

Obsah

Předmluva	15
Poděkování	17
Úvod	19
Naším nepřítelem už není nevzdělanost, ale nepozornost	19
Co je v pátém vydání nového	20
Všem	21
Část první: Výběr oběti	23
Případová studie – Google je váš kamarád	24
Nabít a připravit	24
1. Sběr informací	27
1.1 Co všechno lze zjistit	28
1.2 Informace o připojení k Internetu	29
Krok první: Ujasněte si, co všechno vás zajímá.	29
Krok druhý: Sežeňte si dostatečné pravomoci.	29
Krok třetí: Veřejně dostupné informace.	29
Krok čtvrtý: Informace dostupné pomocí WHOIS a DNS	37
Krok pátý: Průzkum DNS	47
Krok šestý: Průzkum sítě	51
1.3 Shrnutí	53
2. Skenování	55
2.1 Jak najít živé systémy	56
2.2 Nalezení síťových služeb	63
Skenovací techniky	63
Nalezení TCP a UDP služeb	65
Port skenery pro Windows	70
Přehled skenovacích nástrojů	74
2.3 Identifikace operačního systému	76
Aktivní testování síťového rozhraní	77
Pasivní identifikace operačního systému	80
2.4 Shrnutí	82

3. Průzkum terénu	85
3.1 Sběr bannerů	86
3.2 Průzkum běžných síťových služeb.....	88
3.3 Shrnutí	128
Část druhá: Útoky na operační systém.....	129
„Mám Macka, jsem v bezpečí!“	129
Hodný a zlý.....	131
4. Útoky na Windows	133
4.1 Čím se zabývat nebudeme	135
4.2 Útoky na dálku	135
Útoky na proprietární síťové protokoly	136
Internetové služby systému Windows	151
4.3 Útoky na blízko	157
Jak získat vyšší oprávnění	157
Koncovka.....	158
Vzdálený přístup a zadní vrátka	167
Přesměrování portů.....	170
Obrana proti útokům na blízko	171
Zametání stop	174
4.4 Bezpečnostní nástroje Windows	177
Pravidelná aktualizace systému	177
Zásady skupiny	177
IPSec.....	178
Program runas.....	179
Prostředí .NET.....	180
Windows firewall.....	180
Šifrovaný souborový systém EFS	181
Windows XP Service Pack 2	181
Závěr aneb břemeno bezpečnosti.....	183
4.5 Shrnutí	183
5. Útoky na Unix	185
5.1 Honba za rootem	185
Stručné opakování	186
Hledání slabých míst.....	186
5.2 Místní versus vzdálený přístup	187

5.3 Útoky na dálku	187
Datové útoky	190
Chci svůj shell	200
Běžné typy útoků na dálku	203
5.4 Útoky na blízko	223
5.5 Co dělat po úspěšném útoku	235
Zotavení systému po instalaci rootkitu	244
5.6 Shrnutí	245
6. Útoky na vytáčené linky a VoIP	247
6.1 Přípravy	248
6.2 Skenování telefonních čísel	249
Hardware	249
Právní důsledky	250
Náklady	251
Software	251
6.3 Skriptované útoky hrubou silou aneb udělejte si sami	262
6.4 Telefonní ústředny	271
6.5 Obrana proti útokům na telefonní ústřednu	274
6.6 Virtuální soukromé sítě	278
6.7 Voice over IP	281
Slabá místa VoIP	282
6.8 Shrnutí	286
Část třetí: Útoky na síť	289
Případová studie – Bezdrátové sítě	290
7. Síťová zařízení	291
7.1 Průzkum sítě	292
Obrana proti programu dig	293
7.2 Autonomní systémy	295
Autonomní systémy a traceroute	295
show ip bgp	296
7.3 Veřejné diskusní skupiny	297
7.4 Hledání síťových služeb	298
7.5 Slabá místa sítě	302
Fyzická vrstva	303
Linková vrstva	304

