Índice

Prólogo 13

Capítulo I
Introducción a la fortificación 15
1. Introducción a la fortificación de entornos 15
2. Defensa en profundidad 17
Procedimientos, concienciación y políticas 18
Seguridad física 19
Seguridad del perímetro 19
Seguridad en la red interna 21
Seguridad a nivel de servidor 22
Seguridad en la aplicación 22
Seguridad a nivel de la información 23
3. Mínimo privilegio posible 24
4. Mínimo punto de exposición 24
5. Gestión de riesgos 26

Capítulo II
Protección física 29
1. BIOS / UEFI 29
2. Gestor de arranque. GRUB y GRUB2 30
Impacto de un gestor de arranque no protegido 30
Protección del gestor de arranque 33
3. Protección del sistema de ficheros 35
Concepto de acceso a un sistema de ficheros 35

Cifrado de disco o particiones 36
4. Cifrado de ficheros 46
Sobre GPG y su modo de funcionamiento 47
Cifrado simétrico con GPG 48
Cifrado asimétrico con GPG 49
5. Otras protecciones 51

Capítulo III
Protección perimetral 53
1. iptables 53
¿Qué es iptables? 53
Funcionamiento de iptables 53
Decisión de enrutamiento 54
Tablas 54
Agregando reglas con iptables 56
Listando reglas con iptables 58
Eliminando reglas aplicadas 58
Cambiando política por defecto 59
Haciendo las reglas permanentes 59
Firewall de ‘2 patas’ 60
Firewall de ‘3 patas’ 65
Front-ends para iptables 74
iptables e ipv6 75
2. VPN 77
Definición y tipos 77
PPTP, Point-to-point Tunneling Protocol 78
OpenVPN 82
3. Monitorización de la red 99
Icinga 99

Capítulo IV
Protección de la red interna 109

1. Spoofing o suplantación de identidad 109
ARP Poisoning 110
DHCP Spoofing 115
ICMP Redirect 118
2. VLAN 120
Configuración de VLAN en Linux 121
3. IPsec 122
Sobre el funcionamiento de IPsec 123
IPsec con Linux 127
4. IDS Snort 147
Instalación de Snort desde los repositorios oficiales de Debian 149

Capítulo V
Protección de la capa de aplicación 155
1. Jaulas con chroot 155
Prueba de concepto de una jaula con chroot 156
2. Permisos especiales, atributos y ACL 159
Un poco de teoría básica de permisos 159
Permisos especiales 160
Atributos 162
ACL, Access Control List 164
3. Elevación de privilegios con 'sudo' 168
Instalación de sudo y análisis de sus componentes 168
Ejemplo de configuración para sudo 172
4. Limitación de recursos 174
Inicio de sesión, passwords y límites 174
Cuotas de almacenamiento 184
Monit 187
5. Port-Knocking 190
SPA, Single Packet Authorization 191
6. Actualizaciones seguras en Debian 196
¿Es seguro apt? 196

7. HIDS, Host-based Intrusion Detection System 202
OSSEC 202

Capítulo VI
Fortificación de un entorno LAMP 213
1. Instalación de un entorno LAMP 213
2. MySQL 216
Dirección de escucha 216
Carga de ficheros locales 216
Renombrar el usuario root 217
Comprobar existencia de usuarios anónimos 217
Controlar los privilegios de los usuarios 218
mysql_secure_installation 218
3. PHP 218
expose_php 219
display_errors 219
open_basedir 219
disable_functions 220
Deshabilitar RFI 220
Suhosin 221
4. Apache 222
Configuraciones globales 222
Deshabilitar información ofrecida por el servidor 223
Configuraciones por contexto 224
mod_security 228
HTTPS 230

Capítulo VII
Fortificación y seguridad en SSH 235
1. Introducción a SSH 235
Funcionamiento del protocolo 235
La primera conexión 237

\ \ \

2. Configuración del servicio 237
Archivos del servicio 238
Directivas básicas 240
Autenticación con contraseña 243
Clave pública y clave privada 244
Resumen del proceso de conexión 246
3. Aplicaciones con SSH 248
Copia segura con SCP 248
FTP seguro con SFTP 250
SSHFS: El sistema de archivos de SSH 250
X11 forwarding con SSH 252
Fail2ban 252
4. Tunneling 255
SSH: tunneling 255
Túneles TCP/IP con port forwarding mediante SSH 258
5. SOCKS con SSH 258
Habilitando y utilizando SOCKS 259

Capítulo VIII Logging. 263
1. Consideraciones previas 263
2. rsyslogd 264
Clasificación de mensajes. Facility y severity 264
Configuración de rsyslogd 265
3. Rotación de logs 267
Ficheros de configuración de logrotate 267
Output channels y logrotate 270
4. Logging remoto o centralizado 271
Configuración de la máquina A 271
Configuración de la máquina B 271
Otras configuraciones interesantes 273

Capítulo IX
Identidades digitales 275
El riesgo del robo y el segundo factor de autenticación 276
1. Latch 277
Obtención de cuenta y de un identificador de aplicación 278
Instalación del plugin de Latch en GNU/Linux 280
Protegiendo el login de Ubuntu 280
Protegiendo el acceso por SSH 282
Protegiendo las operaciones sudo y su 284
Protegiendo las claves públicas/privadas 285

Índice alfabético 287