

ARTUR M. KALINOWSKI

METODY INWIGILACJI I ELEMENTY INFORMATYKI ŚLEDCZEJ

POZYSKIWANIE ŚLADÓW - KONSOLA WMI - KEYLOGGERY
ODZYSKIWANIE DANYCH - SZYFROWANIE - INWIGILACJA
BLOKOWANIE - STEGANOGRAFIA

METODY INWIGILACJI I ELEMENTY INFORMATYKI ŚLEDCZEJ



Tytuł: Metody inwigilacji i elementy informatyki śledczej

ISBN: 978-83-923745-4-1

Copyright © 2011 by Wydawnictwo CSH.

All Rights Reserved.

Autor: Artur Michał Kalinowski

Redakcja: Dutkon

Skład: Adekwatna

Wszelkie prawa zastrzeżone. Nieautoryzowane rozpowszechnianie całości lub fragmentu niniejszej publikacji w jakiegokolwiek postaci jest zabronione. Wykonywanie kopii metodą kserograficzną, fotograficzną, a także kopiowanie książki na nośniku filmowym, magnetycznym lub innym powoduje naruszenie praw autorskich niniejszej publikacji.

Wszystkie znaki występujące w tekście są zastrzeżonymi znakami firmowymi bądź towarowymi ich właścicieli.

Autor oraz wydawnictwo CSH dołożyli wszelkich starań, by zawarte w tej książce informacje były kompletne i rzetelne. Nie biorą jednak żadnej odpowiedzialności ani za ich wykorzystanie, ani za związane z tym ewentualne naruszenie praw patentowych lub autorskich. Autor oraz wydawnictwo CSH nie ponoszą również żadnej odpowiedzialności za ewentualne szkody wynikłe z wykorzystania informacji zawartych w książce oraz na dołączonych nośnikach.

Wydawnictwo CSH

82-500 Kwidzyn

ul. Długa 27

e-mail: wydawnictwo@csh.pl

Najnowsze informacje związane z projektem znajdziecie Państwo pod adresem

<http://www.MetodyInwigilacji.pl>. Serdecznie zapraszamy!

Printed in Poland.

Spis treści

Wskazówki prawne	9
Art. 267.	9
Art. 268.	10
Art. 268a.	10
Art. 269.	10
Art. 269a.	11
Art. 269b.	11
Wstęp	13
1. Podstawy pozyskiwania dowodów działalności użytkownika na komputerze	15
1.1. Ślady pozostawione poza komputerem lokalnym	16
1.2. Na czym polega zbieranie podstawowych śladów działalności?	17
1.3. Podstawowe zasady zbierania danych do analizy	19
1.3.1. Gromadzenie danych do analizy z pracującego systemu	20
1.3.2. Pozyskiwanie danych z nośników	24
1.4. Przygotowanie środowiska do analizy	26
1.4.1. Podstawowe narzędzia wykorzystywane w analizie i pozyskiwaniu danych	27
1.4.1.1. Narzędzia do analizy online (używane na działającym systemie)	27
1.4.1.2. Narzędzia do analizy offline (używane do analizy obrazów nośników oraz plików)	30
1.4.2. Spojrzenie na analizę danych przeprowadzaną na badanym komputerze	31
1.4.3. Gromadzenie danych do analizy z wykorzystaniem innego komputera	53
1.5. Pułapki i błędy popełniane podczas niewłaściwego zbierania i analizy dowodów	63
1.5.1. Dokumentowanie daty rozpoczęcia gromadzenia śladów	63
1.5.2. Rola właściwej kolejności pozyskiwania dowodów	64
1.5.3. Użycie odpowiednich narzędzi	65
1.5.4. Wykorzystywanie innych źródeł danych	70

1.5.5. Weryfikacja zebranego materiału i zabezpieczenie sumą kontrolną ...	71
1.5.6. Stosowanie odpowiednich uprawnień	71
1.5.7. Dokumentowanie prowadzonych czynności	72
1.5.8. Ograniczone zaufanie	72
1.5.9. Użycie narzędzi w odpowiedni sposób	73

