

INDICE

Dedicatoria	
Agradecimiento	
Introducción	

CAPITULO I

INTERNET

1.1	Antecedentes Históricos	1
1.2	Qué es el Internet	5
1.3	Ventajas del uso de Internet	6
1.3.1	Internet y la telefonía celular	9
1.3.2	Publicidad en el Internet	10
1.3.3	Internet en la educación	11
1.3.4	El Internet en la medicina	13
1.3.5	El comercio electrónico	14
1.4	Desventajas del uso de Internet	16
1.5	Como trabaja Internet	18
1.5.1	Como viaja la información por Internet	20
1.6	Servicios	23
1.6.1	Correo electrónico	24
1.6.1.1	Funcionamiento del e-mail	25
1.6.1.2	Anatomía de un mensaje de correo	26
1.6.1.3	Funcionamiento del software para e-mail	28
1.6.1.4	Funcionamiento de una lista de correo	29
1.6.2	World Wide Web	30
1.6.2.1	Funcionamiento de la World Wide Web	31
1.6.3	Telnet	32
1.6.3.1	Funcionamiento de Telnet	33
1.6.4	Transferencia de archivos	35

1.6.4.1	Funcionamiento de una sesión FTP	36
1.6.5	Internet Relay Chat	38
1.6.5.1	Funcionamiento de IRC	39

CAPITULO II

SEGURIDAD DE UNA RED

2.1	Introducción	41
2.2	Niveles de Seguridad	43
2.2.1	Nivel D1	43
2.2.2	Nivel C1	43
2.2.3	Nivel C2	44
2.2.4	Nivel B1	45
2.2.5	Nivel B2	45
2.2.6	Nivel B3	46
2.2.7	Nivel A	46
2.3	Planeación de seguridad en redes	46
2.4	Política de Seguridad	48
2.4.1	Importancia	48
2.4.2	Aspectos a considerarse en el diseño de una Política de Seguridad	50
2.4.2.1	Análisis del riesgo	51
2.4.2.2	Identificación de amenazas	54
2.4.2.3	Identificación del uso adecuado de los recursos	56
2.4.2.4	Plan de acción cuando se sobrepasa una Política de Seguridad	58
2.4.2.5	Diseño de una Política de Seguridad	60
2.5	Políticas de seguridad del Sitio	60
2.5.1	Factores externos que influyen en las políticas de seguridad	62
2.5.2	Diseño de la Política de Seguridad para la Universidad Técnica del Norte	63

CAPITULO III

SEGURIDAD EN EL SERVIDOR

3.1	Sistema Operativo Linux	80
3.1.1	Qué es Linux	80
3.1.2	Algunas buenas razones para usar Linux	80
3.1.3	Linux como Servidor Internet e Intranet	82
3.2	Seguridad Física	83
3.2.1	Ubicación física del servidor y acceso físico a él	84
3.2.1.1	Centro de Operaciones de Red	85
3.2.2	Contraseña del BIOS y consola	86
3.2.3	Control biométrico de acceso	87
3.2.4	Hardware de red	89
3.2.5	Dispositivos antirrobo	91
3.2.6	Números únicos, marcado y otras técnicas	92
3.3	Instalación del Servidor	93
3.4	Seguridad y Optimización del sistema	94
3.4.1	BIOS	95
3.4.2	Política de Seguridad	96
3.4.3	Longitud del password	96
3.4.4	La cuenta root	97
3.4.5	Establecer el tiempo de inactividad de la cuenta root	97
3.4.6	LILO y el archivo lilo.conf	98
3.4.7	Deshabilitando las teclas CTRL-ALT-DELETE	100
3.4.8	El archivo /etc/services	101
3.4.9	El archivo /etc/security	101
3.4.10	Cuentas especiales	102
3.4.11	Controlando la forma como se inicia un sistema de archivos	103
3.4.12	Iniciando el directorio /boot como de solo lectura	104
3.4.13	Shell logging	105
3.4.14	Proteger los archivos bajo /etc/rc.d/init.d	107
3.4.15	El archivo /etc/rc.d/rc.local	107
3.4.16	Encontrando archivos .rhosts	108