Odposlech přepínaných sítí	305
Síťová vrstva	315
Chyby v konfiguraci	319
Útoky na směrovací protokoly	323
Útoky na protokoly používané pro správu sítě	331
7.6 Shrnutí	332
8. Útoky na bezdrátové sítě	333
8.1 Hledání bezdrátových sítí	334
Vybavení	334
8.2 Skenování a průzkum sítě	345
Odposlech bezdrátových sítí	345
8.3 Zabezpečení bezdrátových sítí	353
SSID	353
Omezení přístupu pomocí MAC adres	354
8.4 Útok	356
Kontrola MAC adres	356
Útoky na WEP	358
Zabezpečení WEP	359
8.5 Nástroje pro zneužití chyb WEP	359
8.6 Útoky na protokol LEAP	362
8.7 Útoky typu Denial of Service	365
8.8 802.1X	366
8.9 Tabulka pro převod mezi decibely a watty	366
8.10 Shrnutí	368
9. Firewally	369
9.1 Přehled firewallů	369
9.2 Identifikace firewallu	370
Pokročilé techniky detekce firewallů	374
9.3 Skenování skrz firewally	376
9.4 Filtrování paketů	379
9.5 Chyby v aplikačních proxy	382
Chyby ve WinGate	383
9.6 Shrnutí	385

10. Útoky na dostupnost služeb.....	387
10.1 Běžné typy útoků na dostupnost služeb.....	388
Starší útoky na dostupnost služeb	389
Moderní útoky na dostupnost služeb.....	390
10.2 Obrana proti DoS útokům	394
Praktické cíle	394
Jak odolat DoS útoku	395
Detekce DoS útoků	398
Reakce na DoS útoky.....	399
10.3 Shrnutí	402
Část 4: Útoky na software	403
Případová studie — Jen ti nejlepší.....	403
11. Útoky na kód.....	405
11.1 Klasické způsoby útoku na kód	406
Přetečení paměti a chyby v návrhu	406
Nedostatečná kontrola vstupu	410
11.2 Obrana proti útokům na kód	413
Lidé: Jak změnit kulturu.....	413
Security Development Lifecycle (SDL).....	415
Technologie	421
Doporučená četba	422
11.3 Shrnutí	422
12. Útoky na web.....	423
12.1 Útoky na webové servery	424
Ukázkové soubory	425
Prozrazení zdrojového kódu.....	426
Chybný převod do normálního tvaru	426
Rozšíření serveru	427
Nedostatečná kontrola vstupu.....	428
Programy pro hledání bezpečnostních chyb	429
12.2 Útoky na webové aplikace.....	430
Hledání zranitelných aplikací pomocí Google	430
Stahování webových stránek	432
Analýza webových aplikací	433
Běžné chyby webových aplikací.....	441
12.3 Shrnutí	449

13. Útoky na uživatele Internetu	451
13.1 Chyby v internetových klientech.....	452
Stručné dějiny útoků na uživatele Internetu	452
JavaScript a Active Scripting	455
Cookies	456
Cross-site skriptování (XSS)	457
Útoky na rámce a bezpečnostní zóny	458
Útoky na SSL	459
Jak dosáhnout spuštění cizího kódu	461
Útoky prostřednictvím e-mailu	461
Instant messaging	464
Chyby v klientech firmy Microsoft	465
Obrana proti chybám v klientech od Microsoftu	470
Online služby	484
13.2 Sociální útoky, phishing a krádeže totožnosti	486
Phishingové techniky	487
13.3 Otravný software aneb spyware, adware a spam.....	490
Běžné způsoby infekce	490
Blokování, hledání a čištění otravného softwaru	491
13.4 Škodlivý software neboli malware	494
Typy malwaru a běžné techniky	494
Hledání a čištění malwaru	500
13.5 Fyzická bezpečnost.....	504
13.6 Shrnutí	504
Část 5: Dodatky.....	505
A. Porty	507
B. 14 nejčastějších bezpečnostních chyb.....	511
Rejstřík	513