

Spis treści

| | |
|--|-----------|
| PODZIĘKOWANIA | 13 |
| PRZEDMOWA | 15 |
| WSTĘP | 17 |
| Dlaczego warto przeczytać tę książkę? | 17 |
| Instalowanie Pythona | 18 |
| Jakie informacje znajdują się w książce? | 18 |
| 1 | |
| KONFIGURACJA ŚRODOWISKA | 23 |
| Wirtualne laboratorium | 23 |
| Konfiguracja VirtualBox | 24 |
| Konfiguracja pfSense | 25 |
| Konfiguracja sieci wewnętrznej | 27 |
| Konfiguracja pfSense | 27 |
| Konfigurowanie Metasploitable | 30 |
| Konfigurowanie Kali Linux | 31 |
| Konfigurowanie maszyny Ubuntu Linux Desktop | 32 |
| Twój pierwszy atak: wykorzystanie backdoora w Metasploitable | 33 |
| Uzyskiwanie adresu IP serwera Metasploitable | 34 |
| Korzystanie z backdoora w celu uzyskania dostępu | 35 |
| I | |
| PODSTAWY SIECI | 37 |
| 2 | |
| PRZECHWYTYWANIE RUCHU ZA POMOCĄ TECHNIKI | |
| ARP SPOOFING | 39 |
| Jak przesyłane są dane w Internecie | 39 |
| Pakiety | 40 |
| Adresy MAC | 40 |
| Adresy IP | 41 |
| Tabele ARP | 42 |
| Ataki ARP spoofing | 43 |
| Wykonywanie ataku ARP spoofing | 43 |
| Wykrywanie ataku ARP spoofing | 48 |
| Ćwiczenia | 49 |

| | |
|--------------------------------------|----|
| Sprawdź tabele ARP | 50 |
| Zaimplementuj ARP spoofer w Pythonie | 50 |
| MAC flooding | 51 |

3

| | |
|---|-----------|
| ANALIZA PRZECHWYCONEGO RUCHU | 52 |
| Pakiety i stos protokołów internetowych | 52 |
| Pięciowarstwowy stos protokołów internetowych | 54 |
| Przeglądanie pakietów w Wiresharku | 58 |
| Analizowanie pakietów zebranych przez zaporę sieciową | 53 |
| Przechwytywanie ruchu na porcie 80 | 64 |
| Ćwiczenia | 65 |
| pfSense | 66 |
| Eksplorowanie pakietów w narzędziu Wireshark | 67 |

4

| | |
|---|-----------|
| TWORZENIE POWŁOK TCP I BOTNETÓW | 68 |
| Gniazda i komunikacja międzyprocesowa | 58 |
| Uzgadnianie połączenia TCP (ang. TCP handshake) | 69 |
| Odwrócona powłoka TCP (ang. TCP reverse shell) | 71 |
| Dostęp do maszyny ofiary | 73 |
| Skanowanie w poszukiwaniu otwartych portów | 73 |
| Tworzenie klienta odwróconej powłoki | 75 |
| Tworzenie serwera TCP, który czeka na połączenia klientów | 77 |
| Ładowanie odwróconej powłoki na serwer Metasploitable | 78 |
| Botnety | 80 |
| Ćwiczenia | 82 |
| Serwer botów dla wielu klientów | 82 |
| Skany SYN | 83 |
| Wykrywanie skanów XMas | 84 |

II

| | |
|---------------------|-----------|
| KRYPTOGRAFIA | 85 |
|---------------------|-----------|

5

| | |
|--------------------------------------|-----------|
| KRYPTOGRAFIA I RANSOMWARE | 87 |
| Szyfrowanie | 87 |
| ' Szyfr z kluczem jednorazowym | 88 |
| Generatory liczb pseudolosowych | 91 |
| Niebezpieczne tryby szyfru blokowego | 92 |
| Bezpieczne tryby szyfru blokowego | 93 |
| Szyfrowanie i odszyfrowywanie pliku | 95 |
| Szyfrowanie wiadomości e-mail | 96 |
| Kryptografia klucza publicznego | 96 |
| Teoria Rivesta-Shamira-Adlemana | 97 |

| | |
|--|-----|
| Podstawy matematyczne RSA | 98 |
| Szyfrowanie pliku za pomocą RSA | 99 |
| Optymalne dopełnienie szyfrowania asymetrycznego | 102 |
| Tworzenie oprogramowania ransomware | 103 |
| Ćwiczenia | 106 |
| Serwer ransomware | 106 |
| Rozszerzanie funkcjonalności klienta ransomware | 107 |
| Nierozwiązane szyfrogramy | 107 |

