

Spis treści

O autorze 10

O recenzencie 10

Przedmowa 11

Podziękowania 15

Wstęp 17

Po co czytać tę książkę? 17

Co znajdziesz w tej książce? 18

Jak korzystać z tej książki? 19

Skontaktuj się ze mną 20

1. Podstawy sieci komputerowych 21

Architektura sieci i protokoły sieciowe 21

Zestaw protokołów internetowych 23

Enkapsulacja danych 25

Nagłówki, stopki i adresy 25

Transmisja danych 27

Trasowanie w sieci 28

Mój model analizy protokołów sieciowych 29

Podsumowanie 31

2. Przechwytywanie ruchu sieciowego 33

Bierne przechwytywanie ruchu sieciowego 34

Wireshark - podstawy 34

Alternatywne techniki biernego przechwytywania 37

Śledzenie wywołań funkcji systemowych 37

Linuksowy program strace 38

Monitorowanie połączeń sieciowych za pomocą programu DTrace 39

Monitor procesów Windows 41

Zalety i wady biernego przechwytywania 43

Czynne przechwytywanie ruchu sieciowego 43

Proxy sieciowe 44

Proxy z przekierowaniem portów 44

Proxy SOCKS 48

Proxy HTTP 53

Proxy przekazujące HTTP 54

Proxy odwrotne HTTP 57

Podsumowanie 60

3. Struktura protokołów sieciowych 61

Struktury protokołów binarnych 62

Dane numeryczne 62

Tekst i dane czytelne dla człowieka 68

Binarne dane o zmiennej długości 72

Data i czas 75

Czas w systemach Unix/POSIX 76

Znacznik FILETIME w systemie Windows 76

Wzorzec typ - długość - wartość 76

Multipleksowanie i fragmentacja 77

Informacje sieciowe 79

Strukturalne formaty binarne 80

Struktury protokołów tekstowych 81

Dane numeryczne 81

Wartości logiczne (boolowskie) 82

Data i czas 82

Dane zmiennej długości 82

Strukturalne formaty tekstowe 83

Kodowanie danych binarnych 86

Kodowanie szesnastkowe 86

Base64 87

Podsumowanie 89

4. Zaawansowane techniki przechwytywania ruchu sieciowego 91

Przetrasowywanie ruchu 92

Program Traceroute 92

Tablice trasowania 93

Konfigurowanie routera 95

Włączanie trasowania w Windows 96

Włączanie trasowania w systemach uniksowych 96

NAT - translacja adresów sieciowych 97

Włączanie SNAT 97

Konfigurowanie SNAT w Linuksie 98

Włączanie DNAT 99

Przekierowanie ruchu do bramy 101

Ingerencja w DHCP 101

Infekowanie ARP 104

Podsumowanie 107

5. Analiza "na drucie" 109

SuperFunkyChat - aplikacja generująca ruch 109

Uruchamianie serwera 110

Uruchamianie aplikacji klienckiej 110

Komunikacja między aplikacjami klienckimi 111

Wireshark na kursie kolizyjnym 112

Generowanie ruchu sieciowego i przechwytywanie pakietów 113

Podstawowa analiza 115

Odczytywanie zawartości sesji TCP 115

Identyfikowanie elementów struktury pakietu na podstawie zrzutu szesnastkowego 117

Podgląd pojedynczych pakietów 117

Odkrywanie struktury protokołu 119

Weryfikowanie założeń 120

Dysekcja protokołu przy użyciu języka Python 121

Dysektory dla Wiresharka w języku Lua 127

Tworzenie dysektora 130

Dysekcja protokołu w języku Lua 131

Parsowanie pakietu komunikatu 132

Czynne analizowanie ruchu za pomocą proxy 135

Konfigurowanie proxy 136

Analiza protokołu przy użyciu proxy 138

Podstawowe parsowanie protokołu 140

Zmiany w zachowaniu się protokołu 142

Podsumowanie 144

6. Inżynieria wsteczna 147

Kompilatory, interpretery i asemblery 148

Języki interpretowane 149

Języki kompilowane	149
Konsolidacja statyczna kontra konsolidacja dynamiczna	150
Architektura x86	150
Zestaw instrukcji maszynowych	151
Rejestry procesora	152
Przepływ sterowania w programie	156
Podstawy systemów operacyjnych	157
Formaty plików wykonywalnych	157
Sekcje pliku wykonywalnego	158
Procesy i wątki	159
Interfejs sieciowy systemu operacyjnego	159
ABI - binarny interfejs aplikacji	162
Statyczna inżynieria wsteczna	164
Krótki przewodnik po IDA	164
Analiza stosu - zmienne lokalne i parametry	167
Rozpoznawanie kluczowych funkcji	168
Dynamiczna inżynieria wsteczna	174
Punkty przerwań	175
Okna debuggera	175
Gdzie ustawiać punkty przerwań?	177
Inżynieria wsteczna a kod zarządzany	177
Aplikacje .NET	178
Dekompilacja za pomocą ILSpy	179
Aplikacje Javy	182
Inżynieria wsteczna a obfuskacja kodu	184
Zasoby dotyczące inżynierii wstecznej	185
Podsumowanie	185

