

Spis treści

O autorze	7
O korektorach merytorycznych	8
Wprowadzenie	9
Rozdział 1. Teoria antagonistycznych operacji i zasady konfliktów komputerowych	13
Teoria konfliktów	14
Atrybuty bezpieczeństwa informacyjnego	15
Teoria gier	16
Zasady konfliktów komputerowych	18
Atak i obrona	20
Zasada podstępny	28
Zasada fizycznego dostępu	30
Zasada człowieczeństwa	32
Zasada ekonomii	33
Zasada planowania	35
Zasada innowacji	37
Zasada czasu	38
Podsumowanie	41
Źródła	41

Rozdział 2. Przygotowanie do bitwy	45
Podstawowe rozważania	46
Komunikacja	46
Planowanie długofalowe	48
Kompetencje	50
Planowanie operacyjne	51
Perspektywa obrony	54
Zbieranie danych	56
Zarządzanie danymi	60
Narzędzia analityczne	66
Kluczowe wskaźniki efektywności zespołu obrony	70
Perspektywa ataku	70
Skanowanie i wykorzystywanie przypadków podatności na zagrożenia	71
Przygotowywanie szkodliwego oprogramowania	74
Narzędzia pomocnicze	76
Kluczowe wskaźniki efektywności zespołu ataku	78
Podsumowanie	78
Źródła	80
Rozdział 3. Najlepiej być niewidzialnym (działania w pamięci)	86
Zdobywanie przewagi	87
Perspektywa ataku	90
Wstrzykiwanie kodu do procesów	90
Operacje prowadzone w pamięci	94
Perspektywa obrony	100
Wykrywanie wstrzykiwania kodu do procesów	101
Przygotowywanie się na działania atakujących	104
Niewidoczna obrona	107
Podsumowanie	108
Źródła	109
Rozdział 4. Nie wyróżniać się z tłumu	112
Perspektywa ataku	114
Możliwości zachowania trwałego dostępu	114
Ukryte kanały dowodzenia i kierowania	119
Łączenie technik ofensywnych	124
Perspektywa obrony	126
Wykrywanie kanałów dowodzenia i kierowania	126
Wykrywanie metod zapewniania trwałego dostępu	132
Pułapki na hakerów	135
Podsumowanie	137
Źródła	138

Rozdział 5. Działania manipulacyjne	141
Perspektywa ataku	142
Czyszczenie zawartości dzienników	142
Podejście hybrydowe	145
Rootkity	147
Perspektywa obrony	148
Integralność danych i jej weryfikacja	149
Wykrywanie rootkitów	150
Manipulowanie atakującymi	151
Rozpraszanie atakujących	153
Oszukiwanie atakujących	155
Podsumowanie	158
Źródła	159
Rozdział 6. Konflikt w czasie rzeczywistym	162
Perspektywa ataku	163
Świadomość sytuacyjna	164
Zbieranie informacji operacyjnych	167
Przemieszczanie się pomiędzy elementami infrastruktury	175
Perspektywa obrony	178
Analizowanie użytkowników, procesów i połączeń	178
Wymuszanie zmiany danych uwierzytelniających	182
Ograniczanie uprawnień	184
Hacking zwrotny	187
Podsumowanie	189
Źródła	189
Rozdział 7. Przez badania do przewagi	193
Rozgrywanie gry	194
Perspektywa ataku	195
Ataki z użyciem technik uszkodzania zawartości pamięci	195
Prowadzenie celowanego rozpoznania	197
Infiltracja celu	199
Kreatywne przemieszczanie się pomiędzy elementami infrastruktury	200
Perspektywa obrony	203
Wykorzystanie narzędzi	203
Modelowanie zagrożeń	204
Badania systemu operacyjnego i aplikacji	205
Rejestrowanie i analizowanie własnych danych	207
Przypisywanie sprawstwa ataku	208
Podsumowanie	208
Źródła	209

Rozdział 8. Sprzątanie	212
Perspektywa ataku	213
Pobieranie danych	213
Kończenie operacji	220
Perspektywa obrony	222
Odpowiedź na włamanie	223
Działania naprawcze	226
Planowanie przyszłości	228
Publikowanie wyników	229
Podsumowanie	229
Źródła	230