

STRUČNÝ OBSAH

ČÁST 1 PŘÍPRAVA PŮDY

| | | |
|---|---------------------|----|
| 1 | Hledání stop | 9 |
| 2 | Skenování | 33 |
| 3 | Inventarizace | 61 |

ČÁST 2 HACKOVÁNÍ SYSTÉMU

| | | |
|---|-------------------------------------|-----|
| 4 | Hackování Windows 95, 98 a ME | 113 |
| 5 | Hackování Windows NT | 133 |
| 6 | Hackování Novell NetWare | 191 |
| 7 | Hackování Unixu | 229 |

ČÁST 3 HACKOVÁNÍ SÍTĚ

| | | |
|----|---|-----|
| 8 | Hacking vytáčeného spojení, PBX, hlasové pošty a sítí VPN | 293 |
| 9 | Síťová zařízení | 333 |
| 10 | Hackování bezdrátových sítí | 373 |
| 11 | Firewally | 409 |
| 12 | Útoky typu DoS | 429 |

ČÁST 4 HACKOVÁNÍ SOFTWARE

| | | |
|----|---|-----|
| 13 | Slabá místa vzdáleného přístupu | 451 |
| 14 | Pokročilé metody | 471 |
| 15 | Hackování webů | 505 |
| 16 | Hackování internetového uživatele | 537 |

ČÁST 5 PŘÍLOHY

| | | |
|---|--|-----|
| A | Porty | 591 |
| B | 14 nejdůležitějších bezpečnostních děr | 597 |
| | Rejstřík | 599 |

OBSAH

| | |
|---|-------|
| PŘEDMLUVA | XVIII |
| PODĚKOVÁNÍ | XX |
| ÚVOD | XXI |
| NAŠÍM NEJVĚTŠÍM NEPŘÍTELEM JE VLASTNÍ NEDBALOST | XXI |
| Co je nového ve třetím vydání | xxi |

ČÁST 1

PŘÍPRAVA PŮDY

| | |
|---|-----------|
| STUDIE: MONITOROVÁNÍ SÍŤOVÉ BEZPEČNOSTI | 2 |
| Reakce na útok s pomocí systému NSM | 7 |
| 1 Hledání stop | 9 |
| CO TO JE VYHLEDÁVÁNÍ STOP? | 10 |
| HLEDÁNÍ STOP V INTERNETU | 10 |
| Krok 1. Určení sféry zájmů | 11 |
| Krok 2. Mapování sítě | 14 |
| Krok 3. Zkoumání DNS | 23 |
| Krok 4. Průzkum sítě | 27 |
| SHRNUTÍ | 31 |
| 2 Skenování | 33 |
| IDENTIFIKACE FUNKČNÍCH SYSTÉMŮ | 34 |
| IDENTIFIKACE BĚŽÍCÍCH SLUŽEB | 40 |
| Typy skenů | 40 |
| Identifikace služeb TCP a UDP | 42 |
| Skenery na platformě Windows | 46 |

| | | |
|----------|---|-----------|
| | IDENTIFIKACE OPERAČNÍHO SYSTÉMU | 53 |
| | AUTOMATIZOVANÉ UTILITY | 58 |
| | SHRNUTÍ | 59 |
| 3 | Inventarizace | 61 |
| | ZÁKLADY INVENTARIZACE BANNERŮ | 63 |
| | INVENTARIZACE BĚŽNÝCH SÍŤOVÝCH SLUŽEB | 65 |
| | SHRNUTÍ | 108 |

ČÁST 2

HACKOVÁNÍ SYSTÉMU

| | | |
|----------|--|------------|
| | STUDIE: NÁSTRAHY PENETRAČNÍCH TESTŮ | 110 |
| 4 | Hackování Windows 95, 98 a ME | 113 |
| | SÍŤOVÉ ÚTOKY NA WIN9X | 115 |
| | Přímé připojení ke sdíleným prostředkům | 115 |
| | Zadní vrátka a trojští koně | 120 |
| | Chyby v serverových aplikacích | 124 |
| | LOKÁLNÍ ÚTOKY NA WIN9X | 125 |
| | WINDOWS MILLENIUM (ME) | 130 |
| | Síťové útoky na WinMe | 130 |
| | Lokální útoky na WinMe | 130 |
| | SHRNUTÍ | 131 |
| 5 | Hackování Windows NT | 133 |
| | PŘEHLED | 135 |
| | Co zde nenajdete | 135 |
| | ÚTOKY BEZ AUTENTIZACE | 136 |
| | Útoky na SMB | 136 |
| | Útoky na IIS | 151 |
| | ÚTOKY S AUTENTIZACÍ | 159 |
| | Zvýšení privilegií | 159 |
| | Vykrádání údajů | 164 |
| | Vzdálené ovládání a zadní vrátka | 172 |
| | Přesměrování portů | 176 |
| | Obecná opatření proti útokům s autentizací | 177 |
| | Zahlázení stop | 181 |
| | BEZPEČNOSTNÍ NÁSTROJE RODINY NT | 183 |
| | Včasná aplikace záplat | 183 |

