

SPIS TREŚCI

O autorach.....	10
O współautorach.....	12
O recenzencie technicznym.....	14
Przedmowa.....	15
Podziękowania.....	17
Wprowadzenie.....	19
Naszym wrogiem nie jest już ignorancja – jest nim brak czujności.....	19
Co nowego w piątym wydaniu.....	20
Część I. Budowa podstaw.....	23
Studium przypadku: znajdź drogę poprzez Google.....	24
Ładuj i strzelaj z Google.....	24
Rozdział 1. Footprinting.....	27
Co to jest footprinting?.....	28
Z czego wynika konieczność oznaczania?.....	29
Footprinting w Internecie.....	29
Krok 1: ustalenie zakresu działania.....	29
Krok 2: uzyskanie autoryzacji.....	30
Krok 3: informacje dostępne publicznie.....	30
Krok 4: wylizywanie WHOIS i DNS.....	41
Krok 5: odpytywanie DNS.....	53
Krok 6: rekonesans sieciowy.....	58
Podsumowanie.....	61
Rozdział 2. Skanowanie.....	63
Badanie aktywności systemu.....	64
Pingowanie.....	64
Wykrywanie działających lub nasłuchujących usług.....	73
Typy skanowania.....	74

Identyfikowanie działających usług TCP i UDP	75
Skanery portów dla Windows.....	81
Przeciwdziałanie skanowaniu portów	86
Rozpoznawanie systemu operacyjnego	88
Aktywny fingerprinting stosu	89
Pasywny fingerprinting stosu	93
Podsumowanie	96
Rozdział 3. Wyliczanie	97
Prosty banner grabbing	98
Wyliczanie podstawowych usług sieciowych.....	101
Podsumowanie	151
Część II. Haking systemów	153
Mam Macintosha – muszę być bezpieczny!	154
Dobre i złe wieści	155
Rozdział 4. Hakowanie Windows.....	157
Ogólny rzut oka.....	159
O czym nie będziemy mówili	160
Ataki niewierzytelnione	160
Ataki na własne protokoły sieciowe Windows.....	161
Implementacje Windows Internet Service.....	183
Ataki z uwierzytelnianiem	191
Poszerzanie uprawnień	191
Kradzież informacji	194
Zdalna kontrola i tylne drzwi	205
Przekierowanie portu	210
Ogólne metody przeciwdziałania uwierzytelnionej penetracji.....	211
Zacieranie śladów	216
Funkcje bezpieczeństwa Windows	219
Uaktualnianie systemu za pomocą łątek.....	219
Zasady grup	220
IPSec.....	222
runas.....	223
.NET Framework	224
Ściana ogniowa Windows	225
Encrypting File System (EFS).....	225
Windows XP Service Pack 2	226
Zakończenie: ciężar bezpieczeństwa Windows.....	228
Podsumowanie	229
Rozdział 5. Haking Uniksa	231
Poszukiwanie roota	231
Krótki przegląd.....	232
Odwzorowanie słabych punktów.....	232
Dostęp zdalny i lokalny	233
Dostęp zdalny.....	234

Ataki sterowane danymi	238
Chcę swoją powłokę	251
Typowe rodzaje ataków zdalnych	256
Dostęp lokalny	281
Po zdobyciu praw roota	296
Usuwanie rootkita	308
Podsumowanie	309
Rozdział 6. Hakowanie komunikacji zdalnej i VOIP.....	313
Przygotowania.....	314
War-dialing	316
Sprzęt	317
Kwestie prawne	318
Koszty peryferyjne	318
Oprogramowanie	319
Skrypty brute-force – sposób domowy	333
Hakowanie central PBX.....	345
Hakowanie poczty głosowej	349
Hakowanie wirtualnych sieci prywatnych (VPN)	355
Ataki na Voice over IP.....	359
Podstawowe metody ataku	360
Podsumowanie	366
Część III. Hacking sieciowy	369
Rozdział 7. Urządzenia sieciowe.....	373
Wykrywanie	374
Detekcja	374
Sprawdzanie systemów autonomicznych	378
Normalny traceroute	378
traceroute z informacjami ASN	378
show ip bgp.....	379
Publiczne grupy dyskusyjne	380
Wykrywanie usług	381
Luki w zabezpieczeniach sieci	387
Warstwa 1 modelu OSI.....	388
Warstwa 2 modelu OSI.....	390
Podśluchiwanie przełącznika.....	391
Warstwa 3 modelu OSI.....	403
dsniff.....	406
Niepoprawne konfiguracje	409
Hacking protokołów trasowania.....	415
Hakowanie protokołu zarządzania.....	425
Podsumowanie	426
Rozdział 8. Hacking bezprzewodowy	429
Bezprzewodowy footprinting.....	430
Sprzęt	431

