

SPIS TREŚCI

Wstęp	1
1. Charakterystyka metod pozyskiwania informacji z otwartych źródeł	7
1.1. Otwarte źródła	8
1.1.1. Informacje z otwartych źródeł	10
1.1.2. SOCMINT – wywiad w ramach mediów społecznościowych	13
1.2. Sieć indeksowana i nieindeksowana	16
1.3. Rekonesans pasywny i aktywny	21
1.3.1. Rekonesans pasywny	22
1.3.1.1. Wyszukiwanie w witrynach internetowych na podstawie zapytania tekstowego	22
1.3.1.2. Wyszukiwanie w archiwach Internetu	29
1.3.1.3. Wyszukiwanie obrazów i wyszukiwanie na podstawie obrazu	29
1.3.1.4. Wyszukiwanie na podstawie zdjęcia twarzy	36
1.3.1.5. Wyszukiwanie IoT	36
1.3.1.6. Wyszukiwanie informacji na podstawie certyfikatu	42
1.3.1.7. Wyszukiwanie informacji o organizacji na podstawie analizowanych plików, adresów URL i domen	45
1.3.1.8. Wyszukiwarki kont w serwisach internetowych	47
1.3.1.9. Wyszukiwanie zdjęć profilowych (awatarów)	53
1.3.1.10. Inne narzędzia	54
1.3.2. Rekonesans aktywny	56
1.3.2.1. Skanowanie portów / usług	57
1.3.2.2. Enumeracja subdomen	57
1.3.2.3. Enumeracja SMTP	59
1.3.2.4. Nietechniczne rodzaje aktywnego rozpoznania	59
1.4. Ograniczenia etyczne	60
2. Analiza informacji pozyskanych z zasobów internetowych jako fundament wywiadu	65
2.1. Cykl wywiadowczy	68
2.2. Weryfikacja pozyskanych informacji	70
2.2.1. Weryfikacja pochodzenia	71
2.2.2. Weryfikacja źródeł	71

2.2.3. Weryfikacja czasu	72
2.2.4. Weryfikacja miejsca	73
2.2.5. Weryfikacja motywacji	81
2.2.6. Dodatkowa warstwa weryfikacji	81
2.2.7. Ustandaryzowane metody weryfikacji	82
2.3. Analiza zebranych danych	83
2.4. Błędy poznawcze w ocenie danych	85
2.4.1. Wzorce w ludzkim rozumowaniu	87
2.4.2. Rodzaje błędów poznawczych i ich wpływ na efekty rozpoznania otwartoźródłowego	88
2.5. Synteza i poprawne wyciąganie wniosków w celu uniknięcia błędów poznawczych	91
2.5.1. Techniki analityczne	93
2.5.2. Określanie prawdopodobieństwa	97
2.6. Inne czynniki ludzkie wpływające na proces prowadzenia wywiadu otwartoźródłowego	99
3. Wykorzystanie wywiadu opartego na otwartych źródłach w zakresie bezpieczeństwa osobistego, technologicznego i biznesowego	101
3.1. Zagrożenia dla bezpieczeństwa infrastruktury teleinformatycznej	102
3.1.1. Błędna konfiguracja serwisów internetowych	103
3.1.2. Zasady bezpieczeństwa operacyjnego i osobistego	110
3.2. Zagrożenia dla bezpieczeństwa osobistego	111
3.3. Zagrożenia dla bezpieczeństwa biznesowego i operacyjnego	115
4. Możliwe do wprowadzenia zalecenia bezpieczeństwa w zakresie przeciwdziałania wywiadowi otwartoźródłowemu	121
4.1. Zasady wynikające z norm, standardów i innych wytycznych	123
4.2. Stosowanie zasad bezpieczeństwa operacyjnego (OPSEC) i osobistego (PERSEC)	126
4.3. <i>Sock puppets</i> – konta alternatywnych tożsamości	128
4.4. Rozpoznanie otwartoźródłowe jako element świadomości podatności na atak	134
4.5. Rozszerzenie zasad bezpieczeństwa na otoczenie kluczowych osób w organizacjach	135
Podsumowanie	138
Bibliografia	144
Spis rysunków	150
Spis tabel	152
Wykaz skrótów	153