

Obsah

O autorovi	16
O odborných korektorech	17
Věnování	18
Poděkování	19
Ikony používané v této knize	20
Konvence pro zápis syntaxe příkazů	20
Úvod	21
Cíle a metody výkladu	21
Pro koho je kniha určena?	21
Uspořádání knihy	22
KAPITOLA 1	
Hackerři jsou tady!	23
Co se v kapitole dozvíte	23
Od základů: hledá se cíl útoku	23
Krádež zdánlivě nevinných informací	25
Příležitostný cíl	26
Jste příležitostným cílem?	27
Záměrně zvolený cíl	28
Jste záměrně zvoleným cílem?	29
Jak celý útok probíhá	30
Obhlídka a průzkum terénu (neboli „bojová porada“)	30
Sledování	34
Soupis prostředí	37
Získání přístupu	40
Rozšíření oprávnění	43
Zahlázení stop	44
Organizace pro bezpečnost sítí	47
Koordinační centrum CERT	47
Organizace SANS	48
Centrum internetové bezpečnosti CIS	48
SCORE	48



Internet Storm Center	49
Metabáze ICAT	49
Security Focus	49
Co se od bezpečnostních organizací dozvíme	49
Přehled nejčastějších útoků a zneužití	50
Shrnutí	53
Otázky ke cvičení	53

KAPITOLA 2

Bezpečnostní zásady a reakce na události	55
Co se v kapitole dozvíte	55
Definice důvěry	58
Zásady přípustného užívání	60
Celkový přehled zásad	61
Účel dokumentu	61
Působnost dokumentu	61
Užití dokumentu a jeho vlastnictví	61
Bezpečnost a důvěrné informace	62
Nepřípustné užívání	64
Uskutečňování zásad	66
Závěrem	66
Zásady pro práci s hesly	67
Celkový přehled	67
Účel dokumentu	67
Působnost dokumentu	67
Obecné zásady	68
Obecná pravidla pro zadávání hesel	69
Standardy pro ochranu hesel	70
Uskutečňování zásad	71
Závěrem	71
Zásady zabezpečení sítí VPN (Virtual Private Network)	72
Účel dokumentu	72
Působnost dokumentu	72
Vlastní popis zásad	73
Závěrem	74
Zásady pro extranetová připojení	74
Účel dokumentu	75

Působnost dokumentu	75
Bezpečnostní revize	75
Dohoda o připojení cizího subjektu	75
Potvrzení věcných požadavků	76
Kontaktní osoba	76
Zavedení konektivity	76
Modifikace nebo změny konektivity a přístupu	76
Ukončení přístupu	76
Závěrem	77
Certifikace ISO a bezpečnost	77
Vzorové zásady zabezpečení na Internetu	79
Shrnutí	79
Otázky ke cvičení	80
KAPITOLA 3	
Přehled bezpečnostních technologií	81
Co se v kapitole dozvíte	81
Základní principy návrhu zabezpečení	82
Filtrování paketů v přístupových seznamech (ACL)	84
Analogie s nákupním seznamem	86
Omezení mechanismu filtrování paketů	89
Stavová inspekce paketů (SPI)	89
Podrobné řízení toku paketů ve stavové inspekci	90
Omezení metody stavové inspekce paketů	92
Překlady síťových adres (NAT)	92
Zvýšení bezpečnosti sítě	94
Omezení mechanismu NAT	95
Proxy a ochrana na úrovni aplikací	96
Omezení možností proxy	97
Filtrování obsahu	98
Omezení metody filtrování obsahu	101
Infrastruktura veřejného klíče (PKI)	101
Omezení mechanismů PKI	102
Technologie AAA	103
Autentizace	104
Autorizace	104



Účtování	105
Protokol RADIUS (Remote Authentication Dial-In User Service)	105
Protokol TACACS+ (Terminal Access Controller Access Control System)	107
TACACS+ nebo RADIUS?	108
Shrnutí	108
Otázky ke cvičení	109
KAPITOLA 4	
Bezpečnostní protokoly	111
Co se v kapitole dozvíte	111
Šifrování DES	113
Síla šifrovacího mechanismu	114
Omezení algoritmu DES	114
Šifrování Triple DES	115
Síla šifrovacího mechanismu	116
Omezení algoritmu 3DES	116
Algoritmus otisku zprávy MD5	116
Jak funguje haš podle MD5	118
Protokol PPTP	118
Funkce protokolu PPTP	119
Omezení protokolu PPTP	120
Protokol L2TP	121
Protokol L2TP a PPTP	122
Výhody protokolu L2TP	122
Činnost protokolu L2TP	123
Bezpečný shell SSH	125
SSH a telnet	126
Činnost protokolu SSH	129
Tunelování a předávání portů	130
Omezení shellu SSH	131
Shrnutí	131
Otázky ke cvičení	131

KAPITOLA 5

Firewally	133
Co se v kapitole dozvíte	133
Nejčastější otázky k firewallům	134
Kdo vlastně potřebuje firewall?	135
Proč potřebuji firewall i já?	135
Mám vůbec něco, co mi stojí za to chránit?	135
Co všechno firewall dělá?	136
Firewally tvoří „zásady zabezpečení“	137
Přehled činnosti firewallu	140
Firewall v akci	141
Implementace firewallu	142
Stanovení zásad příchozího přístupu	144
Stanovení zásad odchozího přístupu	145
Nejprve základy: život v demilitarizované zóně (DMZ)	145
Případové studie	147
Případová studie: mít či nemít demilitarizovanou zónu?	147
Případová studie: provoz firewallu s poštovním serverem uvnitř chráněné sítě	148
Případová studie: provoz firewallu s poštovním serverem v demilitarizované zóně	151
Omezení firewallů	154
Shrnutí	154
Otázky ke cvičení	155

