

# ÍNDICE

---

---

<b>INTRODUCCIÓN .....</b>	<b>15</b>
<b>CAPÍTULO 1. CONCEPTOS BÁSICOS .....</b>	<b>17</b>
1.1. Amenazas de seguridad .....	18
1.1.1. Ataques pasivos .....	19
1.1.2. Ataques activos .....	20
1.2. Tipos de ataques .....	20
<b>CAPÍTULO 2. BUSCAR UN VECTOR DE ATAQUE .....</b>	<b>23</b>
2.1. Localizar el objetivo .....	24
2.1.1. Bases de datos WHOIS .....	24
2.1.2. Consultas DNS inversas .....	25
2.1.3. Transferencias de zonas DNS no autorizadas .....	26
2.1.4. Barridos de pings .....	28
2.1.5. Trazado de rutas .....	28
2.2. Analizar el objetivo .....	29
2.2.1. Identificar los servicios TCP y UDP .....	30
2.2.2. Identificar el sistema operativo .....	32
2.2.2.1. xprobe2 .....	33
2.2.2.2. nmap .....	34
2.2.3. Identificar las versiones de los servicios .....	35
<b>CAPÍTULO 3. HACKING DE SISTEMAS.....</b>	<b>37</b>
3.1. Escaneo de vulnerabilidades.....	37
3.1.1. Microsoft Baseline Security Analyzer (MBSA) .....	40
3.1.2. GFI Languard.....	41
3.1.3. Retina Network Security Scanner .....	41

3.1.4.	Shadow Security Scanner .....	42
3.1.5.	Nessus.....	43
3.1.5.1.	Instalación .....	43
3.1.5.2.	Configuración.....	44
3.1.5.3.	Utilización en GNU/Linux .....	45
3.1.5.4.	Utilización en Windows .....	47
3.1.6.	SARA.....	49
3.1.7.	Contra medidas .....	51
3.2.	Explotar las vulnerabilidades del sistema (Metasploit) .....	51
3.2.1.	Instalación.....	53
3.2.2.	Buscar sistemas vulnerables .....	54
3.2.3.	Utilización mediante consola.....	55
3.2.4.	Utilización mediante interfaz web .....	56
3.2.5.	Contra medidas .....	58
3.3.	Ataques contra contraseñas de sistemas Windows .....	58
3.3.1.	Obtención del fichero SAM.....	62
3.3.2.	Crackeando el SAM (tablas rainbow).....	67
3.3.3.	Obtener la contraseña.....	69
3.3.4.	LiveCD ophcrack.....	70
3.3.5.	Contra medidas .....	72
3.4.	Ataques contra contraseñas de sistemas GNU/Linux .....	74
3.4.1.	John the Ripper .....	74
3.4.2.	@stack LC5 .....	75
3.4.3.	Contra medidas .....	77

## **CAPÍTULO 4. HACKING DE REDES .....** **79**

4.1.	Introducción.....	79
4.2.	Man in the middle.....	79
4.2.1.	¿Cómo funciona ARP? .....	81
4.2.2.	Windows (Cain & Abel) .....	83
4.2.2.1.	ARP spoofing.....	83
4.2.2.2.	DNS spoofing y phishing .....	86
4.2.2.3.	Robando contraseñas.....	86
4.2.3.	GNU/Linux (arpoison).....	87
4.2.3.1.	Etthercap .....	88
4.2.4.	Contra medidas .....	91
4.3.	Sniffers .....	91
4.3.1.	Sniffers.....	91
4.3.2.	Sniffer de VoIP .....	92
4.3.2.1.	Cain & Abel .....	93
4.3.2.2.	Wireshark .....	94
4.3.3.	Otros sniffers .....	95
4.3.4.	Detectar sniffers en una red .....	96
4.3.5.	Contra medidas .....	97

4.4. Técnicas de ocultación y navegación anónima (torpark).....	97
4.4.1. Instalación.....	98
4.4.2. Utilización.....	100
4.4.3. Comprobación.....	100
4.5. Rompiendo redes inalámbricas.....	101
4.5.1. Detección de redes inalámbricas.....	103
4.5.2. Ataques a redes abiertas.....	104
4.5.3. Ataques WEP.....	105
4.5.4. Ataques WPA/PSK.....	108
4.5.5. Airoscript.....	110
4.5.6. Contramedidas.....	111
<b>CAPÍTULO 5. HACKING DE SERVIDORES WEB.....</b>	<b>113</b>
5.1. Introducción.....	113
5.2. Búsqueda de vulnerabilidades.....	114
5.2.1. Nikto.....	114
5.2.1.1. Introducción.....	114
5.2.1.2. Utilización.....	115
5.2.1.3. Ejemplo.....	116
5.2.2. Http Analyzer.....	116
5.2.3. Achilles.....	118
5.3. XSS (Cross Site Scripting).....	119
5.3.1. Ejemplo.....	122
5.3.2. Contramedidas.....	125
5.4. Remote File Inclusión (RFI) y Local File Inclusión (LFI).....	126
5.4.1. Ejemplo.....	127
5.4.2. Contramedidas.....	128
5.5. Inyección de SQL.....	128
5.5.1. Introducción.....	128
5.5.2. Explotar la vulnerabilidad.....	129
5.5.3. Blind SQL y otras lindezas.....	131
5.5.4. Absinthe.....	134
5.5.5. Contramedidas.....	137
<b>CAPÍTULO 6. HACKING DE APLICACIONES.....</b>	<b>139</b>
6.1. Introducción.....	139
6.2. Crack.....	140
6.2.1. Introducción.....	140
6.3. KeyLoggers.....	144
6.3.1. Keyloggers hardware (Keyghost).....	144
6.3.2. Keyloggers software (perfect Keylogger).....	146
6.3.2.1. Instalación.....	146
6.3.2.2. Logs.....	148
6.3.2.3. Configuración.....	148
6.3.2.4. Infectar un ejecutable con el keylogger.....	149

6.3.2.5. Comprobación.....	150
6.3.3. Contramedidas .....	151
6.4. Troyanos.....	152
6.4.1. Introducción.....	152
6.4.1.1. Partes de un troyano .....	153
6.4.1.2. Tipos de troyanos .....	153
6.4.2. Primeros pasos .....	154
6.4.2.1. Primeros pasos .....	154
6.4.2.2. Crear el troyano.....	154
6.4.2.3. Conectarnos a un equipo infectado.....	158
6.4.3. Contramedidas .....	159
6.5. Rootkits .....	160
6.5.1. Instalación y configuración de un Rootkit .....	161
6.5.2. Contramedidas .....	162
6.6. Virus.....	162
6.6.1. Ejemplo de un virus .....	163
6.6.2. Generadores de virus .....	166
6.7. Ocultación para el antivirus.....	167
6.7.1. Cifrado del ejecutable .....	167
6.7.2. Modificar la firma .....	168
<b>APÉNDICE I. HERRAMIENTAS Y URL REFERENCIADAS.....</b>	<b>171</b>
<b>APÉNDICE II. RETOS DE SEGURIDAD.....</b>	<b>175</b>
<b>PÁGINA WEB .....</b>	<b>177</b>
<b>ÍNDICE ALFABÉTICO.....</b>	<b>179</b>