

# Spis treści

<b>O autorze</b>	<b>7</b>
<b>O korektorach merytorycznych</b>	<b>8</b>
<b>Wprowadzenie</b>	<b>9</b>
<b>Rozdział 1. Teoria antagonistycznych operacji i zasady konfliktów komputerowych</b>	<b>13</b>
<b>Teoria konfliktów</b>	<b>14</b>
Atrybuty bezpieczeństwa informacyjnego	15
Teoria gier	16
<b>Zasady konfliktów komputerowych</b>	<b>18</b>
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
<b>Podsumowanie</b>	<b>41</b>
<b>Źródła</b>	<b>41</b>

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

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

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