| | |
|---|-----|
| Group Policy | 184 |
| IPSec | 185 |
| runas | 186 |
| .NET Framework | 187 |
| Internet Connection Firewall | 188 |
| Šifrovaný souborový systém EFS | 188 |
| Poznámka o Raw Sockets a dalších nedoložených tvrzeních | 189 |
| SHRNUTÍ | 189 |

| | | |
|----------|---------------------------------------|------------|
| 6 | Hackování Novell NetWare | 191 |
| | PŘIPOJIT SE, ALE NEDOTÝKAT | 193 |
| | ZMAPOVÁNÍ BINDERY A NDS STROMŮ | 194 |
| | JAK OTEVŘÍT ODEMKNUTÉ DVEŘE | 200 |
| | SBÍRÁNÍ INFORMACÍ PO PŘIHLÁŠENÍ | 202 |
| | ZÍSKÁNÍ ADMINA | 206 |
| | ZRANITELNOST APLIKACÍ | 208 |
| | SPOOFING ÚTOKY (PANDORA) | 215 |
| | A JSTE JAKO ADMIN NA SERVERU | 217 |
| | ZÍSKÁNÍ NDS SOUBORŮ | 219 |
| | OŠETŘENÍ LOGŮ | 223 |
| | ZÁZNAMY KONZOLY (CONSOLE LOGS) | 225 |
| | SHRNUTÍ | 228 |

| | | |
|----------|---|------------|
| 7 | Hackování Unixu | 229 |
| | HLEDÁNÍ ROOTA | 230 |
| | Krátký přehled | 230 |
| | Mapování slabých míst | 230 |
| | VZDÁLENÝ VERSUS LOKÁLNÍ PŘÍSTUP | 231 |
| | VZDÁLENÝ PŘÍSTUP | 232 |
| | Datové útoky | 235 |
| | Já chci shell | 241 |
| | Běžné typy síťových útoků | 244 |
| | LOKÁLNÍ PŘÍSTUP | 265 |
| | KONTO SUPERUŽIVATELE JE NAŠE, CO DÁL? | 277 |
| | Rootkity | 278 |
| | Uvedení napadeného systému do původního stavu | 287 |
| | SHRNUTÍ | 288 |

HACKOVÁNÍ SÍTĚ

| | | |
|-----------|--|------------|
| | STUDIE: TUNELOVÁNÍ SKRZ FIREWALLY | 292 |
| 8 | Hacking vytáčeného spojení, PBX, hlasové pošty a sítě VPN | 293 |
| | PŘÍPRAVA K ÚTOKU | 294 |
| | HROMADNÉ VYTÁČENÍ | 296 |
| | Hardware | 296 |
| | Právní otázky | 297 |
| | Náklady na meziměstské hovory | 297 |
| | Software | 297 |
| | ÚTOKY HRUBOU SILOU | 310 |
| | ÚTOKY NA POBOČKOVÉ ÚSTŘEDNY | 319 |
| | SYSTÉMY HLASOVÉ POŠTY | 323 |
| | ÚTOKY NA VPN | 327 |
| | SHRNUTÍ | 331 |
| 9 | Síťová zařízení | 333 |
| | OBJEVOVÁNÍ | 334 |
| | Detekce | 334 |
| | VYHLEDÁNÍ AUTONOMNÍHO SYSTÉMU | 337 |
| | Normální trasování | 338 |
| | Trasování s informacemi o ASN | 338 |
| | show ip bgp | 338 |
| | VEŘEJNÉ DISKUSNÍ SKUPINY | 339 |
| | DETEKCE SLUŽEB | 340 |
| | BEZPEČNOSTNÍ CHYBY NA SÍTĚ | 345 |
| | Vrstva OSI 1 – fyzická | 346 |
| | Vrstva OSI 2 – linková | 347 |
| | DETEKCE MÉDIA DRUHÉ VRSTVY | 347 |
| | Odposlouchávání na přepínané síti | 347 |
| | Vrstva OSI 3 – síťová | 354 |
| | Nesprávné konfigurace | 358 |
| | Hackování směrovacích protokolů | 363 |
| | SHRNUTÍ | 372 |
| 10 | Hackování bezdrátových sítí | 373 |
| | PŘŮZKUM TERÉNU V BEZDRÁTOVÉ SÍTĚ | 374 |
| | Vybavení | 375 |