6

TLS I PROTOKÓŁ DIFFIEGO-HELLMANA 109

| | |
|---|-----|
| Zabezpieczenia warstwy transportowej (TLS) | 110 |
| Uwierzytelnianie wiadomości | 111 |
| Urzędy certyfikacji i podpisy | 112 |
| Urzędy certyfikacji | 113 |
| Używanie algorytmu Diffiego-Hellmana do obliczania klucza współdzielonego | 115 |
| Krok 1.: Generowanie parametrów współdzielonych | 115 |
| Krok 2.: Generowanie pary kluczy publiczny - prywatny | 115 |
| Dlaczego haker nie może obliczyć klucza prywatnego? | 118 |
| Krok 3.: Wymiana klucza i klucz jednorazowy | 118 |
| Krok 4.: Obliczanie współdzielonego tajnego klucza | 119 |
| Krok 5.: Otrzymywanie klucza | 120 |
| Atak na algorytm Diffiego-Hellmana | 121 |
| Krzywa eliptyczna Diffiego-Hellmana | 121 |
| Matematyka krzywych eliptycznych | 122 |
| Algorytm podwajania i dodawania | 123 |
| Dlaczego haker nie może użyć G_{xy} i ax_y do obliczenia klucza prywatnego A ? | 124 |
| Zapisywanie do gniazd TLS | 124 |
| Bezpieczne gniazdo klienta | 125 |
| Bezpieczne gniazdo serwera | 126 |
| Usuwanie SSL (ang. stripping SSL) i obejście HSTS (ang. HSTS bypass) | 128 |
| Ćwiczenie: Dodaj szyfrowanie do serwera ransomware | 129 |

III

SOCJOTECHNIKA 131

7

PHISHING I DEEPPFAKE 133

| | |
|---|-----|
| Wyrafinowany i podstępny atak socjotechniczny | 133 |
| Fałszywe e-maile | 134 |
| Wykonywanie wyszukiwania DNS (ang. DNS lookup) przez serwer pocztowy | 135 |
| Komunikacja za pomocą SMTP | 135 |

| | |
|---|-----|
| Tworzenie sfałszowanego e-maila | 138 |
| Podszywanie się pod e-maile w protokole SMTPS | 140 |
| Fałszowanie stron internetowych | 141 |
| Tworzenie fałszywych filmów | 144 |
| Dostęp do Google Colab | 145 |
| Importowanie modeli uczenia maszynowego | 146 |
| Ćwiczenia | 148 |
| Klonowanie głosu | 148 |
| Wyłudzenie informacji | 149 |
| Audyty SMTP | 149 |

8

| | |
|---|------------|
| SKANOWANIE CELÓW | 151 |
| Analiza sieci powiązań | 151 |
| Maltego | 153 |
| Bazy danych z ujawnionymi poświadczeniami | 156 |
| Przejmowanie karty SIM | 157 |
| Google dorking | 158 |
| Skanowanie całego Internetu | 159 |
| Masscan | 159 |
| Shodan | 163 |
| Ograniczenia IPv6 i NAT | 165 |
| Protokół internetowy w wersji 6 (IPv6) | 165 |
| NAT | 165 |
| Bazy danych podatności | 167 |
| Skanery podatności | 169 |
| Ćwiczenia | 172 |
| Skanowanie za pomocą nmap | 172 |
| Discover | 173 |
| Tworzenie własnego narzędzia OSINT | 175 |

IV

| | |
|--------------------------|------------|
| WYKORZYSTANIE LUK | 177 |
|--------------------------|------------|

9

| | |
|--|------------|
| ZASTOSOWANIE METODY FUZZINGU DLA PODATNOŚCI TYPU ZERO-DAY | 179 |
| Studium przypadku: Wykorzystanie luki Heartbleed dla OpenSSL | 180 |
| Tworzenie exploita | 181 |
| Rozpoczęcie programu | 181 |
| Tworzenie wiadomości Client Hello | 182 |
| Odczytywanie odpowiedzi serwera | 184 |
| Tworzenie złośliwego żądania Heartbeat | 185 |
| Nieuprawniony odczyt pamięci | 186 |
| Tworzenie funkcji exploita | 187 |

