Indice generale

Ringraziamenti ..... **xiii**

Introduzione ..... **xv**

Che cosa troverete in questo libro xv
Gli esercizi di scripting xvi
Come usare questo libro xvii
Gli autori xvii
Il revisore tecnico xviii

Capitolo 1 La shell bash **1**

Configurazione dell'ambiente 1
Accesso alla shell bash 2
Installazione di un editor di testo 2
Esplorazione della shell 2
Controllo delle variabili d'ambiente 3
Esecuzione di comandi Linux 4
Gli elementi di uno script bash 6
La riga shebang 6
Commenti 7
Comandi 8
Esecuzione 8
Debug 8
Sintassi di base 9
Variabili 10
Assegnamento e accesso alle variabili 10
Annullamento dell'assegnamento delle variabili 11
Ambito (visibilità) delle variabili 12
Operatori aritmetici 13
Array 14
Stream 15
Operatori di controllo 16

Operatori di redirezione 17
Argomenti posizionali....20
Richiedere l'input 22
Codici di uscita 23
Esercizio 1 – Registrare il nome e la data 24
Riepilogo 25

Capitolo 2 Controllo del flusso ed elaborazione del testo....27

Operatori di test 27
Condizioni if 28
Collegare più condizioni....31
Test del successo del comando 31
Controllo di condizioni aggiuntive 32
Funzioni 33
Restituzione dei valori....33
Accettare argomenti....34
Cicli e controlli....35
L'istruzione while 35
L'istruzione until....37
L'istruzione for 38
Le istruzioni break e continue....39
Istruzioni case 41
Elaborazione e parsing del testo....42
Filtraggio con grep 42
Filtraggio con awk....43
Modifica degli stream con sed 44
Controllo dei job 45
Gestione del background e del foreground....45
Mantenere i lavori in esecuzione dopo il logout 46
Personalizzazioni per i penetration tester 47
Collocazione degli script nei percorsi ricercabili....47
Abbreviare i comandi con gli alias 47
Personalizzazione del profilo ~/.bashrc....48
Importazione di script personalizzati 49
Cattura delle attività nella sessione del terminale 49
Esercizio 2 – Ping di un dominio 50
Riepilogo 50

Capitolo 3 Creazione di un laboratorio di hacking....51

Precauzioni di sicurezza del laboratorio 51
Installazione di Kali....52
L'ambiente target 53
Installazione di Docker e Docker Compose 54
Clonazione del repository del libro 55
Installazione dei container Docker 56
Test e verifica dei container....56

L'architettura della rete 57
La rete pubblica 57
La rete aziendale 58
Interfacce di rete Kali 58
Le macchine 59
Gestione del laboratorio 59
Spegnimento 59
Rimozione 60
Ricostruzione 60
Accesso alle singole macchine laboratorio 60
Installazione di altri strumenti di hacking 61
WhatWeb 61
RustScan 62
Nuclei 62
dirsearch 63
Linux Exploit Suggester 2 63
Gitjacker 63
pwncat 64
LinEnum 64
unix-privesc-check 65
Assegnazione di alias agli strumenti di hacking 66
Riepilogo 66

Capitolo 4 Ricognizione 69

Creazione di elenchi di target riutilizzabili 69
Indirizzi IP consecutivi 70
Possibili sottodomini 71
Individuazione degli host 73
ping 73
Nmap 75
arp-scan 76
Esercizio 3 – Ricezione di alert sui nuovi host 76
Scansione delle porte 78
Nmap 78
RustScan 80
Netcat 81
Esercizio 4 – Organizzare i risultati della scansione 82
Rilevamento di nuove porte aperte 83
Acquisizione dei banner 85
Utilizzo dell'acquisizione attiva del banner 86
Rilevamento delle risposte HTTP 87
Utilizzo degli script Nmap 89
Rilevamento dei sistemi operativi 90
Analisi dei siti web e di JSON 92
Riepilogo 94