3.5	Pluggable Authentication Modules -PAM	109
3.5.1	La longitud del password	110
3.5.2	Deshabilitar todos los accesos a la consola	112
3.5.3	Tablas de control de acceso	113
3.5.4	Limitar recursos	114
3.5.5	Bloqueando usuarios que pueden ejecutar el comando su al root	115
3.6	Administración de Red TCP/IP	116
3.6.1	Archivos para manejo de red	116
3.6.1.1	Los archivos /etc/sysconfig/network-scripts/ifcfg-ethN	116
3.6.1.2	El archivo /etc/resolv.conf	118
3.6.1.3	El archivo /etc/host.conf	118
3.6.1.4	El archivo /etc/sysconfig/network	119
3.6.1.5	El archivo /etc/sysctl.conf	119
3.6.1.6	El archivo /etc/hosts	120
3.6.2	Asegurando la Red TCP/IP	121
3.6.2.1	Prevenir que el servidor responda a solicitudes ping	122
3.6.2.2	Rechazar solicitudes de broadcast	122
3.6.2.3	Protocolos de ruteo	122
3.6.2.4	Habilitar la protección TCP SYN Cookie	123
3.6.2.5	Deshabilitar ICMP Redirect Acceptance	124
3.6.2.6	Habilitar la protección de mensajes de error dañinos	124
3.6.2.7	Habilitar la protección de IP spoofing	124
3.6.3	Optimizando la Red TCP/IP	125
3.6.3.1	Recursos TCP/IP	125
3.6.3.2	Recursos buffer-space	126
3.6.3.3	Recursos buffer-size	126
3.6.3.4	El parámetro ip_local_port_range	127
3.6.3.5	Los parámetros ipfrag_high_thresh e ipfrag_low_thresh	127
3.7	Firewall de filtrado de paquetes - IPTABLES	127
3.7.1	Como filtrar paquetes entrantes	133
3.7.1.1	Filtrado de dirección origen remota	134
3.7.1.2	Usurpamiento de dirección origen y direcciones ilegales	134
3.7.1.3	Bloquear sitios problemáticos	136

3.7.1.4	Limitar paquetes entrantes a aquellos procedentes de hosts remotos seleccionados.	137
3.7.1.5	Filtrado de dirección destino local	137
3.7.1.6	Filtrado de puerto origen remoto	138
3.7.1.7	Filtrado de puerto destino local	139
3.7.1.8	Filtrado del estado de la conexión TCP entrante	139
3.7.2	Sondeos y exploraciones	140
3.7.2.1	Exploraciones de puerto generales	141
3.7.2.2	Exploraciones de puerto dirigidas	142
3.7.2.3	Destinos comunes en los puertos de servicio	142
3.7.3	Ataques por denegación de servicio	143
3.7.3.1	Ataques masivos mediante SYN TCP	144
3.7.3.2	Ataques masivos mediante ping	145
3.7.3.3	Ataques masivos mediante TCP	145
3.7.3.4	Bombas de redirección ICMP	146
3.7.4	Como filtrar paquetes salientes	146
3.7.4.1	Filtrado de dirección origen local	147
3.7.4.2	Filtrado de dirección destino remota	147
3.7.4.3	Filtrado de puerto origen local	148
3.7.4.4	Filtrado de puerto destino remoto	149
3.7.4.5	Filtrado saliente de estado de la conexión TCP	149
3.7.5.	Creación e instalación del firewall de Linux RedHat 7.1	150
3.7.5.1	Cuál es la política de seguridad del firewall	151
3.7.5.2	Política de seguridad del firewall de la UTN	152
3.7.5.3	Topología	153
3.8	OpenSSL	155
3.8.1	Ventajas de la criptografía	156
3.8.2	Configurar OpenSSL	157
3.8.3	Algunos usos del software OpenSSL	157
3.8.3.1	Herramientas de Administración de OpenSSL	157
3.8.3.1.1	Qué implica la certificación de un Sitio de Web	158
3.8.3.1.2	Qué es un certificado SSL	158
3.8.3.1.3	Cuál es la vigencia de la certificación de un Sitio Web	159
3.8.4	Asegurando OpenSSL	159

