIREWALL EN INTERNET

Los Firewalls en Internet administran los accesos posibles del Internet a la red privada. Sin un firewall, cada uno de los servidores propios del sistema se exponen al ataque de otros servidores en el Internet. Esto significa que la seguridad en la red privada depende de la "Dureza" con que cada uno de los servidores cuenta y es únicamente seguro tanto como la seguridad en la fragilidad posible del sistema.

El firewall permite al administrador de la red definir un "check point" (embudo), manteniendo al margen los usuarios no-autorizados (tal, como., hackers, crakers, vándalos, y espías) fuera de la red, prohibiendo potencialmente la entrada o salida al vulnerar los servicios de la red, y proporcionar la protección para varios tipos de ataques posibles. Uno de los beneficios clave de un firewall en Internet es que ayuda a simplificar los trabajos de administración, una vez que se consolida la seguridad en el sistema firewall, es mejor que distribuirla en cada uno de los servidores que integran nuestra red privada.

El firewall ofrece un punto donde la seguridad puede ser monitoreada y si aparece alguna actividad sospechosa , este generara una alarma ante la posibilidad de que ocurra un ataque, o suceda algún problema en el transito de los datos. Esto se podrá notar al acceder la organización al Internet, la pregunta general es "si" pero "cuando" ocurrirá el ataque. Esto es extremadamente importante para que el administrador audite y lleve una bitácora del trafico significativo a través del firewall. También, si el administrador de la red toma el tiempo para responder una alarma y examina regularmente los registros de base. Esto es innecesario para el firewall, desde que el administrador de red desconoce si ha sido exitosamente atacado.

Con el paso de algunos años, Internet ha experimentado una crisis en las direcciones, logrando que el direccionamiento IP sea menos generoso en los recursos que proporciona. Por este medio se organizan las compañías conectadas al Internet, debido a esto hoy no es posible obtener suficientes registros de direcciones IP para responder a la población de usuarios en demanda de los servicios. Un firewall es un lugar lógico para desplegar un Traductor de Direcciones de Red (NAT) esto puede ayudar aliviando el espacio de direccionamiento acortando y eliminando lo necesario para re-enumerar cuando la organización cambie del Proveedor de Servicios de Internet (ISPs).

Un firewall de Internet es el punto perfecto para auditar o registrar el uso del Internet. Esto permite al administrador de red justificar el gasto que implica la conexión al Internet, localizando con precisión los cuellos de botella potenciales del ancho de banda, y promueve el método de cargo a los departamentos dentro del modelo de finanzas de la organización.

Un firewall de Internet ofrece un punto de reunión para la organización. Si una de sus metas es proporcionar y entregar servicios información a consumidores, el firewall de Internet es ideal para desplegar servidores WWW y FTP.

Genera un punto de falla simple. Enfatizando si este punto de falla se presenta en la conexión al Internet, aun así la red interna de la organización puede seguir operando - únicamente el acceso al Internet esta perdido.

La preocupación principal del administrador de red, son los múltiples accesos al Internet, que se pueden registrar con un monitor y un firewall en cada punto de acceso que posee la organización hacia el Internet. Estos dos puntos de acceso significa dos puntos potenciales de ataque a la red interna que tendrán que ser monitoreados regularmente

5.2 LIMITACIONES DE UN FIREWALL

Un firewall no puede protegerse contra aquellos ataques que se efectúen fuera de su punto de operación.
Por ejemplo, si existe una conexión dial-out sin restricciones que permita entrar a nuestra red protegida, el usuario puede hacer una conexión SLIP o PPP al Internet. Los usuarios con sentido común suelen "irritarse" cuando se requiere una autenticación adicional requerida por un Firewall Proxy Server (FPS) lo cual se puede ser provocado por un sistema de seguridad circunvecino que esta incluido en una conexión directa SLIP o PPP del ISP.

Este tipo de conexiones derivan la seguridad provista por firewall construido cuidadosamente, creando una puerta de ataque. Los usuarios pueden estar consientes de que este tipo de conexiones no son permitidas como parte de integral de la arquitectura de la seguridad en la organización.

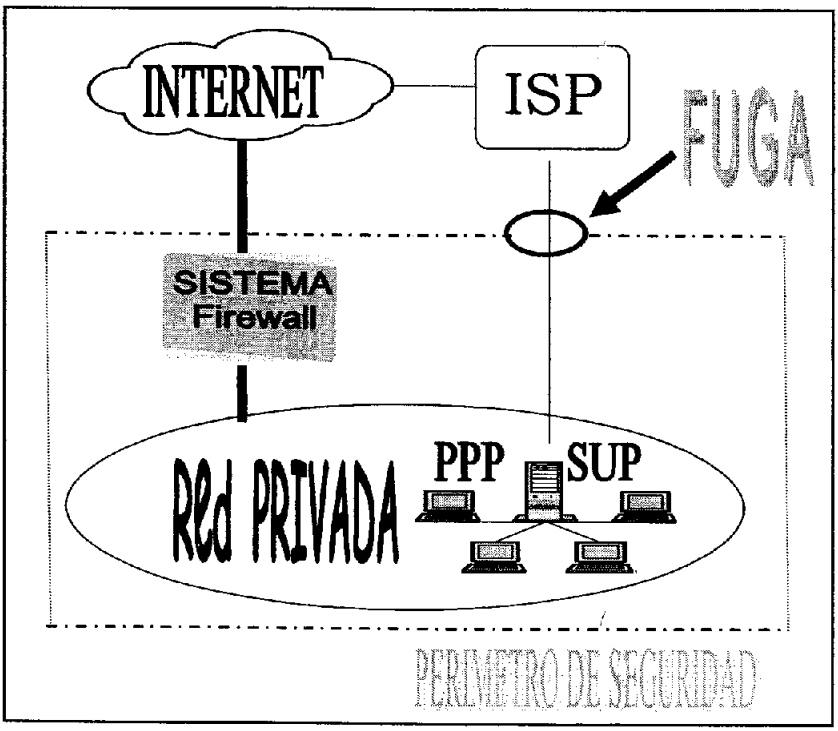


FIG. 13 EJEMPLO DE FALLA EN EL PERÍMETRO DE SEGURIDAD

5.3 CONEXIÓN CIRCUNVECINA AL FIREWALL DE INTERNET.

El firewall no puede protegerse de las amenazas a que esta sometido por traidores o usuarios inconscientes. El firewall no puede prohibir que los traidores o espías corporativos copien datos sensitivos en disquetes o tarjetas PCMCIA y substraigan estas del edificio.

El firewall no puede proteger contra los ataques de la "Ingeniería Social", por ejemplo un Hacker que pretende ser un supervisor o un nuevo empleado despistado, persuade al menos sofisticado de los usuarios a que le permita usar su contraseña al servidor del corporativo o que le permita el acceso "temporal" a la red.

Para controlar estas situaciones, los empleados deberían ser educados acerca de los varios tipos de ataque social que pueden suceder, y a cambiar sus contraseñas si es necesario periódicamente.

El firewall no puede protegerse contra los ataques posibles a la red interna por virus informativos a través de archivos y software. Obtenidos del Internet por sistemas operativos al momento de comprimir o descomprimir archivos binarios, el firewall de Internet no puede contar con un sistema preciso de SCAN, para cada tipo de virus que se puedan presentar en los archivos que pasan a través de el.

La solución real esta en que la organización debe ser consciente en instalar software anti-viral en cada despacho para protegerse de los virus que llegan por medio de disquetes o cualquier otra fuente.

Finalmente, el firewall de Internet no puede protegerse contra los ataques posibles en la transferencia de datos, estos ocurren cuando aparéntenme datos inocuos son enviados o copiados a un servidor interno y son ejecutados despachando un ataque.

Por ejemplo, una transferencia de datos podría causar que un servidor modificara los archivos relacionados a la seguridad haciendo mas fácil el acceso de un intruso al sistema.

Como nosotros podemos ver, el desempeño de los servidores Proxy en un servidor de defensa es un excelente medio de prohibición a las conexiones directas por agentes externos y reduce las amenazas posibles por los ataques con transferencia de datos.

HERRAMIENTAS DEL HACKER

Es difícil describir el ataque "típico" de un hacker debido a que los intrusos poseen diferentes niveles de técnicos por su experiencia y son además son motivados por diversos factores. Algunos hackers son intrigosos por el desafío, otros mas gozan de hacer la vida difícil a los demás, y otros tantos substraen datos delicados para algún beneficio propio.

5.4 RECOLECCIÓN DE INFORMACIÓN

Generalmente, el primer paso es saber en que forma se recolecta la información y además que tipo de información es. La meta es construir una base de datos que contenga la organización de la red y colectar la información acerca de los servidores residentes.

Esta es una lista de herramientas que un hacker puede usar para colectar esta información: El protocolo SNMP puede utilizarse para examinar la tabla de ruteo en un dispositivo inseguro, esto sirve para aprender los detalles mas íntimos acerca del objetivo de la topología de red perteneciente a una organización.

El programa TraceRoute puede revelar el numero de redes intermedias y los ruteadores en torno al servidor especifico.

El protocolo Whois que es un servicio de información que provee datos acerca de todos los dominios DNS y el administrador del sistema responsable para cada dominio. No obstante que esta información es anticuada.

Servidores DNS pueden accesarce para obtener una lista de las direcciones IP y sus correspondientes Nombres (Programa Nslookup).

El protocolo Finger puede revelar información detallada acerca de los usuarios (nombres de Login, números telefónicos, tiempo y ultima sesión, etc.) de un servidor en especifico.

El programa Ping puede ser empleado para localizar un servidor particular y determinar si se puede alcanzar. Esta simple herramienta puede ser usada como un programa de escaneo pequeño que por medio de llamadas a la dirección de un servidor haga posible construir una lista de los servidores que actualmente son residentes en la red.

5.5 SONDEO DEL SISTEMA PARA DEBILITAR LA SEGURIDAD

Después que se obtienen la información de red perteneciente a dicha organización, el hacker trata de probar cada uno de los servidores para debilitar la seguridad.

Estos son algunos usos de las herramientas que un hacker puede utilizar automáticamente para explorar individualmente los servidores residentes en una red:

Una vez obtenida una lista no obstantemente pequeña de la vulnerabilidad de servicios en la red, un hacker bien instruido puede escribir un pequeño programa que intente conectarse a un puerto especificando el tipo de servicio que esta asignado al servidor en cuestión.

La corrida del programa presenta una lista de los servidores que soportan servicio de Internet y están expuestos al ataque.

Están disponibles varias herramientas del dominio publico, tal es el caso como el Rastreador de Seguridad en Internet (ISS) (Internet Security Scanner) o la Herramienta para Análisis de Seguridad para Auditar Redes (SATAN) (Security Analysis Tool for Auditing Networks), el cual puede rastrear una subred o un dominio y ver las posibles fugas de seguridad. Estos programas determinan la debilidad de cada uno de los sistemas con respecto a varios puntos de vulnerabilidad comunes en un sistema.

El intruso usa la información colectada por este tipo de rastreadores para intentar el acceso no-autorizado al sistema de la organización puesta en la mira.

Un administrador de redes hábil puede usar estas herramientas en su red privada para descubrir los puntos potenciales donde esta debilitada su seguridad y así determina que servidores necesitan ser remendados y actualizados en el software.

5.6 ACCESO A SISTEMAS PROTEGIDOS

El intruso utiliza los resultados obtenidos a través de las pruebas para poder intentar accesar a los servicios específicos de un sistema.

Después de tener el acceso al sistema protegido, el hacker tiene disponibles las siguientes opciones:

Puede atentar destruyendo toda evidencia del asalto y además podrá crear nuevas fugas en el sistema o en partes subalternas con el compromiso de seguir teniendo acceso sin que el ataque original sea descubierto.

Pueden instalar paquetes de sondeo que incluyan códigos binarios conocidos como "caballos de Troya" protegiendo su actividad de forma transparente. Los paquetes de sondeo colectan las cuentas y contraseñas para los servicios de Telnet y FTP permitiendo al hacker expandir su ataque a otras maquinas.

Pueden encontrar otros servidores que realmente comprometan al sistema. Esto permite al hacker explotar vulnerablemente desde un servidor sencillo todos aquellos que se encuentren a través de la red corporativa.

Si el hacker puede obtener acceso privilegiado en un sistema compartido, podrá leer el correo, buscar en archivos.

5.7 BASES PARA EL DISEÑO DECISIVO DEL FIREWALL

Cuando se diseña un firewall de Internet, se tiene que tomar algunas decisiones que pueden ser asignadas por el administrador de red:

Posturas sobre la política del Firewall.
La política interna propia de la organización para la seguridad total.
El costo financiero del Proyecto "Firewall".
Los componentes o la construcción de secciones del Firewall.

5.8 POLÍTICAS DEL FIREWALL.

Las posturas del sistema firewall describen la filosofía fundamental de la seguridad en la organización. Estas son dos posturas diametralmente opuestas que la política de un firewall de Internet puede tomar:

"No todo lo específicamente permitido esta prohibido"

"Ni todo lo específicamente prohibido esta permitido"

La primera postura asume que un firewall puede obstruir todo el trafico y cada uno de los servicios o aplicaciones deseadas necesariamente para ser implementadas básicamente caso por caso.

Esta propuesta es recomendada únicamente a un limitado numero de servicios soportados cuidadosamente seleccionados en un servidor. La desventaja es que el punto de vista de "seguridad" es mas importante que - facilitar el uso - de los servicios y estas limitantes numeran las opciones disponibles para los usuarios de la comunidad. Esta propuesta se basa en una filosofía conservadora donde se desconocen las causas acerca de los que tienen la habilidad para conocerlas.

La segunda postura asume que el firewall puede desplazar todo el trafico y que cada servicio potencialmente peligroso necesitara ser aislado básicamente caso por caso. Esta propuesta crea ambientes mas flexibles al disponer mas servicios para los usuarios de la comunidad. La desventaja de esta postura se basa en la importancia de "facilitar el uso" que la propia - seguridad - del sistema. También además, el administrador de la red esta en su lugar de incrementar la seguridad en el sistema conforme crece la red. Desigual a la primer propuesta, esta postura esta basada en la generalidad de conoćer las causas acerca de los que no tienen la habilidad para conocerlas.

5.9 POLÍTICA INTERNA DE LA SEGURIDAD

Tan discutidamente escuchada, un firewall de Internet no esta solo - es parte de la política de seguridad total en una organización -, la cual define todos los aspectos en competentes al perímetro de defensa. Para que esta sea exitosa, la organización debe de conocer que es lo se esta protegiendo.

La política de seguridad se basara en una conducción cuidadosa analizando la seguridad, la asesoría en caso riesgo, y la situación del negocio. Si no se posee con la información detallada de la política a seguir, aun que sea un firewall cuidadosamente desarrollado y armado, estará exponiendo la red privada a un posible atentado.

5.10 COSTO DEL FIREWALL

¿Cuanto puede ofrecer una organización por su seguridad?, un simple paquete de filtrado firewall puede tener un costo mínimo ya que la organización necesita un ruteador conectado al Internet, y dicho paquete ya esta incluido como estándar del equipo. Un sistema comercial de firewall provee un incremento mas a la seguridad pero su costo puede ser de $32,000 hasta $240,000 pesos dependiendo de la complejidad y el numero de sistemas protegidos. Si la organización posee al experto en casa, un firewall casero puede ser construido con software de dominio publico pero este ahorro de recursos repercuten en términos del tiempo de desarrollo y el despliegue del sistema firewall. Finalmente requiere de soporte continuo para la administración, mantenimiento general, actualización de software, reparación de seguridad, e incidentes de manejo.

5.11 COMPONENTES DEL SISTEMA FIREWALL

Después de las decisiones acerca de los ejemplos previos, la organización puede determinar específicamente los componentes del sistema. Un firewall típico se compone de uno, o una combinación, de los siguientes obstáculos.

