

# Spis treści

Rozdział 13.	Zakończ...	22
99	...	...
501	...	...
701	O autorce	9
	O korektorze merytorycznej	11
117	Podziękowania	13
Rozdział 14.	Przedmowa	15
111	Wprowadzenie	17
Rozdział 1.	Podstawowe narzędzia sieciowe i bezpieczeństwa	19
151	Ping	20
Rozdział 25.	IPConfig	23
154	NSLookup	26
153	Tracert	28
151	NetStat	28
151	PuTTY	33
Rozdział 2.	Rozwiązywanie problemów w systemie Microsoft Windows	37
157	Monitor niezawodności	38
150	Rejestrator kroków	40
167	PathPing	42
151	MTR	44
157	Sysinternals	45
151	Windows Master Control Panel	49
Rozdział 3.	Badanie sieci za pomocą Nmap	51
151	Identyfikacja struktury sieci	52
154	Poszukiwanie otwartych portów	54
151	Identyfikacja działających usług	56
151	Wykrywanie wersji systemów operacyjnych	59
154	Narzędzie Zenmap	59

<b>Rozdział 4.</b>	<b>Zarządzanie podatnościami na niebezpieczeństwa</b>	<b>63</b>
	Zarządzanie podatnościami na niebezpieczeństwa	64
	OpenVAS	66
	Nexpose Community	77
<b>Rozdział 5.</b>	<b>Monitorowanie bezpieczeństwa</b>	<b>83</b>
	Systemy wykrywania włamań oparte na analizie logów	84
	Agenty programowe pakietu OSSEC	87
	Analiza logów	92
<b>Rozdział 6.</b>	<b>Ochrona komunikacji bezprzewodowej</b>	<b>95</b>
	Standard 802.11	96
	Narzędzie inSSIDer	98
	Narzędzie Wireless Network Watcher	99
	Narzędzie Hamachi	100
	Sieć Tor	107
<b>Rozdział 7.</b>	<b>Wireshark</b>	<b>111</b>
	Narzędzie Wireshark	111
	Model warstwowy OSI	114
	Przechwytywanie pakietów	117
	Stosowanie filtrów i oznaczania kolorami	121
	Badanie zawartości pakietów	122
<b>Rozdział 8.</b>	<b>Zarządzanie dostępem</b>	<b>127</b>
	Uwierzytelnianie, autoryzacja i rozliczalność	128
	Zasada minimalnego i wystarczającego zakresu uprawnień	129
	Jednokrotne logowanie	131
	Platforma JumpCloud	133
<b>Rozdział 9.</b>	<b>Zarządzanie logami</b>	<b>139</b>
	Podgląd zdarzeń systemu Windows	140
	Interpreter Windows PowerShell	143
	Narzędzie BareTail	146
	Narzędzie syslog	148
	Narzędzie SolarWinds Kiwi	150
<b>Rozdział 10.</b>	<b>Pakiet Metasploit</b>	<b>157</b>
	Przeprowadzanie rekonesansu	159
	Instalacja narzędzia	160
	Uzyskiwanie dostępu	167
	Maszyna wirtualna Metasploitable2	172
	Usługi webowe z podatnościami	176
	Interpreter Meterpreter	179

<b>Rozdział 11. Bezpieczeństwo aplikacji webowych</b>	<b>181</b>
Tworzenie aplikacji webowych	182
Zbieranie informacji	185
System nazw domen DNS	188
Obrona w głąb	190
Narzędzie Burp Suite	192
<b>Rozdział 12. Zarządzanie aktualizacjami i konfiguracją</b>	<b>201</b>
Zarządzanie aktualizacjami i instalacją poprawek	202
Zarządzanie konfiguracją	210
Narzędzie Clonezilla Live	216
<b>Rozdział 13. Zabezpieczanie ósmej warstwy modelu OSI</b>	<b>223</b>
Ludzka natura	224
Ataki socjotechniczne	227
Edukacja	228
Narzędzie Social Engineer Toolkit	231
<b>Rozdział 14. Kali Linux</b>	<b>241</b>
Wirtualizacja	242
Optymalizacja pracy systemu Kali Linux	255
Korzystanie z narzędzi systemu Kali Linux	257
<b>Rozdział 15. Praktyki kontrolne CIS</b>	<b>269</b>
Podstawowe praktyki kontrolne CIS	270
Podsumowanie	284