3.8.4.1	Cambiando los permisos por default de las claves OpenSSL	159
3.9	OpenSSH	160
3.9.1	Configurando OpenSSH	160
3.9.2	Configuración de OpenSSH para un usuario	161
3.9.3	Algunos usos de OpenSSH	163
3.10	Linux sXid	163
3.10.1	Compilando y optimizando sXid	163
3.10.2	Configurando sXid	165
3.10.2.1	El archivo de configuración de sXid: /etc/sxid.conf	166
3.10.2.2	El archivo Cron de sXid: /etc/cron.daily/sxid	167
3.11	Linux Logcheck	168
3.11.1	Compilando y optimizando Logcheck	169
3.11.2	Configurando Logcheck	171
3.12	Linux PortSentry	172
3.12.1	Compilando y optimizando PortSentry	173
3.12.2	Configurando PortSentry	174
3.12.2.1	El archivo de configuración: /etc /portsentry /portsentry.conf	175
3.12.2.2	El archivo /etc/portsentry/portsentry.ignore	176
3.12.2.3	El archivo de Modos de PortSentry: /etc/ portsentry /portsentry.modes	177
3.12.2.4	El archivo de inicialización de PortSentry: /etc /rc.d/ init.d /portsentry	178
3.12.2.5	El archivo de rotación de PortSentry: /etc /logrotate.d /portsentry	180
3.13	Linux Tripwire	180
3.13.1	Compilando y optimizando Tripwire	181
3.13.2	Configurando Tripwire	183
3.13.2.1	El archivo de configuración de Tripwire: /etc/tw.config	183
3.13.2.2	El archivo Cron de Tripwire: /etc/cron.daily/tripwire	185
3.14	Linux Xinetd	186
3.14.1	Configurando Xinetd	186
3.15	Servidor de Nombres de Dominio - DNS	187
3.15.1	Cómo funciona DNS	189
3.15.2	Configurando ISC BIND & DNS	190
3.15.3	Ejecutando ISC BIND & DNS en una cárcel chroot	190
3.16	Servidor de Correo Electrónico - Sendmail	192

3.16.1	Configurando Sendmail	194
3.16.2	Asegurando Sendmail	194
3.16.2.1	Restringir el shell "smrsh"	195
3.16.2.2	El mensaje de saludo de SMTP	196
3.16.2.3	Cambiar los permisos para los archivos del directorio: /etc/mail	197
3.16.2.4	Hacer inmutables los archivos del directorio: /etc/mail	198
3.17	Protocolo de Acceso a Mensajes Internet - UW IMAP	199
3.17.1	Configurando UW - IMAP	199
3.18	Servidor Proxy - Squid	199
3.18.1	Configurando Squid	201
3.18.2	Asegurando Squid	201
3.18.2.1	Inmunizando el archivo de configuración de Squid	202
3.18.2.2	Memoria física	202
3.19	Servidor FTP - WU FTPD	202
3.19.1	Ejecutando WU FTPD en una cárcel chroot	203
3.19.2	Asegurando WU FTPD	204
3.19.2.1	El comando upload	205
3.19.2.2	El archivo especial .notar	205
3.19.2.3	El comando noretrieve	206
3.20	Servidor Web - Apache	207
3.20.1	Configurando Apache	208
3.20.2	Asegurando Apache	208
3.20.2.1	Cambiando los permisos de algunos archivos y directorios del Servidor Web	209
3.20.2.2	Inmunizar el archivo de configuración: /etc /httpd /conf /httpd.conf	209
3.20.2.3	Crear el archivo .dbpasswd para autenticar usuarios	209
3.21	Servidor para compartir archivos - Samba	321
3.21.1	Configurando Samba	213
3.21.2	Asegurando Samba	213
3.21.2.1	Crear el archivo de password encriptado para conexión de clientes	213
3.21.2.2	Inmunizando el archivo de configuración de Samba	215