1. Ruteador Filtra-paquetes.

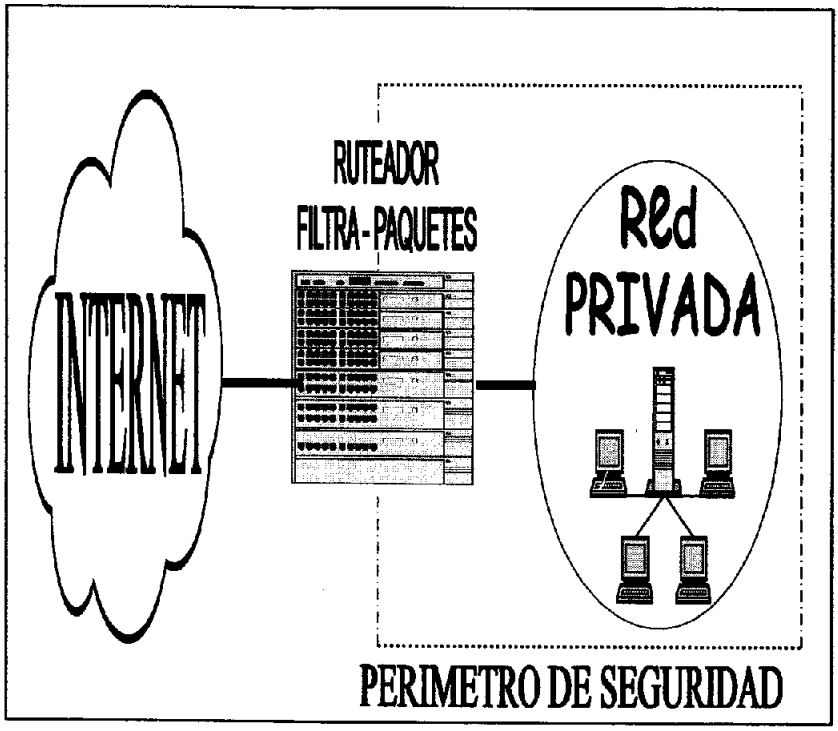


FIG. 14 RUTEADOR FILTRA PAQUETES

2. Gateway a Nivel-aplicación.

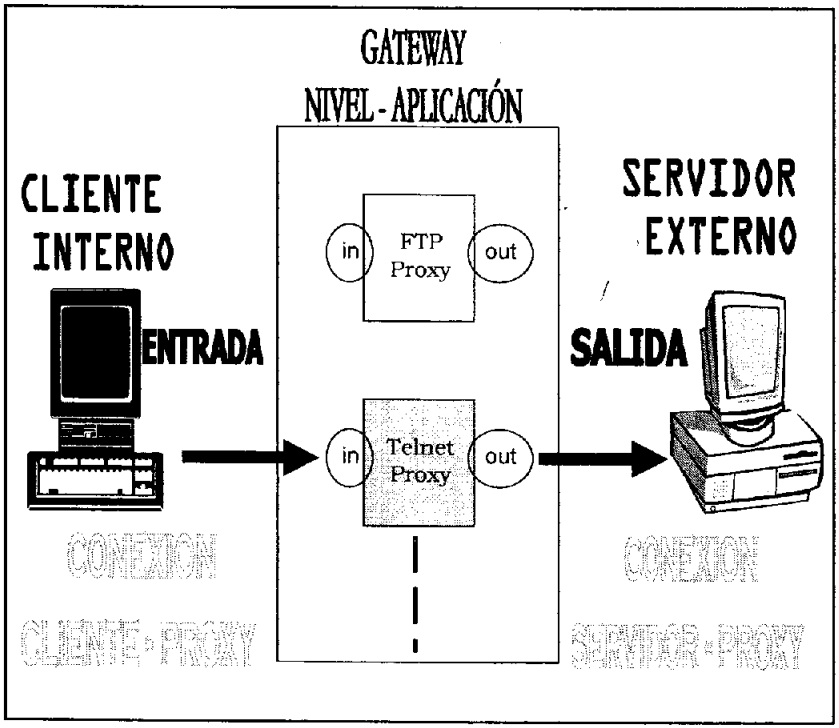


FIG. 15 GATEWAY A NIVEL APLICACIÓN

3. Gateway a Nivel-circuito.

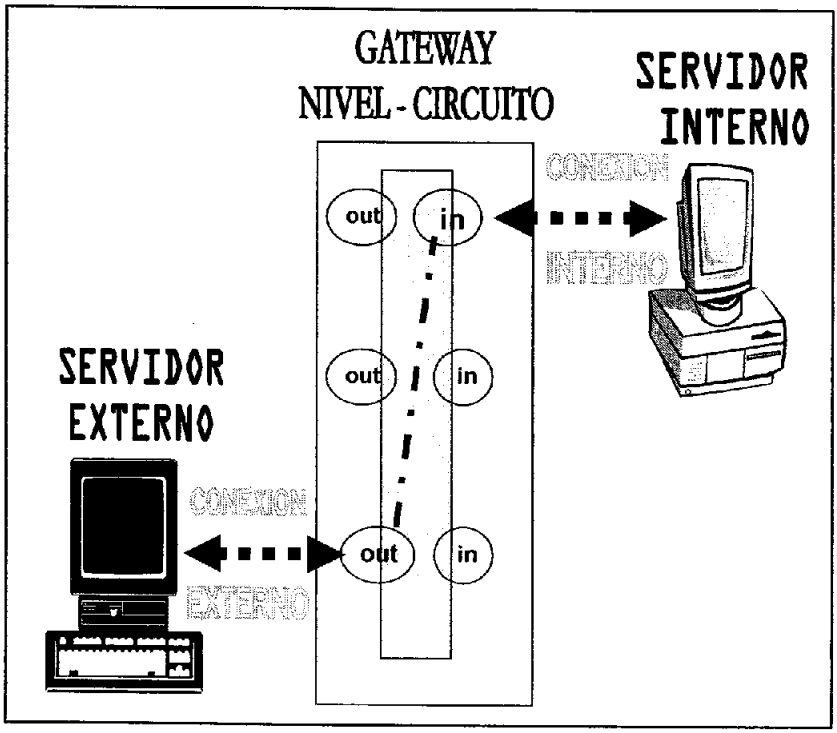


FIG. 16 GATEWAY A NIVEL CIRCUITO

5.12 EDIFICANDO OBSTÁCULOS: RUTEADOR FILTRA-PAQUETES

Este ruteador toma las decisiones de rehusar/permitir el paso de cada uno de los paquetes que son recibidos. El ruteador examina cada datagrama para determinar si este corresponde a uno de sus paquetes filtrados y que a su vez haya sido aprobado por sus reglas. Las reglas de filtrado se basan en revisar la información que poseen los paquetes en su encabezado, lo que hace posible su desplazamiento en un proceso de IP. Esta información consiste en la dirección IP fuente, la dirección IP destino, el protocolo de encapsulado (TCP, UDP, ICMP, o IP tunnel), el puerto fuente TCP/UDP, el puerto destino TCP/UDP, el tipo de mensaje ICMP, la interfase de entrada del paquete, y la interfase de salida del paquete. Si se encuentra la correspondencia y las reglas permiten el paso del paquete, este será desplazado de acuerdo a la información a la tabla de ruteo, si se encuentra la correspondencia y las reglas niegan el paso, el paquete es descartado. Si estos no corresponden a las reglas, un parámetro configurable por incumplimiento determina descartar o desplazar el paquete.

5.12.1 Servicio dependiente del filtrado

Las reglas acerca del filtrado de paquetes a través de un ruteador para rehusar/permitir el trafico esta basado en un servicio en especifico, desde entonces muchos servicios vierten su información en numerosos puertos TCP/UDP conocidos.

Por ejemplo, un servidor Telnet esta a la espera para conexiones remotas en el puerto 23 TCP y un servidor SMTP espera las conexiones de entrada en el puerto 25 TCP. Para bloquear todas las entradas de conexión Telnet, el ruteador simplemente descarta todos los paquetes que contengan el valor del puerto destino TCP igual a 23. Para restringir las conexiones Telnet a un limitado numero de servidores internos, el ruteador podrá rehusar el paso a todos aquellos paquetes que contengan el puerto destino TCP igual a 23 *y* que no contengan la dirección destino IP de uno de los servidores permitidos.

Algunas características típicas de filtrado que un administrador de redes podría solicitar en un ruteador filtra-paquetes para perfeccionar su funcionamiento serian:

Permitir la entrada de sesiones Telnet únicamente a una lista especifica de servidores internos.

Permitir la entrada de sesiones FTP únicamente a los servidores internos especificados.

Permitir todas las salidas para sesiones Telnet.

Permitir todas las salidas para sesiones FTP.

Rehusar todo el trafico UDP.

5.12.2 Servicio independiente del filtrado

Este tipo de ataques ciertamente son difíciles de identificar usando la información básica de los encabezados debido a que estos son independientes al tipo de servicio. Los ruteadores pueden ser configurados para protegerse de este tipo de ataques pero son mas difíciles de especificar desde entonces las reglas para el filtrado requieren de información adicional que pueda ser estudiada y examinada por la tabla de ruteo, inspeccionando las opciones especificas IP, revisando fragmentos especiales de edición, etc. Algunos ejemplos de este tipo de ataques incluye:

5.12.3 Agresiones Originadas Por El Direccionamiento IP.

Para este tipo de ataque, el intruso trasmite paquetes desde afuera pretendiendo pasar como servidor interno los paquetes poseen una dirección fuente IP falsa de un servidor interno del sistema. El agresor espera que usando este impostor se pueda penetrar al sistema para emplearlo seguramente como dirección fuente donde los paquetes que trasmita sean autentificados y los del otro servidor sean descartados dentro del sistema. Los ataques por seudo-fuentes pueden ser frustrados si descartamos la dirección fuente de cada paquete con una dirección fuente "interno" si el paquete arriba en una de las interfaces del ruteador "externo".

5.12.4 Agresiones Originadas En El Ruteador.

En un ataque de ruteo, la estación de origen especifica la ruta que un paquete deberá de tomar cuando cruce a través del Internet. Este tipo de ataques son diseñados para cuantificar las derivaciones de seguridad y encauzan al paquete por un inesperado camino a su destino. Los ataques originados en el ruteador pueden ser frustrados simplemente descartando todos los paquetes que contengan fuentes de ruteo opcionales.

5.12.5 Agresiones Por Fragmentación.

Por este tipo de ataques, los intrusos utilizan las características de fragmentación para crear fragmentos extremadamente pequeños y obligan a la información del encabezado TCP a separarse en paquetes. Estos pequeños fragmentos son diseñados para evitar las reglas definidas por el filtrado de un ruteador examinando los primeros fragmentos y el resto pasa sin ser visto. Aunque si bien únicamente es explotado por sencillos decodificadores , una agresión pequeñísima puede ser frustrada si se descartan todos los paquetes donde el tipo de protocolo es TCP y la fragmentación de compensación IP es igual a 1.

5.12.6 Beneficios del ruteador filtra-paquetes

La mayoría de sistemas firewall son desplegados usando únicamente ruteadores filtra-paquetes. Otros que tienen tiempo planean los filtros y configuran el ruteador, sea este pequeño o no , el costoso para implementar la filtración de paquetes no es cara; desde que los componentes básicos de los ruteadores incluyen revisiones estándar de software para dicho efecto. Desde entonces el acceso a Internet es generalmente provisto a través de interfaces WAN, optimando la operación del ruteador moderando el trafico y definiendo menos filtros. Finalmente, el ruteador de filtrado es por lo general transparente a los usuarios finales y a las aplicaciones por lo que no se requiere de entrenamiento especializado o software especifico que tenga que ser instalado en cada uno de los servidores.

5.12.7 Limitaciones del ruteador filtra-paquetes

Definir el filtrado de paquetes puede ser una tarea compleja porque el administrador de redes necesita tener un detallado estudio de varios servicios de Internet, como los formatos del encabezado de los paquetes, y los valores específicos esperados a encontrase en cada campo. Si las necesidades de filtrado son muy complejas, se necesitara soporte adicional con lo cual el conjunto de reglas de filtrado puede empezar a complicar y alargar el sistema haciendo mas difícil su administración y comprensión. Finalmente, estas serán menos fáciles de verificar para las correcciones de las reglas de filtrado después de ser configuradas en el ruteador. Potencialmente se puede dejar una localidad abierta sin probar su vulnerabilidad.

Cualquier paquete que pasa directamente a través de un ruteador puede ser posiblemente usado como parte inicial un ataque dirigido de datos. Haciendo memoria este tipo de ataques ocurren cuando los datos aparentemente inocuos se desplazan por el ruteador a un servidor interno. Los datos contienen instrucciones ocultas que pueden causar que el servidor modifique su control de acceso y seguridad relacionando sus archivos facilitando al intruso el acceso al sistema.

Generalmente, los paquetes entorno al ruteador disminuyen conforme el numero de filtros utilizados se incrementa. Los ruteadores son optimizados para extraer la dirección destino IP de cada paquete, haciendo relativamente simple la consulta a la tabla de ruteo, y el desplazamiento de paquetes para la interface apropiada de la transmisión. Si esta autorizado el filtro, no únicamente podrá el ruteador tomar la decisión de desplazar cada paquete, pero también sucede aun aplicando todas las reglas de filtrado. Esto puede consumir ciclos de CPU e impactar el perfecto funcionamiento del sistema.

El filtrado de paquetes IP no puede ser capaz de proveer el suficiente control sobre el trafico. Un ruteador Filtra-Paquetes puede permitir o negar un servicio en particular, pero no es capaz de comprender el contexto/dato del servicio. Por ejemplo, un administrador de red necesita filtrar el trafico de una capa de aplicación - limitando el acceso a un subconjunto de comandos disponibles por FTP o Telnet, bloquear la importación de Mail o Newsgroups concerniente a tópicos específicos. Este tipo de control es muy perfeccionado a las capas altas por los servicios de un servidor Proxy y en Gateways a Nivel-aplicación.

5.12.8 Gateways a nivel-aplicación

Los gateways nivel-aplicación permiten al administrador de red la implementación de una política de seguridad estricta que la que permite un ruteador filtra-paquetes. Mucho mejor que depender de una herramienta genérica de filtra-paquetes para administrar la circulación de los servicios de Internet a través del firewall, se instala en el gateway un código de propósito-especial (un servicio Proxy) para cada aplicación deseada. Si el administrador de red no instala el código Proxy para la aplicación particular, el servicio no es soportado y no podrán desplazarse a través del firewall.

Aun cuando, el código Proxy puede ser configurado para soportar únicamente las características especificas de una aplicación que el administrador de red considere aceptable mientras niega todas las otras.

Un aumento de seguridad de este tipo incrementa nuestros costos en términos del tipo de gateway seleccionado, los servicios de aplicaciones del Proxy, el tiempo y los conocimientos requeridos para configurar el gateway, y un decrecimiento en el nivel de los servicios que podrán obtener nuestros usuarios, dando como resultado un sistema carente de transparencia en el manejo de los usuarios en un ambiente "amigable". Como en todos los casos el administrador de redes debe de balancear las necesidades propias en seguridad de la organización con la demanda de "fácil de usar" demandado por la comunidad de usuarios.

Es importante notar que los usuarios tienen acceso por un servidor Proxy, pero ellos jamás podrán seccionar en el Gateway a nivel-aplicación. Si se permite a los usuarios seccionar en el sistema de firewall, la seguridad es amenazada desde el momento en que un intruso puede potencialmente ejecutar muchas actividades que comprometen la efectividad del sistema.

Por ejemplo, el intruso podría obtener el acceso de root, instalar un caballo de troya para colectar las contraseñas, y modificar la configuración de los archivos de seguridad en el firewall.

5.12.9 Servidor de defensa

Un ruteador filtra-paquetes permite la circulación directa de los paquetes dentro y fuera del sistema, diferente a esto el Gateway a nivel-aplicación deja que la información circule entre los sistemas pero no permite el intercambio directo de paquetes. El principal riesgo de permitir que los paquetes se intercambien dentro y fuera del sistema se debe a que el servidor residente en los sistemas de protección de la red podrá ser asegurado contra cualquier amenaza representada por los servicios permitidos.

Un Gateway a nivel-aplicación por lo regular es descrito como un "servidor de defensa" porque es un sistema diseñado específicamente blindado y protegido contra cualquier ataque. Hay varias características de diseño que son usadas para hacer mas seguro un servidor de defensa:

La plataforma de Hardware del servidor de defensa ejecuta una versión "segura" de su sistema operativo. Por ejemplo, si el servidor de defensa es una plataforma UNIX, se ejecutara una versión segura del sistema operativo UNIX que es diseñado específicamente para proteger los sistemas operativos vulnerables y garantizar la integridad del firewall.

Únicamente los servicios que el administrador de redes considera esenciales son instalados en el servidor de defensa. La lógica de operación es que si el servicio no esta instalado, este puede ser atacado. Generalmente, un conjunto limitado de aplicaciones Proxy tales como Telnet, DNS, FTP, SMTP, y autenticación de usuarios son instalados en este servidor.

El servidor de defensa podrá requerir de una autenticación adicional para que el usuario accese a los servicios Proxy. Por ejemplo, el servidor de defensa es ideal para colocar un sistema fuerte de supervisión de autorización (tal como la tecnología "una-sola vez" de contraseña donde una tarjeta inteligente generaba un código de acceso único por medios criptográficos). Adicionalmente, cada servicio Proxy podrá requerir de autorización propia después que el usuario tenga acceso a su sesión.

Cada Proxy es configurado para soportar únicamente un subconjunto de aplicaciones estándar de un conjunto de comandos. Si un comando estándar no es soportado por la aplicación Proxy, es porque simplemente no esta disponible para el usuario.

Cada Proxy esta configurado para dejar acceder únicamente a los servidores especificados en el sistema. Esto significa que existe un conjunto de características/comandos que podrán ser aplicados para un subconjunto de sistemas en la red protegida.

Cada Proxy mantiene la información detallada y auditada de todos los registros del trafico, cada conexión , y la duración de cada conexión. El registro de audición es un herramienta esencial para descubrir y finalizar el ataque de un intruso.

Cada Proxy es un programa pequeño y sencillo específicamente diseñado para la seguridad de redes. Este permite que el código fuente de la aplicación pueda revisar y analizar posibles intrusos y fugas de seguridad. Por ejemplo, una típica aplicación UNIX mail puede tener alrededor de 20,000 líneas de código cuando un correo Proxy puede contener menos de mil.

Cada Proxy es independiente de todas las demás aplicaciones Proxy en el servidor de defensa. Si se suscitara un problema con la operación de cualquier Proxy, o si se descubriera un sistema vulnerable, este puede desinstalarse sin afectar la operación de las demás aplicaciones. Aun, si la población de usuarios requiere el soporte de un nuevo servicio, el administrador de redes puede fácilmente instalar el servicio Proxy requerido en el servidor de defensa.

Un Proxy generalmente funciona sin acceso al disco lo único que hace es leer su archivo de configuración inicial . desde que la aplicación Proxy no ejecuta su acceso al disco para soporte, un intruso podrá encontrar mas dificultades para instalar caballos de Troya perjudiciales y otro tipo de archivos peligrosos en el servidor de defensa.

Cada Proxy corre como un usuario no-privilegiado en un directorio privado y seguro del servidor de defensa.

5.12.10 Sistema de seguridad por el Gateway a nivel-aplicación.

El Telnet Proxy nunca permite al usuario remoto que se registre o tenga acceso directo al servidor interno. El cliente externo ejecuta un Telnet al servidor de defensa donde es autorizado por la tecnología "una-sola vez" de contraseña. Después de ser autentificado, el cliente obtiene acceso a la interfase de usuario del Telnet Proxy. Este únicamente permite un subconjunto de comandos Telnet y además determina cual de los servidores son disponibles para el acceso vía Telnet.

Outside-Client > telnet servidor_defensa
Username: Larry Emd
Challenge Number "237936"
Challenge Response: 723456
Trying 200.43.67.17 ...

HostOS UNIX (servidor_defensa)
bh-telnet-proxy> help
Valid commands are:

connect hostname
help/?
Quit/exit
bh-telnet-proxy> connect servidor_interno
HostOS UNIX (servidor_interno)

login: Larry Emd
Password: ######
Last login: Wendnesday June 15 11:17:15
Welcome

Servidor_Interno >_0

Los usuarios externos especifican el servidor de destino y el Telnet Proxy una vez hecha la conexión, los comandos internos son desplazados hacia el cliente externo. El cliente externo cree que el Telnet Proxy es el servidor interno real, mientras el servidor interno cree que el Telnet Proxy es un cliente externo.

Se presenta la salida en pantalla de la terminal de un cliente externo como la "conexión" a el servidor interno una vez establecida. Nótese que el cliente no se esta registrando al servidor de defensa - el usuario comienza su sesión autentificándose por el servidor de defensa e intercambia respuestas, una vez que se le ha permitido seccionar se comunica con el Telnet Proxy -. Después de pasar el intercambio de respuestas, el servidor Proxy limita un conjunto de comandos y destinos que están disponibles para los clientes externos.

La autenticación puede basarse en "algo conocido por los usuarios" (como una contraseña) o "algo que tengan" que posean físicamente (como una tarjeta electrónica) cualquiera de las dos. Ambas técnicas están sujetas a plagio, pero usando una combinación de ambos métodos se incrementa la probabilidad del uso correcto de la autenticación. En el ejemplo de Telnet, el Proxy transmite un requerimiento de registro y el usuario, con la ayuda de su tarjeta electrónica, obtendrá una respuesta de validación por un numero. Típicamente, se le entrega al usuario su tarjeta desactivada para que el introduzca un PIN y se le regresa la tarjeta, basada en parte como llave "secreta" de encriptación y con un reloj interno propio, una vez que se establece la sesión se obtiene un valor de respuesta encriptado.

5.12.11 Beneficios del gateway a nivel-aplicación

Son muchos los beneficios desplegados en un gateway a nivel-aplicación. Ellos dan a la administración de red un completo control de cada servicio desde aplicaciones Proxy limitadas por un conjunto de comandos y la determinación del servidor interno donde se puede accesar a los servicios. Aun cuando, el administrador de la red tenga el completo control acerca de que servicios que son permitidos desde la carencia de un servicio Proxy para uno en particular significa que el servicio esta completamente bloqueado.

Los gateways a nivel-aplicación tienen la habilidad de soportar autenticaciones forzando al usuario para proveer información detallada de registro. Finalmente, las reglas de filtrado para un gateway de este tipo son mucho mas fáciles de configurar y probar que en un ruteador filtra-paquetes.

5.12.12 Limitaciones del gateway a nivel-aplicación

Probablemente una de las grandes limitaciones de un gateway a nivel-aplicación es que requiere de modificar la conducta del usuario o requiere de la instalación de software especializado en cada sistema que accese a los servicios Proxy. Por ejemplo, el acceso de Telnet vía gateway a nivel-aplicación demanda modificar la conducta del usuario desde el momento en que se requiere de dos pasos para hacer una conexión mejor que un paso. Como siempre, el software especializado podrá ser instalado en un sistema terminado para hacer las aplicaciones del gateway transparentes al permitir a los usuarios especificar el servidor de destino, mejor que el propio, en un comando de Telnet.

