



Spis treści

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

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

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