CAPITULO IV

FIREWALLS

4.1	Introducción	216
4.2	Objetivos de los firewalls	218
4.3	Beneficios de un firewall	219
4.4	Limitaciones de un firewall	221
4.5	Firewalls de software y hardware	224
4.5.1	Firewalls de software	224
4.5.2	Firewalls de hardware	226
4.6	Clases de firewalls por tipos	227
4.6.1	Basados en filtrado de paquetes	227
4.6.1.1	Beneficios del filtrado de paquetes	231
4.6.1.2	Limitaciones del filtrado de paquetes	232
4.6.2	Basados en proxies	234
4.6.2.1.	Como funcionan los servicios proxy	235
4.6.2.2.	Beneficios de los proxies	237
4.6.2.3	Limitaciones de los proxies	238
4.6.3	Con transparencia	240
4.7	Arquitecturas de firewalls	240
4.7.1	Arquitectura de anfitrión con doble acceso	241
4.7.2	Arquitectura de anfitrión de protección	242
4.7.3	Arquitectura de subred de protección	244
4.8	Aspectos básicos para el diseño de un firewall	246
4.8.1	Postura sobre la política del firewall	246
4.8.2	Política interna de seguridad	247
4.8.3	Costo del firewall	248
4.8.4	Componentes de un firewall	249
4.9	Instalación y administración de un firewall	251
4.10	Mantenimiento del firewall	253
4.10.1	Mantenimiento	254
4.10.2	Monitoreo del sistema	255
4.10.3	Actualización	261

CAPITULO V

METODOLOGÍA PARA LA IMPLEMENTACIÓN DE FIREWALLS DE SOFTWARE

5.1	Protocolos de comunicación	264
5.1.1	El conjunto de protocolos TCP/IP	265
5.1.2	Protocolo de Control de Transmisión (TCP)	268
5.1.2.1	Unidades de datos del protocolo (TCP)	270
5.1.2.2	Establecimiento de conexiones	273
5.1.2.3	Transferencia de datos	275
5.1.3	Cierre de conexiones	276
5.1.4	Protocolo de Datagramas de Usuario (UDP)	278
5.2	Análisis de la Política de Seguridad	279
5.3	Aspectos económicos para la implementación de firewalls de software	285
5.4	Determinación de los componentes de un firewall de software	287
5.5	Elección del tipo de firewall a implementarse	288
5.6	Implementación de un prototipo de firewall de software utilizando Java	290
5.6.1	Puertos	291
5.6.2	Sockets	292
5.6.3	Manejo de comunicaciones en Java	293
5.6.3.1	Servicio orientado a conexión	293
5.6.3.2	Creación del Server Socket	294
5.6.3.3	Espera de conexiones de clientes	295
5.6.3.4	Operaciones en el cliente	295
5.6.3.5	Envío y recepción de datos a través de sockets	296
5.6.4	Prototipo de firewall de software	298
5.7	Evaluación del firewall implementado	307

CAPITULO VI

FIREWALLS DE HARDWARE

6.1	Estudio del Firewall SonicWall (documentación disponible www.sonicWall.com)	312
6.1.1	Introducción	312
6.1.2	Tipos de Firewalls SonicWall	313
a)	SonicWall SOHO2/10/50	313
b)	SonicWall TELE2	316
c)	SonicWall XPRS2	318
d)	SonicWall PRO	320
e)	SonicWall PRO VX	322
6.2	Estudio del Firewalls de WatchGuard (documentación disponible www.watchGuard.com)	324
6.2.1	Introducción.	324
6.2.2	Tipos de Firewalls WatchGuard	324
a)	Firebox SOHO - WatchGuard	325
b)	Firebox 700 – WatchGuard	327
c)	Firebox 1000 – WatchGuard	328
d)	Firebox 2500 – WatchGuard	331
e)	Firebox 4500 – WatchGuard	333
6.3	Estudio del Firewall Cisco Secure PIX 515(documentación disponible www.cisco.com)	336
6.3.1	Introducción.	336
6.3.2	Tipos de Firewalls Cisco Secure PIX 515	338
a)	PIX 515: Software restringido	338
b)	PIX 515: Software no restringido	339
c)	PIX 515: Paquete integrado de protección en caso de error	339
d)	Mejora del PIX-515-R al PIX-515-UR	339
6.4	Comentario sobre el firewall de hardware que se podría instalar en la Universidad Técnica del Norte.	344

CAPITULO VII

CONCLUSIONES Y RECOMENDACIONES

7.1 Verificación de la Hipótesis

7.2 Conclusiones

7.3 Recomendaciones

7.4 Bibliografía

Referencias bibliográficas y gráficas

Anexos (CD ver índice para referencia)