

OBSAH

O AUTORECH	xvi
O SPOLUAUTORECH	xvii
O ODBORNÝCH KONZULTANTECH	xviii
Předmluva	xix
Poděkování	xxi
Úvod	xxiii
ZABEZPEČENÍ WINDOWS 2000 – SKUTEČNOST NEBO SMYŠLENKA?	xxiii
JAK JE TATO KNIHA USPOŘÁDÁNA	xxv
KAPITOLY: METODOLOGIE HACKINGU BEZ TAJEMSTVÍ	xxv
ZÁKLADNÍ STAVEBNÍ BLOKY: ÚTOKY A OPATŘENÍ PROTI NIM	xxvii
ONLINE ZDROJE A NÁSTROJE	xxix
VŠEM NAŠIM ČTENÁŘŮM	xxix

ČÁST 1

PODKLADY

1	Základy systémového a síťového zabezpečení	3
	ZÁKLADNÍ PRAKTIKY V OBLASTI ZABEZPEČENÍ	4
	SOUHRN	7
	ODKAZY A DALŠÍ LITERATURA	7

2	Bezpečnostní architektura Windows 2000 z pohledu hackera	9
	MODEL ZABEZPEČENÍ WINDOWS 2000	10
	PRINCIPY ZABEZPEČENÍ	12
	Uživatelé	12
	Vestavěné účty	12
	Skupiny	13
	Speciální identity	15
	Další principy a kontejnery zabezpečení	15
	SAM a služba Active Directory	15
	DOMÉNOVÉ LESY, STROMY A DOMÉNY	17
	Rozsah platnosti: místní, globální a univerzální	18
	Vztahy důvěryhodnosti	19
	Administrativní hranice: doménový les nebo doména?	19
	IDENTIFIKÁTORY SID	21
	SLOŽÍME JEDNOTLIVÉ ČÁSTI DOHROMADY: OVĚŘOVÁNÍ A AUTORIZACE	23
	Token	23
	Síťové ověřování	26
	AUDITOVÁNÍ	28
	SOUHRN	29
	ODKAZY A DALŠÍ LITERATURA	30

ČÁST 2

ANALÝZA

3	Vyhledávání stop a skenování	35
	VYHLEDÁVÁNÍ STOP	36
	SKENOVÁNÍ	41
	DŮLEŽITOST NEPŘETRŽITÉHO VYHLEDÁVÁNÍ STOP A SKENOVÁNÍ	50
	SOUHRN	50
	ODKAZY A DALŠÍ LITERATURA	51
4	Inventarizace	53
	PŘEDEHRA: POSOUZENÍ VÝSLEDKŮ ZÍSKANÝCH SKENOVÁNÍM	54
	Názvy NetBIOS vs. IP-adresy	54
	INVENTARIZACE SÍTÍ NETBIOS	55
	INVENTARIZACE WINDOWS 2000 DNS	61
	Inventarizace počítačů Windows 2000	62
	INVENTARIZACE SNMP	76
	INVENTARIZACE SLUŽBY ACTIVE DIRECTORY	79
	SOUHRN	84
	ODKAZY A DALŠÍ LITERATURA	85

5	Hackování služeb CIFS/SMB	89
	HÁDÁNÍ HESEL SMB	90
	Ukončení existujících prázdných relací s cílovým počítačem	91
	Posouzení výstupních údajů z inventarizací	91
	Jak se vyhnout uzamčení účtu	92
	Důležitost účtu administrátora a servisních účtů	93
	ODPOSLOUCHÁVÁNÍ PROCESU OVĚŘOVÁNÍ SMB	104
	SOUHRN	117
	ODKAZY A DALŠÍ LITERATURA	118
6	Zvýšení privilegií	121
	PŘEDVÍDÁNÍ POJMENOVANÝCH KANÁLŮ	122
	POŽADAVKY NETDDE SPUŠTĚNÉ POD ÚČTEM SYSTEM	125
	OBECNĚ PLATNÁ OPATŘENÍ PROTI ZVÝŠENÍ PRIVILEGIÍ ÚČTŮ	127
	SOUHRN	128
	ODKAZY A DALŠÍ LITERATURA	128
7	Přechod k interaktivnímu ovládání	131
	OVLÁDÁNÍ POČÍTAČE Z PŘÍKAZOVÉHO ŘÁDKU	132
	OVLÁDÁNÍ POČÍTAČE Z GRAFICKÉHO UŽIVATELSKÉHO ROZHRANÍ (GUI) ...	139
	SOUHRN	141
	ODKAZY A DALŠÍ LITERATURA	141
8	Rozšiřování okruhu působnosti	143
	AUDITOVÁNÍ	144
	DOBÝVÁNÍ HESEL	146
	Získání zpětně uhodnutelných hesel	146
	Získávání hesel ve formátu prostého textu z LSA cache	147
	CRACKOVÁNÍ HESEL	148
	Zranitelné místo hashů LM	148
	HLEDÁNÍ SOUBORŮ	156
	TROJSKÉ KONĚ GINA	161
	SNIFFING (ČENICHÁNÍ)	162
	NAPADÁNÍ DALŠÍCH POČÍTAČŮ	164
	PŘESMĚROVÁNÍ PORTŮ	168
	SOUHRN	171
	ODKAZY A DALŠÍ LITERATURA	171

