

Indice generale

Ringraziamenti	xiii
Prefazione	xv
Introduzione	xvii
Perché leggere questo libro?	xvii
Installazione di Python.....	xviii
I contenuti del libro	xviii
L'autore	xxi
Il revisore tecnico	xxi
Capitolo 1 Impostazione	1
Il laboratorio virtuale	1
Configurazione di VirtualBox.....	2
Configurazione di pfSense	3
Configurazione della rete interna	4
Impostazione di pfSense.....	6
Configurazione di Metasploitable.....	8
Configurazione di Kali Linux.....	9
Configurazione del desktop Ubuntu Linux	10
Il vostro primo hacking: sfruttare una backdoor in Metasploitable.....	10
Ottenere l'indirizzo IP del server Metasploitable	12
Utilizzare la backdoor per ottenere l'accesso.....	12
Parte I Le basi delle connessioni di rete	15
Capitolo 2 Cattura del traffico con l'ARP Spoofing.....	17
Come vengono trasmessi i dati in Internet	17
Pacchetti.....	17

	Indirizzi MAC.....	18
	Indirizzi IP.....	18
	Tabelle ARP.....	20
	Attacchi ARP Spoofing.....	20
	Esecuzione di un attacco ARP Spoofing.....	21
	Rilevamento di un attacco ARP Spoofing.....	25
	Esercizi.....	27
	Ispezionare le tabelle ARP.....	27
	Implementare uno spoofer ARP in Python.....	27
	MAC Flooding.....	28
Capitolo 3	Analisi del traffico catturato.....	29
	I pacchetti e lo stack dei protocolli di Internet.....	29
	Lo stack a cinque livelli dei protocolli Internet.....	32
	Visualizzazione dei pacchetti in Wireshark.....	35
	Analisi dei pacchetti raccolti dal firewall.....	40
	Cattura del traffico sulla porta 80.....	40
	Esercizi.....	42
	pfSense.....	42
	Esplorazione dei pacchetti in Wireshark.....	42
Capitolo 4	Creazione di shell TCP e botnet.....	45
	Socket e comunicazioni fra processi.....	45
	Handshake TCP.....	46
	Una reverse shell TCP.....	48
	Accesso alla macchina della vittima.....	50
	Scansione alla ricerca delle porte aperte.....	50
	Sfruttamento di un servizio vulnerabile.....	52
	Scrittura di un client reverse shell.....	52
	Scrittura di un server TCP che ascolta le connessioni client.....	54
	Caricamento della reverse shell sul server Metasploitable.....	55
	Botnet.....	56
	Esercizi.....	58
	Un server bot multIClient.....	58
	Scansioni SYN.....	59
	Rilevamento delle scansioni XMas.....	60
Parte II	Crittografia.....	61
Capitolo 5	Crittografia e ransomware.....	63
	Crittografia.....	63
	One-Time Pad.....	64
	Generatori di numeri pseudocasuali.....	67
	Modalità di cifratura a blocchi non sicure.....	68
	Modalità di cifratura a blocchi sicure.....	69

Crittografia e decrittografia di un file	71
Crittografia dei messaggi di posta elettronica	72
Crittografia a chiave pubblica	72
La teoria alla base dell'algoritmo Rivest-Shamir-Adleman	73
Operazioni matematiche per i calcoli di RSA	74
Crittografia di un file con RSA	75
OAEP (Optimal Asymmetric Encryption Padding)	78
Scrittura di un ransomware	78
Esercizi	81
Il server ransomware	81
Estensione del client ransomware	82
Codici irrisolti	83

Capitolo 6 TLS e Diffie-Hellman85

Il protocollo TLS	86
Autenticazione del messaggio	87
Autorità di certificazione e firme	88
Autorità di certificazione	89
Utilizzo di Diffie-Hellman per calcolare una chiave condivisa.....	91
Passo 1: generazione dei parametri condivisi.....	91
Passo 2: generazione della coppia di chiavi pubblica-privata.....	92
Passo 3: condivisioni di chiavi e nonce	94
Passo 4: calcolo della chiave segreta condivisa	95
Passo 5: derivazione della chiave	96
Attaccare l'algoritmo Diffie-Hellman	96
Diffie-Hellman a curva ellittica	97
La matematica delle curve ellittiche.....	97
Algoritmo double-and-add	98
Scrittura di socket TLS	100
Il socket client sicuro	100
Il socket server sicuro.....	101
SSL Stripping e HSTS Bypass	102
Esercizio: aggiungete la crittografia al vostro server ransomware...103	

