

Spis treści

O AUTORZE	4
O RECENZENCIE TECHNICZNYM	4
PODZIĘKOWANIA	4
WPROWADZENIE	11
1	
PIERWSZE KROKI — PODSTAWOWY SYSTEM LINUKSOWY I MAPA SIECI	17
Linuksowe systemy operacyjne	18
(1) Tworzenie wirtualnej maszyny Ubuntu	19
Wybór hiperwizora	19
VMware Workstation i VMware Player dla systemu Windows	19
VMware Fusion i VMware Fusion Player dla systemu macOS	20
VirtualBox	21
(2) Tworzenie fizycznego systemu linuksowego	22
Tworzenie rozruchowego dysku USB w systemie Windows	22
Tworzenie rozruchowego dysku USB w systemie macOS	23
Używanie rozruchowego dysku USB	23
(3) Tworzenie chmurowego systemu linuksowego	24
Finalizowanie instalacji Linuksa	25
Hartowanie systemu Ubuntu	26
(4) Instalowanie pakietów systemowych	27
(5) Zarządzanie użytkownikami Linuksa	28
(6) Zabezpieczanie dostępu zdalnego	30
Generowanie kluczy SSH	30
Zdalne logowanie z wykorzystaniem SSH	33
(7) Zapisywanie konfiguracji maszyn wirtualnych	34
Tworzenie migawek w programie VMware	34
Tworzenie migawek w programie VirtualBox	34

Topologia sieci	34
(8) Sprawdzanie swojego adresu IP	36
W Windowsie	36
W Macu	36
W Linuksie	37
(9) Tworzenie mapy sieci	37
(10) Przenoszenie plików	40
Podsumowanie	41

2

ARCHITEKTURA I SEGMENTACJA SIECI42

Urządzenia sieciowe	43
Koncentratory	43
Przełączniki	43
Routery	44
Tworzenie stref zaufania	44
Segmentacja fizyczna	44
Segmentacja logiczna	45
(11) Segmentowanie sieci	45
Segmentacja Ethernetu	46
Podsumowanie	49

3

FILTROWANIE RUCHU SIECIOWEGO ZA POMOCĄ ZAPÓR50

Typy zapór	51
iptables	52
(12) Instalacja iptables	53
Reguły zapory iptables	54
Konfigurowanie iptables	56
Rejestrowanie działania iptables	60
pfSense	62
(13) Instalacja zapory pfSense	63
Hartowanie zapory pfSense	65
Reguły zapory pfSense	66
(14) Testowanie zapory	68
Podsumowanie	69

4

ZABEZPIECZANIE SIECI BEZPRZEWODOWYCH70

(15) Wyłączanie IPv6	71
(16) Ograniczanie dostępu urządzeń sieciowych	72
Tworzenie listy zasobów	73
Statyczne adresowanie IP	74
Filtrowanie adresów MAC	76

(17) Segmentowanie sieci	78
(18) Konfigurowanie uwierzytelniania bezprzewodowego	79
WEP	79
WPA/WPA2	80
WPA3	80
Podsumowanie	83
5	
Tworzenie wirtualnej sieci prywatnej	84
Wady zewnętrznych usług VPN i zdalnego dostępu	85
OpenVPN	85
EasyRSA	86
Wireguard	86
(19) Tworzenie sieci VPN z wykorzystaniem OpenVPN	87
Konfigurowanie urzędu certyfikacji	88
Tworzenie certyfikatu i klucza serwera OpenVPN	89
Konfigurowanie OpenVPN	93
(20) Tworzenie VPN za pomocą Wireguarda	101
Instalowanie rozwiązania Wireguard	101
Konfigurowanie par kluczy	101
Konfigurowanie rozwiązania Wireguard	102
Testowanie VPN	108
Podsumowanie	109
6	
Serwer proxy Squid — lepszy internet, więcej prywatności	110
Po co używać serwera proxy?	111
(21) Konfigurowanie Squida	112
Instalowanie i wstępne konfigurowanie Squida	112
Konfigurowanie urządzeń do używania Squida	116
Testowanie Squida	117
Blokowanie i akceptowanie domen	118
Ochrona informacji osobistych z wykorzystaniem Squida	120
Wyłączanie buforowania określonych witryn	121
Raporty serwera proxy	121
Podsumowanie	124
7	
Blokowanie reklam internetowych	125
Blokowanie reklam na poziomie przeglądarki	125
(22) Blokowanie reklam w Google Chrome	126
(23) Blokowanie reklam w przeglądarce Mozilla Firefox	127
(24) Ustawienia prywatności w przeglądarce Brave	128