9	Zahlazení stop	173
	VYTVÁŘENÍ NOVÝCH UŽIVATELSKÝCH ÚČTŮ	174
	TROJSKÉ KONĚ V ROLI PŘIHLAŠOVACÍ OBRAZOVKY	175
	VZDÁLENÉ OVLÁDÁNÍ	175
	Sady programů pro serverová zadní vrátka	175
	KDE BÝVAJÍ ZADNÍ VRÁTKA A TROJSKÉ KONĚ UMÍSTĚNY	177
	Složky pro samočinné spouštění	177
	Klíče systémového registru pro samočinné spouštění	177
	Ovladače	178
	Jak pomocí domovské stránky webového prohlížeče nahrát kód	179
	Plánované úlohy	179
	ROOTKIT	180
	ZAKRÝVÁNÍ STOP	181
	Pročištění protokolů	181
	Skrývání souborů	181
	OBECNÁ PROTIPATŘENÍ	185
	Automatizované nástroje	185
	SOUHRN	192
	ODKAZY A DALŠÍ LITERATURA	192

ČÁST 4

ZNEUŽITÍ ZRANITELNÝCH SLUŽEB A KLIENTŮ

10	Hackování IIS 5 a webových aplikací	197
	HACKOVÁNÍ IIS 5	198
	Základy hackování IIS	198
	Přetečení bufferu v IIS 5	203
	Procházení souborovým systémem	213
	Zápis souborů na webovém serveru	219
	Zvýšení privilegií útočníka na IIS 5	224
	Útoky odhalující zdrojový kód	228
	NÁSTROJE PRO ZHODNOCENÍ BEZPEČNOSTI WEBOVÉHO SERVERU	238
	Stealth HTTP Scanner	238
	SSLProxy	239
	Achilles	240
	HACKOVÁNÍ WEBOVÝCH APLIKACÍ	243
	Ukázková studie: Průnik webovou aplikací	244
	SOUHRN	246
	ODKAZY A DALŠÍ LITERATURA	248

11	Hackování SQL Serveru	253
	UKÁZKOVÁ STUDIE: PRŮNIK DO SQL SERVERU	254
	KONCEPCE ZABEZPEČENÍ SQL SERVERU	257
	Sítové knihovny	258
	Režimy zabezpečení	258
	Login	259
	Uživatelé	259
	Role	259
	Protokolování	260
	Novinky a změny SQL Serveru 2000	261
	HACKOVÁNÍ SQL SERVERU	262
	Sběr údajů o zabezpečení SQL Serveru	262
	Nástroje a postupy pro hackování SQL Serveru	264
	Znamá zranitelná místa SQL Serveru	274
	Útoky pomocí injekce SQL kódu	278
	Zneužívání rozšířených uložených procedur pro manipulaci se systémem Windows 2000	283
	NEJLEPŠÍ POSTUPY PRO ZABEZPEČENÍ SQL SERVERU	286
	SOUHRN	290
	ODKAZY A DALŠÍ LITERATURA	291
12	Hackování Terminal Serveru	293
	ZÁKLADY TECHNOLOGIE TERMINAL SERVICES	294
	Server	295
	Protokol RDP (Remote Desktop Protocol)	295
	Klienti	295
	IDENTIFIKACE A INVENTARIZACE TERMINAL SERVICES	296
	ÚTOKY NA TERMINAL SERVICES	299
	Braňte se co nejlépe!	302
	Základní zabezpečení serveru TS	303
	Pokročilé vlastnosti zabezpečení serveru TS	305
	SOUHRN	306
	ODKAZY A DALŠÍ LITERATURA	307
13	Hackování internetových klientů Microsoftu	309
	KATEGORIE ÚTOKŮ	310
	IMPLEMENTACE ÚTOKŮ NA INTERNETOVÉ KLIENTY	311
	Zákeřné webové stránky	311
	Zákeřné e-mailové zprávy	311
	Zákeřný příspěvek do diskusní skupiny Usenet	314