KAPITOLA 6

Bezpečnost směrovačů	157
Co se v kapitole dozvíte	157
Hranový směrovač jako hrdlo sítě	160
Omezení směrovačů hrdla sítě	162
Hranový směrovač jako inspektor paketů	163
Výhody firewallové množiny funkcí FFS	164
Obsahová inspekce paketů	166
Detekce vniknutí v systému Cisco IOS	170
Kdy využívat IDS ve firewallu FFS	172



Přehled činnosti IDS ve FFS	172
Omezení firewallu FFS	174
Šablona zabezpečení Secure IOS Template	175
Shrnutí	187
Otázky ke cvičení	188

KAPITOLA 7

Virtuální privátní síť (VPN) s protokolem IPSec	189
Co se v kapitole dozvíte	189
Analogie: VPN jako bezpečné propojení „ostrovních sítí“	191
Přehled sítí VPN	192
Výhody sítě VPN a její cíle	195
Strategie při implementaci sítě VPN	195
Oddělení tunelů	197
Přehled sítí VPN s protokolem IPSec	197
Autentizace a integrita dat	200
Tunelování dat	200
Režimy šifrování	201
Protokoly IPSec	203
Přehled činnosti protokolu IPSec	206
Konfigurace směrovače v roli partnera VPN	210
Konfigurace protokolu ISAKMP	210
Konfigurace protokolu IPSec	213
Konfigurace firewallu ve VPN pro clientský přístup	216
Shrnutí	218
Otázky ke cvičení	218

KAPITOLA 8

Bezpečnost bezdrátových sítí	219
Co se v kapitole dozvíte	219
Nejprve základy: co jsou to bezdrátové sítě LAN	221
Co znamená zkratka Wi-Fi?	222
Výhody bezdrátové sítě LAN	223
Bezdrátová síť znamená rádiová síť	223

Činnost bezdrátových sítí	224
Režimy provozu	224
Pokrytí sítě	226
Dostupnost šířky pásma	227
Bezdrátové „Válečné hry“	227
WarChalking	228
WarDriving	229
WarFlying	232
WarSpamming	232
WarSpying	233
Hrozby v bezdrátových sítích	234
Odposlech	234
Útoky s odepřením služeb	236
Pirátské a neoprávněné přístupové body	237
Nesprávně konfigurované přístupové body	239
Zneužívání sítě	239
Zabezpečení bezdrátových sítí	239
Identifikátor SSID	240
Připojení daného zařízení k přístupovému bodu	241
Wired Equivalent Privacy (WEP)	241
Filtrování adres MAC	243
Protokol EAP (Extensible Authentication Protocol)	243
Jak zvýšit bezpečnost bezdrátových sítí	246
A opět základy: nástroje pro prolomení bezdrátových sítí	247
Nástroj NetStumbler	247
Odposlech paketů v bezdrátové síti	248
AirSNORT	249
Shrnutí	250
Otázky ke cvičení	250

KAPITOLA 9

Detekce vniknutí a počítačové návnady	251
Co se v kapitole dozvíte	251
Nejprve základy: detekce vniknutí	253
Přehled funkcí systému IDS	256
Jak se vniknutí detekuje?	260
Rekonstrukce komunikačního proudu	260

Analýza protokolu	260
Detekce anomálií	260
Nalezení projevu či vzorku útoku	261
Analýza systémových protokolů	262
Kombinace několika metod	262
Prevence vniknutí	262
Reakce a operace prevenčních systémů IPS	263
Detekční produkty IDS	264
Omezení detekčních systémů IDS	266
A opět základy: co je to návnada	269
Strategie návrhu počítačové návnady	271
Nevýhody systému v roli návnady	271
Shrnutí	272
Otázky ke cvičení	272
KAPITOLA 10	
Pracovní nástroje	273
Co se v kapitole dozvíte	273
Nejprve základy: analýza zranitelných míst	275
Základní typy útoků	275
Posuzování bezpečnosti a testování průniku	283
Posouzení zranitelných míst a možností průniku zevnitř	284
Posouzení zranitelných míst a možností průniku zvenčí	285
Posouzení fyzické bezpečnosti	286
Různé další posudky	287
Nástroje pro vyhledávání zranitelných míst	288
Funkce nástrojů pro hledání zranitelných míst a jejich výhody	289
Nessus	290
Retina	293
Produkty pro testování průniků	296
Produkt Core Impact podle výrobce	297
Přesnost hledání a detekcí	297
Dokumentace	297
Dokumentace a podpora	298
Aktualizace zranitelných míst	298
Core Impact v činnosti	298
Shrnutí	302
Otázky ke cvičení	302

PŘÍLOHA

Odpovědi na otázky ke cvičení	303
Kapitola 1	303
Kapitola 2	304
Kapitola 3	306
Kapitola 4	307
Kapitola 5	307
Kapitola 6	308
Kapitola 7	310
Kapitola 8	311
Kapitola 9	312
Kapitola 10	313
Slovníček pojmů	315
Rejstřík	331