Indice generale

Autori e revisore tecnico vii

Il revisore tecnico vii
Ringraziamenti viii

Introduzione xi

Rassegna del libro e della tecnologia xi
Come è organizzato il libro xii
Per chi è questo libro xiii
Gli strumenti di cui avrete bisogno xiii
Che cosa c'è sul sito web xiv
Riepilogo xiv

Capitolo 1 Introduzione a Wireshark 1

Che cos'è Wireshark? 1
Un momento ideale per usare Wireshark? 2
Evitare di lasciarsi sopraffare 3
L'interfaccia utente di Wireshark 3
Pannello Packet List 5
Pannello Packet Details 5
Pannello Packet Bytes 8
Filtri 8
Filtri di cattura 9
Filtri di visualizzazione 12
Riepilogo 16

Capitolo 2 Configurazione del laboratorio 17

Kali Linux 18
Virtualizzazione 19
Terminologia e concetti di base 20
Vantaggi della virtualizzazione 20

VirtualBox 21
Installare VirtualBox 21
Installare il VirtualBox Extension Pack 27
Creare una macchina virtuale Kali Linux 29
Installare Kali Linux 36
Il W4SP Lab 42
Requisiti 42
Qualche parola su Docker 43
Che cos'è GitHub? 44
Creare l'utente del laboratorio 45
Installare il W4SP Lab sulla macchina virtuale Kali 45
Impostare il W4SP Lab 48
La rete del Lab 49
Riepilogo 51

Capitolo 3 Elementi fondamentali 53

Reti 54
I livelli OSI 54
Networking fra macchine virtuali 57
Sicurezza 58
La triade della sicurezza 59
Sistemi di rilevamento e prevenzione delle intrusioni 59
Falsi positivi e falsi negativi 60
Malware 60
Spoofing e poisoning 60
Analisi di pacchetti e protocolli 62
La storia di un'analisi di protocollo 62
Porte e protocolli 66
Riepilogo 67

Capitolo 4 Cattura dei pacchetti 69

Sniffing 70
Modalità promiscua 70
Avviare la prima cattura 71
TShark 75
Trattare con la rete 79
Macchina locale 79
Sniffing di localhost 80
Sniffing su interfacce di macchina virtuale 84
Sniffing con hub 88
Porte SPAN 90
Network tap 92
Bridge Linux trasparenti 93
Reti wireless 96
Caricare e salvare file di cattura 98
Formati di file 98

Buffer circolari e file multipli 101
File di cattura recenti 106
Dissettori 107
W4SP Lab: gestire traffico HTTP non standard 108
Filtrare nomi di file SMB 109
Colorazione dei pacchetti 113
Vedere le catture di altri 116
Riepilogo 116

Capitolo 5 Diagnosi degli attacchi 119

Tipo di attacco: Man-in-the-Middle 120
Perché gli attacchi MitM sono efficaci 120
Come vengono condotti gli attacchi MitM: ARP 121
W4SP Lab: condurre un attacco MitM ARP 123
W4SP Lab: condurre un attacco MitM DNS 130
Come prevenire attacchi MitM 136
Tipo di attacco: Denial of Service 137
Perché gli attacchi DoS sono efficaci 137
Come vengono condotti gli attacchi DoS 139
Come prevenire attacchi DoS 143
Tipo di attacco: Advanced Persistent Threat 144
Perché gli attacchi APT sono efficaci 144
Come vengono condotti gli attacchi APT 145
Esempio di traffico APT in Wireshark 145
Come prevenire attacchi APT 149
Riepilogo 150

Capitolo 6 Wireshark offensivo 151

Metodologia d'attacco 151
Ricognizione con Wireshark 153
Sfuggire ai sistemi IPS/IDS 154
Montaggio e frammentazione di sessioni 156
Puntare all'host, non all'IDS 157
Coprire le tracce e preparare vie d'uscita 157
Exploitation 158
Impostare il W4SP Lab con Metasploitable 158
Lanciare la console Metasploit 159
L'exploit VSFTP 159
Debug con Wireshark 161
Shell in Wireshark 162
Flusso TCP che mostra una bind shell 163
Flusso TCP che mostra una reverse shell 169
Avviare ELK 174
Cattura remota su SSH 176
Riepilogo 176

Capitolo 7 TLS, USB, keylogger e grafici di rete.....179

Decifrare SSL/TLS 179
Decifrare SSL/TLS con chiavi private 181
Decifrare SSL/TLS con chiavi di sessione 184
USB e Wireshark 187
Catturare traffico USB in Linux 188
Catturare traffico USB in Windows 190
Keylogger in TShark 193
Rappresentazione grafica della rete 196
Lua con la libreria Graphviz 197
Riepilogo 202

Capitolo 8 Scripting con Lua 203

Perché Lua? 203
Elementi fondamentali dello scripting 204
Variabili 206
Funzioni e blocchi 207
Cicli 209
Condizionali 210
Installazione 211
Controllare se esiste il supporto per Lua 211
Inizializzazione di Lua 213
Impostazione per Windows 213
Impostazione per Linux 213
Strumenti 214
Hello World con TShark 216
Script per il conteggio dei pacchetti 217
Script per la cache ARP 221
Creare dissettori per Wireshark 224
Tipi di dissettori 224
Perché serve un dissettore 224
Esperimento 232
Estendere Wireshark 233
Script per la direzione dei pacchetti 233
Uno script per segnalare sospetti 235
Snooping di trasferimenti di file SMB 237
Riepilogo 240

Indice analitico.....241