| | |
|--|-----|
| Składanie wszystkiego w całość | 187 |
| Fuzzing | 188 |
| Prosty przykład | 188 |
| Tworzenie własnego fuzzera | 189 |
| American Fuzzy Lop | 190 |
| Wykonanie symboliczne | 195 |
| Wykonanie symboliczne dla programu testowego | 195 |
| Ograniczenia wykonania symbolicznego | 196 |
| Dynamiczne wykonanie symboliczne | 197 |
| Używanie D5E do łamania hasła | 200 |
| Tworzenie wykonywalnego pliku binarnego | 200 |
| Instalowanie i uruchamianie Angr | 201 |
| Program Angr | 202 |
| Ćwiczenia | 204 |
| Zdobądź flagą za pomocą Angr | 204 |
| Fuzzing protokołów internetowych | 204 |
| Fuzzing projektu open source | 205 |
| Zaimplementuj własny mechanizm DSE | 206 |

10

| | |
|--|------------|
| TWORZENIE TROJANÓW | 207 |
| Studium przypadku: Odtworzenie działania Drovoruba za pomocą Metasploita | 208 |
| Budowanie serwera atakującego | 208 |
| Tworzenie klienta ofiary | 210 |
| Wgrywanie złośliwego oprogramowania | 211 |
| Korzystanie z agenta atakującego | 212 |
| Dlaczego potrzebujemy modułu jądra ofiary | 212 |
| Ukrywanie złośliwego oprogramowania w pliku | 213 |
| Tworzenie trojana | 213 |
| Hosting trojana | 217 |
| Pobieranie zainfekowanego pliku | 218 |
| Kontrolowanie pracy złośliwego kodu | 219 |
| Omijanie antywirusa za pomocą enkoderów | 221 |
| Enkoder Base64 | 222 |
| Tworzenie modułu Metasploit | 224 |
| Enkoder Shikata Ga Nai | 225 |
| Tworzenie trojana Windows | 227 |
| Ukrywanie trojana w grze Saper | 227 |
| Ukrywanie trojana w dokumencie programu Word (lub innym pliku) | 228 |
| Tworzenie trojana na Androida | 229 |
| Dekonstrukcja pliku APK w celu wyświetlenia złośliwego kodu | 230 |
| Ponowne budowanie i podpisywanie pliku APK | 232 |
| Testowanie trojana na Androida | 234 |
| Ćwiczenia | 237 |

| | |
|--|-----|
| Evil-Droid | 238 |
| Tworzenie własnej złośliwej aplikacji w Pythonie | 239 |
| Zaciemnij kod | 240 |
| Zbuduj plik wykonywalny dla konkretnej platformy | 241 |

11

BUDOWANIE I INSTALOWANIE ROOTKITÓW W LINUXIE 242

| | |
|--|-----|
| Tworzenie modułu jądra Linux | 243 |
| Tworzenie kopii zapasowej maszyny wirtualnej Kali Linux | 243 |
| Pisanie kodu modułu | 244 |
| Kompilowanie i uruchamianie modułu jądra | 245 |
| Modyfikowanie wywołań systemowych | 247 |
| Jak działają wywołania systemowe | 248 |
| Zastosowanie techniki hookingu dla wywołań systemowych | 250 |
| Przechwytywanie wywołania systemowego odpowiedzialnego za zamknięcie systemu | 251 |
| Ukrywanie plików | 256 |
| Struktura linux_dirent | 256 |
| Tworzenie kodu do hookingu | 257 |
| Zastosowanie Armitage do włamywania się do hosta i instalowania rootkita | 258 |
| Skanowanie sieci | 260 |
| Wykorzystywanie luki hosta | 261 |
| Instalowanie rootkita | 262 |
| Ćwiczenia | 262 |
| Keylogger | 262 |
| Samoukrywający się moduł | 265 |

12

KRADZIEŻ I ŁAMANIE HASEŁ 266

| | |
|--|-----|
| SQL injection | 266 |
| Kradzież haseł z bazy danych witryny | 268 |
| Wyszukiwanie plików na serwerze WWW | 269 |
| Wykonywanie ataku typu SQL injection | 270 |
| Tworzenie własnego narzędzia do wstrzykiwania zapytań SQL | 271 |
| Omówienie żądań HTTP | 271 |
| Tworzenie programu do wstrzykiwania zapytań | 273 |
| Korzystanie z SQLMap | 275 |
| Uzyskiwanie skrótów hasła | 277 |
| Anatomia skrótów MD5 | 278 |
| Łamanie skrótów | 281 |
| Solenie skrótów za pomocą klucza jednorazowego | 282 |
| Budowanie narzędzia łamiącego posolony skrót | 282 |
| Popularne narzędzia do łamania skrótów i do brutalnego łamania haseł | 283 |
| John the Ripper | 283 |

| | |
|---|-----|
| Hashcat | 284 |
| Hydra | 285 |
| Ćwiczenia | 286 |
| Wstrzykiwanie kodu NoSQL | 286 |
| Brutalne logowanie do aplikacji webowej | 288 |
| Burp Suite | 288 |