5.12.13 Gateway a nivel-circuito

Un Gateway a nivel-circuito es en si una función que puede ser perfeccionada en un Gateway a nivel-aplicación. A nivel-circuito simplemente trasmite las conexiones TCP sin cumplir cualquier proceso adicional en filtrado de paquetes.

5.12.14 La operación de una conexión típica Telnet a través de un Gateway a Nivel-circuito.

Tal como se menciono anteriormente, este gateway simplemente trasmite la conexión a través del firewall sin examinarlo adicionalmente, filtrarlo, o dirigiendo el protocolo de Telnet. El gateway a nivel-circuito acciona como una cable copiando los bytes antes y después entre la conexión interna y la conexión externa. De cualquier modo, la conexión del sistema externo actúa como si fuera originada por el sistema de firewall tratando de beneficiar el encubrir la información sobre la protección de la red.

El Gateway a nivel-circuito se usa frecuentemente para las conexiones de salida donde el administrador de sistemas somete a los usuarios internos. La ventaja preponderante es que el servidor de defensa puede ser configurado como un Gateway "híbrido" soportando nivel-aplicación o servicios Proxy para conexiones de venida y funciones de nivel-circuito para conexiones de ida.

Esto hace que el sistema de firewall sea fácil de usar para los usuarios internos quienes desean tener acceso directo a los servicios de Internet mientras se proveen las funciones del firewall necesarias para proteger la organización de los ataques externos.

CAPITULO 6

REDES

CAPITULO 6

REDES

6. REDES

Cada uno de los tres siglos pasados ha estado dominado por una sola tecnología. El siglo XVIII fue la etapa de los grandes sistemas mecánicos que acompañaron a la Revolución Industrial. El siglo XIX fue la época de la máquina de vapor; Durante el siglo XX, la tecnología clave fue la recolección, procesamiento y distribución de información.

Entre otros desarrollos, hemos presenciado la instalación de redes telefónicas en todo el mundo, a la invención de la radio y la televisión, al nacimiento y crecimiento sin precedente de la industria de las computadora, así como a la puesta en orbita de los satélites de comunicación.

A medida que terminaban los últimos años del siglo pasado, se dio una rápida convergencia de estas áreas, y también las diferencias entre la captura, transporte almacenamiento y procesamiento de información están desapareciendo con rapidez en los inicios de este siglo.

Organizaciones con centenares de oficinas dispersas en una amplia área geográfica esperan tener la posibilidad de examinar en forma habitual el estado actual de todas ellas, simplemente oprimiendo una tecla. A medida que crece nuestra habilidad para recolectar procesar y distribuir información, la demanda de mas sofisticados procesamientos de información crece todavía con mayor rapidez.

La industria de computadoras demostró tener un progreso espectacular en muy corto tiempo, el viejo modelo de tener una sola computadora para satisfacer todas las necesidades de cálculo de una organización se reemplazo con rapidez por otro que considera un número grande de computadoras separadas, pero interconectadas, que efectúan el mismo trabajo. Estos sistemas, se conocen con el nombre de Redes de Computadoras. Estas nos dan a entender una serie interconectada de computadoras autónomas. Se dice que las maquinas están interconectadas, si son capaces de intercambiar información.

La conexión no necesita hacerse a través de un hilo de cobre, con el uso de láser, microondas y satélites de comunicaciones se han mejorado enormemente dichas conexiones y su uso es cada vez mas frecuente.

Al indicar que las computadoras son autónomas, excluimos los sistemas en los que una maquina pueda forzosamente arrancar, parar o controlar a otra, éstas no se consideran autónomas.

Preguntas relativas a la seguridad en general

¿Qué medidas podemos tomar para tener una red segura?

¿Cómo podemos hacer una red segura?

Asegurar una red no es un proceso simple, y no existe una receta simple para hacerlo. Sin embargo, los siguientes puntos básicos siempre nos ayudarán:

6.1 SEGURIDAD FÍSICA

El primer paso para considerar una red segura es asegurarla físicamente Tanto para evitar intrusiones como para asegurar la conectividad. El no permitir que la red crezca sin un plan, crear una infraestructura apta para llevar el cableado, atenerse completamente a los estándares propuestos por los fabricantes, el mantener la claridad y limpieza en todos los puntos importantes de nuestro cableado constituyen lo necesario para decir que tenemos cableado estructurado. El cableado estructurado nos evita negaciones de servicio, ya que es más difícil que haya pérdida de señal o interferencia eléctrica con buen cableado.

No podemos dejar de lado, claro está, el mantener un claro registro de dónde tenemos instalados puntos de red, a quién pertenecen, la direcci&oacut; en MAC (dirección física del adaptador de red) de los dispositivos que ahí conectemos, y siempre que sea posible no instalar puntos en espacios públicos, ya que para un intruso es muchas veces mucho más fácil conectarse a través de la red local que buscar el acceso remotamente.

Si tenemos una red inalámbrica es mucho más difícil asegurar físicamente nuestra red. De todos modos, utilizando las capacidades de cifrado de las redes inalámbricas, como las que menciono aquí, ubicando nuestros puntos de acceso tan al centro de nuestras instalaciones como sea posible para evitar "derramar" señal, y en general utilizando el sentido común al instalar nuestra red, podremos evitar exponernos de más.

Recuerden que una red inalámbrica puede ser muy conveniente y económica, pero si es instalada sin el cuidado necesario, puede ser nuestra mayor vulnerabilidad. Les sugiero fuertemente no instalar redes inalámbricas sin antes haber hecho un estudio en el que concluyan que las ventajas son superiores a los riesgos.

6.2 SEGURIDAD PERIMETRAL

Una vez que tenemos confianza en nuestra instalación de red, tenemos que definir perímetros de seguridad, los cuales serán divididos por uno o varios Firewalls. La configuración más simple consiste en solamente poner un firewall entre nuestra red local y nuestra salida a Internet, permitiendo únicamente la entrada y salida a las conexiones autorizadas. Sin embargo, esta configuración es muy simplista.

Para una red importante y de complejidad mediana, les recomiendo fuertemente tener delimitados cuando menos los siguientes perímetros:

Servidores de uso interno
Servidores de uso externo
Red local
Red inalámbrica

El poder controlar gradularmente el acceso entre áreas les dará una gran flexibilidad para definir las reglas de filtrado de paquetes, incrementando fuertemente la seguridad de su red. Es importante recordar que la mayor parte de ataques, tanto intencionales como no intencionales, que sufre cualquier organización tienden a venir del interior de la misma.

6.3 MONITOREAR CONSTANTEMENTE LA RED

Parte importante de la seguridad en una red consiste en monitorearla activamente. Hay muchas condiciones que pueden llevarnos a fallas, y muy fáciles de corregir -o por lo menos diagnosticar- si contamos con herramientas de monitoreo. Podemos utilizar herramientas libres como MRTG, que nos da un reporte gráfico-diario, semanal, mensual y anual- de los datos que le configuremos.

Otro aspecto importante a monitorear es los intentos de ataque que estemos recibiendo, para saber de qué protegernos, cuáles son nuestros principales riesgos, quién está intentando atacarnos, por qué medios, y qué es lo que buscan. Para ello, podemos instalar sistemas de detección de intrusos (IDSs, por sus siglas en inglés). El IDS más poderoso y popular hoy en día es libre, y se llama Snort. Hay varios proyectos que agregan capacidades a Snort, como ACID, Hogwash y Demarc.

6.4 MANTENER LAS COMPUTADORAS AL DÍA

La instalación de nuestra red puede haber sido muy segura. Podemos tener Firewalls delimitando cada área específica. Sin embargo, si no mantenemos actualizados nuestros sistemas operativos, programas y herramientas, nuestra red no podrá ser considerada segura. Es muy frecuente, en software tanto libre como propietario, que sean encontradas fallas de programación que pueden traducirse en agujeros de seguridad - un administrador de redes responsable debe mantener sus sistemas con los parches al día, para no sufrir ataques prevenibles.

6.5 PROTECCIÓN DE DATOS EN LOS MEDIOS DIGITALES

La gran expansión de los medios digitales; Internet; la telefonía móvil y la televisión interactiva en el marco de las comunicaciones han traído consigo la proliferación de negocios a través de estos medios electrónicos.

El tráfico de datos generados en las comunicaciones electrónicas aumenta diariamente poniendo en peligro la intimidad de las personas.

El respeto a los usuarios de estos negocios exige que el tráfico de datos generados en todas las comunicaciones electrónicas se vea sometido a prescripciones legales para facilitar su aplicación y desarrollo.

Así, una de las preocupaciones de cualquier usuario de la red, es asegurarse, cuando navega por Internet, que los datos que suministra -en un Chat, en foros de discusión, o en compras- no serán capturados, copiados, modificados o utilizados sin su previo consentimiento.
Por ello entiendo que la confianza del usuario en la preservación de su intimidad en la sociedad digital, es básica para el desarrollo de la sociedad de la información y de todas las actividades lícitas que se llevan en la red.

Con el objetivo de informar sobre estos aspectos, presentamos una serie de artículos relacionados con las comunicaciones electrónicas y su impacto en la normativa de protección de datos.

Aspectos que deben tenerse en cuenta en el sitio Web de Comercio Electrónico

La mayoría de los formularios de recogida de datos que se encuentran en portales y comercios electrónicos, no incluyen ninguna de las disposiciones que la Ley prevé para garantizar el correcto y legal tratamiento de los datos del usuario.

Lo cierto es que, entre los principales problemas que existen en el tratamiento de datos en Internet, el primero y principal es la falta de información y consentimiento del usuario al tratamiento de sus datos. De hecho en el debate sobre la privacidad en la red ha trascendido a la prensa internacional tanto en Estados Unidos como en Europa. De este nivel de concienciación creciente cabe esperar también un mayor nivel de exigencia por parte de los usuarios.

La introducción de avisos legales relacionados con privacidad de los datos de los usuarios es un método sencillo y que además no presenta ninguna complicación técnica, así en el momento que se produce el acceso al sitio Web y antes de registrar los datos.

6.6 LAS CLÁUSULAS DE INFORMACIÓN

El tratamiento de datos se produce, especialmente, durante "el contacto inicial" entre el usuario de Internet y un sitio Web, ya sea únicamente para buscar información o bien para concluir una transacción comercial.

Por ello la información que seguidamente detallaremos debe mostrarse directamente en la pantalla antes de que se produzca la captación de los datos, garantizando así el correcto tratamiento de los datos.

Los diferentes formularios Web de recogida de datos de carácter personal deben contener la información y los aspectos, relativos al consentimiento e información del usuario cuyos datos van a ser tratados.

En este sentido, debe existir en la Web un aviso fácilmente localizable y de comprensión asequible que contenga la información siguiente:

I. Identificación de la compañía.
II. Una dirección de e-mail, postal u otro sistema de comunicación, a través de los cuales se puedan ejercer los derechos de acceso, cancelación, oposición y de especificación de las finalidades para las que autoriza el uso de sus datos.
III. Caso de que se produzca captación de datos, este extremo deberá manifestarse en el aviso.
IV. Las consideraciones establecidas en el apartado III) se harán extensivas a la colocación de Cookies.
V. De la finalidad o finalidades a que se destina la información obtenida.
VI. En su caso, de la intención de ceder los datos, especificando la información que se cede así como la finalidad a la que se destinarán los datos cedidos.

Asimismo, en la página inicial del sitio y en todos los lugares donde se recojan datos en línea deberá poderse acceder directamente a información completa sobre la política de protección de privacidad del sitio (incluida la forma que tienen los usuarios afectados de ejercer sus derechos de acceso, rectificación, cancelación y oposición).

6.7 RESPECTO A LA COLOCACIÓN DE COOKIES.

Las Cookies pueden contener datos personales o cualquier otro tipo de información relacionada con el interfase usuario-servidor. La normativa en materia de protección de datos define los datos personales como "cualquier información concerniente a personas físicas identificadas o identificables". Por ello, si el contenido de la cookie que contiene la Web asocia los datos con el usuario, su contenido puede ser considerado dato personal.

Caso de que no pueda producirse dicha asociación el contenido de la cookie no podrá ser considerado como dato personal, ya que no podrá ser asociado a una persona identificada o identificable.

6.8 RESPECTO A LA FINALIDAD DE LOS DATOS RECOGIDOS.

Cada usuario debe, en cualquier momento, poder determinar la finalidad o finalidades a que consiente sean destinados sus datos, o excluir alguna finalidad inicialmente consentida.

En ningún caso, la compañía podrá utilizar la información para finalidades distintas de las que haya consentido el usuario, salvo que, previamente, le haya advertido de la intención de hacerlo otorgándole un plazo y procedimiento razonable de oposición.

A este respecto, es útil el redactar finalidades concretas pero amplias, para poder utilizar dichos datos en la forma en que la empresa lo precise.

6.9 RESPECTO A LAS CESIONES Y LA FINALIDAD DE LA CESIÓN.

La información relativa a la posible cesión de datos deberá siempre identificar a los cesionarios o, en todo caso, hacer referencia a las características de las empresas o personas a quienes vayan a cederse, así como a las finalidades perseguidas por la cesión.

Caso que la información que se solicite se considere dato de carácter personal, debe de contemplarse todos los aspectos que se han comentado.

En este sentido, recomendamos se incluya un aviso en la página de registro antes de que se pueda dar el "click" de aceptar. Entendemos, asimismo, que resulta conveniente que el acceso a dicha página desde cualquier parte de la Web se realice mediante un enlace (hiperenlace).

6.10 SÍNTOMAS PARA DETECTAR UN VIRUS

A veces los mejores antivirus no son capaces de detectar todos los virus, ya que se estima que cada día nacen o se crean al menos 10 nuevos virus. Si nuestra vacuna falla podemos sin embargo percibir ciertos cambios en nuestras computadoras como los que siguen:

1. Aparecen o desaparecen archivos. Esto se nota porque a veces se pierde el fichero EXE de un programa.
2. El disco duro trabaja más de lo habitual. Esto se ve desde el indicador led del disco duro, que parpadea cuando estamos inactivos.
3. Aparecen en la pantalla mensajes extraños o de aviso, que nada tienen que ver con los habituales mensajes de Windows.
4. Desaparece espacio en el disco duro sin cargar en él nuevos datos. Por ello debemos tener controlada la capacidad de nuestro disco.
5. No se puede acceder al disco duro. Esto ya es un problema grave.
6. Pueden modificarse algunos nombres de ficheros. Por ello, se deben chequear de vez en cuando los ficheros más habituales.

6.11 OBJETIVOS DE LAS REDES

Las redes en general, consisten en "compartir recursos", y uno de sus objetivos es hacer que todos los programas, datos y equipos estén disponibles para cualquier usuario de la red que así lo solicite, sin importar la localización física del recurso y del usuario.

En otras palabras, el hecho de que el usuario se encuentre a miles de kilómetros de distancia de los datos, no debe evitar que éste los pueda utilizar como si fueran originados localmente.

Un segundo objetivo consiste en proporcionar una alta fiabilidad, al contar con fuentes alternativas de suministro. La presencia de múltiples CPU´s significa que si una de ellas deja de funcionar, las otras pueden ser capaces de encargarse de su trabajo, aunque el rendimiento global sea menor.

Otro objetivo es el ahorro económico. Las computadoras pequeñas tienen una mejor relación costo / rendimiento, comparada con la ofrecida por las máquinas grandes. Estas son, a grandes rasgos, diez veces más rápidas que el más rápido de los microprocesadores, pero su costo es miles de veces mayor.

Este desequilibrio ha ocasionado que muchos diseñadores construyan sistemas constituidos por poderosos ordenadores personales, uno por usuario y con los datos guardados en una o más máquinas que funcionan como servidor de archivo compartido.

Este objetivo conduce al concepto de redes con varias computadoras en el mismo edificio. A este tipo de red se le denomina LAN, en contraste con lo extenso de una WAN.

Un punto muy relacionado es la capacidad para aumentar el rendimiento del sistema en forma gradual a medida que crece la carga, simplemente añadiendo mas procesadores.

Otro objetivo del establecimiento de una red, es que puede proporcionar un poderoso medio de comunicación entre personas que se encuentran muy alejadas entre sí.

Una forma que muestra el amplio potencial del uso de redes como medio de comunicación es Internet y el uso del correo electrónico (e-mail), que se envía a una persona situada en cualquier parte del mundo que disfrute de este servicio.

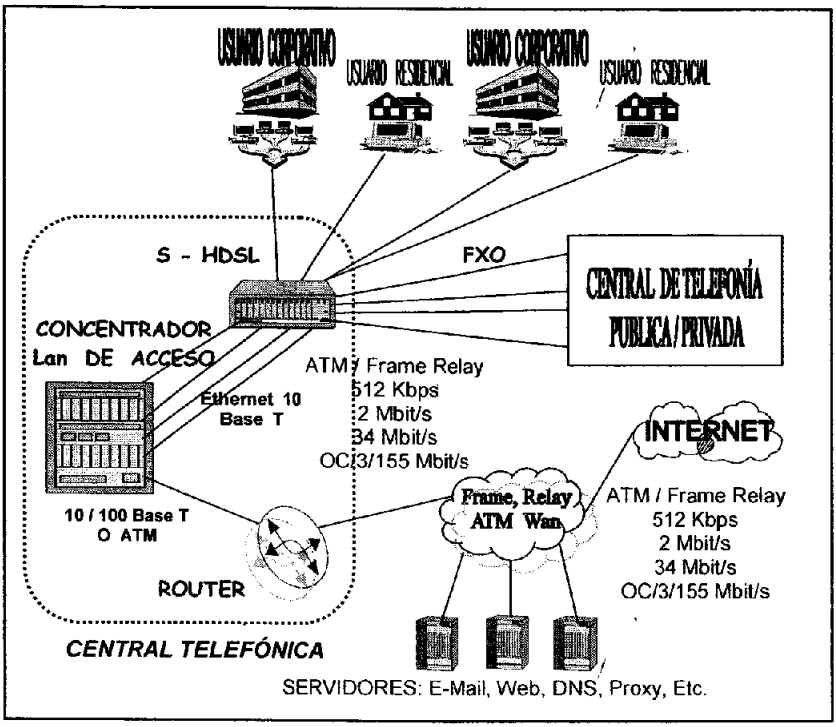


FIG. 17 ESQUEMA DE COMUNICACIÓN

6.12 ESTRUCTURAS

Definir el concepto de redes implica diferenciar entre el concepto de redes físicas y redes de comunicación.

Respecto a la estructura física, los modos de conexión y los flujos de datos, etc.; una Red la constituyen dos o más computadoras que comparten determinados recursos, sea hardware (impresoras, sistemas de almacenamiento, etc.) o software (aplicaciones, archivos, datos, etc.).

Desde una perspectiva más comunicativa y que expresa mejor lo que puede hacerse con las redes, podemos decir que existe una red cuando están involucrados un componente humano que comunica, un componente tecnológico (computadoras, telecomunicaciones) y un componente administrativo (institución que mantiene los servicios). Así, a una Red más que varias computadoras conectadas, la constituyen personas que solicitan, proporcionan e intercambian experiencias e informaciones a través de sistemas de comunicación.

Las redes deberían ser lo más transparentes posibles, de tal forma que el usuario final no requiera tener conocimiento de la tecnología (equipos y programas) utilizada para la comunicación.