Skanowanie i wyliczanie sieci bezprzewodowych	447
Sniffery bezprzewodowe	448
Narzędzia do monitorowania bezprzewodowego	452
Identyfikacja sieciowych środków obrony	459
SSID	460
Kontrola dostępu w oparciu o adresy MAC	461
Uzyskiwanie dostępu (hakowanie 802.11)	464
Kontrola dostępu MAC	466
Ataki na algorytm WEP	468
Zabezpieczanie WEP	469
Narzędzia do atakowania słabych punktów WEP	469
Ataki na LEAP	474
Ataki z odmową usługi (DoS)	477
Ogólne omówienie 802.1X	478
Źródła dodatkowe	479
Podsumowanie	482
Rozdział 9. Ściany ogniowe.....	485
Ogólny obraz ściany ogniowej.....	485
Identyfikacja ściany ogniowej	486
Zaawansowane techniki rozpoznawania ścian ogniowych	491
Skanowanie poprzez ściany ogniowe	494
Filtrowanie pakietów	498
Luki w aplikacjach pośredniczących	502
Luki w WinGate	504
Podsumowanie	506
Rozdział 10. Ataki Denial of Service.....	509
Typowe techniki ataku DoS	511
Stara szkoła DoS: luki w zabezpieczeniach	511
Nowoczesne techniki DoS: wyczerpanie zasobów	513
Przeciwdziałanie atakom DoS	520
Krótko o celach praktycznych	520
Odporność na DoS	521
Wykrywanie ataków DoS	526
Reagowanie na ataki DoS	527
Podsumowanie	531
Część IV. Hakowanie oprogramowania.....	533
Studium przypadku: tylko elita.....	534
Rozdział 11. Hakowanie kodu.....	535
Typowe techniki ataku przy użyciu exploitów.....	536
Przepełnienia bufora i błędy projektu.....	536
Ataki z zatwierdzaniem danych wejściowych.....	542
Typowe metody przeciwdziałania	546
Ludzie: zmiana kultury	546
Proces: Security in the Development Lifecycle (SDL)	548

Technologia	556
Zalecane lektury dodatkowe	558
Podsumowanie	559
Rozdział 12. Hakowanie aplikacji internetowych.....	561
Hakowanie serwera internetowego	562
Pliki próbek	563
Ujawnianie kodu źródłowego	565
Ataki ze sprowadzaniem do postaci kanonicznej	565
Rozszerzenia serwera	566
Przepełnienia bufora	568
Skanery luk w serwerach internetowych	570
Hakowanie aplikacji internetowych.....	572
Wyszukiwanie aplikacji podatnych na atak za pomocą Google.....	572
Przeszukiwanie Internetu.....	573
Analiza aplikacji internetowej.....	575
Typowe luki w aplikacjach internetowych.....	587
Podsumowanie	599
Rozdział 13. Hakowanie użytkowników internetu	601
Luki w internetowym oprogramowaniu klienckim.....	602
Historia hakingu oprogramowania klienckiego w skrócie	602
JavaScript i Active Scripting	607
Cookies	608
Cross-Site Scripting (XSS).....	610
Luki Cross-Frame/Domain.....	611
Ataki SSL	613
Ładunki i punkty zrzutu.....	616
Hakowanie poczty elektronicznej.....	616
Komunikatory internetowe	621
Eksploity oprogramowania internetowego Microsoft oraz środki przeciwdziałania im	622
Ogólne środki bezpieczeństwa klienckiego oprogramowania Microsoft.....	631
Dlaczego nie używać oprogramowania klienckiego innego niż Microsoft?	643
Internetowe oprogramowanie klienckie producentów innych niż Microsoft	646
Serwisy online	651
Ataki socjotechniczne: phishing i kradzież tożsamości.....	655
Techniki phishingu	656
Oprogramowanie irytujące i zwodnicze: spyware, adware i spam.....	660
Typowe techniki wprowadzania.....	661
Oprogramowanie blokujące, wykrywające i usuwające.....	662
Malware	666
Warianty złośliwego oprogramowania i typowe techniki	666
Wykrywanie i usuwanie złośliwego oprogramowania.....	675
Fizyczne zabezpieczenia użytkowników końcowych.....	680
Podsumowanie	681

Część V. Dodatki.....	683
Dodatek A. Porty	685
Dodatek B. Wykaz 14 najpoważniejszych luk w zabezpieczeniach	691
Skorowidz	693