

SADRŽAJ

PREDGOVOR Katie Moussouris	xi
-----------------------------------	-----------

ZAHVALNICE	xv
-------------------	-----------

UVOD	xvii
-------------	-------------

Zašto da čitate ovu knjigu	xviii
Šta se nalazi u knjizi	xviii
Kako da koristite knjigu	xx
Kontakt	xx

1	
OSNOVE UMREŽAVANJA	1

Arhitektura i protokoli mreža	1
Paket internet protokola (IPS)	2
Kapsuliranje podataka	4
Zaglavlja, podnožja i adrese	5
Prenos podataka	6
Rutiranje u mreži	7
Moj model za analizu mrežnih protokola	8
Zaključak	10

2	
HVATANJE SAOBRAĆAJA APLIKACIJE	11

Pasivno hvatanje mrežnog saobraćaja	12
Kratak pregled aplikacije Wireshark	12
Alternativne pasivne tehnike hvatanja saobraćaja	14
Praćenje sistemskih poziva	14
Uslužni program strace u Linuxu	16
Praćenje mrežnih veza pomoću alatke DTrace	16
Process Monitor u Windowsu	18
Prednosti i nedostaci pasivnog hvatanja saobraćaja	19
Aktivno hvatanje mrežnog saobraćaja	20
Mrežni posrednici	21
Posrednik za prosleđivanje priključaka	21
SOCKS posrednik	24
HTTP posrednici	29
Prosleđivanje HTTP posrednika	30
Reverzni HTTP posrednik	32
Zaključak	35

3	STRUKTURE MREŽNIH PROTOKOLA	37
Strukture binarnih protokola		38
Numerički podaci		38
Logičke vrednosti		41
Bit indikatori		42
Binarni format endian		42
Tekstualni i drugi čitljivi podaci		43
Binarni podaci sa promenljivom dužinom		47
Datumi i vremena		50
Vreme u POSIX-u / Unixu		50
FILETIME u Windowsu		50
Obrazac TLV		51
Multipleksiranje i fragmentacija		51
Informacije o mrežnoj adresi		53
Strukturirani binarni formati		53
Strukture tekstualnih protokola		55
Numerički podaci		55
Tekstualne logičke vrednosti		55
Datumi i vremena		56
Podaci sa promenljivom dužinom		56
Strukturirani tekstualni formati		56
Kodiranje binarnih podataka		59
Heksadecimalno kodiranje		59
Sistem Base64		60
Zaključak		62
4	NAPREDNO HVATANJE SAOBRAĆAJA APLIKACIJE	63
Menjanje putanje saobraćaja		64
Praćenje mrežne putanje		64
Tabele za rutiranje		65
Konfigurisanje rutera		66
Rutiranje u Windowsu		67
Rutiranje u *nix sistemima		67
Prevođenje mrežnih adresa		68
Izvorna NAT tabela		68
Konfigurisanje izvorne NAT tabele u Linuxu		69
Odredišna NAT tabela		70
Prosleđivanje saobraćaja ka mrežnom prolazu		71
Lažiranje DHCP saobraćaja		71
Trovanje ARP protokola		74
Zaključak		78
5	ANALIZA SAOBRAĆAJA	79
Aplikacija koja proizvodi saobraćaj: SuperFunkyChat		80
Pokretanje servera		80
Pokretanje klijenata		81
Komunikacija između klijenata		81

Kratak pregled analize pomoću alatke Wireshark	82
Generisanje mrežnog saobraćaja i hvatanje paketa	83
Osnovna analiza	84
Čitanje sadržaja TCP sesije	85
Identifikovanje strukture paketa pomoću opcije Hex Dump	86
Prikaz pojedinačnih paketa	87
Određivanje strukture protokola	88
Testiranje pretpostavki	89
Seciranje protokola pomoću jezika Python	90
Izrada Wireshark disektora u jeziku Lua	96
Definisanje disektora	98
Seciranje u jeziku Lua	99
Raščlanjivanje paketa poruke	100
Korišćenje posrednika za aktivnu analizu saobraćaja	103
Podešavanje posrednika	103
Analiza protokola pomoću posrednika	106
Dodavanje osnovnog raščlanjivanja protokola	107
Menjanje ponašanja protokola	108
Zaključak	110

6

OBRNUTO INŽENJERSTVO APLIKACIJA

111

Kompajleri, interpreter i asembleri	112
Interpretirani jezici	112
Kompajlirani jezici	113
Statičko i dinamičko povezivanje	113
Arhitektura x86	114
Arhitektura skupa instrukcija	114
Registri procesora	116
Tok programa	119
Osnove operativnih sistema	119
Formati izvršnih datoteka	120
Odeljci	120
Procesi i programske niti	121
Interfejs za umrežavanje operativnog sistema	121
Binarni interfejs za aplikacije	124
Statičko obrnuto inženjerstvo	125
Kratko uputstvo za korišćenje besplatnog disasemblera IDA Pro	126
Analiza promenljivih i argumenata steka	128
Identifikovanje ključnih funkcionalnosti	129
Dinamičko obrnuto inženjerstvo	135
Definisanje tačaka prekida	136
Prozori programa za otkrivanje grešaka	136
Gde se definišu tačke prekida	137
Upravljeni jezici obrnutog inženjerstva	138
.NET aplikacije	138
Korišćenje alatke ILSpy	139
Java aplikacije	142
Kako se radi sa maskiranjima	143
Izvori informacija o obrnutom inženjerstvu	144
Zaključak	145

