

# Obsah

<b>Úvod</b> .....	<b>13</b>
Dělení knihy .....	13
Poděkování .....	13
<b>Část 1. Lokální bezpečnost</b>	
<b>1. Free software</b> .....	<b>17</b>
Shrnutí .....	19
Otázky .....	19
<b>2. Obecně o bezpečnosti</b> .....	<b>21</b>
Shrnutí .....	22
Otázky .....	22
<b>3. Druhy útočníků</b> .....	<b>23</b>
Shrnutí .....	24
Otázky .....	24
<b>4. Fyzické zajištění serveru</b> .....	<b>25</b>
Elektrřina .....	25
Teplota a vlhkost vzduchu .....	26
Oheň .....	27
Voda .....	27
Shrnutí .....	27
Otázky .....	28
<b>5. Boot</b> .....	<b>29</b>
Shrnutí .....	31
Otázky .....	32
<b>6. Jádro</b> .....	<b>33</b>
Shrnutí .....	35
Otázky .....	35
<b>7. LIDS - Linux Intrusion Detection System</b> .....	<b>37</b>
Shrnutí .....	41
Otázky .....	41
<b>8. Distribuce GNU/Linuxu</b> .....	<b>43</b>
Debian .....	43
Slackware .....	43
Gentoo/SourceMage .....	43
Red Hat .....	44
Fedora .....	44

OpenBSD .....	44
SuSE .....	44
Mandrake .....	44
Shrnutí .....	45
Otázky .....	45
<b>9. Social engineering .....</b>	<b>47</b>
Shrnutí .....	48
Otázky .....	48
<b>10. Školení uživatelů .....</b>	<b>49</b>
Shrnutí .....	49
Otázky .....	50
<b>11. Uživatelé a skupiny .....</b>	<b>51</b>
Shrnutí .....	53
Otázky .....	53
<b>12. Hesla .....</b>	<b>55</b>
Shrnutí .....	57
Otázky .....	57
<b>13. Útok na subsystém hesel .....</b>	<b>59</b>
John the Ripper .....	59
Single režim .....	60
Slovníkový režim .....	60
Inkrementální režim .....	60
Externí režim .....	61
Shrnutí .....	62
Otázky .....	62
<b>14. Autentizační mechanismus PAM .....</b>	<b>63</b>
Shrnutí .....	65
Otázky .....	65
<b>15. Souborový systém .....</b>	<b>67</b>
Shrnutí .....	70
Otázky .....	70
<b>16. ACL .....</b>	<b>71</b>
Shrnutí .....	72
Otázky .....	72
<b>17. Journal .....</b>	<b>73</b>
Shrnutí .....	74
Otázky .....	74

<b>18. Disková pole.....</b>	<b>75</b>
RAID 0.....	75
RAID 1.....	75
RAID 2.....	76
RAID 3.....	76
RAID 4.....	76
RAID 5.....	76
RAID 6.....	76
RAID 10.....	77
RAID 30 a RAID 50.....	77
Realizace pole.....	78
Softwarová disková pole.....	78
Shrnutí.....	82
Otázky.....	82
<b>19. Quota.....</b>	<b>83</b>
Shrnutí.....	85
Otázky.....	85
<b>20. Šifrovaný souborový systém.....</b>	<b>87</b>
Shrnutí.....	88
Otázky.....	88
<b>21. Tripwire.....</b>	<b>89</b>
Shrnutí.....	91
Otázky.....	91
<b>22. Adresář /tmp.....</b>	<b>93</b>
Shrnutí.....	93
Otázky.....	93
<b>23. Proměnná PATH.....</b>	<b>95</b>
Shrnutí.....	96
Otázky.....	96
<b>24. Logování.....</b>	<b>97</b>
Shrnutí.....	101
Otázky.....	101
<b>25. Analýza logů.....</b>	<b>103</b>
Swatch.....	103
Shrnutí.....	105
Otázky.....	105

