

# Indice generale

<b>Introduzione .....</b>	<b>vii</b>
<b>Ringraziamenti .....</b>	<b>ix</b>
<b>Capitolo 1    Che cos'è un hacker .....</b>	<b>1</b>
Etica e identità hacker .....	3
Vademecum hacker .....	6
<b>Capitolo 2    La cassetta degli attrezzi .....</b>	<b>7</b>
Conoscenze informatiche .....	7
Strumenti software .....	9
Da Linux in poi .....	10
Tutto quel che serve .....	11
Sicurezza a due facce .....	14
Hardware .....	16
Per iniziare bene .....	20
<b>Capitolo 3    Come funziona un programma .....</b>	<b>21</b>
Scrivere un programma .....	22
Via, verso il codice macchina .....	27
Reverse engineering in 10 minuti .....	29
Un codice al bivio .....	31
Questione di vulnerabilità .....	32
<b>Capitolo 4    Come funziona una rete .....</b>	<b>39</b>
Una rete in poche parole .....	39
Protocolli .....	40
Porte .....	42
Come si trasmettono i dati .....	45
Qualcosa in più sull'OSI Model .....	46
Gli elementi di una rete .....	47
Quasi tutto non è tutto (e ci mancherebbe!) .....	49

<b>Capitolo 5</b>	<b>Un perfetto, potente, laboratorio hacker .....</b>	<b>51</b>
	Installare Kali Linux .....	51
	Installazione come app Windows.....	52
	Installazione in macchina virtuale.....	54
	Usare Kali Linux con Workstation Player.....	57
	Usare Kali Linux con VirtualBox.....	60
	Usare Kali Linux “live” da chiavetta USB .....	61
	Installare Wireshark .....	64
	Installare Metasploit .....	67
<b>Capitolo 6</b>	<b>Tutto sul tuo obiettivo.....</b>	<b>71</b>
	Prime informazioni.....	72
	Operatori di Google.....	73
	Open Source Intelligence .....	75
	Controlli rapidi.....	85
	Whois: di chi è il sito?.....	85
	Netcraft: qualcosa in più .....	86
	Nslookup: IP, ma non solo .....	87
	Analisi delle porte .....	89
	SYN scan .....	90
	Scansione dettagliata .....	93
	Scansione su porta specifica .....	94
	Scansione UDP .....	94
<b>Capitolo 7</b>	<b>A caccia di vulnerabilità .....</b>	<b>97</b>
	Trovare vulnerabilità .....	97
	Scovare vulnerabilità con Nessus.....	98
	Installare Nessus.....	99
	Usare una vulnerabilità.....	104
	Scansione di Web Application.....	104
<b>Capitolo 8</b>	<b>Un primo attacco.....</b>	<b>107</b>
	Metasploit.....	107
	Avviare Metasploit.....	109
	Una macchina ancora più vulnerabile.....	118
	Anatomia di un attacco .....	121
<b>Capitolo 9</b>	<b>Attacchi (un po’) più complessi.....</b>	<b>125</b>
	Attaccare una macchina Linux .....	125
	Attacco dall’Alfa all’Omega.....	128
	Un attacco completo a Windows.....	130
<b>Capitolo 10</b>	<b>Primi attacchi web .....</b>	<b>137</b>
	Costruire una backdoor .....	137
	WordPress, SQL Injection e dintorni.....	142
	Trovare vulnerabilità in WordPress.....	145
	A caccia di un exploit .....	146
	SQL Injection .....	149
<b>Capitolo 11</b>	<b>Qualche attacco avanzato .....</b>	<b>155</b>
	Cross-Site Scripting (XSS) .....	155

Test XSS.....	156
Preparare un attacco XSS.....	158
Cross-Site Request Forgery (CSRF) .....	161
ARP Poisoning.....	161
Un po' di teoria.....	161
In che cosa consiste l'ARP Poisoning.....	163
Preparare l'attacco.....	164
Lanciare un attacco ARP Poisoning .....	166
Privilege escalation .....	170
Privilege escalation in Windows.....	170
Privilege escalation in Linux.....	174
<b>Capitolo 12 Attacchi wireless .....</b>	<b>179</b>
Lo strumento giusto.....	179
Attivare il monitor mode .....	181
Scansione delle reti wireless.....	181
Qualcosa su WEP, WPA e WPA2.....	183
Attacco dizionario a una rete WPA/WPA2.....	183
Il segreto dell'attacco WPA/WPA2 .....	184
Intercettare il WPA handshake.....	184
Deauthentication attack .....	185
Attacco dizionario .....	186
Attacco al WPS.....	187
La vulnerabilità di partenza .....	187
L'attacco in pratica.....	187
Attacco Rogue Access Point.....	188
Creare un server malevolo .....	191
<b>Capitolo 13 Qualche attacco fisico.....</b>	<b>193</b>
WiFi Pineapple.....	194
Installazione.....	196
Attacco Man in the Middle con WiFi Pineapple Nano.....	200
Bypassare password di Windows e Mac.....	202
Attacco BadUSB.....	203
<b>Indice analitico.....</b>	<b>205</b>