

# Obsah

<b>Úvod</b> .....	<b>xv</b>
<b>I: ZÁKLADY POČÍTAČOVÉ BEZPEČNOSTI</b> .....	<b>1</b>
<b>1: Úvod</b> .....	<b>3</b>
Co je to počítačová bezpečnost? .....	6
Co je to operační systém? .....	7
Historie Unixu .....	8
Unix a bezpečnost .....	15
Úloha této knihy .....	20
<b>2: Strategie a doporučení</b> .....	<b>23</b>
Plánování bezpečnostních potřeb .....	24
Odhad rizika .....	27
Analýza poměru nákladů a efektu .....	30
Strategie .....	35
Bezpečnost a zatemňování .....	40
<b>II: ZODPOVĚDNOST UŽIVATELŮ</b> .....	<b>47</b>
<b>3: Uživatelé a hesla</b> .....	<b>49</b>
Uživatelská jména .....	49
Hesla .....	51

Zadávání hesla .....	57
Změna hesla .....	58
Ověření nového hesla .....	59
Volba hesla .....	61
Jednorázová hesla.....	6
Shrnutí .....	68
<b>4: Uživatelé, skupiny a superuživatel .....</b>	<b>71</b>
Uživatelé a skupiny.....	71
Speciální uživatelská jména.....	78
su: Změna identity.....	84
Shrnutí .....	90
<b>5: Souborový systém Unixu .....</b>	<b>91</b>
Soubory .....	91
Použití přístupových práv .....	100
umask .....	113
Použití přístupových práv adresářů .....	115
SUID.....	118
Soubory zařízení .....	129
chown: Změna vlastníka souboru .....	132
chgrp: Změna skupiny souboru .....	134
Neobvyklé a nedobré nápady.....	134
Shrnutí .....	137
<b>6: Kryptografie .....</b>	<b>139</b>
Stručná historie kryptografie.....	139
Co je to šifrování?.....	142
Šifrovací systém Enigma .....	147
Obvyklé šifrovací algoritmy .....	149
Výtahy zpráv a digitální podpisy .....	167
Šifrovací programy na Unixu.....	174
des: Data Encryption Standard .....	178
Šifrování a zákonné úpravy v USA.....	190

<b>III: BEZPEČNOST SYSTÉMU.....</b>	<b>195</b>
<b>7: Zálohy.....</b>	<b>197</b>
Zálohujte! .....	198
Příklady zálohovacích strategií.....	210
Zálohování systémových souborů.....	215
Zálohovací software .....	218
<b>8: Ochrana účtů.....</b>	<b>225</b>
Nebezpečné účty.....	225
Sledování formátu souborů .....	235
Omezení přihlášení .....	236
Správa nevyužívaných účtů.....	237
Ochrana superuživatelského účtu.....	243
Systém šifrování hesel v Unixu .....	246
Jednorázová hesla.....	250
Metody pro správu konvenčních hesel.....	255
<b>9: Kontrola integrity.....</b>	<b>271</b>
Prevence.....	273
Detekce změn.....	277
Slovo závěrem .....	286
<b>10: Auditing a logging.....</b>	<b>289</b>
Základní logovací soubory .....	290
Účtování procesů v souborech acct/pacct .....	299
Logovací soubory jednotlivých příkazů .....	302
Záznamy práce uživatelů se souborovým systémem .....	307
Systémový log Unixu (syslog) .....	309
Swatch: sledování logovacích souborů.....	318
Ručně vedené záznamy .....	321
Správa logovacích souborů .....	324
<b>11: Ochrana proti programovému ohrožení.....</b>	<b>327</b>
Programové ohrožení - definice .....	327
Poškození .....	337

Autoři.....	338
Vstup .....	339
Ochrana .....	340
Ochrana vašeho systému.....	353
<b>12: Fyzická bezpečnost.....</b>	<b>357</b>
Často opomíjená hrozba.....	357
Ochrana počítačového hardwaru.....	359
Ochrana dat.....	374
Příběh: nevydařená inspekce .....	384
<b>13: Personální bezpečnost .....</b>	<b>389</b>
Průzkum minulosti .....	390
V práci .....	391
Lidé z vnějšku.....	395
<b>IV: BEZPEČNOST SÍTĚ A INTERNETU .....</b>	<b>397</b>
<b>14: Telefonní bezpečnost.....</b>	<b>399</b>
Teorie funkce modemů.....	399
Sériová rozhraní.....	401
Sériový protokol RS-232 .....	401
Modemy a bezpečnost .....	405
Modemy a Unix .....	411
Zvýšení bezpečnosti modemů.....	418
<b>15: UUCP.....</b>	<b>421</b>
Popis UUCP .....	422
Verze UUCP.....	426
UUCP a bezpečnost.....	427
Bezpečnost v UUCP Version 2 .....	430
Bezpečnost na BNU UUCP .....	437
Další bezpečnostní úvahy.....	445
Bezpečnostní problémy prvních verzí UUCP .....	446
UUCP na sítích .....	447
Shrnutí.....	448