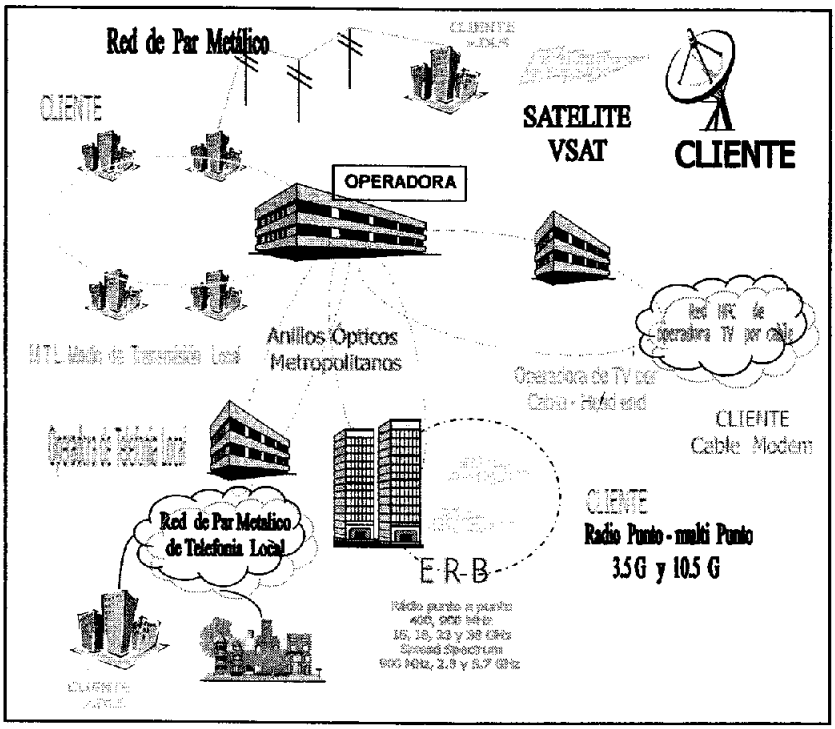


FIG. 18 EJEMPLO DE INTERCONEXIONES

6.13 TECNOLOGÍAS DE TRANSMISIÓN

Al crear una red, se toman en cuenta dos factores principales: el medio físico de transmisión y las reglas que rigen la transmisión de datos. El primer factor se llama nivel físico y el segundo protocolo.

En el nivel físico generalmente encontramos señales de voltaje que tienen un significado preconcebido. Estas señales se agrupan e interpretan para formar entidades llamadas paquetes de datos. La forma de acceder a estos paquetes la determina la tecnología de transmisión, aceptándose dos tipos:

1. Las redes de tipo Broadcast se caracterizan porque todos los miembros (nodos) pueden acceder a todos los paquetes que circulan por el medio de transmisión.

2. Las redes Point To Point sólo permiten que un nodo se conecte a otro en un momento dado.

6.14 MODELO CLIENTE / SERVIDOR

En vez de construir sistemas informáticos como elementos monolíticos, existe el acuerdo general de construirlos como sistemas Cliente / Servidor. El Cliente (un usuario de PC) solicita un servicio (por ejemplo imprimir) que un Servidor (un procesador conectado a la LAN) le proporciona. Este enfoque común de la estructura de los sistemas informáticos se traduce en una separación de las funciones que anteriormente formaban un todo. Los detalles de la realización van desde los planteamientos sencillos hasta la posibilidad real de manejar todas las PC's de modo uniforme.

TECNOLOGÍA DE OBJETOS

Otro de los enfoques para la construcción de los sistemas parte de la hipótesis de que deberían estar compuestos por elementos perfectamente definidos, objetos cerrados y materializados haciendo de ellos agentes independientes. La adopción de los objetos como medios para la construcción de sistemas informáticos ha colaborado a la posibilidad de intercambiar los diferentes elementos.

6.15 SISTEMAS ABIERTOS

Esta definición alude a sistemas informáticos cuya arquitectura permite una interconexión y una distribución fácil. En la práctica, el concepto de sistema abierto se traduce en desvincular todos los componentes de un sistema y utilizar estructuras análogas en todos los demás. Esto conlleva una mezcla de normas (que indican a los fabricantes lo que deberían hacer) y de asociaciones (grupos de entidades afines que les ayudan a realizarlo).

El efecto final es que sean capaces de "hablar" entre sí.

El objetivo último de todo el esfuerzo invertido en los sistemas abiertos consiste en que cualquiera pueda adquirir computadoras de diferentes fabricantes, las coloque donde quiera, utilice conexiones de banda ancha para enlazarlas entre sí y las haga funcionar como una máquina compuesta, capaz de sacar provecho de las conexiones de alta velocidad.

Parece lógico suponer que las computadoras podrán trabajar en conjunto cuando dispongan de una conexión entre ellas. Pero ¿Cómo conseguir, sin embargo, que computadoras de diferentes fabricantes en distintos países funcionen en común a través de todo el mundo?.

Hasta hace poco, un equipo podía comunicarse con otro de su misma "familia", pero tenía grandes dificultades para hacerlo con un "extraño".

6.16 EL MODELO OSI

El modelo conceptual OSI (Open System Interconection) es utilizado por, prácticamente, la totalidad de las redes del mundo. Este modelo fue creado por el ISO (International Standard Organization), y consiste en siete niveles o capas donde cada una de ellas define las funciones que deben proporcionar los protocolos con el propósito de intercambiar información entre varios sistemas.

Esta clasificación permite que cada protocolo fuera desarrollado con una finalidad determinada, lo cual simplifica el proceso de implementación. Cada nivel depende de los que están por debajo de él, y a su vez proporciona alguna funçionalidad a los niveles superiores.

Los siete niveles del modelo OSI son los siguientes:

1. Capa Física: esta capa tiene que ver con el envío de bits en un medio físico de transmisión y asegura que si de un extremo del medio se envía un 1 (carga eléctrica) del otro lado se reciba ese 1. Brinda los medios eléctricos, mecánicos, de procedimiento y funcionales para activar y mantener el enlace físico entre los sistemas.

Capa de Enlace: en esta capa se toman los bits que entrega la Capa Física y se agrupan para formar marcos de bits (Frames). Se realiza un chequeo de errores sobre cada frame. Si un marco se pierde o se daña en el medio físico este capa se encarga de retransmitirlo, aunque en ocasiones dicha operación provoca que un mismo marco se duplique en el destino. Dado el caso es obligación detectar tal anomalía y corregirla. También en esta capa se decide cómo acceder al medio físico.

2. Capa de Red: se encarga de controlar la operación de la subred (medios físicos y dispositivos de enrutado). Una tarea primordial es decidir cómo hacer que los paquetes lleguen a su destino desde su origen en el formato predefinido por un protocolo.

Otra función importante en este nivel es la resolución de los cuellos de botella. En estos casos se pueden tener varias rutas para dar salida a los' paquetes y en base a algunos parámetros de eficiencia o disponibilidad se eligen rutas dinámicas de salida.
A los efectos de la obtención de estadísticas, se registran el tipo y cantidad de paquetes que circulan.

3. Capa de Transporte: El objetivo de esta capa es el de tomar datos de la capa de Sesión y asegurarse que dichos datos llegan a su destino. En ocasiones los datos que viene de la capa de sesión exceden el tamaño de transmisión (MTU Maximum Transmisión Unit) de la interfaz de la red, por lo cual es necesario particionarlos y enviarlos en unidades mas pequeñas, lo cual da origen a la fragmentación y ensamblado de paquetes cuyo control, se realiza en esta capa.

La ultima labor importante de la capa de Transporte es ofrecer un mecanismo de nombrado que sirva para identificar y diferenciar las múltiples conexiones existentes,

así como determinar en que momento se inicial y terminan las "conversaciones"; es decir, en esta capa hay un mecanismo de control de flujo.
Por ejemplo: Si el usuario "a" en el nodo (A) quiere iniciar una sesión de trabajo remoto en un nodo (B), existirá una conexión que debe ser diferenciada de la conexión que el usuario "b" necesita para transferir un archivo del nodo (B) al nodo (A).

4. Capa de Sesión: Esta ofrece el servicio de establecer sesiones de trabajo entre nodos diferentes de una red, sincroniza y establece puntos de chequeo. Por ejemplo, si se hace necesario transferir un archivo muy grande entre dos nodos que tienen una alta probabilidad de sufrir una caída, es lógico pensar que una transmisión ordinaria nunca terminaría porque algún interlocutor perderá la conexión. La solución es que se establezcan puntos de chequeo cada pocos minutos, de manera que, si la conexión se rompe, mas tarde se pueda reiniciar a partir del punto de chequeo, lo cual ahorra tiempo y permite la finalización de la transferencia.

5. Capa de Presentación: Esta provee las facilidades para transferir datos con la sintaxis propia de las aplicaciones o el nodo. En esta capa es posible convertir los datos a un formato independiente de los nodos que interviene en la transmisión.

6. Capa de Aplicación: En esta capa se encuentran las aplicaciones de red que permiten explotar los recursos de otros nodos. Dicha explotación se hace, por ejemplo, a través de una emulación de una terminal que trabaja en un nodo remoto, interpretando una gran variedad de secuencias de caracteres de control que permiten desplegar en la terminal local los resultados, aun cuando estos sean gráfico. Otra forma de explotación se da cuando se transmite desde una computadora origen que almacena sus archivos en un formato distinto al del destino. Es posible que el programa de transferencia realice las conversiones necesarias de manera que el archivo pueda usarse inmediatamente bajo alguna aplicación.

6.16.1 Transmisión de Datos en el Modelo OSI

Un envío de datos típico bajo el modelo de referencia OSI comienza con una aplicación en un nodo cualquiera de la red. Esta Aplicación genera los datos que quiere enviar a su contraparte en otro nodo.

1. La Capa de Aplicación toma los datos y los encapsula añadiendo un encabezado que puede contener información de control o estar vacío. Envía el paquete resultante a la Capa de Presentación.

2. La Capa de Presentación recibe el paquete y no intenta decodificarlo o separar sus componentes, sino que lo toma como datos y le añade un encabezado con información de control de esta capa.

3. Las Capa de Sesión y de Transporte reciben el paquete, que también son sólo datos para ellas y le añaden un encabezado de control. El resultado es enviado a la capa inferior.

4. La Capa de Red se encarga de enrutar el paquete a su destino.

5. Las Capas de Red, Enlace de datos y Física toman, respectivamente, el paquete que les envía la capa superior y añaden a éste un encabezado definido por el protocolo que corresponde a cada capa y pasan el resultado a la capa inferior.

6. La Capa Física, por último, traducirá el último paquete a las señales apropiadas para que viajen por el medio físico hasta el nodo destino.

7. En el nodo destino comienza el camino inverso; es decir que cada capa quita su encabezado de control y envía el paquete a la capa superior hasta llegar a la de Aplicación en el nodo destino.

Como puede apreciarse, todas las capas, excepto la de Aplicación, procesan los paquetes realizando operaciones que sirven para verificar que el paquete de datos real esté íntegro, o para que éste llegue a su destino sin que los datos sufran alguna alteración.

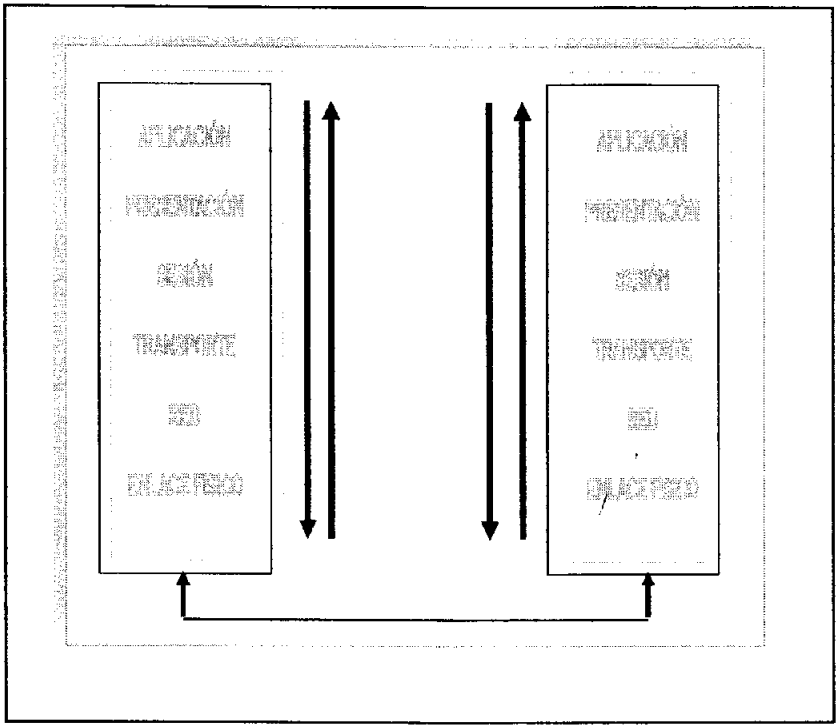


FIG. 19 ESQUEMA DE TRANSMISIÓN DE DATOS

6.17 PROTOCOLOS DE RED

En las redes, las computadoras deben comunicarse entre si e intercambiar datos con sistemas operativos y hardware muy diferentes.

En el nivel físico, esto se realiza a través de placas de redes, y una conexión entre las mismas. Lógicamente se debe establecer una comunicación "del mismo lenguaje" entre distintos sistemas operativos y placas, este lenguaje es lo que se llama protocolo.

Algunos protocolos se encargan de transportar datos, mientras que otros se encargan de la comunicación entre computadoras, y otros de convertir correctamente los datos.

Así **Protocolo** es el conjunto de normas (lenguaje de reglas y símbolos) que rige cada tipo de comunicación entre dos computadoras (intercambio de información).

Actualmente existen protocolos para cualquier tipo de comunicación que nos imaginemos; muchos de ellos han caído en desuso y otros se encuentran en su plenitud de utilización. Esto es el producto de una sociedad cada vez mas intercomunicada y relacionada, en donde lo importante es que la información llegue a su destino si, pero también lo es que llegue en las mismas condiciones en que ha sido enviada y en el tiempo previsto.

Algunos de los protocolos mas conocidos y difundidos ampliamente son:

6.17.1 NETBIOS – NETBEUI – NWLINK – WINS

Network Basic Input Output System, es el protocolo mas sencillo. Esta compuesto por menos de 20 comandos que se ocupan del intercambio de datos. Se ha perfeccionado y ampliado recibiendo el nuevo nombre de NETBEUI (NETBIOS Extended User Interface) pero continua utilizando el juego de comandos del NETBIOS y luego para hacerlo compatible con otros protocolos (como IPX – SPX) se amplio nuevamente recibiendo el nombre de NWLINK (NetWare Link).

NETBIOS toma el puerto 137 – 139 en computadoras que utilizan el sistema operativo WINDOWS, esta considerado el protocolo mas fácilmente vulnerable de los existentes, al punto de que cualquier especialista de seguridad recomienda no utilizarlo.

6.17.2 TCP / IP

En los años 80s. Una gran cantidad de instituciones estaban interesadas en conectarse a una gran red que se expandía por todo EE. UU. (ahora Internet). Para esto definieron un conjunto de reglas que establecen como conectar computadoras entre si para lograr el intercambio de información.

Basado en las capas del modelo OSI, se definió un conjunto de protocolos de TCP / IP, que consta de 4 capas principales y que se han convertido en un estándar a nivel mundial.

6.17.3 LAS CAPAS DEL MODELO TCP / IP

El Transmission Communication Protocol/Internet Protocol es actualmente el protocolo más ampliamente utilizado por su independencia del Sistema Operativo y hardware utilizado. Es un eficaz protocolo orientado por paquetes; es particularmente adecuado como plataforma para protocolos de los más distintos servicios y aplicaciones que se pueden conseguir a través de la red.

TCP/IP no es un único protocolo, sino que en realidad lo que se conoce con este nombre es un conjunto de protocolos que cubren los distintos niveles del modelo OSI.

Los dos protocolos más importantes son el TCP (Transmission Control Protocol) y el IP (Internet Protocol), que son los que dan nombre al conjunto. Se diferencian cuatro capas en las que se agrupan los protocolos, y que se relacionan con los niveles OSI.

Aplicación: Se corresponde con los niveles OSI de Aplicación, Presentación y Sesión.

Aquí se incluyen protocolos destinados a proporcionar servicios, tales como correo electrónico (SMTP), transferencia de archivos (FTP), conexión remota (Telnet) y otros más recientes como el protocolo HTTP (Hypertext Transfer Protocol).

Transporte: Coincide con el nivel de Transporte del modelo OSI. Esta capa está implantada por dos protocolos: el Transmission Control Protocol (TCP) y el User Datagram Protocol (UDP). El primero es un protocolo confiable (reliable) y orientado a conexiones, lo cual significa que ofrece un medio libre de errores para enviar paquetes. El segundo es un protocolo no orientado a conexiones (connectionless) y no es confiable (unreliable). El TCP se prefiere para la transmisión de datos a nivel red de área amplia y el UDP para redes de área local.

Internet: Es el nivel de Red del modelo OSI. Incluye al protocolo IP, que se encarga de enviar los paquetes de información a sus destinos correspondientes. Es utilizado con esta finalidad por los protocolos del nivel de transporte.

Interfaz de red: correspondiente al nivel de Enlace y Físico de la pila OSI. Los protocolos que pertenecen a este nivel son los encargados de la transmisión a través del medio físico al que se encuentra conectado cada Host, como puede ser una línea punto a punto o una red Ethernet.

La capa inferior, que podemos nombrar como Física respecto al modelo OSI, contiene varios estándares (conocidos con el nombre del IEEE 802.X) que establecen las reglas para enviar datos por cable coaxial delgado (10Base2), cable coaxial grueso (10Base5), par trenzado (10BaseT), fibra óptica (10BaseF) y su propio método de acceso.

El TCP/IP necesita funcionar sobre algún tipo de red o de medio físico que proporcione sus propios protocolos para el nivel de enlace de Internet. Por este motivo hay que tener en cuenta que los protocolos utilizados en este nivel pueden ser muy diversos y no forman parte del conjunto TCP/IP. Sin embargo, esto no debe ser problemático puesto que una de las funciones y ventajas principales del TCP/IP es proporcionar una abstracción del medio; de forma que sea posible intercambiar información entre medios diferentes y tecnologías que inicialmente son incompatibles.

Para transmitir información a través de TCP/IP, ésta debe ser dividida en unidades de menor tamaño. Esto proporciona grandes ventajas en el manejo de los datos que se transfieren.

En TCP/IP cada una de estas unidades de información recibe el nombre de "Datagrama" (datagram), y son conjuntos de datos que se envían como mensajes independientes.

6.17.4 FUNCIONAMIENTO

Las aplicaciones de red presentan los datos a TCP. Este divide los datos en trozos (paquetes), y le otorga a cada uno un número. El conjunto de paquetes ordenados pueden representar imágenes, documentos, videos, o cualquier otra información que el usuario desee enviar.

Luego, TCP presenta los datos a IP, quien agrega su información de control (como ser dirección de origen y destino). Si por algún motivo IP no puede entregar algún paquete, TCP pedirá el reenvió de los faltantes. Por último TCP se encarga de reensamblar los paquetes en el orden correcto, basándose en los números asignados previamente.

6.17.5 COMPARACIÓN CON EL MODELO OSI

Si bien TCP/IP está basado en OSI, este último no tuvo éxito debido a causas como el momento de su introducción, la tecnología existente en ese momento, malas implementaciones y políticas por parte de los investigadores. Sin embargo OSI es un buen modelo y TCP/IP es un buen conjunto de protocolos y la combinación de ambos es la que permite contar con las comunicaciones que se tienen hoy.

El modelo TCP/IP no tiene bien divididas las Capas de Enlace de Datos, Presentación y Sesión y la experiencia ha demostrado que en la mayoría de los casos son de poca utilidad.

Los estándares 802.X junto con el protocolo IP realizan todas las funciones propuestas en el modelo OSI hasta la Capa de Red. Los protocolos TCP y UDP cumplen con la Capa de Transporte. Finalmente, las aplicaciones ya mencionadas son ejemplos prácticos y reales de la funcionalidad de la Capa de Aplicación.