VLASTNÍ ÚTOKY	314
Přetečení bufferu	314
Spouštění příkazů	318
Zápis lokálních souborů	321
Nakažená datová část: červi VBS v adresáři	326
Čtení místních souborů	329
Vyvolání odchozích klientských připojení	332
NYNÍ VŠE SLOŽÍME DOHROMADY: KOMPLETNÍ ÚTOK NA KLIENTA	333
VŠEOBECNÁ PROTIOPATŘENÍ	337
Proč se úplně nevzdát internetových klientů od Microsoftu?	339
Zóny zabezpečení Internet Exploreru	340
Antivirové programy pro klienty a servery	345
Filtrování obsahu na síťových branách	346
SOUHRN	346
ODKAZY A DALŠÍ LITERATURA	347
14 Fyzické útoky	351
OFFLINE ÚTOKY PROTI DATABÁZI SAM	352
DŮSLEDKY PRO SYSTÉM EFS	354
SOUHRN	361
ODKAZY A DALŠÍ LITERATURA	362
15 Odepření služby (DoS)	365
SOUČASNÉ ÚTOKY DOS NA SYSTÉMY WINDOWS 2000	367
NEJÚČINNĚJŠÍ ZPŮSOBY OCHRANY PROTI ÚTOKŮM DOS	375
Nejlepší postupy	376
Rady určené pro systém Windows 2000	376
SOUHRN	379
ODKAZY A DALŠÍ LITERATURA	379

ČÁST 5

BRÁNÍME SE

16 Prostředky a nástroje pro zabezpečení Windows 2000	383
ŠABLONY ZABEZPEČENÍ A NÁSTROJ KONFIGURACE	
A ANALÝZA ZABEZPEČENÍ	384
Šablony zabezpečení	385
Konfigurace a analýza zabezpečení	388
ZÁSADY SKUPINY	388

Definované zásady skupiny	389
Práce se zásadami skupiny	390
Jak jsou zásady skupiny aplikovány	391
IPSEC	393
Přednosti filtrů IPsec	393
Známa omezení filtrů IPsec	393
Podrobný návod pro vytvoření zásady IPsec	398
Správa filtrů z příkazové řádky – nástroj ipsecpol	404
Nástroje pro IPsec	406
KERBEROS	407
ŠIFROVACÍ SOUBOROVÝ SYSTÉM	408
RUNAS	409
OCHRANA SOUBORŮ SYSTÉMU WINDOWS	411
Jak obejít Ochranu souborů	411
SOUHRN	413
ODKAZY A DALŠÍ LITERATURA	413

17 Budoucnost Windows 2000 415

BUDOUCNOST WINDOWS: HARMONOGRAM DALŠÍHO VÝVOJE	416
.NET FRAMEWORK	416
Common Language Runtime (CLR)	417
Třídy .NET Framework	418
ASP.NET	418
KÓDOVÝ NÁZEV WHISTLER	418
Verze nového systému	418
Prostředky pro zabezpečení ve Whistleru	419
Poznámka k různým bezvýznamným tvrzením	428
SOUHRN	429
ODKAZY A DALŠÍ LITERATURA	429

A Kontrolní seznam zabezpečení Windows 2000 431

KUPČE, MĚJ SE NA POZORU! (ROLE A ZODPOVĚDNOSTI)	432
CO UDĚLAT JEŠTĚ PŘED ZAČÁTKEM INSTALACE	432
ZÁKLADNÍ ZPEVNĚNÍ SYSTÉMU	433
Ruční úpravy systému	433
Doporučení pro šablony zabezpečení	437
Zásady skupiny	440
Různé konfigurace	440
ÚVAHY O ZABEZPEČENÍ IIS 5	441
ÚVAHY O ZABEZPEČENÍ SQL SERVERU	444
ÚVAHY O ZABEZPEČENÍ SERVERU TERMINAL SERVICES	446

Hacking bez tajemství: Windows 2000

OPATŘENÍ PROTI ÚTOKŮM TYPU DOS	447
ZABEZPEČENÍ INTERNETOVÝCH KLIENTŮ	448
PROVĚŘUJTE, PROVĚŘUJTE, PROVĚŘUJTE!	449
ODKAZY A DALŠÍ LITERATURA	450
Rejstřík	451