Capitolo 5 Scansione delle vulnerabilità e fuzzing 95

Scansione di siti web con Nikto 95
Creazione di uno scanner di indicizzazione delle directory 97
Identificazione delle voci sospette del file robots.txt 98
Esercizio 5 – Esplorare gli endpoint non indicizzati 99
Forza bruta sulle directory con dirsearch 100
Esplorazione dei repository Git 102
Clonazione del repository 102
Visualizzazione dei commit con git log 103
Estrazione delle informazioni dal registro git 103
Ispezione dei file del repository 104
Scansione delle vulnerabilità con Nuclei 105
Il funzionamento dei template 105
Scrivere un template personalizzato 106
Applicazione del template 107
Esecuzione di una scansione completa 108
Esercizio 6 – Analizzare i risultati di Nuclei 111
Fuzzing per i file nascosti 112
Creazione di un elenco di possibili nomi di file 112
Fuzzing con ffuf 113
Fuzzing con Wfuzz 114
Valutazione dei server SSH con l'engine di scripting di Nmap 115
Esercizio 7 – Combinare più strumenti per trovare problemi in FTP 116
Riepilogo 116

Capitolo 6 Acquisire una web shell 119

Vulnerabilità dell'upload di file arbitrari 120
Fuzzing per l'upload di file arbitrari 121
Bypassare i controlli di upload dei file 123
File poliglotti dannosi 125
Altre tecniche di bypass 126
Upload di file con Burp Suite 127
Installazione di web shell 130
Individuazione di vulnerabilità all'attraversamento di directory 131
Caricamento di payload dannosi 132
Esecuzione di comandi dalla web shell 133
Esercizio 8 – Creare un'interfaccia per la web shell 134
Limiti delle web shell 136
Mancanza di persistenza 136
Mancanza di risposte in tempo reale 136
Funzionalità limitate 136
Iniezione di comandi del sistema operativo 136

Esercizio 9 – Creare un'interfaccia per l'iniezione di comandi 139
Bypassare le restrizioni all'iniezione di comandi.....141
Offuscamento e codifica 141
Globbing.....141
Riepilogo 143

Capitolo 7 Shell inverse 145

Come funzionano le reverse shell.....145
Controlli in ingresso e in uscita.....146
Payload e listener shell 146
La sequenza di comunicazione 146
Esecuzione di una connessione.....148
Impostazione di un listener Netcat.....148
Creazione di un payload 148
Invio e inizializzazione del payload 149
Esecuzione dei comandi 150
In ascolto con pwncat.....151
Bypassare i controlli di sicurezza.....152
Crittografia e incapsulamento del traffico 153
Alternare le porte di destinazione.....154
Generazione di shell TTY con dispositivi pseudo-terminali 156
Il modulo pty di Python 156
socat.....157
Attacchi a file binari post-exploit 157
Inviare Netcat.....158
Uploading di file con pwncat.....159
Scaricare file binari da siti attendibili 159
Esercizio 10 – Mantenere una connessione continua a reverse shell.....160
Accesso iniziale a forza bruta.....161
Esercizio 11 – Attacco a forza bruta su un server SSH.....162
Riepilogo 164

Capitolo 8 Raccolta di informazioni locali.....165

Gli standard nella gerarchia del file system 166
L'ambiente della shell 167
Variabili d'ambiente.....167
Informazioni sensibili nei profili Bash 167
Utenti e gruppi.....168
Account locali 168
Gruppi locali 169
Accesso alla cartella home 170
Shell valide 171
Processi.....172
Visualizzazione dei file di processo 172
Esecuzione di ps 174

Esame dei processi radice 175
Il sistema operativo 175
Esercizio 12 – Script per rilevare il sistema operativo Linux 176
Sessioni di login e attività dell'utente 176
Raccolta delle sessioni utente 176
Investigare sui comandi eseguiti 177
Reti 178
Interfacce di rete e percorsi 178
Connessioni e vicini 181
Regole del firewall 182
File di configurazione dell'interfaccia di rete 183
Risolutori di domini 183
Installazioni di software 184
Storage 186
Dispositivi a blocchi 186
Il file Filesystem Tab 188
File log 189
File log di sistema 189
File log delle applicazioni 189
Esercizio 13 – Cercare ricorsivamente i file log 190
Kernel e bootloader 190
File di configurazione 191
Task pianificati 193
Cron 193
At 195
Esercizio 14 – Script per job di cron per cercare le credenziali 196
Hardware 196
Virtualizzazione 198
Utilizzo di strumenti dedicati 198
Strumenti disponibili in loco 199
Raccolta di informazioni con LinEnum 199
Esercizio 15 – Aggiungere funzionalità a LinEnum 200
Riepilogo 201

