

# Obsah

<b>Úvod</b>	<b>7</b>
<b>Kapitola 1: Bezpečnost unixových systémů</b>	<b>11</b>
1. Zabezpečení přípojných bodů	12
2. Vyhledávání SUID a SGID programů	13
3. Vyhledávání adresářů s právem zápisu pro skupinu a pro všechny	14
4. Vytváření flexibilní hierarchie přístupových práv pomocí POSIX ACL	15
5. Ochrana logů před modifikací	17
6. Delegace administrativních úloh	19
7. Automatická kontrola kryptografických signatur	21
8. Kontrola spuštěných služeb	23
9. Zakázat službě připojit se na rozhraní	25
10. Omezení služeb pomocí izolovaného prostředí	26
11. proftpd s autentizací prostřednictvím MySQL	29
12. Ochrana před přepsáním zásobníku	31
13. Ochrana jádra pomocí grsecurity	32
14. Omezení aplikací pomocí grsecurity	36
15. Omezení systémových volání pomocí Sysrtrace	38
16. Automatické vytváření politik pro sysrtrace	41
17. Řízení přihlášení pomocí PAM	43
18. Omezené shelly	46
19. Zavedení limitů na systémové prostředky	48
20. Automatické aktualizace systému	49
<b>Kapitola 2: Bezpečnost systémů Windows</b>	<b>51</b>
21. Kontrola instalovaných aktualizací	52
22. Výpis otevřených souborů a procesů, které je vlastní	57
23. Vypsání spuštěných služeb a otevřených portů	60
24. Zapnutí logování	61
25. Zabezpečení logovacích záznamů	62

26. Změna maximální velikosti logů	63
27. Vypnutí implicitně povoleného sdílení	64
28. Šifrování složky dočasných souborů	65
29. Smazání stránkovacího souboru při ukončení Windows	67
30. Omezení aplikací, které mohou uživatelé spouštět	68

## **Kapitola 3: Bezpečnost sítě** **71**

31. Detekce podvržených ARP údajů	72
32. Vytvoření statické ARP tabulky	74
33. Firewall pomocí Netfilteru	76
34. Firewall pomocí PacketFilteru na OpenBSD	79
35. Vytvoření autentizační brány	84
36. Firewall ve Windows	86
37. Ochrana okolí před vlastní sítí	89
38. Testování firewallu	90
39. Filtrace MAC adres pomocí NetFilteru	92
40. Blokování detekce operačního systému	94
41. Oklamání nástrojů pro vzdálenou detekci operačního systému	96
42. Vytvoření inventárního soupisu sítě	99
43. Vyhledávání slabých míst v síti	102
44. Synchronizace času na serverech	107
45. Vytvoření vlastní certifikační autority	108
46. Distribuce certifikační autority ke klientům	111
47. Šifrování protokolů POP a IMAP prostřednictvím SSL	112
48. Nastavení protokolu SMTP s podporou TLS	114
49. Vzdálená detekce odposlechu provozu	116
50. Instalace serveru Apache s podporou SSL a suEXEC	120
51. Zabezpečení démona BIND	123
52. Zabezpečení MySQL	125
53. Bezpečné sdílení souborů v Unixu	128

## **Kapitola 4: Logování** **131**

54. Nastavení centrálního logovacího serveru	132
55. Jemnější nastavení démona syslogd	133
56. Integrace Windows do infrastruktury syslogu	135
57. Automatická sumarizace logů	141

58. Automatické sledování logů	143
59. Agregace logů ze vzdálených systémů	145
60. Záznam uživatelských aktivit pomocí účtování procesů	150

## **Kapitola 5: Sledování a vyhodnocování trendů** **153**

61. Sledování dostupnosti	154
62. Grafické zobrazení trendů	161
63. Zobrazení síťových statistik v reálném čase programem ntop	163
64. Audit síťového provozu	166
65. Shromažďování statistik pomocí pravidel firewallu	168
66. Vzdálený odposlech Ethernetu	169

## **Kapitola 6: Bezpečné tunely** **173**

67. Nastavení IPsec na Linuxu	174
68. Nastavení IPsec na FreeBSD	176
69. Nastavení IPsec na OpenBSD	179
70. Tunelování protokolem PPTP	181
71. Oportunistické šifrování pomocí FreeS/WAN	184
72. Předávání a šifrování provozu pomocí SSH	186
73. Rychlé přihlašování pomocí SSH klíčů	188
74. Použití proxy Squid prostřednictvím SSH	189
75. SSH jako SOCKS proxy	191
76. Šifrování a tunelování provozu pomocí SSL	193
77. Tunelování spojení přes HTTP	196
78. Tunel pomocí VTun a SSH	197
79. Automatický generátor konfigurace pro VTun	202
80. Vytvoření multiplatformní VPN	207
81. PPP tunel	211

## **Kapitola 7: Detekce narušení sítě** **215**

82. Detekce narušení systémem Snort	216
83. Sledování záznamů IDS	220
84. Sledování v reálném čase	222
85. Správa sítě senzorů	228
86. Vytváření vlastních pravidel pro Snort	234
87. Prevence a blokování útoků pomocí nástroje Snort_inline	238

---

88. Automatické nastavení firewallu pomocí SnortSam	240
89. Detekce anomálního chování	243
90. Automatická aktualizace pravidel Snortu	244
91. Vytvoření distribuované sítě neviditelných senzorů	245
92. Snort a Barnyard v silně zatíženém prostředí	246
93. Detekce a ochrana před napadením webových aplikací	249
94. Simulace sítě zranitelných systémů	252
95. Zaznamenávání aktivit honeypotu	256
<b>Kapitola 8: Reakce a obnova po incidentu</b>	<b>259</b>
96. Vytvoření obrazu souborového systému	260
97. Ověření integrity souborů a nalezení modifikovaných souborů	261
98. Nalezení kompromitovaných balíčků pomocí RPM	265
99. Vyhledávání root-kitů	266
100. Nalezení provozovatele sítě	268
<b>Rejstřík</b>	<b>271</b>