2. Pozostawianie śladów działalności w sieci lokalnej i w Internecie 75

2.1. Ślady pozostawiane w sieci lokalnej	76
2.2. Ślady pozostawiane w Internecie	88
2.3. Informacje ujawniane przez przeglądarkę internetową	89
2.3.1. Jakie informacje przeglądarka ujawnia domyślnie?	91
2.3.2. Na ile udawanie innej przeglądarki i innego systemu jest skuteczne? ...	95
2.3.3. Czy łącząc się przez serwer proxy lub sieć Tor, jesteśmy bezpieczniejsi?	102
2.3.4. W jaki sposób zdalnie zbadać, czy dany użytkownik odwiedzał określone strony?	115
2.3.5. W jaki sposób nie będąc administratorem forum, pozyskać informacje o adresie IP, systemie i przeglądarce innych użytkowników?	130
2.3.6. Jak wykorzystać zebrane informacje do przeprowadzenia prostego i łatwego ataku?	135
2.4. Ślady pozostawione przez program pocztowy	136
2.4.1. Analiza wiadomości pocztowej z punktu widzenia odbiorcy	137
2.4.2. Ślady pozostawiane w momencie odbierania wiadomości	140
2.4.3. Jak sprawdzić, czy odbiorca odczytał e-mail, gdy nie wysłał potwierdzenia odbioru?	141
2.4.4. W jaki sposób ustalić obieg wiadomości e-mail?	143
2.5. Ślady pozostawiane przez inne programy	144

3. Ślady pozostawione w systemie lokalnym 147

3.1. Rodzaje śladów pozostawianych w systemie	148
3.2. Miejsca, gdzie pozostawiane są ślady - zbieranie dowodów działalności ...	151
3.2.1. Pamięć operacyjna	151
3.2.1.1. Pliki hiberfil.sys oraz pagefile.sys	152
3.2.2. Rejestr systemu	155
3.2.3. Sieć	171
3.2.3.1. Ślady po połączeniach z innymi komputerami	171
3.2.3.2. Sprawdzanie, jakie programy są powiązane z danymi połączeniami sieciowymi	172
3.2.3.3. Wykorzystanie whois i traceroute do przybliżonej lokalizacji maszyny o danym IP	173
3.2.3.4. Wykrywanie użycia serwerów proxy oraz tunelowania	175
3.2.3.5. Pozyskiwanie informacji w środowisku Active Directory	181
3.2.3.6. Sniffing sieciowy i zabezpieczenie przed sniffingiem	190
3.2.4. Analiza dzienników zdarzeń i logów	194
3.2.5. Analiza pliku miniatur	205
3.2.6. Analiza plików tymczasowych	206
3.2.6.1. Pliki w folderze plików tymczasowych	207
3.2.6.2. Tymczasowe pliki robocze programów	213