Parte III Ingegneria sociale.....105

Capitolo 7 Phishing e deepfake107

Un sofisticato e subdolo attacco di ingegneria sociale	107
E-mail fasulle	108
Ricerca DNS di un server di posta.....	109
Comunicare con SMTP.....	109
Scrivere un e-mail spoofer	111
Spoofing SMTPS delle e-mail.....	113
Siti web fasulli	115
Creazione di video deepfake	117

Accesso a Google Colab	118
Importazione dei modelli di machine learning	118
Esercizi	121
Clonazione vocale	121
Phishing su larga scala	121
Auditing SMTP	122

Capitolo 8 Scansione dei target.....125

Analisi dei collegamenti	125
Maltego	127
Database di credenziali trapelate	130
SIM Jacking.....	131
Google Dorking	131
Scansione dell'intera Internet	132
Masscan.....	133
Shodan	136
Limiti IPv6 e NAT	137
Il protocollo Internet versione 6 (IPv6).....	138
Il sistema NAT	138
Database di vulnerabilità	140
Scanner di vulnerabilità.....	142
Esercizi	144
Scansioni nmap.....	145
Discover	146
Scrivere uno strumento OSINT	148

Parte IV Sfruttamento delle informazioni.....149

Capitolo 9 Fuzzing: ricerca di vulnerabilità zero-day151

Caso di studio: sfruttamento della vulnerabilità	
Heartbleed OpenSSL	151
Creazione di un exploit	152
Avvio del programma	153
Scrittura del messaggio Client Hello	154
Lettura della risposta del server.....	156
Creazione della richiesta di Heartbeat dannosa	157
Lettura del contenuto della memoria sottratta	158
Scrittura della funzione di exploit	158
Composizione	159
Fuzzing.....	159
Un esempio semplificato.....	160
Scrittura di un fuzzer	160
American Fuzzy Lop	162

Esecuzione simbolica	166
Esecuzione simbolica del programma di test	166
Limiti dell'esecuzione simbolica	167
Esecuzione simbolica dinamica.....	168
Utilizzo di DSE per decifrare una password.....	171
Creazione di un file binario eseguibile	171
Installazione ed esecuzione di Angr	172
Il programma Angr	173
Esercizi	174
Capture the Flag con Angr.....	174
Fuzzing di protocolli web	174
Fuzzing di un progetto open-source.....	176
Implementazione di un vostro motore di esecuzione concolico.....	176

Capitolo 10 Realizzazione di Trojan.....177

Caso di studio: replicazione di Drovorub utilizzando Metasploit ..	178
Costruzione del server di hacking	179
Costruzione del client per la vittima	180
Upload dell'impianto.....	181
Utilizzo dell'agente di hacking.....	181
Perché abbiamo bisogno di un modulo kernel per la vittima ..	182
Nascondere un impianto in un file legittimo	183
Creazione di un trojan	183
Ospitare il Trojan	187
Download del file infetto	187
Controllo dell'impianto	189
Elusione dell'antivirus utilizzando gli encoder	190
L'encoder Base64.....	191
Scrivere un modulo Metasploit	193
Shikata Ga Nai	194
Creazione di un trojan per Windows	196
Nascondere il Trojan in Minesweeper.....	196
Nascondere il Trojan in un documento Word (o in un altro file innocuo).....	197
Creazione di un trojan per Android.....	198
Decostruzione dell'APK per visualizzare l'impianto.....	198
Ricostruzione e firma dell'APK.....	200
Test del trojan per Android.....	202
Esercizi	205
Evil-Droid.....	205
Scrittura un nuovo impianto Python.....	206
Celare un impianto.....	208
Create un eseguibile specifico per la piattaforma	208