(25) Blokowanie reklam z wykorzystaniem Pi-Hole	128
Konfigurowanie serwera Pi-Hole	129
Używanie serwera Pi-Hole	133
Konfigurowanie DNS w punktach końcowych	135
Podsumowanie	137
 8	
WYKRYWANIE, USUWANIE I BLOKOWANIE ZŁOŚLIWEGO OPROGRAMOWANIA	138
Microsoft Defender	139
Wybieranie narzędzi do wykrywania złośliwego oprogramowania i wirusów	140
Farma antywirusowa	141
Sygnatury i heurystyka	141
(26) Instalowanie programu Avast w systemie macOS	141
(27) Instalowanie programu ClamAV w Linuksie	143
(28) Używanie witryny VirusTotal	146
(29) Zarządzanie poprawkami i aktualizacjami	147
Windows Update	147
Aktualizowanie systemu macOS	148
Aktualizowanie Linuksa za pomocą programu apt	148
(30) Automox	150
Instalowanie Automoxa	150
Używanie Automoxa	151
Podsumowanie	152
 9	
BACKUP DANYCH	153
Typy backupu	153
Harmonogram backupu	155
Lokalne i zdalne kopie zapasowe	155
Co kopiować i jakiej pamięci masowej używać?	156
(31) Kopia zapasowa w systemie Windows	156
(32) Używanie narzędzia Kopia zapasowa i przywracanie w systemie Windows	157
(33) Używanie Time Machine w systemie macOS	159
(34) Używanie linuksowego narzędzia duplicity	161
Tworzenie lokalnych kopii zapasowych za pomocą duplicity	161
Tworzenie sieciowych kopii zapasowych za pomocą duplicity	162
Przywracanie kopii zapasowych duplicity	163
Dodatkowe funkcje duplicity	163
Rozwiązania do backupu w chmurze	165
Backblaze	165
Carbonite	166
Migawki maszyn wirtualnych	167
Testowanie i przywracanie kopii zapasowych	169
Podsumowanie	169

10	
MONITOROWANIE SIECI POPRZEC DETEKCJĘ I ALARMOWANIE	171
Metody monitorowania sieci	172
Punkty dostępu do ruchu sieciowego	172
Analizatory portów przełącznika	174
(35) Konfigurowanie portu SPAN	175
Security Onion	175
(36) Budowanie systemu Security Onion	176
Instalowanie Security Onion	177
(37) Instalowanie pakietu Wazuh	184
Instalowanie agenta Wazuh w systemie Windows	184
Instalowanie agenta Wazuh w systemie macOS	186
Instalowanie agenta Wazuh w systemie Linux	188
(38) Instalowanie osquery	189
Instalowanie osquery w systemie Windows	190
Instalowanie osquery w systemie macOS	190
Instalowanie osquery w systemie Linux	191
Krótki kurs monitorowania bezpieczeństwa sieci	191
Używanie osquery	191
Używanie Wazuh	194
Używanie Security Onion jako narzędzia SIEM	196
Podsumowanie	199
11	
ZARZĄDZANIE BEZPIECZEŃSTWEM UŻYTKOWNIKÓW W TWOJEJ SIECI	200
Hasła	201
Menedżery haseł	201
Wykrywanie złamanych haseł	202
Uwierzytelnianie wieloskładnikowe	203
Dodatki do przeglądarek	204
Adblock Plus	204
Ghostery	205
Internet rzeczy	206
Dodatkowe zasoby	207
Podsumowanie	207