7	BEZBEDNOST MREŽNIH PROTOKOLA	147
Algoritmi za šifrovanje		148
Supstitucione šifre		149
XOR šifrovanje		150
Generatori slučajnih brojeva		151
Šifrovanje simetričnim ključem		151
Blokovske šifre		152
Režimi blokovskog šifrovanja		155
Dopunjavanje u blokovskom šifrovanju		158
Napad „padding oracle”		159
Šifre toka		161
Šifrovanje asimetričnim ključem		162
RSA algoritam		162
RSA dopunjavanje		164
Algoritam Diffie–Hellman za razmenu ključeva		165
Algoritmi za potpisivanje		166
Kriptografski algoritmi za heširanje		167
Asimetrični algoritmi za potpisivanje		167
Kodovi za proveru verodostojnosti poruke		168
Infrastruktura javnog ključa		171
X.509 sertifikati		172
Provera lanca sertifikata		173
Studija slučaja: bezbednost transportnog protokola		174
Usaglašavanje za TLS vezu		175
Početno pregovaranje		176
Provera identiteta u krajnjoj tački		176
Uspostavljanje šifrovanja		178
Ispunjavanje bezbednosnih zahteva		179
Zaključak		180

8	IMPLEMENTIRANJE MREŽNIH PROTOKOLA	181
Ponavljanje postojećeg uhvaćenog mrežnog saobraćaja		181
Hvatanje saobraćaja alatkom Netcat		182
Korišćenje jezika Python za ponovno slanje uhvaćenog UDP saobraćaja		184
Promena namene posrednika za analizu		185
Promena namene postojećeg izvršnog koda		190
Promena namene koda u .NET aplikacijama		191
Promena namene koda u Java aplikacijama		196
Neupravljanje izvršne datoteke		198
Šifrovanje i rad sa TLS-om		202
Šifrovanje na delu		202
Dešifrovanje TLS saobraćaja		203
Zaključak		209

9

OSNOVNI UZROCI BEZBEDNOSNE RANJIVOSTI

211

Klase bezbednosne ranjivosti	212
Daljinsko izvršavanje koda	212
Uskraćivanje usluga	212
Obelodanjivanje informacija	213
Zaobilaženje provere identiteta	213
Premošćavanje ovlašćenja	213
Ranjivosti zbog oštećenja u memoriji	214
Bezbedni i nebezbedni programski jezici	214
Prekoraćenja memorijskog bafera	215
Indeksiranje bafera izvan granica	220
Napad proširivanjem podataka	221
Otkazi pri dinamičkoj dodeli memorije	222
Podrazumevani akreditivi ili akreditivi upisani u kôd	222
Nabrajanje korisnika	223
Greška tokom pristupa resursima	224
Kanonizovanje	224
Preobimne greške	226
Napadi iscrpljivanjem memorije	227
Napadi iscrpljivanjem skladišta	228
Napadi iscrpljivanjem procesora	229
Algoritamska složenost	229
Podesiva kriptografija	231
Ranjivosti zbog znakovnog niza formata	232
Injektovanje komande	233
SQL injektovanje	233
Zamena znakova za kodiranje teksta	235
Zaključak	236

10

PRONALAZENJE I ISKORIŠĆAVANJE BEZBEDNOSNIH RANJIVOSTI 237

Faz testiranje	238
Najjednostavniji faz test	238
Faz testiranje sa mutiranjem	239
Generisanje testnih slučajeva	239
Trijaža ranjivosti	240
Aplikacije za otkrivanje grešaka	240
Kako da povećate verovatnoću pronalazjenja osnovnog uzroka otkaza	247
Iskorišćavanje najčešćih ranjivosti	250
Iskorišćavanje ranjivosti zbog oštećivanja podataka u memoriji	250
Ranjivost zbog proizvoljnog upisa u memoriju	257
Pisanje koda komandnog okruženja	260
Početak	260
Jednostavna tehnika za otkrivanje grešaka	263
Sistemske pozivi	264
Izvršavanje drugih programa	268
Generisanje koda komandnog okruženja pomoću alatke Metasploit	270
Ublažavanje zloupotreba oštećenja podataka u memoriji	271
Sprečavanje izvršavanja	272
Sprečavanje zloupotrebe povratno orijentisanog programiranja	273

Randomizacija rasporeda adresnog prostora (ASLR)	275
Otkrivanje prekoračenja steka pomoću memorijskih kolačića	278
Zaključak	281

KOMPLETI ALATKI ZA ANALIZU MREŽNIH PROTOKOLA 283

Alatke za pasivno hvatanje saobraćaja i analizu mrežnog protokola	283
Microsoft Message Analyzer	284
TCPDump and LibPCAP	284
Wireshark	285
Aktivno hvatanje i analiza mrežnog saobraćaja	286
Canape	286
Canape Core	287
Mallory	287
Povezivanje i testiranje protokola na mreži	288
Hping	288
Netcat	288
Nmap	288
Testiranje veb-aplikacija	289
Burp Suite	289
Zed Attack Proxy (ZAP)	290
Mitmproxy	290
Radni okviri za faz testiranje, generisanje paketa i iskorišćavanje ranjivosti	291
American Fuzzy Lop (AFL)	291
Kali Linux	292
Metasploit Framework	292
Scapy	293
Sulley	293
Lažiranje i preusmeravanje na mreži	293
DNSMasq	293
Ettercap	293
Obrnuto inženjerstvo izvršnih datoteka	294
Java Decompiler (JD)	294
IDA Pro	295
Hopper	295
ILSpy	296
.NET Reflector	296

SPISAK TERMINA KORIŠĆENIH U KNJIZI 299

INDEKS 303