6.18 NIVEL FÍSICO DEL MODELO TCP / IP "ARP" Y "RARP"

El Address Resolution Protocol no se dedica al transporte de datos sino a convertir las direcciones IP en direcciones de la red física.

El protocolo consigue la dirección mediante la difusión de un paquete de petición ARP que contiene la dirección IP del sistema destinatario. Todos los ordenadores de la red detectan estas difusiones y aquel que contenga la dirección IP solicitada, la transmitirá al sistema solicitante mediante una respuesta de paquete ARP. Luego el solicitante almacena estas direcciones en una tabla para su uso posterior; y esta tabla además servirá de referencia a otros equipos para evitar la búsqueda de las mimas direcciones.

El Reverse Address Resolution Protocol realiza el trabajo inverso de ARP. Es decir que obtiene la dirección IP a partir de una dirección física.

6.19 NIVEL DE DATOS DEL MODELO TCP / IP "SLIP"

El Serial Link Internet Protocol/Point to Point Protocol brinda una conexión de velocidad aceptable, con al posibilidad de admitir varias conexiones simultaneas con un mismo MODEM. El mecanismo es sencillo: se llama al proveedor, quien oficia de puente entre su computadora y el resto de la red, y una vez establecida la comunicación se tiene acceso total a los servicios.
Es un protocolo sencillo y pequeño, pensando en su fácil implementación; y en la baja velocidad de los enlaces telefónicos, por lo que ha caído en desuso.

Este protocolo apoya solamente IP, no provee detección de errores ni de autenticación y tienen la desventaja de que existen muchas implementaciones incompatibles entre ellas.

6.19.1 PPP

El Point to Point Protocol fue desarrollado por el IETF (Internet Engineering Task Force) en 1993 para mejorar algunas deficiencias de SLIP, y crear un estándar internacional.

PPP es un protocolo mucho más amplio, más potente y adaptable. Proporciona un método de enlace bidireccional full dúplex para transportar datagramas multiprotocolo sobre enlaces simples (conexión directa) de un equipo a otro (punto a punto), en cualquier situación sin importar el tipo de conexión, el hardware ni el sistema operativo.

Sus principales características son:

1. Es transparente a las capas superiores.

2. Transmite protocolos IP, IPX, Apple Talk, etc.

3. Es ampliable ya que no fue pensando para solucionar un problema en concreto.

PPP esta dividido en dos subprotocolos:

1. LCP (Link Control Protocol): es el encargado de comenzar una conexión (fase abierta), definir como se producirá el intercambio de datos (tamaño de los paquetes, identificación, tiempos de espera, etc.) y de finalizar la conexión (enlace muerto).

2. NCP (Network Control Protocol): se encarga de negociar y configura las opciones de los diferentes protocolos de red (IP, IPX, etc.) abriéndolos de a uno por vez. Una vez que un NCP ha alcanzado el estado abierto, PPP transportará los correspondientes paquetes. Cualquier paquete recibido mientras su NCP no esté en el estado abierto es descartado.

6.20 NIVEL DE RED DEL MODELO TCP / IP "IPXSPX"

El Internetwork Packet Exchange Sequenced Packet Exchange es el protocolo de nivel de red propietario de NetWare (para su sistema operativo Novell) siendo utilizados en las redes tipo LAN.

6.20.1 IP

El Internet Protocol define la base de todas las comunicaciones en Internet. Es utilizado por los protocolos del nivel de transporte (como TCP) para encaminar los datos hacia su destino. IP tiene únicamente la misión de encaminar el datagrama, sin comprobar la integridad de la información que contiene. Para ello se utiliza una nueva cabecera que se antepone al datagrama que se está tratando.

La cabecera IP tiene un tamaño de 160 bits y está formada por varios campos de distinto significado entre los que se destaca el tipo de protocolo de transporte del datagrama, el número de paquete (para su posterior ensamble), la dirección de origen y la de destino, etc.

Es de notar que este protocolo no garantiza la llegada de los paquetes a destino (conexión sin garantía), ni su orden; tan solo garantiza la integridad del encabezado IP. La fiabilidad de los datos deben garantizarla los niveles superiores. También, se trata de una transmisión sin conexión porque cuando se envía el paquete, no se avisa al receptor para que esté preparado (no existe una conexión directa emisor-receptor). De hecho, muchas veces se mandan paquetes a un destino inexistente o que no se encuentra disponible.

El protocolo IP identifica a cada equipo que se encuentre conectado a la red mediante su correspondiente dirección. Esta dirección es un número de 32 bits que debe ser único para cada Host, y normalmente suele representarse como cuatro cifras de 8 bits separadas por puntos (por ejemplo: 205.025.076.223)

En el nivel IP se definen los siguientes aspectos de intercambio de información:

1. Un mecanismo de direcciones que permite identificar de manera univoca al emisor y al receptor, sin considerar las ubicaciones ni las arquitecturas de las redes a las cuales pertenece cada uno. Este mecanismo permite la universalidad de la red.

2. Un concepto relativo al transporte de los paquetes de datos, para que el mismo llegue al receptor a través de los nodos de las redes involucradas. Dentro de cada red tendrá que haber al menos un receptor (Router) que esté conectado con otra computadora en otra red en el exterior. Los routers reconocen un paquete y comprueban que no sea para alguna maquina conectada a su red y entonces lo mandan a otra, más cercana al destino. Esto se hace sucesivas veces hasta que el paquete llega al router de la red donde se encuentra la computadora destinataria del mensaje.

3. Un formato para los paquetes (cabecera). Con esta, el Router podrá identificar al destinatario del mensaje, ya que como se explico, uno de los datos de la cabecera es el nombre de destino del mensaje.

La dirección IP se utiliza para identificar tanto a la computadora en concreto como la red a la que pertenece, de manera que sea posible distinguir a los ordenadores que se encuentran conectados a una misma red. Con este propósito, y teniendo en cuenta que en Internet se encuentran conectadas redes de tamaños muy diversos, se establecieron cuatro clases diferentes de direcciones, las cuales se representan mediante tres rangos de valores:

1. Clase A: son las que en su primer byte tienen un valor comprendido entre 1 y 126, incluyendo ambos valores. Estas direcciones utilizan únicamente este primer byte para identificar la red, quedando los otros tres bytes disponibles para cada uno de las computadoras (Hosts) que pertenezcan a esta misma red. Esto significa que podrán existir más de dieciséis millones de Hosts en cada una de las 126 redes de esta clase. Este tipo de direcciones es usado por redes muy extensas.

2. Clase B: estas direcciones utilizan en su primer byte un valor comprendido entre 128 y 191, incluyendo ambos. En este caso el identificador de la red se obtiene de los dos primeros bytes de la dirección, debiendo ser un valor entre 128.001 y 191.254 (no es posible utilizar los valores 0 y 255 por tener un significado especial). Los dos últimos bytes de la dirección constituyen el identificador de la computadora permitiendo, por consiguiente, un número máximo de 64.516 ordenadores en la misma red. Este tipo de direcciones tendría que ser suficiente para la gran mayoría de las organizaciones grandes.

3. Clase C: en este caso el valor del primer byte tendrá que estar comprendido entre 192 y 223, incluyendo ambos valores. Este tercer tipo de direcciones utiliza los tres primeros bytes para el número de la red, con un rango desde 192.001.001 hasta 223.254.254. De esta manera queda libre un byte para el Host, lo que permite que se conecten un máximo de 254 computadoras en cada red.

4. Clase D: esta clase se usa con fines de multidifusión a más de un dispositivo. El rango es desde 224.0.0.0 hasta 239.255.235.255.

Actualmente se utilizan las redes Clase E que comprenden el rango desde 240.0.0.0 hasta 247.255.255.255.

DNS NOMBRE DE DOMINIO

Ya que para el ser humano se hace difícil recordar direcciones IP como 209.89.67.156 se creo lo que conocemos como DNS (Domain Name Server), el cual es el encargado de convertir la dirección IP en un nombre de dominio generalmente fácil de recordar y viceversa. Así www.mipagina.com.mx, será entendida gracias al servicio de DNS como 110.56.12.106.

6.20.2 PUERTOS

Para acceder desde el nivel de red al nivel de aplicaciones no sirve simplemente indicar la dirección IP, se necesitaran mas especificaciones para que el Host de destino pueda escoger la aplicación correcta.

Estas especificaciones harán necesaria la definición de PUERTO, un puerto se representa por un valor de 16 Bits y hace la diferencia entre los posibles receptores de un mensaje.

La combinación Dirección IP + PUERTO identifican una región de memoria única denominada Socket . Al indicar este Socket, se puede trasladar el paquete a la dirección correcta (FTP, Telnet, WWW, etc.) y, si además recibe el puerto desde donde fue enviado el mensaje, se podrá suministrar una respuesta.

Actualmente existen miles de puertos ocupados de los 2^{16} = 65535 posibles, de los cuales apenas unos cuantos son los mas utilizados y se encuentran divididos en tres rangos:

- Desde el puerto 0 hasta el 1023: son los puertos conocidos y usados por aplicaciones de servidor.
- Desde el 1024 hasta el 49151: son los registrados y asignados dinámicamente.
- Desde el 49152 hasta el 65535: son los puertos privados.

APPLE TALK

Este protocolo (de nivel de red) está incluido en el Sistema Operativo de Apple Macintosh desde su aparición, permite interconectar computadoras y periféricos con gran sencillez para el usuario, ya que no requiere ningún tipo de configuración por su parte.

6.21 NIVEL DE TRANSPORTE DEL MODELO TCP/IP "TCP"

El Protocolo de Control de Transmisión (TCP) nació principalmente por la necesidad de una comunicación "segura" entre el emisor y el destinatario del mensaje. Así, las aplicaciones pueden encargarse de su tarea sin preocuparse de la seguridad en la comunicación.

TCP divide el mensaje original en datagramas de menor tamaño (múltiplo de 32 bits), y por lo tanto, mucho más manejables. Los datagramas serán dirigidos a través del protocolo IP de forma individual. El protocolo TCP se encarga, además, de añadir cierta información necesaria al inicio de cada uno de los datagramas (cabecera). Luego, se ocupa de que los datos sean entregados y que los paquetes sean reensamblados correctamente asegurando así que lo que se recibe sea efectivamente lo enviado.

Si ocurriera algún error en la transmisión, TCP se encargará de reenviar los paquetes.

TCP sabrá que hubo errores o que el paquete fue entregado correctamente gracias a un paquete de respuesta (acuse de recibo) que envía el destinatario al emisor (para que vuelva a realizar el envió) en donde indica si faltan paquetes, tamaños o datos erróneos, etc.

Las principales características de este protocolo son:

1. Servicio orientado a conexión: el destino recibe exactamente la misma secuencia de bytes que envía el origen.

2. Conexión de circuito virtual: durante la transferencia, el protocolo en las dos maquinas continua comunicándose para verificar que los datos se reciban correctamente.

3. Transferencia con memoria intermedia: la aplicación utiliza paquetes del tamaño que crea adecuado, pero el software de protocolo puede dividir el flujo en subpaquetes o armar uno con un grupo de ellos, independientemente de la aplicación. Esto se realiza para hacer eficiente el tráfico en la red. Así, si la aplicación genera piezas de un byte, el protocolo puede armar datagramas razonablemente más largos antes de hacer el envío, o bien, forzar la transferencia dividiendo el paquete de la aplicación en datagramas más pequeños.

4. Flujo no estructurado: se refiere a la posibilidad de envió de información de control de estado junto a los datos propiamente dichos.

5. Conexión full duplex: permite la transferencia concurrente en ambas direcciones, sin ninguna interacción. La ventaja es evidente: el protocolo puede enviar datagramas desde el origen al receptor e información de control en sentido opuesto, reduciendo el tráfico en la red.

Los puertos proporcionan una manera de distinguir entre las distintas transferencias, ya que un mismo sistema puede estar utilizando varios servicios o transferencias simultáneamente, e incluso puede que por medio de usuarios distintos.

El Puerto de Origen (16 bits) contendrá un número cualquiera que sirva para realizar esta distinción. Además, el programa cliente que realiza la petición también debe conocer el número de puerto en el que se encuentra el servidor adecuado. Mientras que el programa del usuario utiliza números prácticamente aleatorios, el servidor deber tener asignado un número estándar para que pueda ser utilizado por el cliente.

Cuando es el servidor el que envía los datos, los números de puertos de origen y destino se intercambian.

El campo Tamaño de la Cabecera (4 bits) contiene la longitud total de la cabecera TCP expresada en el número de palabras de 32 bits que ocupa (el tamaño real divido 4). Esto permite determinar el lugar donde comienzan los Datos.

En la transmisión de datos a través del protocolo TCP la fiabilidad es un factor muy importante. Para poder detectar los errores y pérdida de información en los datagramas, es necesario que el cliente envíe de nuevo al servidor unas Señales de Confirmación (32 bits) una vez que se ha recibido y comprobado la información satisfactoriamente. Si el servidor no obtiene la señal de confirmación adecuada transcurrido un período de tiempo razonable, el datagrama completo se volverá a enviar.

Por razones de eficiencia los datagramas se envían continuamente sin esperar la confirmación, haciéndose necesaria la numeración, mediante los Números de Secuencia (32 bits), de los mismos para que puedan ser ensamblados en el orden correcto.

También puede ocurrir que la información del datagrama llegue con errores a su destino. Para poder detectarlos, cuando sucede esto, se incluye un CheckSum (16 bits), el cual contiene un valor calculado a partir de la información del datagrama completo. En el otro extremo el receptor vuelve a calcular este valor, comprobando que es el mismo que el suministrado en la cabecera.

Si el valor es distinto significará que el datagrama es incorrecto.

La forma en que TCP numera los datagramas es contando los bytes de datos que contiene cada uno de ellos y añadiendo esta información al campo correspondiente de la cabecera del datagrama siguiente.

De esta manera el primero empezará en cero; el segundo contendrá el tamaño de la parte de datos; el tercero contendrá la suma de ese número más el tamaño de los datos del segundo datagrama; y así sucesivamente. Por ejemplo, para un tamaño fijo de 500 bytes de datos en cada datagrama, la numeración sería la siguiente: 0 para el primero, 500 para el segundo, 1000 para el tercero, etc.

Existe otro factor más a tener en cuenta durante la transmisión de información, y es la potencia y velocidad con que cada computadora puede procesar los datos que le son enviados.

Si esto no se tuviera en cuenta, el equipo de mayor potencia podría enviar la información demasiado rápido al receptor, de manera que éste no pueda procesarla. Este inconveniente se soluciona mediante un campo Window (16 bits), en el cual se introduce un valor indicando la cantidad de información que el receptor está preparado para procesar en un momento dado.

El campo Opciones (32 bits) permite que una aplicación negocie durante la configuración de la conexión, características como el tamaño máximo del segmento TCP. Si este campo tiene el primer octeto a cero, indica que no hay opciones, quedando un datagrama de 160 bits.

Por último cada datagrama tendrá un Estado que le indicará al servidor el contenido, motivo y la forma en que deberá ser atendido ese paquete. Este campo puede contiene los siguientes estados (Estado = 1 Verdadero):

Bit 5 (URGent): Identifica datos urgentes.

Bit 4 (ACKnowledge): Indica que el campo de confirmación es válido.

Bit 3 (PuSH): Aunque el buffer de datos no este lleno, se fuerza el envío.

Bit 2 (ReSeT): Abortar la conexión. Todos los buffers asociados se vacían.

Bit 1 (SYnchronize sequence Number): Sincronizar los números de secuencia.

Bit 0 (FINish): Se solicita el cerrado de la conexión.

Todas estas características se traducen en un "protocolo pesado" por el envío de señales de confirmación y la velocidad se ve sacrificada en pos de la fiabilidad de los datos.

6.22 UDP

El User **D**atagram **P**rotocol puede ser la alternativa al TCP en algunos casos en los que no sea necesario el gran nivel de complejidad proporcionado por el TCP. Puesto que UDP no admite numeración de los datagramas, este protocolo se utiliza principalmente cuando el orden en que se reciben los mismos no es un factor fundamental, cuando se quiere enviar información de poco tamaño que cabe en un único datagrama o si la fiabilidad de los datos no es un factor de relieve.

Cuando se utiliza UDP la garantía de que un paquete llegue a su destino es mucho menor que con TCP debido a que no se utilizan las señales de confirmación. Por todas estas características la cabecera del UDP es bastante menor en tamaño que la de TCP. Esta simplificación resulta en una mayor eficiencia en determinadas ocasiones. Es utilizado en redes con muy buen cableado.

6.23 NIVEL DE APLICACIÓN DEL MODELO TCP/IP "ICMP" Y "FTP"

El **I**nternet **C**ontrol **M**essage **P**rotocol es de características similares al UDP, pero con un formato aún más simple. Su utilidad no está en el transporte de datos "de usuario", sino en los mensajes de error y de control necesarios para los sistemas de la red.

El **F**ile **T**ransfer **P**rotocol se incluye como parte del TCP/IP, estando destinado proporcionar el servicio de transferencia de archivos. El FTP depende del protocolo TCP para las funciones de transporte, y guarda alguna relación con Telnet (protocolo para la conexión remota).

FTP utiliza dos canales de conexión separados: uno es el canal de comandos que permanece abierto durante toda la sesión y el otro es el canal de transmisión de archivos.

El FTP permite acceder a algún servidor que disponga de este servicio y realizar tareas tales como moverse a través de su estructura de directorios, ver y descargar archivos al ordenador local, enviar o copiar archivos directamente de un servidor a otro de la red.

Lógicamente y por motivos de seguridad se hace necesario contar con el permiso previo para poder realizar todas estas operaciones. El servidor FTP pedirá el nombre de usuario y clave de acceso al iniciar la sesión (login). Este debe ser suministrado correctamente para poder utilizar el servicio.

La manera de utilizar FTP es por medio de una serie de comandos, los cuales suelen variar dependiendo del sistema en que se esté ejecutando el programa, pero básicamente con la misma funcionalidad. Existen aplicaciones de FTP para prácticamente todos los sistemas operativos.

Existe una forma muy utilizada para acceder a fuentes de archivos de carácter público por medio de FTP y es el acceso FTP Anónimo, mediante el cual se pueden copiar archivos de uso público. Generalmente el acceso anónimo tendrá algunas limitaciones en los permisos, siendo normal en estos casos que no se permita realizar acciones tales como añadir archivos o modificar los existentes.

El FTP proporciona dos modos de transferencia de archivos: ASCII y binario. El modo de transferencia ASCII se utiliza cuando se quiere transmitir archivos de texto puro. El binario se debe utilizar en cualquier otro caso (datos que no son texto plano).

6.24 HTTP

Este **HiperText Tranfer Protocol** es la base de toda comunicación desarrollada en la Web. Utilizado desde principios de lo 90 es un protocolo ASCII que se ocupa de establecer una comunicación TCP segura entre el cliente y el servidor a través del puerto 80.

HTTP es un protocolo de aplicación para sistemas de información distribuidos, e hipermediático. Es un protocolo genérico, sin estado, orientado a objetos, que se puede utilizar para muchas tareas, como servidores de nombres y sistemas de gestión de objetos distribuidos, por medio de la ampliación de sus métodos de petición o comandos.

Sus principales características son:

1. Protocolo de Aplicación: aunque generalmente se implementa sobre el TCP/IP, también es capaz de hacerlo sobre otros protocolos de capas más bajas. HTTP presupone únicamente un transporte fiable, así que puede utilizar cualquier protocolo que garantice este requisito mínimo.