| | |
|---|------------|
| SKENOVÁNÍ A INVENTARIZACE BEZDRÁTOVÉ SÍTĚ | 387 |
| Odposlouchávání na bezdrátové síti | 387 |
| Nástroje pro monitorování | 389 |
| Omezení přístupu podle MAC adresy | 396 |
| ZÍSKÁNÍ PŘÍSTUPU (HACKOVÁNÍ 802.11) | 397 |
| Omezení přístupu podle MAC adresy | 399 |
| Útoky na algoritmus WEP | 400 |
| Zabezpečení algoritmu WEP | 401 |
| NÁSTROJE PRO ZNEUŽITÍ SLABIN WEP | 402 |
| ÚTOKY TYPU DOS | 405 |
| PŘEHLED 802.1X | 405 |
| SHRNUTÍ | 406 |
| 11 Firewally | 409 |
| TYPY FIREWALLŮ | 410 |
| IDENTIFIKACE FIREWALLU | 410 |
| Pokročilé vyhledávání firewallů | 415 |
| SKENOVÁNÍ SKRZ FIREWALLY | 418 |
| FILTROVÁNÍ PAKETŮ | 422 |
| ZRANITELNOST APLIKAČNÍCH PROXY SERVERŮ | 424 |
| Chyby programu WinGate | 426 |
| SHRNUTÍ | 428 |
| 12 Útoky typu DoS | 429 |
| MOTIVACE ÚTOČNÍKŮ | 430 |
| TYPY DOS ÚTOKŮ | 431 |
| Obsazení přenosové kapacity linky | 431 |
| Přivlastnění systémových zdrojů | 432 |
| Chyby v programech | 432 |
| Útoky na DNS a systémy směrování paketů | 432 |
| OBECNÉ DOS ÚTOKY | 433 |
| Cílové systémy | 435 |
| DOS ÚTOKY NA UNIX A WINDOWS NT | 438 |
| Síťové útoky typu DoS | 439 |
| Distribuované útoky DoS | 442 |
| Lokální útoky typu DoS | 447 |
| SHRNUTÍ | 448 |

HACKOVÁNÍ SOFTWARE

| | | |
|-----------|---|------------|
| | STUDIE: NA BRZKOU SHLEDANOU! | 450 |
| 13 | Slabá místa vzdáleného přístupu | 451 |
| | ODHALENÍ SOFTWARE PRO VZDÁLENÝ PŘÍSTUP | 452 |
| | PŘIPOJENÍ | 452 |
| | SLABÁ MÍSTA | 453 |
| | VNC (VIRTUAL NETWORK COMPUTING) | 459 |
| | TERMINAL SERVER OD MICROSOFTU A CITRIX ICA | 462 |
| | Server | 462 |
| | Klient | 462 |
| | Datové spojení | 463 |
| | Vyhledávání cílů | 463 |
| | Útok na Terminal Server | 465 |
| | Další úvahy o bezpečnosti | 468 |
| | Zdroje | 469 |
| | SHRNUTÍ | 470 |
| 14 | Pokročilé metody | 471 |
| | PŘEBÍRÁNÍ SPOJENÍ | 472 |
| | ZADNÍ VRÁTKA | 474 |
| | TROJŠTÍ KONĚ | 493 |
| | Whack-A-Mole | 494 |
| | KRYPTOGRAFIE | 496 |
| | Terminologie | 496 |
| | Třídy útoků | 496 |
| | Útoky na Secure Shell (SSH) | 497 |
| | NARUŠENÍ OPERAČNÍHO SYSTÉMU: ROOTKIT Y A NÁSTROJE PRO VYTVÁŘENÍ SNÍMKŮ SYSTÉMU | 498 |
| | PRÁCE S LIDMI | 501 |
| | SHRNUTÍ | 502 |
| 15 | Hackování webů | 505 |
| | HACKING WEBOVÝCH SERVERŮ | 506 |
| | Odhalení zdrojového textu | 506 |
| | Kanonizace | 508 |
| | Útoky na WebDAV | 509 |
| | Přeplnění vyrovnávací paměti | 511 |

| | |
|--|------------|
| Chyby serveru Cold Fusion | 517 |
| Skenery chyb webových serverů | 520 |
| HACKING WEBOVÝCH APLIKACÍ | 521 |
| Hledání zranitelné webové aplikace vyhledávačem Google | 521 |
| Procházení webových odkazů | 522 |
| Vyhodnocení webových aplikací | 523 |
| Časté chyby webových aplikací | 529 |
| SHRNUTÍ | 535 |

| | | |
|-----------|--|------------|
| 16 | Hackování internetového uživatele | 537 |
| | NEPŘÁTELSKÝ MOBILNÍ KÓD | 538 |
| | Microsoft ActiveX | 539 |
| | Bezpečnostní díry v Javě | 548 |
| | Pozor na cookies | 551 |
| | Chyby rámců HTML (frame) Internet Exploreru | 556 |
| | ZNEUŽITÍ SSL | 557 |
| | ZNEUŽÍVÁNÍ ELEKTRONICKÉ POŠTY | 559 |
| | Generování e-mailů | 560 |
| | Vykonání libovolného kódu prostřednictvím e-mailu | 562 |
| | Outlook a červi šířící se pomocí adresáře | 574 |
| | Útoky pomocí příloh dopisů (attachmentů) | 576 |
| | Uložení přílohy na disk bez spolupráce uživatele | 579 |
| | Iniciování odchozích spojení | 583 |
| | ÚTOKY NA IRC | 585 |
| | GLOBÁLNÍ OBRANA PROTI ÚTOKŮM NA INTERNETOVÉHO UŽIVATELE | 586 |
| | SHRNUTÍ | 588 |

ČÁST 5

PŘÍLOHY

| | | |
|----------|---|------------|
| A | Porty | 591 |
| B | 14 nejdůležitějších bezpečnostních děr | 597 |
| | Rejstřík | 599 |