7. Bezpieczeństwo protokołów sieciowych 187

Algorytmy szyfrowania 188

Szyfry podstawieniowe 189

Szyfrowanie XOR 190

Generatory liczb (pseudo)losowych 191

Kryptografia symetryczna 192

Szyfry blokowe 193

Tryby operacyjne szyfrów blokowych 196

Dopełnianie szyfrowanych bloków 199

Atak na dopełnienie z udziałem wyroczni 200

Szyfry strumieniowe 202

Kryptografia asymetryczna 202

Algorytm RSA 204

Dopełnianie w szyfrowaniu RSA 206

Wymiana kluczy Diffiego-Hellmana 206

Algorytmy podpisów 208

Algorytmy haszowania 208

Asymetryczne algorytmy podpisów 209

Kody uwierzytelniania komunikatów 210

Infrastruktura klucza publicznego 213

Certyfikaty X.509 213

Weryfikacja certyfikatów w łańcuchu 215

Analiza przypadku: protokół TLS 216

Uzgadnianie TLS 216

Negocjowanie wstępne 217

Uwierzytelnianie punktów końcowych 218

TLS a wymagania w zakresie bezpieczeństwa 221

Podsumowanie 223

8. Implementowanie protokołu sieciowego 225

Reprodukcja przechwyconego ruchu sieciowego 226

Przechwytywanie ruchu za pomocą Netcat 226

Reprodukcja przechwyconych pakietów UDP 229

Reimplementacja proxy 230

Ponowne wykorzystywanie kodu wykonywalnego 236

Kod aplikacji .NET 237

Kod aplikacji w Javie 242

Binarny kod maszynowy 243

Neutralizacja szyfrowania w protokole TLS 249

Rozpoznawanie stosowanego algorytmu szyfrowania 250

Deszyfracja danych protokołu TLS 251

Podsumowanie 257

9. Implementacyjne zagrożenia bezpieczeństwa aplikacji 259

Kategorie zagrożeń bezpieczeństwa 260

Zdalne wykonywanie kodu 260

Blokada usług 260

Ujawnianie poufnych informacji 260

Omijanie uwierzytelniania 261

Omijanie autoryzacji 261

Niszczanie zawartości pamięci 262

Pamięciowe bezpieczeństwo języków programowania 262

Przepiętnienie bufora w pamięci 263

Błędy w indeksowaniu tablic	269
Niedozwolona ekspansja danych	270
Błędy dynamicznego przydziału pamięci	270
Domyślne i hardkodowane dane uwierzytelniające	271
Enumeracja użytkowników	272
Nieprawidłowy dostęp do zasobów	273
Postać kanoniczna nazwy zasobu	273
Przegadana diagnostyka	275
Wyczerpanie pamięci	276
Wyczerpanie przestrzeni w pamięci masowej	278
Wyczerpanie mocy procesora	278
Kosztowne algorytmy	279
Konfigurowalna kryptografia	281
Niebezpieczne formatowanie łańcuchów	282
Wstrzykiwanie poleceń systemowych	283
Wstrzykiwanie kodu SQL	284
Niebezpieczna konwersja tekstu	286
Podsumowanie	287
 10. Wykrywanie i eksploatacja luk w zabezpieczeniach	289
Testowanie fazyjne	290
Najprostszy test fazyjny	290
Fuzzer mutacyjny	291
Generowanie przypadków testowych	292
Segregacja luk	292
Debugowanie aplikacji	293
Narzędzia wspomagające analizę awarii	300

Eksploatowanie typowych luk 303

Eksploatowanie nadpisywania pamięci 303

Nieuprawniony zapis do plików wskutek nadpisywania zawartości pamięci 311

Tworzenie kodu powłoki 314

Warsztat 315

Int3 - proste debugowanie 317

Wywołania systemowe 318

Wywoływanie zewnętrznych programów 323

Generowanie kodu powłoki za pomocą Metasploita 325

Zapobieganie eksploatowaniu nadpisywania pamięci 327

DEP - zapobieganie wykonywaniu danych 327

Zapobieganie powrotom pod spreparowane adresy 328

ASLR - randomizacja przestrzeni adresowej 331

Kanarki na stosie 334

Podsumowanie 337

A. Narzędzia wspomagające analizę protokołów sieciowych 339

Bierne przechwytywanie ruchu sieciowego i jego analiza 340

Microsoft Message Analyzer 340

TCPDump i LibPCAP 341

Wireshark 341

Czynne przechwytywanie ruchu sieciowego i jego analiza 342

Canape 342

Canape Core 343

Mallory 344

Połączenia sieciowe i analizowanie protokołów 344

HPing 344

Netcat 344

NMap 345

Testowanie aplikacji webowych 345

Burp Suite 346

Zed Attack Proxy (ZAP) 347

Mitmproxy 347

Testowanie fazyjne, generowanie pakietów, eksploatacja luk 348

American Fuzzy Lop (AFL) 348

Kali Linux 349

Metasploit 349

Scapy 349

Sulley 350

Podsluchiwanie sieci i przekierowywanie pakietów 350

DNSMasq 350

Ettercap 350

Inżynieria wsteczna kodu wykonywalnego 351

Java Decompiler (JD) 351

IDA/IDA Pro 352

Hopper 353

ILSpy 353

.NET Reflector 354

Skorowidz 355