2. Sistemas de información distribuidos, colaboradores, de hipermedios: HTTP soporta sistemas de información distribuidos es decir, sistemas esparcidos por múltiples servidores.

3. Genérico: HTTP no dicta el contenido de los datos que transfiere; simplemente actúa como un conducto para mover datos de aplicación, por lo que se puede transferir cualquier tipo de información por medio de HTTP.

4. Sin estado: HTTP no mantiene un estado. Cuando se solicita una transferencia a través de HTTP, se crea la conexión, se produce la transferencia y se termina la conexión. Esta es una de las debilidades de HTTP; sin información de estado, cada página Web está sola. Por ejemplo, es difícil desarrollar una aplicación basada en la Web que permita que un usuario se conecte en una página y que mantenga esta información de conexión durante todo el tiempo que el usuario esté accediendo activamente al destino. Cualquier documento transferido a través de HTTP no tiene ningún contexto y es completamente independiente de todos los documentos transferidos antes de él.

5. Orientado a objetos, escritura y negociación de la representación de los datos: HTTP no está orientado a objetos en el mismo sentido que un lenguaje de programación. Esta descripción significa simplemente que HTTP tiene etiquetas que indican el tipo de datos que se van a transferir por medio de la red, así como métodos, que son comandos que indican qué debe transferirse.

6. Sistema creado independientemente de los datos que se transfieren: Debido a que HTTP sólo mueve datos, no necesita tener información sobre cada uno de los tipos a transferir. Por ejemplo, un servidor Web no necesita un conocimiento específico sobre el funcionamiento interno del formato de un archivo de vídeo para hacer el envío.

La comunicación que se establece en una conexión HTTP es de muy corta duración. El cliente establece la conexión con el servidor HTTP y le solicita un documento determinado. El servidor recibe la consulta, la evalúa y envía el documento solicitado (si existe) o un mensaje de error en caso contrario. Luego el servidor finaliza la conexión sin que existan otros estados intermedios.

El protocolo HTTP en su estructura, divide el mensaje en encabezado (Header) y en cuerpo (Entity), separados entre sí por una línea en blanco.

6.25 SMTP

El servicio de correo electrónico se proporciona a través del protocolo Simple Mail Transfer Protocol, (empleando redes TCP/IP) y permite enviar mensajes a otros usuarios de la red. A través de estos mensajes no sólo se puede intercambiar texto, sino también archivos binarios de cualquier tipo.

Generalmente los mensajes de correo electrónico no se envían directamente a las computadoras personales de cada usuario, sino a un servidor de correo que actúa como almacén de los mensajes recibidos. Los mensajes permanecerán en este sistema hasta que el usuario los transfiera a su propio equipo para leerlos de forma local,(vía POP).

El cliente de correo envía una solicitud a su e-mail Server (al puerto 25) para enviar un mensaje (y almacenarlo en dicho servidor). El Server establece una conexión SMTP donde emisor y receptor intercambian mensajes de identificación, errores y el cuerpo del mail.

Luego de esto el emisor envía los comandos necesarios para la liberación de la conexión.

6.26 POP

El servidor POP (**P**ost **O**ffice **P**rotocol) fue diseñado para la recuperación de correo desde el e-mail Server hacia la computadora destinataria del mensaje.

Al igual que sucede con SMTP, inicialmente el proceso escucha el puerto del protocolo POP (el 110) y cuando el emisor solicita el mensaje se establece una conexión full duplex donde se intercambian los mensajes Emisor-Server para luego finalizar la conexión cuando se hallan enviado cada uno de los mails que se almacenaban en el servidor.

Actualmente el protocolo POP se encuentran en su tercera implementación por lo que generalmente se escuchará sobre POP3.

6.27 MIME

Multipurpose **I**nternet **M**ail Extensions es una extensión del protocolo SMTP y se creo con el fin de soportar algunos juegos de caracteres extendidos (no USASCII) no soportados por este último (principalmente el francés y el alemán).

MIME especifica tres campos que se incluyen en la cabecera del mensaje, para hacer la conversión adecuada al sistema no USASCII utilizado:

1. MIMEVersión: especifica la versión de MIME utilizado para codificar el mensaje.

2. ContentType: especifica el tipo y subtipo de los datos no ASCII.

3. ContenetTranferEncoding: especifica el tipo de codificación usado para traducir los datos en ASCII.

NNTP

El **N**etwork **N**ews **T**ransfer **P**rotocol fue diseñado para permitir la distribución, solicitud, recuperación y envío de noticias (News). NNTP está basado en las especificaciones de UseNet (tratado también en este capítulo) pero con algunas modificaciones en su estructura que le permiten ser adaptables a otros grupos de noticias no UseNet.

SNMP

El Simple Network Management Protocol se utiliza para monitorizar, controlar y administrar múltiples redes físicas de diferentes fabricantes, donde no existe un protocolo común en la capa de Enlace. La estructura de este protocolo se basa en utilizar la capa de aplicación para evitar el contacto con la capa de enlace y, aunque es parte de la familia TCP/IP no depende del IP ya que fue diseñado para ser independiente y puede correr igual de fácil sobre, por ejemplo, IPX de Novell.

6.28 ESTRUCTURA BÁSICA DE LA WEB

La estructura básica de la World Wide Web (WWW) consiste en que el protocolo HTTP actúa como un transporte genérico que lleva varios tipos de información del servidor al cliente. Hoy en día las conexiones a servidores Web son las más extendidas entre usuarios de Internet, hasta el punto tal de que muchas personas piensan que este servicio es el único existente, junto al IRC. Inicialmente se ideo para que unos cuantos físicos intercambiaran información entre universidades, hoy es uno de los pilares fundamentales de muchas empresas.

Cada entidad servidor se identifica de forma única con un Localizador de Recursos Universal (URL) que a su vez está relacionado unívocamente con una dirección IP.

El tipo más común de datos transportado a través de HTTP es HTML (HiperText Markup Language). Además de incluir directrices para la "compresión" de textos, también tiene directrices que proporcionan capacidades como las de enlaces de hipertexto y la carga de imágenes en línea. Los recursos hiperenlazados y los archivos de imágenes en línea están identificados con los URL intercalados dentro del documento HTML.

A pesar de que algunos servidores Web personales de gama baja sólo pueden enviar páginas estáticas, la mayoría de los servidores HTTP admiten la CGI (Common Gateway Interface). Con CGI se pueden escribir programas que se integran en la Web y que realizan tareas tales como el proceso de formularios y las búsquedas en bases de datos, las cuales HTML no puede ejecutar.

La principal limitación de CGI es que está restringida a programas en el lado del servidor. Por ejemplo, utilizando CGI, la única forma en la que se puede interactuar con los usuarios es suministrándoles formularios ha completar. Las tecnologías orientadas a objetos como Java afrontan esta limitación, permitiendo al servidor que envíe al cliente pequeños programas para ejecutarlos localmente.

6.29 SERVICIOS DE INTERNET

Como sabemos, Internet es en la actualidad, la red de computadoras más grande del mundo. Sin embargo la importancia de Internet no reside solamente en el número de máquinas interconectadas sino en los servicios que brinda.

Los servicios y recursos de Internet (Gopher, News, Archie, WWW, etc.) son accesibles de diversas formas, principalmente tres: por Telnet, por E-Mail y por un programa cliente.

A través de Telnet o E-Mail, el servicio presenta una interfase ANSI (sin gráficos), sólo con caracteres alfanuméricos. Con un programa cliente, la gestión es más sencilla, visual y agradable, como sucede en la WWW donde se presentan cada una de las páginas en formato gráfico.

6.30 TELNET

Este protocolo fue diseñado para proporcionar el servicio de conexión remota (remote login). Forma parte del conjunto de protocolos TCP/IP y depende del protocolo TCP para el nivel de transporte.

El protocolo Telnet es un emulador de terminal que permite acceder a los recursos y ejecutar los programas de un equipo remoto en la red, de la misma forma que si se tratara de una terminal real directamente conectado al sistema remoto. Una vez establecida la conexión el usuario podrá iniciar la sesión con su clave de acceso. De la misma manera que ocurre con el protocolo FTP, existen servidores que permiten un acceso libre cuando se especifica "anonymous" como nombre de usuario.

El sistema local que utiliza el usuario se convierte en una terminal "no inteligente" donde todos los caracteres pulsados y las acciones que se realicen se envían al Host remoto, el cual devuelve el resultado de su trabajo. Para facilitar un poco la tarea a los usuarios, en algunos casos se encuentran desarrollados menús con las distintas opciones que se ofrecen.

Para utilizar Telnet se ejecuta un programa especial, llamado Telnet en el cliente. Este programa utiliza TCP para conectarse a un sistema específico (su servidor) en el puerto 23 (por defecto) . Una vez que se establece la conexión, Telnet actúa como un intermediario entre el cliente y el servidor.

La mayoría de las computadoras que permiten este tipo de acceso cuentan con los programas necesarios para diversos servicios de Internet, como Gopher, Wais, FTP o cualquier otro programa/cliente disponible en el Server. Estas conexiones suelen ser más económicas (pero más lentas) y están restringidas a los servicios que brinda el servidor.

6.31 IRC

El Internet Relay Chat es un sistema de coloquio en tiempo real entre personas localizadas en distintos puntos de la red. Es un servicio basado exclusivamente en texto por teclado. Fue desarrollado en 1988 en Finlandia y es sin duda, hoy, uno de los servicios más populares de Internet.

Su gran atractivo es que permite las conversaciones en vivo de múltiples usuarios la mayor parte desconocidos entre sí. El manejo del sistema es muy simple.

El IRC está organizado por redes, cada una de las cuales está formada por servidores que se encargan, entre otras cosas, de ofrecer canales de conversación (existiendo miles de ellos) y transmitir los mensajes entre usuarios.

Para acceder a un servidor de este tipo es necesario disponer de un programa cliente, siendo los cuatro más populares el mIRC, Pirch, Ichat y Microsoft Chat.

Cada servidor IRC está conectado a los servidores más cercanos. De esta manera, todos los servidores IRC están conectados (al menos indirectamente) unos con otros.

IRC mantiene un número de diferentes "Canales", teniendo que elegir al ingresar el canal de interés y pudiendo entrar y salir de los canales cuantas veces se desee y en cuantos canales se desee.

La mayoría de los nombres de canales empiezan con "#". Algunos canales son para discutir de temas específicos y otros surgen en el momento. Hay canales públicos, privados, secretos e individuales.

Se pueden crear canales (obteniendo la condición de Operador) si el que se desea no existe y esperar que otras personas ingresen en él. Se suele entrar en las charlas con apodos (nick), sin dar el nombre real, de manera que los usuarios conserven el anonimato. Cuando la última persona abandona un canal, IRC lo elimina.

6.32 USE NET

Una de las áreas más populares de Internet son los grupos de discusión o NewGroups.

El término UseNet surge de USEr NETwork (red de usuarios) y se refiere al mecanismo que soportan los grupos de discusión.

Los grupos se forman mediante la publicación de mensajes enviados ("posteados") a un grupo en particular (generalmente de un tema específico). El software original de News fue desarrollado para los sistemas UNIX en 1979 por dos estudiantes graduados en la Universidad de Duke, como un mecanismo para la discusión técnica y conferencias.

Es una red que no se centra en un único servidor que distribuye los mensajes, sino en una cadena de servidores que se "pasan" los mensajes de los grupos que soporta ya que, normalmente, los servidores mantienen un grupo limitado de News.

Una vez creado un grupo, se puede enviar cualquier mensaje al mismo, y cualquiera dentro de Internet podrá leerlo, a menos que sea un grupo "moderado", con lo cual nuestros mensajes pasan por la "censura" de un moderador.

Para hacer manejable toda la información que circula, se utiliza un sistema en el que los grupos de discusión se agrupan en categorías denominadas Jerarquías. Cada jerarquía tiene un nombre propio y se dedica a un área de interés particular.

La filosofía de las UseNet es la siguiente: Al dejar un mensaje, no sólo se queda en el grupo en cuestión, sino que también les llega a todos los usuarios suscritos al mismo, vía E - Mail.

Tiene una gran utilidad práctica, ya que si un usuario determinado tiene algún comentario o duda acerca de un tema, puede acudir al grupo temático indicado, dejar un mensaje para pedir ayuda, y con seguridad recibirá la opinión de numerosas personas.

6.33 FINGER

La mayoría de las computadoras de Internet tienen una utilidad que permite buscar información sobre un usuario particular. Este servicio es conocido como Finger (dedo).

En Internet los usuarios se conocen por su identificador. Finger se puede utilizar para encontrar el nombre de un usuario si se conoce su identificador. ya que el objetivo de este servicio es obtener información sobre una persona en particular.

El servicio Finger es un sistema Cliente/Servidor que proporciona tres tipos principales de información:

1. Información pública sobre cualquier usuario.
2. Comprobación de si un usuario está utilizando actualmente un Host determinado en Internet, pudiendo ver un resumen de información para cada usuario que está conectado.
3. Conectar con determinado Host, que se han configurado para ofrecer otros tipos de información.

6.34 WHO IS

¿Quién es? es un servidor de directorio de páginas blancas que permite consultar una base de datos de nombres y direcciones de correo electrónico de un usuario (normalmente una empresa).

El servicio WhoIs contacta a un servidor que tiene información básica sobre las redes que comprenden Internet, y los nombres de las personas que dan mantenimiento. Por ejemplo la solicitud whois Harvard produce una lista de todas las redes de la Universidad de Harvard y las compañías que tienen Harvard como parte de su nombre.

Originalmente, la información sobre los usuarios de Internet se almacenaba en una base de datos central. Hoy en día muchas organizaciones corren este servicio que proporciona información sobre los usuarios de una organización. Uno de los servidores WhoIs más conocido es whois.internic.net que contiene nombres y direcciones de Internet.

Es de remarcar que servicios como Telnet, Finger, Archie, Gopher, WhoIs y Ping están cayendo en desuso a favor de las cada vez más perfeccionadas herramientas basadas en la World Wide Web. De todas maneras siguen brindando gran utilidad a administradores de sistemas y usuarios avanzados, sobre todo en temas de seguridad.

GLOSARIO DE TÉRMINOS

GLOSARIO DE TÉRMINOS

A

ACK (Confirmación): Notificación enviada desde un dispositivo de red a otro para confirmar que ocurrió cierto evento (por ejemplo, la recepción de un mensaje).

ActiveX: Lenguaje desarrollado por Microsoft para la elaboración de aplicaciones exportables a la red y capaces de operar sobre cualquier plataforma a través, normalmente, de navegadores.

Administrador: Persona que se encarga de todas las tareas de mantenimiento de un sistema informático. Tiene acceso total y sin restricciones al mismo. Véase También Root y SysOp.

AH (Authentication Header): Protocolo IP 51. Protocolo de la familia IPSec utilizado para garantizar la integridad de los datos y la autenticación del Host.

ANSI (American National Standard Institute): Asociación sin fines de lucros, formada por fabricantes, usuarios, compañías que ofrecen servicios públicos de comunicaciones y otras organizaciones interesadas en temas de comunicación. Es el representante estadounidense en ISO. Que adopta con frecuencia los estándares ANSI como estándares internacionales.

Antivirus: Programa que es el encargado de evitar que cualquier tipo de virus ingrese al sistema, se ejecute y se reproduzca.. Para realizar esta labor existen muchos programas, que comprueban los archivos para encontrar el código de virus en su interior.

Applet: Pequeña aplicación escrita en Java y que se difunde a través de la red para ejecutarse en el navegador cliente.

Archie: Aplicación que permite localizar los archivos accesibles vía FTP anónimo. Si se conoce el nombre de un archivo, pero no se sabe dónde se encuentra, Archie le permite localizarlo.

Archivo: Conjunto bytes relacionados y tratados como una unidad. Un archivo puede contener programas, datos o ambas cosas.

ARP (Address Resolution Protocol): Este Protocolo de Resolución de Direcciones permite mantener asignaciones de pares formados por las direcciones IP y las direcciones físicas (MAC) de los distintos dispositivos de comunicación. Véase también RARP.

ASCII (American Standard Code for Information Interchange): Código estándar americano para intercambio de información. Sistema de codificación de 7 bits que asigna un número del 0 al 127 a cada letra, número, caracteres especiales y de control recogidos. El uso del octavo BIT no está tan estandarizado aunque se suele utilizar cómo código de paridad calculado (normalmente par).

ASV (Automatic Sign Verification): Sistema de verificación automática de firmas.

Ataque: Intento de traspasar un control de seguridad de un sistema.

B

Backdoor: Puerta trasera de entrada a una computadora, programa o sistema en general. Es utilizado para acceder sin usar un procedimiento normal.

Backup: Copia de seguridad que se realiza con el fin de mantener los datos en forma segura.

Boxing: Uso de aparatos electrónicos o eléctricos (Boxes) para hacer Phreaking.

Bouncer: Técnica que consiste en usar un sistema de puente para conseguir redireccionar la salida a un puerto determinado de otro sistema.

Bastión Host: Sistema configurado para resistir los ataques y que se encuentran instalado en una red en la que se prevé que habrá ataques. Son componentes de los Firewalls ejecutando alguna aplicación o sistema operativo de propósito general.

BBS (Bulletin Board System): Boletín Electrónico. Es un sistema mediante el cual se pone a disposición de los demás una serie de recursos.

Bit: En informática, unidad mínima de información.

Black Box: Aparato que engaña a la central telefónica haciéndole creer que no se levantó el tubo del teléfono cuando en realidad se está produciendo una comunicación.

Bomba Lógica: Programa ilegítimo contenido dentro de un sistema y que ante un hecho o una fecha prevista "explota" causando daño al sistema que lo contiene u a otro. Raramente tienen la capacidad de reproducción.

BPS (Bits por Segundo): Medida de velocidad de transmisión.

BroadCast: Difusión. Tipo de comunicación en que todo posible receptor es alcanzado por una sola transmisión. Véase también Multicast.

Buffer Overflow: Error generado cuando un programa (generalmente un servidor o demonio") recibe una entrada mayor a la que espera, sobrescribiendo áreas críticas de memoria.

Bug: Un error en un programa o en un equipo. Se habla de bug si es un error de diseño, no cuando la falla es provocada por otro motivo.

Byte: Combinación de Bits. En la representación más común 8 bits forman un byte.

C

Caballo de Troya: Programa aparentemente útil el cual contiene código adicional escondido, desarrollado para obtener algún tipo de información o causar algún daño. Véase también Troyano.

CCITT (Comité Consultatif International de Télégraphique et Téléphonique): Organización de la Naciones Unidas constituida, en principio, por las autoridades de Correos, Telégrafos y Teléfonos (PTT) de los países miembros. Se encarga de realizar recomendaciones técnicas sobre teléfonos, telégrafos e interfaces de comunicación de datos, que a menudo se reconocen como estándares. Trabaja en colaboración con ISO (que en la actualidad es miembro de CCITT). Véase también ITUT.

CERT/CC (Computer Emergency Response Team/Coordination Center): Grupo establecido en diciembre de 1988 por Defense Advanced Research Projects Agency (DARPA) para manejar los problemas concernientes a la Seguridad Informática. El CERT es dirigido por expertos en diagnósticos y resolución de problemas de seguridad. Para la resolución de estos problemas están en permanente contacto con usuarios de todo el mundo y las autoridades gubernamentales apropiadas. Por más información consultar http://www.cert.org - http://www.arcert.gov.ar.

Ciberespacio: "(...) alucinación consensual experimentada diariamente por millones de legítimos operadores en todas las naciones. Una representación gráfica de información proveniente de todas las computadoras del sistema humano. Una complejidad inimaginable (...)", y en el que toda la gente dice estar navegando.