<b>26. Zálohování dat.....</b>	<b>107</b>
Shrnutí .....	109
Otázky .....	109
<b>Část 2. Síťová bezpečnost</b>	
<b>27. Jak to chodí na síti .....</b>	<b>113</b>
Na kolik segmentů svou síť rozdělíme? .....	114
Kolik budeme potřebovat serverů? .....	114
Jak oddělíme síť od internetu? .....	115
Jakou bezpečnostní politiku zvolíme? .....	115
Jak budeme zařazovat a školit uživatele? .....	115
Shrnutí .....	116
Otázky .....	116
<b>28. Druhy síťových útoků .....</b>	<b>117</b>
Útok na web server .....	117
Odposlech komunikace.....	118
Denial of service (DoS).....	119
Podvržené IP adresy (IP spoofing) .....	120
Odcizení relace .....	120
Man-in-the-middle [muž uprostřed].....	120
Otázky .....	120
<b>29. Nebezpečné služby .....</b>	<b>121</b>
Finger .....	121
Telnet .....	122
rlogin .....	122
SMTP .....	123
FTP .....	123
CGI skripty .....	124
NTP .....	124
DNS .....	125
Shrnutí .....	125
Otázky .....	126
<b>30. Xinetd .....</b>	<b>127</b>
Shrnutí .....	130
Otázky .....	130
<b>31. E-mail (SMTP) .....</b>	<b>131</b>
Shrnutí .....	132
Otázky .....	133

<b>32. GnuPG.....</b>	<b>135</b>
Shrnutí.....	141
Otázky.....	141
<b>33. SSH.....</b>	<b>143</b>
Konfigurace serveru.....	145
Shrnutí.....	149
Otázky.....	149
<b>34. Iptables.....</b>	<b>149</b>
Shrnutí.....	155
Otázky.....	155
<b>35. Firewall.....</b>	<b>157</b>
Vyčleňte pro firewall samostatný počítač.....	157
Chraňte nejen síť, ale i samotný firewall.....	157
Firewall by měl propustit jen to, co je výslovně povoleno.....	157
Společně s firewallem by neměl počítač poskytovat další služby.....	157
Když už máme firewall, měl by chránit celou síť.....	158
Chraňte síť proti podvržení falešných IP adres.....	158
Chraňte síť před DoS útoky.....	159
Shrnutí.....	160
Otázky.....	160
<b>36. Squid.....</b>	<b>161</b>
Šetří vnějším adresním prostorem.....	161
Odděluje fyzicky oba adresní prostory.....	161
V kombinaci s netfilterem umožňuje filtrovat procházející požadavky.....	161
Může poskytovat obsahovou cache.....	161
Umožňuje přidávat další funkce pomocí redirectorů.....	161
Dovoľuje nasadit lepší zabezpečení na jednom místě.....	162
Shrnutí.....	166
Otázky.....	166
<b>37. Přidělování datového pásma.....</b>	<b>167</b>
Shrnutí.....	170
Otázky.....	170
<b>38. Sledování sítě SNMP, MRTG.....</b>	<b>171</b>
Sledování využití přenosového pásma.....	171
Sledování dostupnosti klíčových služeb.....	171
Sledování průběhu routování.....	171
Sledování bezpečnostních děr.....	171

Nezávislost na prostředí .....	171
Minimální vliv na samotnou síť .....	171
Architektura client-server .....	171
Shrnutí .....	174
Otázky .....	174
<b>39. Bezdrátové sítě .....</b>	<b>175</b>
Shrnutí .....	178
Otázky .....	178
<b>40. Skenování portů.....</b>	<b>179</b>
Nmap .....	180
Xprobe2.....	183
pOf .....	184
Shrnutí .....	185
Otázky .....	186
<b>41. Nessus .....</b>	<b>187</b>
Shrnutí .....	191
Otázky .....	191
<b>Část 3. Dodatky</b>	
<b>Dodatek A: Doporučená literatura .....</b>	<b>195</b>
Administrace systému Linux .....	195
Linux – praktická bezpečnost .....	195
Linux – administrace serveru Apache .....	195
Bezpečnost v UNIXu a internetu v praxi .....	196
Kukaččí vejce .....	196
Bezpečnost v Linuxu.....	196
Velký průvodce protokoly TCP/IP: Bezpečnost.....	196
Firewally a proxy-servery.....	197
Linux Dokumentační projekt .....	197
<b>Dodatek B: Odkazy na internetové zdroje.....</b>	<b>199</b>
www.root.cz .....	199
www.linux.cz .....	199
www.abclinuxu.cz .....	199
www.linuxzone.cz .....	199
www.penguin.cz .....	199
www.underground.cz .....	200
www.linux.sk .....	200
www.hysteria.sk .....	200
www.blackhole.sk .....	200
www.linuxsecurity.com .....	200

www.securityfocus.com .....	200
www.cert.org .....	200
www.securitylinux.net .....	201
www.securitysearch.net .....	201
www.faqs.org/faqs/computer-security/ .....	201
www.heavysecurity.com .....	201
www.hackerwhacker.com .....	201
www.freshmeat.net .....	201
www.google.com .....	201
<b>Rejstřík.....</b>	<b>203</b>