<b>16: Síť na bázi TCP/IP .....</b>	<b>449</b>
Síť .....	449
IPv4 - Internet Protocol Version 4 .....	453
Bezpečnost IP .....	470
Další síťové protokoly .....	477
Shrnutí .....	478
<b>17: Služby TCP/IP .....</b>	<b>479</b>
Základy unixovských internetových serverů .....	480
Řízení přístupu k serverům .....	484
Primární unixové síťové služby .....	485
Bezpečnostní dopady síťových služeb .....	530
Sledování sítě programem netstat .....	531
Hlídní sítě .....	534
Shrnutí .....	535
<b>18: Bezpečnost WWW .....</b>	<b>537</b>
Bezpečnost a World Wide Web .....	537
Provoz bezpečného serveru .....	539
Řízení přístupu k souborům na serveru .....	549
Vyloučení možnosti odposlechu .....	555
Rizika na straně prohlížeče .....	560
Závislost na třetích stranách .....	563
Shrnutí .....	564
<b>19: RPC, NIS, NIS+ a Kerberos .....</b>	<b>565</b>
Zabezpečení síťových služeb .....	566
Remote Procedure Call (RPC) .....	567
Secure RPC (AUTH_DES) .....	570
Network Information Service (NIS) .....	579
NIS+ .....	587
Kerberos .....	594
Ostatní síťové autentifikační služby .....	603

<b>20: NFS</b> .....	<b>605</b>
Úvod do NFS.....	605
NFS bezpečnost na straně serveru .....	616
Bezpečnost na straně NFS klienta .....	621
Závěrem.....	631
<b>V: POKROČILÁ TÉMATA</b> .....	<b>635</b>
<b>21: Firewally</b> .....	<b>637</b>
Co je to firewall? .....	638
Vytvoření vlastního firewallu .....	648
Příklad: Cisco router jako propust .....	652
Nastavení brány .....	658
Další doporučení .....	664
Závěrečné poznámky .....	465
<b>22: Wrappery a proxy</b> .....	<b>669</b>
Proč wrappery? .....	669
Wrapper programu sendmail (smap/smapi) .....	670
tcpwrapper.....	674
SOCKS .....	687
UDP Relayer .....	697
Tvorba vlastních wrapperů .....	697
<b>23: Tvorba bezpečných SUID a síťových programů</b> .....	<b>701</b>
Jedna chyba vám může zkazit celý den.....	701
Tipy pro omezení bezpečnostních chyb .....	705
Tipy při tvorbě síťových programů .....	713
Tipy pro tvorbu SUID/SGID programů .....	716
Tipy pro práci s hesly.....	719
Tipy pro práci s generátory náhodných čísel .....	720
<b>VI: POSTUP PŘI NAPADENÍ</b> .....	<b>729</b>

<b>24: Odhalení průniku .....</b>	<b>731</b>
Úvod .....	731
Odhalení útočníka .....	733
Logovací soubory - odhalení stop po útočnickovi.....	745
Úklid po útočnickovi.....	746
Příklad.....	752
Fáze obnovení .....	754
Ošetření škod .....	755
<b>25: Útok zablokováním služeb a možná ochrana..</b>	<b>757</b>
Destruktivní útoky.....	758
Útoky přetížením.....	759
Síťové útoky zablokováním služeb .....	773
<b>26: Počítačová bezpečnost a legislativa USA.....</b>	<b>777</b>
Zákonné možnosti po průniku.....	777
Trestní stíhání.....	778
Občanské spory .....	787
Další zodpovědnost .....	788
<b>27: Komu můžete věřit? .....</b>	<b>797</b>
Můžete věřit počítači? .....	797
Můžete věřit dodávce?.....	801
Můžete věřit lidem? .....	808
Co z toho všeho plyne .....	812
<b>VII: PŘÍLOHY.....</b>	<b>813</b>
<b>A: Bezpečnostní kuchařka.....</b>	<b>815</b>
<b>B: Důležité soubory.....</b>	<b>837</b>
Soubory a zařízení související s bezpečností .....	837
Důležité soubory v domovských adresářích .....	844
SUID a SGID soubory .....	844

<b>C: Procesy v Unixu .....</b>	<b>855</b>
O procesech .....	855
Vytváření procesů .....	864
Signály .....	865
Příkaz kill .....	867
Spuštění Unixu a přihlášení se .....	869
<b>D: Tištěné informace .....</b>	<b>873</b>
Bezpečnost Unixu .....	873
Další počítačová literatura.....	874
Bezpečnostní periodika.....	885
<b>E: Elektronické prameny.....</b>	<b>889</b>
Mailing listy .....	890
Usenetové skupiny .....	894
Stránky WWW .....	895
Software.....	896
<b>F: Organizace .....</b>	<b>905</b>
Profesní organizace .....	905
Americké vládní instituce.....	909
Organizace první pomoci.....	910
<b>G: Tabulka IP služeb .....</b>	<b>921</b>
<b>Rejstřík.....</b>	<b>X933X</b>