Cifrar: Ver Criptografía.

Clave, Contraseña (Password): palabra o frase que permite acceder a un sistema, encriptar un dato, determinar privilegios de usuarios, etc.

Clave Pública: En un Sistema Asimétrico de Cifrado es la clave que todos conocen para Cifrar o descifrar un mensaje.

Clave Privada: : En un Sistema Asimétrico de Cifrado es la clave que solo el emisor del mensaje conocen para cifrar o descifrar un mensaje.

Cliente: Sistema o proceso que solicita a otro sistema o proceso que le preste un servicio. Una computadora que solicita el contenido de un archivo a otra (Servidor) es un cliente de la misma.

Código Fuente: Un programa escrito en un formato entendible por el hombre pero no por la computadora. Necesita ser "traducido" (Compilar) a código máquina para ser interpretado por esta última.

Colgar: Hacer que un sistema deje de funcionar. Desconectar una comunicación telefónica.

Compilador: Programa que toma el Código Fuente de un programa y lo convierte a un ejecutable.

Cookie: Es un pequeño trozo de información enviado por un servidor de Web al sistema de un usuario.

Correo electrónico: aplicación que permite enviar mensajes a otros usuarios de la red sobre la que esté instalado. También denominado E-Mail.

Cortafuegos: Ver Firewall.

Cracker: Persona que quita la protección a programas con sistemas anticopia. Hacker maligno, que se dedica a destruir información.

Criptografía: Ciencia que consiste en transformar un mensaje inteligible en otro que no lo es, mediante la utilización de claves, que solo el emisor y receptor conocen.

D

Datagrama: Conjunto de datos que se envían como mensajes independientes. Unidad utilizada por el protocolo UDP.

Denial of Service (DoS): Negación de Servicio. Acciones que impiden a cualquier sistema funcionar de acuerdo con su propósito.

Detección de Intrusos: Sistemas que agrupa un conjunto de técnicas cuyo propósito es detectar las intrusiones en una computadora o un sistema.

Decoy (Señuelo): Programa diseñado para que vigilar el comportamiento de un usuario.

Diccionarios: Conjunto de palabras almacenadas en un archivo. Su fin es utilizar cada palabra para se probada como posible Password de un sistema que se quiere violar. Véase también Fuerza Bruta.

DNS (Domain Name Server): Servicio que proporciona una dirección IP a partir de un nombre de dominio proporcionado. Este protocolo evita tener que recordar las complicadas combinaciones de números que forman una dirección IP.

E

E-Mail: Ver Correo Electrónico.

EIA (Electronic Industries Association): Asociación vinculada al ámbito de la electrónica. Es miembro de ANSI. Sus estándares se encuadran dentro del nivel 1 del modelo de referencia OSI.

Encriptar: Ver Criptografía.

ESP (Encapsulating Security Payload): Protocolo IP 50. Protocolo de la familia IPSec que incluye las características de AH y agrega, opcionalmente, la confidencialidad de los datos.

Ethernet: Protocolo de comunicación. Especificación de Lan de banda base, inventada por Xerox Corporation y desarrollada conjuntamente por Xerox, Intel y Digital equipment Corporation.

Exploit: Programa que aprovecha un BUG de un sistema. Programa que abusa de algún error de un sistema operativo para conseguir aumentar los privilegios de un usuario o la caída del sistema.

F

Fake Mail: Enviar un correo electrónico falseando el remitente.

FAQ: (Frecuently Asked Questions) Documento donde se vuelcan las preguntas mas frecuentes sobre un tema y sus respuestas.

Finger: Define los estándares para buscar información de un usuario.

Firewall: Barrera de Protección. Es un procedimiento de seguridad que coloca un sistema de computación programado especialmente entre una red segura y una red insegura. Un sistema o combinación de sistemas que fija los limites entre dos o mas redes y restringe la entrada y la salida de la información.

FTP: (File Transfer Protocol) Protocolo del nivel de usuario (protocolos de aplicación) para la transferencia de archivos entre computadoras. También puede hacer referencia a la aplicación que permite transferir archivos de una computadora a otra usando el mismo protocolo.

Fuerza bruta: Es cuando los Crakers se basan en aprovechar diccionarios para comparar las palabras almacenadas en el con los passwords del sistema y obtenerlos.

G

Gateway: Dispositivo de enrutamiento. En la actualidad, se utiliza el termino **Router** para describir los nodos que realizan esta función, mientras que Gateway se refiere a un dispositivo para fines especiales que convierte información de la capa de aplicación de un stack de protocolo a otro.

Gopher: Aplicación de Internet que permite utilizar recursos remotos mediante el uso de un sistema de simples menús. Se tiene a su alcance la mayoría de los recursos de Internet desplegados en diferentes opciones de los distintos menús.

Guest (Invitado): Cuenta publica en un sistema. Su objetivo es la de ser utilizada por alguien que no tiene una cuenta propia.

Gusano: Programa ilegitimo o virus que es capaz de reproducirse a si mismo infinitamente hasta colapsar el sistema en el que se este utilizando hasta lograr su objetivo que es inutilizar el sistema por falta de recursos.

H

Hacker: Una persona que disfruta explorando los detalles de las computadoras y de cómo extender sus capacidades.

Handshake (Saludo): Secuencia de mensajes intercambiados entre dos o más dispositivos de red para garantizar la sincronización de la transmisión.

Hardware: Componentes electrónicos, tarjetas, periféricos y equipo que conforman un sistema de computación.

Hexadecimal: Base 16. Una representación numérica que utiliza los dígitos 0 a 9, con su significado usual, más las letras A a la F para representación de los dígitos hexadecimales con valores de 10 a 15.

Host: Sistema Central. Computadora que permite a los usuarios comunicarse con otros sistemas de una red. Los usuarios se comunican utilizando programas de aplicación, tales como el Correo Electrónico, Telnet y FTP.

HTML (Hyper Text Markup Language): Formato especial de archivos sobre el que está basada la estructura de la aplicación WWW (World Wide Web).

HTTP (HyperText Tranfer Protocol): Es un protocolo de la capa de aplicaciones con la velocidad necesaria para sistemas de información hipermediales en un ambiente distribuido y de colaboración.

Hub (Concentrador): Dispositivo que sirve como centro de una red de topología en estrella.

I

ICMP (Internet Control Message Protocol): Protocolo utilizado para gestionar la comunicación de mensajes de error entre distintos puntos de la red.

ID: Identificación.

IDEA (International Data Encription Algorithm): Algoritmo de encriptación simétrico.

IEEE (Institute of Electrical and Electronics Engineers): Instituto de ingeniería eléctrica y electrónica. Organización profesional entre cuyas actividades se incluye el desarrollo de estándares para comunicaciones y Redes.

IETF (Internet Engineering Task Force): Grupo Encargado de definir Solicitudes de comentarios (RFC).

Ingeniería Social: Arte de convencer a la gente para que realice actos que pueden comprometer un sistema. Obtención de información por medios ajenos a la informática.

INTERNET: Sistema de redes de computación ligadas entre si, con un alcance mundial, que facilita los servicios de comunicación de datos como registro remoto, transferencia de archivos, correo electrónico, grupos de noticias y actualmente lo mas demandado música y videos.

Intruso: Aquella persona que con una variedad de acciones intenta comprometer o transgredir los recursos de hardware y software del equipo o red en cuestión

Invitado: Ver Guest.

IP (Internet Protocol): Protocolo de comunicación sin conexión, que por si mismo proporciona un sistema de datagramas. Es el protocolo que proporciona el servicio de envió de paquetes para los protocolos soportados TCP, UDP e ICMP. Protocolo de capa de red de la pila TCP/IP que ofrece un servicio de internetwork sin conexión. El IP tiene prestaciones para direccionamiento, especificación del tipo de servicio, fragmentación y rearmado y seguridad.

IP Spoofing: Método para falsear la IP en una conexión remota.

IPX/SPX: Es el conjunto de protocolos de bajo nivel utilizados por el sistema operativo de red Network de Novell, SPX actúa sobre IPX para asegurar la entrega de los datos.

IPSec: Protocolo creado por el IETF para brindar seguridad a nivel de red.

IRC (Internet Relay Chat): Charla interactiva en Internet. Protocolo para conversaciones simultáneas; que permite a varias personas comunicarse entre si por escrito y en tiempo real.

ISO (International Organization for Standarization): Organización Voluntaria NO Gubernamental cuyos miembros han desarrollado estándares para las naciones participantes. Uno de sus comités se ocupa de los sistemas de información. Han desarrollado el modelo de referencia OSI y protocolos estándares para varios niveles de este modelo.

ISP (Internet Service Provider): Compañía o individuo dedicado a vender el acceso o servicio a Internet.

ITU-T (International Telecommunication Union Telecommunication Standarization Sector): Union internacional de las telecomunicaciones (ex comité de consultoria internacional para telefonía y telegrafía CCITT) Organización internacional que desarrolla estándares de comunicación.

J

Jargon (Jerga, Jerigonza): Lenguaje peculiar de un determinado grupo, profesión u oficio difícil (y a veces imposible) de entender por los no iniciados

JAVA: Lenguaje de programación desarrollado por SUN para la elaboración de aplicaciones expórtables a la red (Applets) y capaces de operar sobre cualquier plataforma a través normalmente de navegadores.

K

Kerberos: Sistema de seguridad en el que los login y los passwords viajan encriptados a través de la red.

Key Logger: Grabador de teclas pulsadas. Es utilizado cuando se desea conocer las contraseñas, nombres de usuarios o cualquier otra información en donde se utilice el teclado como vía de entrada al sistema.

L

L2TP (Layer To Tunneling Protocol): protocolo estándar del IETF que encapsula las tramas del Protocolo Punto a Punto (PPP) que van a enviarse a través de redes.

Lamer: Termino aplicado por los Hackers a las personas con pocos conocimientos.

LAN (Local Area Network): Red de área local. Red de datos de alta velocidad y bajo nivel de error que cubre un área geográfica relativamente pequeña (hasta unos pocos miles de metros). Las LANs conectan estaciones de trabajo, periféricos, terminales y otros dispositivos en un único edificio u otra área geográficamente limitada. Véase también MAN y WAN.

LINUX: Sistema Operativo de la familia UNIX. El proyecto original pertenece a Linus Torvalds.

Login: Nombre de acceso de un usuario a una red o sistema multiusuario. Este término se le puede aplicar tanto al nombre de su cuenta como al hecho de ingresar a un sistema de este tipo. El usuario debe usar el nombre, así como su contraseña (password), para tener acceso al sistema.

Log: Archivo de registro de actividades.

M

MAC (Media Access Control): Control de acceso al medio. La inferior de las dos subcapas de la capa de enlace de datos definida por IEEE. La subcapa MAC administra el acceso a medios compartidos.

Mail Bomber: Consiste en el envío masivo de mails a una dirección de la víctima.

MainFrame: Gran computadora central.

MAN (Metropolitan Area Network): Red de área metropolitana. En general, una MAN abarca un área geográfica más vasta que una LAN, pero cubre un área geográfica más pequeña que una WAN.

MIME (Multipurpose Internet Mail Extensions): Extensiones de Internet Mail Multipropósito. Ver MultiCast (MultiDifusión): Modo de difusión de información, que permite que ésta pueda ser recibida por múltiples nodos de la red y por lo tanto por múltiples usuarios. Véase también BroadCast.

N

Negación de Servicio: Ver DoS.

Newbie: Término aplicado por los Hackers a los novatos en el hacking.

Newsgroup: Grupo de noticias. Es un servicio Internet que permite el envío y compartición de mensajes entre usuarios que tienen un interés común. Forma habitual de denominar el sistema de listas de correo. También se lo denomina News.

Nodo: Cualquier computadora o periférico conectado directamente a una red.

NetBeui (NetBIOS Extended User Interface): Protocolo de los niveles de transporte y red del modelo ISO/OSI, se integra con NetBIOS para ofrecer un sistema de comunicaciones eficiente en el entorno LAN de grupos de trabajo.

NetBIOS (Network BIOS): Protocolo del nivel de sesión, que establece y mantiene las sesiones de comunicación entre computadores.

Network (Red): Red de computadoras es un sistema de comunicación de datos. Conecta entre sí sistemas informáticos situados en diferentes lugares. Puede estar compuesta por diferentes combinaciones de diversos tipos de redes.

Número IP: Número que identifica de manera única una maquina dentro de la red que utiliza el Protocolo TCP.

O

OSI: Open System Interconnection): Interconexión de sistemas abiertos. Programa de estandarización internacional creado por ISO e ITU-T para desarrollar normas para networking de datos que faciliten la interoperabilidad entre equipos de diversos fabricantes.

P

Password (Clave): Ver Clave, Contraseña.

Patch (Parche): Modificación de un programa ejecutable para solucionar un problema, corregir un Bug o para cambiar su comportamiento.

Payload: Efecto visible de un software maligno.

PC (Personal Computer): Computadora Personal.

Perfil de Usuario: Información a la que el usuario necesita acceder para el desarrollo de sus tareas, criticidad de la información, funciones del puesto, etc.

PGP (Pretty Good Privacy): Privacidad Bastante Buena. Programa de encriptación de correo electrónico para Internet, que utiliza una combinación de claves públicas y privadas.

Phreaker: Persona que usa los medios de comunicaciones sin pagarlos o pagando menos de lo que corresponde.

Pirata Informático: Persona que copia software, con derecho de autor, ilegalmente sin que medie el permiso expreso del desarrollador. No confundir con el término Hacker o Cracker.

PIN: Personal Identification Number. Número de Identificación Personal.

POP (Postal Office Protocol): Protocolo que brinda la posibilidad de que el correo electrónico sea depositado en "buzones" ubicados en algún tipo de sistema servidor de correo, y no directamente en una estación de trabajo.

Port Scanner: Programa que indica los Puertos abiertos de un sistema.

PPP (Point to Point Protocolo): Protocolo de comunicación serie que opera sobre líneas de enlace telefónico alquiladas (dedicadas) para proporcionar conexiones dentro de redes IP.

PPTP (Point to Point Tunneling Protocol): Protocolo antecesor de L2TP fue diseñado para proporcionar comunicaciones autenticadas y cifradas entre un cliente y un Gateway o entre dos Gateways.

Promiscuo (Modo): Normalmente interfaz Ethernet que permite leer toda la información sin importar su destino, aplicable a un segmento de Red.

Protocolo: Conjunto de normas (lenguaje de reglas y símbolos) que rige cada tipo de comunicación entre dos computadoras (intercambio de información).

Proxy: Entidad que, a fin de lograr mayor eficiencia, esencialmente suple otra entidad.

Puerto: Proceso de capa superior que está recibiendo información de capas más bajas.

R

RARP (Reverse Address Resolution Protocol): La función de este Protocolo complementa la función de ARP, pues permite mantener asignaciones de direcciones físicas a direcciones Internet.

Red: Conjunto de computadoras, impresoras, Routers, Switches, y otros dispositivos, que pueden comunicarse entre sí por algún medio de transmisión.

Redirigir: Cambiar el destino de algo. Por ejemplo, redirigir una llamada es hacer que suene en un teléfono distinto del que se intentaba llamar.

RFC (Request For Comment): Documentos especiales escritos y publicados por individuos comprometidos en el desarrollo y mantenimiento de Internet. Tienen el importante propósito de servir de documentación para nuevos desarrollos tecnológicos y ofrecer los estándares sobre los cuales se edificará la nueva tecnología.

Root: Persona que se encarga del mantenimiento del sistema. Tiene acceso total y sin restricciones al mismo. Véase también Administrador y SysOp.

Rootkit: Software que permite a los intrusos depositar Puertas Traseras, Caballos de Troya y diversos mecanismos para asegurar su regreso al sistema atacado, y al mismo tiempo esconderse del resto de los usuarios del sistema, en particular del Administrador.

Router: Dispositivo de capa de red que utiliza una o más métricas para determinar la ruta óptima por la cual se enviará el tráfico de la red. Los routers envían paquetes de una red a otra en base a la información de capa de red. Ocasionalmente llamado Gateway (aunque esta definición de gateway está cayendo en desuso).

S

SATAN (Security Administrator Tool for Analyzing Networks): Herramienta para el Análisis de Administradores de Seguridad de Redes. Aplicación realizada por el informático norteamericano Dan Farmer y el gurú americano-holandés Wietse Venema. Es capaz de establecer el nivel de vulnerabilidad de un Host y de todas las máquinas conectadas a él vía Internet (su dominio).

Server (Servidor): Máquina que ofrece servicios a otras dentro de una red. También llamado Host.

SET (Secure Electronic Transaction): Transacción Electrónica Segura. Protocolo creado y publicado por Visa y MasterCard con el fin de permitir la realización de transacciones electrónicas (compraventas fundamentalmente) a través de la red.

Shell: Intérprete de comandos de un sistema operativo. Es el que se encarga de tomar las órdenes del usuario y hacer que el resto del Sistema Operativo las ejecute.

Shoulder Surfing: Espiar por detrás de un hombro para tratar de ver información interesante. Es un método comúnmente usado para acceder cuentas de otras personas.

Sistema Asimétrico de Cifrado: Sistema mediante el cual se emplea una doble Clave kp (privada) y KP (Pública). Una de ellas es utilizada para Cifrar y la otra para descifrar. El emisor conoce una y el receptor la otra. Cada clave no puede obtenerse a partir de la otra.

Sistema Simétrico de Cifrado: Sistema mediante el cual se emplea la misma Clave para Cifrar y descifrar. El emisor y receptor deben conocerlas.

SLIP (Serial Line Internet Protocol): Es usado para transmitir paquetes IP a través de líneas de comunicación seriales.

SMTP (Simple Mail Transfer Protocol): Protocolo que proporciona la capacidad de almacenamiento y reenvío del correo entre los host de los sistemas de correo de la red.

Sniffer: Es un programa que permite "escuchar furtivamente" en redes de medios de comunicación compartidos (tales como Ethernet). Se ejecuta en una máquina que está conectada a la red, en modo Promiscuo y captura el tráfico de todo el segmento de red.

SNMP (Simple Network Management Protocol): Protocolo que permite obtener información de gestión de los dispositivos conectados a la red.

Socks: Protocolo que permite la conexión a equipos situados detrás un Firewall.

Software: Programas de sistema, utilerías o aplicaciones expresadas en un lenguaje de maquina.

SOLARIS: Sistema Operativo de la empresa Sun. Es una implementación de UNIX.

Spam: Correo electrónico que se recibe sin haberlo solicitado (llamados "e-mail basura"). Un envío masivo de Spam puede provocar un colapso en el sistema que los recibe, en este caso se les denomina MailBombing.

SSL (Secure Sockets Layers): Protocolo que provee una conexión segura entre dos hosts.

SUN OS: Sistema Operativo de la empresa Sun. Es una implementación de UNIX.

SysOp: Persona que se encarga del mantenimiento del sistema. Tiene acceso total y sin restricciones al mismo. Véase también Administrador y Root.

Switch: Dispositivo que opera en la capa de enlace de datos del modelo OSI. Dispositivo electrónico o mecánico que permite establecer una conexión cuando resulte necesario y terminarla cuando ya no hay sesión alguna que soportar.

T

TCP (Transmission Control Protocol): Este Protocolo de Control de Transmisión es un protocolo orientado a conexión. Su función principal es proporcionar mecanismos que ofrezcan seguridad en el proceso de entrega de los paquetes a su destino, así como ordenar paquetes de información y evitar la repetición de éstos.

TCP/IP (Tranfer Control Protocol/Internet Protocol): Arquitectura de red con un conjunto de protocolos que permiten compartir recursos a través de una red. Esta familia de protocolos es la más importante difundida en la actualidad, por ser la base de Internet.