Capitolo 11 Creazione e installazione di rootkit Linux211

Scrittura di un modulo del kernel di Linux	212
Backup della macchina virtuale Kali Linux.....	212
Scrivere il Codice	213
Compilazione ed esecuzione del modulo del kernel.....	214
Alterazione delle chiamate di sistema.....	216
Come funzionano le chiamate di sistema.....	216
Hooking delle syscall	219
Hooking della syscall di chiusura	220
Nascondere i file.....	224
La struct linux_dirent.....	224
Scrittura del codice di hooking.....	225
Utilizzo di Armitage per violare un host e installare un rootkit ...	227
Scansione della rete.....	228
Violazione di un host.....	229
Installazione di un rootkit	230
Esercizi	231
Il keylogger	231
Un modulo che si auto-nasconde.....	233

Capitolo 12 Sottrazione e decifrazione di password.....235

SQL Injection.....	235
Sottrazione delle password dal database di un sito web	237
Enumerazione dei file raggiungibili sul server web	237
Esecuzione di un attacco SQL Injection.....	238
Scrittura di uno strumento di SQL Injection	240
Le richieste HTTP	240
Scrivere il programma di iniezione	242
Utilizzo di SQLMap	243
Hash delle password	246
Anatomia dell'hashing MD5	247
Violazione dei codici hash	249
Complicare i codici hash con un nonce	250
Costruzione di un cracker di codici hash con salt	251
Strumenti di cracking dei codici hash e a forza bruta.....	251
John the Ripper	252
Hashcat	252
Hydra.....	253
Esercizi	254
NoSQL Injection	254
Web Login a forza bruta	255
Burp Suite.....	256

Capitolo 13 Exploit Cross-Site Scripting (XSS).....259

XSS (Cross-Site Scripting)	259
In che modo il codice JavaScript può essere dannoso.....	261
Attacchi Stored XSS	263
Attacchi Reflected XSS	265
Ricerca di vulnerabilità con OWASP Zed Attack Proxy	266
Utilizzo dei payload di Browser Exploitation Framework	268
Iniezione dell'hook di BeEF	268
Esecuzione di un attacco di ingegneria sociale.....	269
Dal browser alla macchina su cui opera	271
Caso di studio: sfruttamento di una versione non aggiornata del browser Chrome	271
Installazione di rootkit tramite exploit su un sito web.....	272
Esercizio: caccia ai bug in un programma Bug Bounty.....	275

Parte V Controllare la rete277**Capitolo 14 Pivoting ed escalation dei privilegi.....279**

Pivoting da un dispositivo dual-homed.....	279
Configurazione di un dispositivo dual-homed	280
Connessione di una macchina alla vostra rete privata	282
Pivoting con Metasploit.....	284
Scrivere un proxy di hacking	286
Estrazione dei codici hash delle password in Linux	288
Dove si trovano in Linux i nomi utente e le password?	288
Esecuzione di un attacco a escalation dei privilegi con Dirty COW	290
Esercizi	293
Aggiunta della funzionalità NAT al vostro dispositivo dual-homed.....	293
Lecture consigliate sull'escalation dei privilegi in Windows	293

Capitolo 15 Muoversi nella rete Windows aziendale295

Creazione di un laboratorio virtuale Windows.....	296
Estrazione dei codici hash delle password con mimikatz	296
Passaggio del codice hash con NT LAN Manager	298
Esplorazione della rete Windows aziendale	300
Attacco al servizio DNS.....	301
Attacco ad Active Directory e ai servizi LDAP.....	303
Scrittura di un client per query LDAP	304
Utilizzo di SharpHound e Bloodhound per l'enumerazione LDAP.....	306
Attacco a Kerberos.....	308

L'attacco Pass-the-Ticket	310
Gli attacchi Golden Ticket e DC Sync	310
Esercizio: Kerberoasting	312

Capitolo 16 Prossimi passi.....313

Impostazione di un ambiente di hacking rinforzato	313
Restare anonimi con Tor e Tails.....	314
Configurazione di un VPS (Virtual Private Server)	315
Configurazione di SSH.....	316
Installazione degli strumenti di hacking.....	318
Rafforzamento del server.....	319
Verifica del server rinforzato	321
Altri argomenti.....	322
Software Defined Radio	322
Attacco all'infrastruttura cellulare	322
Airgap	323
Reverse engineering.....	323
Strumenti di hacking fisico	324
Indagini forensi.....	324
Hacking di sistemi industriali	324
Calcolo quantistico	325
Siate connessi.....	325

Indice analitico.....327