Sommario

Prefazione ..... **VII**

Introduzione ..... **IX**

1) Prima della partita - La configurazione **1**

Impostare una penetration testing box 1
Hardware 2
Software commerciale 3
Kali Linux (http://www.kali.org/) 4
L'host VM Windows 11
Riepilogo 14

2) Prima dello snap - Eseguire la scansione del network **15**

Scansione esterna 15
La Passive Discovery 16
Discover script (in passato si chiamavano Backtrack Script) (Kali Linux) 17
La active discovery esterna/interna 25
Il procedimento per la scansione di un network 25
La scansione delle applicazioni web 37
Il procedimento delle scansioni web 38
Eseguire la scansione di applicazioni web 39
Riepilogo 49

3) Il drive - Sfruttare i risultati delle scansioni **51**

Metasploit (http://www.metasploit.com) (Windows/Kali Linux) 52
I passaggi fondamentali quando si configurano attacchi remoti con Metasploit 52
Eseguire ricerche tramite Metasploit (utilizzare la buona vecchia vulnerabilità ms08- 067) 53
Gli script 55
Esempio di warftp 56
Riepilogo 58

4) Il lancio - Risultati manuali di applicazioni web **61**

I penetration test di applicazioni web 61
SQL injection 62
Cross-Site Scripting (xss) 73
Cross-Site Request Forgery (CSRF) 82

I token delle sessioni 86
Ulteriore convalida fuzzing/input 89
Testare con la logica funzionale/applicativa (business logic) 94
Conclusione 95

5) Il passo laterale - Muoversi nel network 97

Nel network senza credenziali 98
responder.py (https://github.com/SpiderLabs/Responder) (Kali Linux) 98
Con qualsiasi credenziale di dominio (non-admin) 103
Le Group Policy Preference 103
Estrarre credenziali con testo in chiaro 106
Consigli per la fase successiva all'exploitation 109
Con qualsiasi account amministrativo locale o di amministratore del dominio 110
Impossessarsi del network con credenziali e psexec 110
Attaccare il Domain Controller 118
Dopo l'exploitation con PowerSploit (https://github.com/mattifestation/PowerSploit) (Windows) 121
Dopo l'exploitation con powershell (https://code.google.com/p/nishang/) (Windows) 128
L'ARP (Address Resolution Protocol) poisoning 131
ipv4 132
ipv6 137
Passaggi da eseguire dopo l'ARP spoofing 139
sidejacking 139
Hamster/Ferret (Kali Linux) 139
Proxy between host 148
Conclusione 148

6) Lo screen - L'ingegneria sociale 149

I domini doppelganger 149
Gli attacchi smtp 150
Gli attacchi ssh 151
Lo spear phishing 154
Metasploit pro - Il modulo per il phishing 154
Social Engineering Toolkit (Kali Linux) 157
Inviare campagne di spear phishing in massa 162
L'ingegneria sociale with Microsoft Excel 164
Conclusione 168

7) Il kickoff calciato verso un lato del campo - Attacchi che richiedono l'accesso fisico 169

Sfruttare le reti wireless 169
La modalità passiva - Identificazione e riconoscimento 171
Gli attacchi attivi 173
Gli attacchi fisici 183
Clonare schede 183
Pentesting drop box 184
L'ingegneria sociale fisica 188
Conclusione 189

8) Il quarterback sneak - Eludere l'antivirus.....191
Eludere l'antivirus 191
Nascondere WCE all'antivirus (Windows) 192
Python 197
Conclusione 204

9) Squadre speciali - Craccare, exploit e altri trucchetti.....205
Craccare le password 205
John the Ripper (JtR) 207
oclhashcat 208
Cercare le vulnerabilità 213
Searchsploit (Kali Linux) 213
BugTraq 215
Exploit-DB 216
Eseguire query in Metasploit 216
Trucchi e segreti 217
Gli script RC all'interno di Metasploit 217
Scavalcare UAC 219
Scavalcare i filtri web dei vostri domini 220
Windows XP - I trucchi FTP della vecchia scuola 221
Nascondere i vostri file (Windows) 221
Mantenere nascosti questi file (Windows) 223
Windows 7 e 8 - Caricare file sull'host 225

10) Dopo la partita - Analisi e resoconti.....227
Creare un resoconto 228
Elenco delle mie migliori pratiche e dei concetti alla base per la creazione dei resoconti 228

A) Continuare a imparare 231

B) Note finali 239

C) Ringraziamenti speciali 241