

# Índice

<b>Prólogo .....</b>	<b>13</b>
----------------------	-----------

## **Capítulo I**

<b>Introducción a la fortificación.....</b>	<b>15</b>
---	-----------

<b>1. Introducción a la fortificación de entornos .....</b>	<b>15</b>
---	-----------

<b>2. Defensa en profundidad .....</b>	<b>17</b>
--	-----------

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
--	----

<b>3. Mínimo privilegio posible .....</b>	<b>23</b>
---	-----------

<b>4. Mínimo punto de exposición.....</b>	<b>24</b>
---	-----------

<b>5. Gestión de riesgos .....</b>	<b>25</b>
------------------------------------	-----------

## **Capítulo II**

<b>Protección física.....</b>	<b>29</b>
-------------------------------	-----------

<b>1. BIOS / UEFI.....</b>	<b>29</b>
----------------------------	-----------

<b>2. Gestor de arranque. GRUB y GRUB2 .....</b>	<b>30</b>
--	-----------

Impacto de un gestor de arranque no protegido.....	30
--	----

Protección del gestor de arranque.....	33
--	----

<b>3. Protección del sistema de ficheros.....</b>	<b>35</b>
---	-----------

Concepto de acceso a un sistema de ficheros .....	35
---	----

Cifrado de disco o particiones .....	36
--------------------------------------	----

<b>4. Cifrado de ficheros .....</b>	<b>46</b>
Sobre GPG y su modo de funcionamiento .....	47
Cifrado simétrico con GPG .....	48
Cifrado asimétrico con GPG.....	49
<b>5. Otras protecciones .....</b>	<b>51</b>

## Capítulo III

<b>Protección perimetral .....</b>	<b>53</b>
<b>1. iptables.....</b>	<b>53</b>
¿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
<b>2. VPN.....</b>	<b>77</b>
Definición y tipos.....	77
PPTP, Point-to-point Tunneling Protocol .....	78
OpenVPN.....	82
<b>3. Monitorización de la red .....</b>	<b>99</b>
Icinga .....	99
<b>4. Nginx: Utilizando proxy inverso .....</b>	<b>107</b>

## Capítulo IV

<b>Protección de la red interna .....</b>	<b>113</b>
---	------------

<b>1. Spoofing o suplantación de identidad.....</b>	<b>113</b>
ARP Poisoning.....	114
DHCP Spoofing .....	119
ICMP Redirect.....	122
<b>2. VLAN .....</b>	<b>124</b>
Configuración de VLAN en Linux .....	125
<b>3. IPsec .....</b>	<b>126</b>
Sobre el funcionamiento de IPsec.....	127
IPsec con Linux .....	131
<b>4. IDS Snort .....</b>	<b>151</b>
Instalación de Snort desde los repositorios oficiales de Debian .....	153

## Capítulo V

<b>Protección de la capa de aplicación.....</b>	<b>159</b>
<b>1. Jaulas con chroot .....</b>	<b>159</b>
Prueba de concepto de una jaula con chroot.....	160
<b>2. Permisos especiales, atributos y ACL .....</b>	<b>163</b>
Un poco de teoría básica de permisos.....	163
Permisos especiales .....	164
Atributos .....	166
ACL, Access Control List.....	168
<b>3. Elevación de privilegios con ‘sudo’ .....</b>	<b>172</b>
Instalación de sudo y análisis de sus componentes .....	172
Ejemplo de configuración para sudo.....	176
<b>4. Limitación de recursos .....</b>	<b>178</b>
Inicio de sesión, passwords y límites.....	178
Cuotas de almacenamiento .....	188
Monit.....	191
<b>5. Port-Knocking .....</b>	<b>194</b>
SPA, Single Packet Authorization.....	195
<b>6. Actualizaciones seguras en Debian .....</b>	<b>200</b>
¿Es seguro apt? .....	200

<b>7. HIDS, Host-based Intrusion Detection System.....</b>	<b>206</b>
OSSEC .....	206
<b>8. Linux Capabilities: Mejorando el bit SUID / SGID.....</b>	<b>216</b>
<b>9. Listado de buenas prácticas para evitar ‘privesc’ .....</b>	<b>219</b>

## Capítulo VI

<b>Fortificación de un entorno profesional.....</b>	<b>221</b>
<b>1. Instalación de un entorno LAMP .....</b>	<b>221</b>
<b>2. MySQL.....</b>	<b>224</b>
Dirección de escucha .....	224
Carga de ficheros locales .....	224
Renombrar el usuario root .....	225
Comprobar existencia de usuarios anónimos .....	225
Controlar los privilegios de los usuarios .....	226
mysql_secure_installation.....	226
<b>3. PHP.....</b>	<b>226</b>
expose_php .....	227
display_errors .....	227
open_basedir .....	227
disable_functions .....	228
Deshabilitar RFI.....	228
Suhosin .....	229
<b>4. Apache.....</b>	<b>230</b>
Configuraciones globales.....	230
Deshabilitar información ofrecida por el servidor.....	231
Configuraciones por contexto .....	232
mod_security.....	236
HTTPS .....	238
MongoDB .....	245

## Capítulo VII

<b>Fortificación y seguridad en SSH .....</b>	<b>251</b>
---	------------

<b>1. Introducción a SSH .....</b>	<b>251</b>
Funcionamiento del protocolo .....	251
La primera conexión .....	253
<b>2. Configuración del servicio .....</b>	<b>253</b>
Archivos del servicio .....	254
Directivas básicas .....	256
Autenticación con contraseña .....	259
Clave pública y clave privada.....	260
Resumen del proceso de conexión.....	262
<b>3. Aplicaciones con SSH .....</b>	<b>264</b>
Copia segura con SCP.....	264
FTP seguro con SFTP .....	266
SSHFS: El sistema de archivos de SSH .....	266
X11 forwarding con SSH.....	268
Fail2ban .....	268
<b>4. Tunneling.....</b>	<b>271</b>
SSH: tunneling.....	271
Túneles TCP/IP con port forwarding mediante SSH.....	274
<b>5. SOCKS con SSH.....</b>	<b>274</b>
Habilitando y utilizando SOCKS.....	275
<b>Capítulo VIII</b>	
<b>Logging.....</b>	<b>285</b>
<b>1. Consideraciones previas.....</b>	<b>285</b>
<b>2. rsyslogd.....</b>	<b>286</b>
Clasificación de mensajes. Facility y severity .....	286
Configuración de rsyslogd .....	287
<b>3. Rotación de logs .....</b>	<b>289</b>
Ficheros de configuración de logrotate.....	289
Output channels y logrotate .....	291
<b>4. Logging remoto o centralizado.....</b>	<b>292</b>
Configuración de la máquina A.....	293

Configuración de la máquina B .....	293
Otras configuraciones interesantes .....	294

## **Capítulo IX**

### **Identidades digitales .....297**

El riesgo del robo y el segundo factor de autenticación .....	298
---	-----

#### **1. Latch .....299**

Obtención de cuenta y de un identificador de aplicación .....	300
---	-----

Instalación del plugin de Latch en GNU/Linux.....	302
---	-----

Protegiendo el login de Ubuntu .....	302
--------------------------------------	-----

Protegiendo el acceso por SSH.....	304
------------------------------------	-----

Protegiendo las operaciones sudo y su .....	306
---	-----

Protegiendo las claves públicas/privadas.....	307
---	-----

### **Índice alfabético .....309**

### **Índice de imágenes .....315**

### **Otros libros publicados.....319**