Capitolo 9 Escalation dei privilegi 203

Che cos'è l'escalation dei privilegi? 203
Autorizzazioni per i file e le directory di Linux 204
Visualizzazione delle autorizzazioni 204
Impostazione delle autorizzazioni 205
Creazione di liste di controllo degli accessi per i file 206
Visualizzazione di SetUID e SetGID 208
Impostazione dello sticky bit 208
Trovare i file in base alle autorizzazioni 209
Exploit: impostazione errata di SetUID 210
Cercare le credenziali 212
Password e segreti 212

Chiavi private 214
Esercizio 16 – Forzare le passphrase delle chiavi GnuPG 217
Esaminare la configurazione di sudo 218
Abusare dell'editor di testo 221
Download di file sudoers dannosi 221
Dirottare i file eseguibili modificando il PATH 223
Esercizio 17 – Alterare un job di cron 225
Trovare gli exploit del kernel 227
SearchSploit 227
Linux Exploit Suggester 2 228
Attacco agli account adiacenti 228
Escalation dei privilegi con GTFOBins 230
Esercizio 18 – Mapping degli exploit GTFOBins sui file binari locali 231
Automazione dell'escalation dei privilegi 232
LinEnum 232
unix-privesc-check 232
MimiPenguin 233
Linuxprivchecker 233
Bashark 233
Riepilogo 234

Capitolo 10 Persistenza 235

I nemici della persistenza dell'accesso 235
Modifica delle configurazioni dei servizi 236
System V 236
systemd 239
Alterazione di moduli di autenticazione plug-in 240
Esercizio 19 – Programmare uno script bash pam_exec dannoso 240
Generazione di chiavi SSH non autorizzate 241
Riutilizzo degli account di default del sistema 242
Avvelenamento dei file d'ambiente di bash 243
Esercizio 20 – Intercettare i dati manomettendo il profilo 245
Sottrazione delle credenziali 246
Hacking di un editor di testo 247
Comandi eseguiti in streaming 249
Alterare un sudo non proprio sicuro 250
Esercizio 21 – Dirottare le utility delle password 253
Distribuzione di pacchetti dannosi 253
I pacchetti DEB 253
Packaging di software innocuo 255
Conversione di formato dei pacchetti con alien 256
Esercizio 22 – Scrivere un programma per installare pacchetti dannosi 256
Riepilogo 258

Capitolo 11 Sondaggio della rete e movimenti laterali 259

Esplorazione della rete aziendale.....260
Mappatura dei servizi.....260
Frequenza di apertura delle porte.....262
Esercizio 23 – Scansione delle porte in base alle frequenze 263
Exploit sugli script di Cron per volumi condivisi.....264
Verifica dell'exploit.....266
Controllo del contesto dell'utente.....267
Esercizio 24 – Impiantare una reverse shell sul server di backup...267
Exploit su un server di database.....268
Port forwarding 268
Attacco a forza bruta con Medusa 269
Backdoor di WordPress 270
Esecuzione di comandi SQL con Bash 271
Esercizio 25 – Eseguire comandi della shell tramite WordPress 272
Violazione di un server Redis 272
Comandi CLI grezzi.....273
Metasploit 274
Esposizione dei file del database 276
Estrazione di informazioni sensibili 278
Uploading di una web shell con SQL.....279
Riepilogo 280

Capitolo 12 Elusione delle difese ed esfiltrazione.....281

Controlli di difesa 281
Sicurezza degli endpoint 282
Sicurezza delle applicazioni e delle API 283
Sicurezza della rete.....284
Honeypot.....284
Raccolta e aggregazione dei file log 285
Esercizio 26 – Controllare gli host.....286
Mascheramento dei processi dannosi 286
Precaricamento di librerie.....286
Mimetizzazione del processo.....288
Mascheramento del processo.....289
Esercizio 27 – Rotazione del nome dei processi 290
Inserimento di file nella memoria condivisa 292
Disabilitazione dei controlli di sicurezza runtime 293
Manipolazione della cronologia.....295
Manomissione dei metadati della sessione.....296
Nascondere i dati.....297
Codifica 298
Crittografia.....299
Esercizio 28 – Scrivere funzioni per cifrari a sostituzione.....300
Esfiltrazione 301

TCP puro....301
Protocollo DNS....302
Siti di archiviazione di testi....304
Webhook di Slack....304
Frammentazione dei file....305
Numero di righe....305
Dimensioni....306
Frammenti....306
Esercizio 29 – Frammentare i file e pianificare l'esfiltrazione....307
Riepilogo....308

Indice analitico....309