

# Índice general

Índice general	III
<b>1 Introducción.</b>	<b>3</b>
<b>2 Seguridad física.</b>	<b>5</b>
2.1. Acceso a despachos. . . . .	5
2.2. Control de accesos. . . . .	7
2.3. Instalaciones. . . . .	8
<b>3 Servicios.</b>	<b>15</b>
3.1. ¿Qué servicios tenemos instalados? . . . . .	16
<b>4 Tcpwrappers.</b>	<b>27</b>
4.1. Configuración. . . . .	29
<b>5 Anti troyanos.</b>	<b>37</b>
5.1. Chkrootkit. . . . .	38
5.2. Rootkit Hunter. . . . .	40
<b>6 Logs.</b>	<b>43</b>
6.1. syslog. . . . .	44
6.2. Logwatch. . . . .	48
6.3. Rotación de logs. . . . .	48
<b>7 Cortafuegos.</b>	<b>53</b>
7.1. Estudio previo. . . . .	54
7.2. iptables. . . . .	60
7.3. Política por defecto. . . . .	60
7.4. Inicialización. . . . .	62

7.5. Cadena INPUT. . . . .	63
7.6. Scripts de inicio. . . . .	70
<b>8 Control de cambios.</b>	<b>77</b>
8.1. Tripwire. . . . .	78
<b>9 Comprobación remota de puertos.</b>	<b>85</b>
9.1. Nmap. . . . .	86
9.2. Nessus. . . . .	88
<b>10 GPG.</b>	<b>97</b>
10.1. Generación de claves. . . . .	98
10.2. Exportar e importar claves. . . . .	99
10.3. Administración de claves. . . . .	99
10.4. Codificación de documentos. . . . .	101
10.5. Firma de documentos. . . . .	101
<b>11 Análisis forense.</b>	<b>103</b>
11.1. Sleuthkit. . . . .	105
11.2. FIRE . . . . .	108
<b>Bibliografía</b>	<b>117</b>