TELNET: Protocolo estándar utilizado para realizar un servicio de conexión desde una terminal remota.

Terminal: Acceso a una computadora o sistema. Puede tratarse de una computadora completa o un monitor o únicamente el CPU.

TLS (Transport Layer Security): Protocolo que dio origen a SSL.

Tracear: Seguir la pista a través de la Red mediante direcciones IP, ya sea de una persona o de alguna información en especifico.

Trashing: Es hasta cierto punto un arte se trata de revolver la basura informática para encontrar información útil.
Troyano: Programa legitimo que ha sido alterado de alguna forma y que contiene funciones desconocidas (generalmente dañinas). Generalmente no contienen un código que haga que se vuelvan a reproducir.

U

UDP (User Datagram Protocol)): El protocolo de datagramas de usuario es un protocolo no orientado a conexión. Su desventaja principal es que no garantiza que los datagramas sean entregados en su destino.

UNÍX: Sistema operativo generalmente utilizado por servidores para un mejor control de la red.

UPS (Uninterrupted Power Suply): Sistema de energía ininterrumpido.

UseNet: Red que contiene cientos de foros electrónicos de discusión (NewsGroups), las computadoras que procesan los protocolos y finalmente las personas que leen y envían las noticias.

UserName (Usuario): Nombre único que identifica a un usuario y es utilizado como medio de identificación ante un sistema.

V

Virus: Programa que actúa secretamente sin que el usuario se entere generalmente; cuyo código incluye información suficiente y necesaria para que, utilizando los mecanismos de ejecución que le ofrecen otros programas puedan reproducirse y ser susceptibles de mutar; resultando de dicho proceso la modificación, alteración y / o daño de los programas, información y / o hardware afectados.

Vulnerabilidad: Hardware, Software o Firmware que contiene BUGS que permiten su explotación y manejo inadecuado.

W

WAN (Wide Area Network): Red de area extensa. Red de comunicación de datos que sirve a usuarios ubicados a través de una amplia zona geográfica y a menudo utiliza dispositivos de transmisión suministrados por portadoras comunes. Véase también LAN y MAN.

Warez: Programas comerciales ofrecidos por Internet "gratuitamente". Ver Piratería Informática.

Web Sites (Sitio Web): Sistema dedicado al intercambio de información On-Line.

Worm: Ver Gusano.

Windows: Sistema Operativo gráfico de la empresa Microsoft.

WWW (World Wide Web): Gran red de servidores de Internet que brinda servicios de hipertexto y otros a las terminales que corren aplicaciones cliente como por ejemplo un explorador WWW.

X

X.25: Protocolo utilizado principalmente en WAN y, sobre todo, en las redes públicas de transmisión de datos. Funciona por conmutación de paquetes, esto es, que los bloques de datos contienen información del origen y destino de los mismos para que la red los pueda entregar correctamente aunque cada uno circule por un camino diferente.

Xploit: Ver Exploit.

Z

Zapper: Programa que se encarga de borrar los Logs que graban las entradas, acciones y salidas de usuarios.

APÉNDICE
FIGURAS
Y
TABLAS

APÉNDICE "FIGURAS Y TABLAS"

FIGURA 1	EJEMPLO DE CONTRASEÑAS	21
FIGURA 2	EJEMPLO DE ENCRIPTACIÓN	23
FIGURA 3	FORMAS DE PROTECCIÓN	29
FIGURA 4	EJEMPLO DE INTROMISIÓN	35
FIGURA 5	EJEMPLO DE ROBO DE INFORMACIÓN	55
FIGURA 6	TIPO DE ATAQUE SYN	65
FIGURA 7	TIPO DE ATAQUE SYN FLOOD	74
FIGURA 8	TIPO DE ATAQUE SMURF	76
FIGURA 9	EJEMPLO DE INTRODUCCIÓN DE UN VIRUS	89
FIGURA 10	EJEMPLO DE ARCHIVO INFECTADO	91
FIGURA 11	EJEMPLO DE PROGRAMA ANTIVIRUS	99
FIGURA 12	EJEMPLO DE FIREWALL	106
FIGURA 13	EJEMPLO DE FALLA EN EL PERÍMETRO DE SEGURIDAD	108
FIGURA 14	RUTEADOR FILTRA PAQUETES	113
FIGURA 15	GATEWAY A NIVEL APLICACIÓN	114
FIGURA 16	GATEWAY A NIVEL CIRCUITO	115
FIGURA 17	ESQUEMA DE COMUNICACIÓN	132
FIGURA 18	EJEMPLO DE INTERCONEXIONES	133
FIGURA 19	ESQUEMA DE TRANSMISIÓN DE DATOS	138
TABLA 1	PORCENTAJE DE VULNERABILIDADES POR TIPO DE SITIO	60
TABLA 2	CANTIDADES DE CLAVES GENERADAS SEGÚN EL NUMERO DE CARACTERES EMPLEADOS	71

APÉNDICE "[illegible]GURAS Y TABLAS"

FIGURA 1	EJEMPLO DE C[illegible]TRASEÑAS	16
FIGURA 2	EJEMPLO DE ENCRIPTACIÓN	18
FIGURA 3	FORMAS DE PROTECCIÓN	24
FIGURA 4	EJEMPLO DE INTRO[illegible]ISIÓN	29
FIG[illegible] 5	EJEMPLO DE ROBO DE INFORMACIÓN	48
[illegible]RA 6	TIPO DE ATAQUE SYN	57
[illegible]RA 7	TIPO DE ATAQUE SYN FLOOD	66
FIGURA 8	TIPO DE ATAQUE SMURF	68
FIG[illegible]RA 9	EJEMPLO DE INTRODUCCIÓN DE UN VIRUS	81
FIGURA 10	EJEMPLO DE ARCHIVO INFECTADO	83
F[illegible] 11	EJEMPLO DE PROGRAMA ANTIVIRUS	91
[illegible] 12	EJEMPLO DE FIREWALL	97
FIG[illegible] 13	EJEMPLO DE FALLA EN EL PERÍMETRO DE SEGURIDAD	99
[illegible]IGURA 14	RUTEADOR FILTRA PAQUETES	104
[illegible]URA 15	GATEWAY A NIVEL APLICACIÓN	105
[illegible]RA 16	GATEWAY A NIVEL CIRCUITO	106
[illegible]A 17	ESQUEMA DE COMUNICACIÓN	122
[illegible] 18	EJEMPLO DE INTERCONEXIONES	123
[illegible] 19	ESQUEMA DE TRANSMISIÓN DE DATOS	128
[illegible] 1	PORCENTAJE DE VULNERABILIDADES POR TIPO DE SITIO	52
[illegible] 2	CANTIDADES DE CLAVES GENERADAS SEGÚN EL NUMERO DE CARACTERES EMPLEADOS	

CONCLUSIÓN

CONCLUSIÓN

A lo largo de esta investigación, he tratado de plantear un enfoque a las partes que considero mas relevantes sobre la seguridad informática, de una manera sencilla de entender.

En un mundo invadido por la información, en que todo ha venido a darle mayor proyección y facilidad para que un gran número de gente esté informada, y pueda tener la oportunidad de desarrollarse, manejarse y comunicarse de una mejor manera.

El gran avance tecnológico que hemos tenido en menos de diez años en cuanto a la convergencia de voz, datos e imagen, por medio de los programas de computación nos ha abierto la puerta para entrar en un mundo hasta cierto punto complejo pero que continua con fallas en cuanto a la seguridad de la información.

Abierta, Universal, Económica y Segura. Esas son las propiedades que adjudican algunos a la información. Lograr estándares en el mundo altamente tecnificado de hoy es quizás la principal barrera con las que chocan los profesionales para "asegurar la Seguridad".

Por otro lado, la situación internacional actual exige una concientización, por parte de todos, que la información es conocimiento y como tal debemos atribuirle la importancia que merece. Esta importancia incluye estudiar y lograr la forma de protegerla.

Esto plantea una paradoja:

Si sumamos seguridad, bajan las posibilidades de acceder a la información, lo que es igual al Aislamiento y la Marginación.

Si sumamos información, lo hacemos de forma insegura, lo que nos hace Globalmente Vulnerables.

La convergencia de los sistemas multiplica exponencialmente los problemas de seguridad planteados. El equilibro es difícil, el espectro a cubrir es amplio y, como dificultad extra, el campo de trabajo es intangible. Esto hace necesario desarrollar técnicas y/o adaptar las existentes de forma tal que desarrollemos nuestro trabajo de conseguir información y conocimiento dentro de un marco de seguridad.

Cuando se diseña un sistema se lo hace pensando en su Operatividad - Funcionalidad dejando de lado la Seguridad.

Será necesario establecer una correspondencia y pertenencia entre las técnicas adoptadas conformando un sistema de seguridad; y no procedimientos aislados que contribuyan al caos general existente. Esto sólo puede lograrse al integrar la seguridad desde el comienzo, desde el diseño, desde el desarrollo.

Las tecnologías involucradas en estos procesos condicionan las técnicas empleadas, los tiempos condicionan esas tecnologías y, paradójicamente, las legislaciones deben adaptarse a los rápidos cambios producidos. Esto hace obligatorio no legislar sobre tecnologías actuales, sino sobre conceptos y abstracciones que podrán ser implementados con distintas tecnologías en el presente y el futuro.

Es urgente legislar un marco legal adecuado, no solo que castigue a los culpables sino que desaliente acciones hostiles futuras.

Existen infinidad de métodos (muchas veces plasmados en herramientas) que permiten violar un sistema.

El profesional cuenta con la misma tecnología para la evaluación de la seguridad del bien a proteger y otras pensadas para la protección como fin. Esto hace que muchas veces, la seguridad, sea asunto de la aptitud y mentalidad del profesional.

En algunos campos, la Tecnología deberá ampararnos ante la desaparición de elementos naturales. Por mencionar un ejemplo: la firma digital (Tecnología Criptográfica) debe cubrir la brecha que deja la inexistencia de la firma caligráfica en archivos de información.

Algunos pocos métodos realmente novedosos de infiltración ponen en jaque los sistemas de seguridad. Aquí, se prueba la incapacidad de lograr 100% de seguridad, pero también es hora de probar que los riesgos, la amenaza, y por ende los daños pueden ser llevados a su mínima expresión.

Muchas veces vasta con restringir accesos a información no utilizada o que no corresponde a los fines planteados. Otras veces la capacitación será la mejor herramienta para disminuir drásticamente los daños.

He tratado de probar que: La Seguridad Perfecta requiere un nivel de perfección que realmente no existe, y de hecho dudo que algún día exista, pero los riesgos deben y pueden ser manejables.

El costo en el que se incurre suele ser una insignificancia comparada con aquellos luego de producido un daño. El desconocimiento y la falta de información son el principal inconveniente cuando se evalúa la inclusión de seguridad como parte de un sistema.

El desarrollo de software es una "ciencia" imperfecta; y como tál es vulnerable. Es una realidad, y espero haberlo demostrado en "Amenazas Humanas", que la Seguridad involucra manipulación de naturaleza humana.

Es importante comprender que:

1. La Seguridad consiste en Tecnología y Política. Es decir que la combinación de la Tecnología y su forma de utilización determina cuan seguros son los sistemas.

2. El problema de la Seguridad no puede ser resuelto por única vez. Es decir que constituye un viaje permanente y no un destino.

3. En última instancia la Seguridad es una serie de movimientos entre "buenos" y "malos".

A manera de despedida deseo dejar un resumen realizado por el equipo de Microsoft Security Response Center sobre la forma y el cuándo nuestra computadora deja de ser nuestra.

Las 10 Leyes Inmutables de la (in)seguridad

I. Si una mala persona puede persuadirlo para ejecutar su programa en SU computadora, esta deja de ser suya.

II. Si una mala persona puede alterar el sistema operativo en SU computadora, esta deja de ser suya.

III. Si una mala persona tiene acceso físico sin restricción a SU computadora, esta deja de ser suya.

IV. Si usted permite a una mala persona, subir un programa a SU sitio Web, este deja de ser suyo.

V. Las contraseñas débiles constituyen un atentado a la seguridad.

VI. Una sola máquina es segura en la medida que el Administrador es fidedigno.

VII. Los datos encriptados son seguros en la misma medida que la clave de desencriptación lo sea.

VIII. Un antivirus desactualizado sólo es parcialmente mejor que ninguno.

IX. La anonimicidad absoluta no es práctica, ni en la vida real ni en la Web.

X. La tecnología no es un remedio.

Las últimas encuestas de seguridad realizadas por Information Security Magazine, Computer Security Institute, entre otros, confirman que se ha incrementado considerablemente los presupuestos del área de seguridad. Si bien estos recursos, son importantes para fortalecer elementos de la seguridad informática de las organizaciones, también debe fortalecer las estrategias de la Gerencia de la Seguridad, para dar cuenta del uso de los recursos para la protección de la información, es decir generar indicadores de gestión que muestren como avanza la organización en seguridad informática, pues nada ganamos si invertimos y no medimos como esta inversión ha mejorado o disminuido la seguridad informática de las organizaciones en los diferentes temas que cubren las políticas asociadas con la seguridad.

Aunque se ha producido un incremento en el gasto en seguridad, éste ha tenido más que ver con la reparación de daños que con la prevención. Buena prueba de ello son los principales daños que últimamente se han dado y que responden a rutinas de difusión ya conocidas como los virus gusano, que se repiten una y otra vez con éxito, amparándose precisamente en la falta de políticas de seguridad. La protección de datos, de información y de las rutinas de comunicación y trabajo pasa ineludiblemente por una primera detección de los puntos vulnerables o vitales de la red a asegurar para proceder, después, a una consecuente integración de sistemas de seguridad preparados para obrar una política preventiva que convierta el gasto en inversión y que responda a necesidades concretas.

Sí, por supuesto. La seguridad no es un complemento más, es una pieza tan básica en una red como un switch o el cableado. Desgraciadamente han tenido que ocurrir los atentados o robos, para que suba el nivel de protección en muchas empresas, incluso en algunas que lo empiecen a tener. A pesar de todo, queda mucho camino por recorrer, tanto en protección como en formación de los usuarios, que en pocos casos va más allá que enseñar a manejar un procesador de texto.

BIBLIOGRAFÍA

BIBLIOGRAFÍA

LIBROS

ALDEGANI, Gustavo. Miguel. Seguridad Informática. MP Ediciones. 1° Edición. ISBN 9879131266. Uruguay. 1997.

CLOUGH, Bryan. MUNGO Paul. Los Piratas del Chip. Ediciones BSA. EEUU. 1999.

FERNADEZ, Carlos M. Seguridad en Sistemas Informáticos. Ediciones Díaz de Santos S.A., ISBN 8486251958. España. 1988.

Dr. MAX, SEGURIDAD Y ANTIVIRUS, MP Ediciones S. A. ISBN: 9685347298, México 2001.

NOMBELLA, Juan José. Seguridad Informática. Editorial Paraninfo. ISBN 8428323410. España. 1998.

KLANDER Lars. A Prueba de Hackers. Editorial Anaya Multimedia. EEUU. 1998.

LEVIN, Ricardo. Virus Informáticos. Mc Graw Hill. ISBN 0078816475. España. 2002.

LUCENA LÓPEZ, Manuel José. Criptografía y Seguridad en Computadores. Dpto. de Informática Universidad de Jaén. 3° Edición España. 2001.

LUDWIG, Mark A. The Little Black Book of Computer Viruses. Volumen One. American Eagle Publications, Inc. ISBN: 0-929408-02-0.

MCLURE, Stuart. SCAMBRAY, Joel. KURTZ George. Hackers, Secretos y Soluciones para la Seguridad en Redes. Traducción: GÓMEZ BASTIDA, Fulgencio. Osborne McGraw-Hill. ISBN Español: 0072121270. España. 2002.

NOMBELLA, Juan José. Seguridad Informática. Editorial Paraninfo. ISBN 8428323410. España. 1998.

NORTHCUTT, Stephen. NOVAK Judy. Detección de Intrusos. Guía Avanzada. Prentice Hall. 2° Edición. Español 8420531154. España. 2001.

SCHNEIER Bruce. Applied Cryptography. Editorial John Wiley & Sons. 2° Edición. ISBN 0471117099. EEUU. 2003.

STALLINGS, William. Network And Internetwork Security. 2° Edición. Prentice Hall. ISBN 0138690170. EEUU. 2000.

TÉLLES VALDEZ, Julio. Derecho Informático. 2° Edición. Mc Graw Hill. México. 1996.

REVISTAS Y PUBLICACIONES

HERNÁNDEZ, Roberto. Firewalls: Seguridad en las redes e Internet. Boletín de Política Informática N° 2. España. 2000.

LIMA de la LUZ, María. Criminalia N° 16 Año L. Delitos Electrónicos. Ediciones Porrua. México. Enero-Julio 1994.

Compumagazine. La sociedad ante la piratería. MP Ediciones. México. Marzo 1998.

Compumagazine. Piratería: informe especial. MP Ediciones. México. Septiembre 1999.

Compumagazine. Delito informático. MP Ediciones. México. Diciembre 2001.

Compumagazine. Hacking. MP Ediciones. México. Julio 2002.

INTERNET

Nota: Por el continuo movimiento de las direcciones de Internet es posible que alguna de las enumeradas a continuación no se encuentren disponibles para consulta.

ANGEL, José de Jesús Ángel. Generación de Números Pseudoaleatorios usados en Sistemas Criptográficos México.
http://www.seguridata.com

BENSON, Christopher. Estrategias de Seguridad. Inobis Consulting Pty Ltd. Microsoft ©Solutions.
http://www.microsoft.com/latam/technet/articulos/200011/art03/

CULP, Scott. "Las Diez Leyes Inmutables de la Seguridad". Microsoft TechNet.
http://www.microsoft.com/technet/security/

http://www.ods.com.ua/win/eng/security/Max_Security

http://www.itlibrary.com/reference/library/1575212684/ewtoc.html.

http://www.hackemate.com.ar/

http://www.kriptopolis.org

http://www.isecom.org/

http:// cactus.fi.uba.ar/crypto/articulos/tcpipProblems.pdf

GONCALVES, Marcus. Firewalls Complete. Beta Book. Editorial McGraw Hill. ISBN 0070246459. EEUU. 1997.
http://www.ods.com.ua/win/eng/security/firewall

HERZOG, Peter Vincent. OpenSource Security Testing Methodology Manual. Versión en1.0. GNU Public License. EEUU.
http://www.ideahamster.org

HOWARD, John D. Thesis: An Analysis of security on the Internet 1989-1995. Carnegie Institute of Technology. Carnegie Mellon University. 1995. EEUU.
http://www.cert.org

Internet Security Policy: A Technical Guide. http://security.tsu.ru

MANUNTA, Giovanni. Presentación del libro Seguridad: una introducción. Consultor y Profesor de Seguridad de Cranfield University. Revista Virtual Seguridad Corporativa.
http://www.seguridadcorporativa.org

CSI (Computer Security Institute): http://www. gocsi.com

DISA (Defense Information System Agency): http://www.disa.mil

Policía Electrónica Española: http://www.policia.es

Organismo Internacional regulador de Internet: http://www.w3.com

True Secure: http:// www.cybertrust.com/

Bufet Almeida Delitos Informáticos: http://www.bufetalmeida.com

Cyber Cursos: http://www.cybercursos.net

IBM Corporation: http://www.ibm.com

JAVA SUN http://www.javasoft.com/security

LINUX http://www.linux.org.es

MICROSOFT http://www.microsoft.com/security

http://www.securiteam.com

http://www.virusattack.com.ar