13

ATAK TYPU CROSS-SITE SCRIPTING 290

| | |
|---|-----|
| Cross-site scripting | 290 |
| W jaki sposób kod JavaScript może się stać złośliwy | 292 |
| Ataki typu stored XSS | 294 |
| Ataki typu reflected XSS | 296 |
| Znajdowanie luk w zabezpieczeniach za pomocą serwera proxy | |
| OWASP Zed Attack Proxy | 297 |
| Korzystanie z narzędzia Browser Exploitation Framework | 300 |
| Wstrzykiwanie zaczepu BeEF | 300 |
| Wykonywanie ataku socjotechnicznego | 301 |
| Przejście z przeglądarki do komputera | 303 |
| Studium przypadku: Ominięcie zabezpieczeń starej wersji przeglądarki Chrome | 304 |
| Instalowanie rootkitów poprzez wykorzystanie luk w serwisie internetowym | 304 |
| Ćwiczenie: Polowanie na błędy w ramach programu Bug Bounty | 307 |

V

KONTROLOWANIE SIECI 309

14

PIVOTING I PODNOSZENIE UPRAWNIENÍ 311

| | |
|--|-----|
| Pivoting za pomocą urządzenia dual-homed | 312 |
| Konfiguracja urządzenia dual-homed | 312 |
| Podłączanie maszyny do sieci prywatnej | 314 |
| Pivoting za pomocą Metasploita | 316 |
| Tworzenie proxy po stronie atakującego | 319 |
| Pozyskiwanie skrótów haseł w systemie Linux | 321 |
| Gdzie Linux przechowuje nazwy i hasła użytkowników | 321 |
| Wykonywanie ataku Dirty COW w celu podniesienia uprawnień | 323 |
| Ćwiczenia | 326 |
| Dodawanie obsługi NAT do urządzenia dual-homed | 326 |
| Przydatne informacje na temat podnoszenia uprawnień w systemie Windows | 327 |

15

PORUSZANIE SIĘ PO KORPORACYJNEJ SIECI WINDOWS 328

| | |
|---|------------|
| Tworzenie wirtualnego laboratorium Windows | 329 |
| Zdobywanie skrótów haseł za pomocą mimikatz | 329 |
| Przekazywanie skrótu za pomocą NT LAN Manager | 332 |
| Eksploracja firmowej sieci Windows | 333 |
| Atakowanie usługi DNS | 335 |
| Atakowanie usług Active Directory i LDAP | 336 |
| Tworzenie klienta zapytań LDAP | 338 |
| Używanie SharpHound i BtloodHound w celu sondowania usługi LDAP | 340 |
| Atakowanie Kerberos | 342 |
| Atak typu pass-the-ticket | 344 |
| Ataki golden ticket i DC sync | 345 |
| Ćwiczenie: Kerberoasting | 346 |
| | |
| 16 | |
| NASTĘPNE KROKI | 347 |
| Konfigurowanie bezpiecznego środowiska hakerskiego | 347 |
| Jak pozostać anonimowym dzięki narzędziom Tor i Tails | 348 |
| Konfigurowanie wirtualnego serwera prywatnego | 350 |
| Konfigurowanie SSH | 350 |
| Instalowanie narzędzi hakerskich | 352 |
| Utwardzanie serwera | 353 |
| Audyt utwardzonego serwera | 355 |
| Inne tematy | 356 |
| Radia definiowane programowo | 356 |
| Atakowanie infrastruktury telefonii komórkowej | 357 |
| Omijanie sieci typu Air Gap | 358 |
| Inżynieria wsteczna | 358 |
| Fizyczne narzędzia hakerskie | 359 |
| Informatyka śledcza | 359 |
| Hakowanie systemów przemysłowych | 359 |
| Obliczenia kwantowe | 359 |
| Bądź aktywny | 360 |
| | |
| SKOROWIDZ | 361 |