3.2.6.3. Pliki bufora wydruku	215
3.2.7. Analiza czasowa	218
3.2.7.1. Analiza czasowa plików i folderów	221
3.2.7.2. Określenie czasu i rodzaju uruchomionych programów na podstawie folderu Prefetch	237
3.2.7.3. Określenie rodzaju uruchamianych programów na podstawie sygnatur czasowych i modyfikacji plików	239
3.2.7.4. Określanie ostatnio otwieranych dokumentów na podstawie folderu Recent	241
3.2.7.5. Określanie ostatnio odwiedzanych lokalizacji sieciowych - NetHood	243
3.2.8. Wyszukiwanie plików	243
3.2.8.1. Sprawdzanie, jakie pliki były tworzone, modyfikowane lub otwierane w danym czasie	243
3.2.8.2. Sporządzanie listy plików według ich typu i sygnatury czasowej ..	245
3.2.8.3. Sporządzanie listy obrazków wraz z miniaturkami, pobranych lub oglądanych w danym przedziale czasowym	246
3.2.8.4. Wyszukiwanie plików ukrytych w alternatywnych strumieniach danych	247
3.2.9. Przeglądarka internetowa	249
3.2.9.1. Badanie historii przeglądarki	249
3.2.9.2. Pozyskiwanie zapamiętanych haseł z formularzy	258
3.2.9.3. Badanie cookies przeglądarki	260
3.2.9.4. Określanie treści zapytań kierowanych do serwisu Google	262
3.2.10. Poczta elektroniczna	265
3.2.10.1. Przeglądanie pliku poczty innego użytkownika komputera	265
3.2.10.2. Dekodowanie załączników do wiadomości e-mail	270
3.2.10.3. Pozyskiwanie adresów z książki adresowej oraz z pamięci procesu	271
3.2.11. Analiza komunikatorów	275
3.2.11.1. Pozyskiwanie treści rozmów z komunikatorów	275
3.2.12. Analiza usuniętych plików	281
3.2.12.1. Kosz	281
3.2.12.2. Punkt przywracania	290
3.2.12.3. Volume Shadow Copy	293
3.2.12.4. Skasowane pliki i dane w wolnych obszarach dysku	296
3.2.12.5. Dane w slack space	298
3.2.12.6. Odzyskiwanie danych z pamięci pendrive i karty pamięci	299
3.2.13. Komputer	302
3.2.13.1. Sprawdzanie, jak długo komputer jest włączony	302
3.2.13.2. Ustawienie automatycznego logowania czasu włączenia, pracy oraz wyłączenia komputera	303
4. Ograniczanie śladów działalności	305
4.1. Ograniczanie ilości śladów pozostawianych w Internecie	306
4.1.1. Podstawowe zasady bezpieczeństwa	307
4.1.2. Mechanizmy i metody wpływające na zwiększenie anonimowości ..	311
4.2. Ograniczenie ilości śladów pozostawionych w komputerze	315
4.2.1. Usuwanie danych pozostawionych przez przeglądarkę	319
4.2.2. Usuwanie danych tymczasowych	319
4.3. Ukrywanie danych	320

4.3.1. Ukrywanie danych z wykorzystaniem alternatywnych strumieni danych NTFS	321
4.3.2. Ukrywanie plików w innych plikach	323
4.3.2.1. Ataki na steganografię	332
4.3.3. Ukrywanie danych w niewykorzystanych obszarach dysku	337
4.4. Szyfrowanie danych	342
4.4.1. Szyfrowanie plików	342
4.4.2. Ataki na szyfrogramy	345
4.4.3. EFS - szyfrowanie plików i folderów oraz jego skuteczność	353
4.5. Działania utrudniające pozyskiwanie dowodów	355
5. Odzyskiwanie dostępu do komputera i łamanie haseł	357
5.1. Uzyskiwanie dostępu administracyjnego do komputera	358
5.1.1. Narzędzia pozwalające ujawnić hasło administratora	359
5.1.1.1. W jaki sposób tworzyć hasła, by utrudnić ich złamanie z wykorzystaniem specjalistycznych narzędzi?	361
5.1.2. Resetowanie haseł	361
5.1.2.1. Resetowanie haseł a korzystanie z EFS	363
5.2. Uzyskiwanie dostępu do danych w komputerze	363
5.2.1. Konsola odzyskiwania, tryb awaryjny i naprawa systemu	364
5.2.2. Wykorzystanie dystrybucji live	365
6. Techniki z pogranicza hakerstwa	367
6.1. Wykradanie danych	368
6.1.1. Z szyfrowanych dysków (np. szyfrowanych z użyciem FreeOTFE) ..	368
6.1.2. Z firm, które stosują automatyczne szyfrowanie pendrive'ów	373
6.1.2.1. Wykradanie danych z użyciem alternatywnych strumieni danych NTFS	373
6.1.2.2. Kodowanie danych w nazwach plików	374
6.1.3. Z komputerów, do których możliwe jest jedynie połączenie przez zdalny pulpit lub VNC	378
6.2. Łamanie haseł e-mail, FTP i podobnych	383
6.2.1. Łamanie haseł do kont poczty elektronicznej	383
6.2.1.1. Generowanie słownika haseł	391
6.2.2. Łamanie haseł FTP do stron WWW	392
6.3. Podszywanie się pod cudze konta e-mail	393
6.3.1. Wysyłanie fałszywych wiadomości e-mail i fałszywych potwierdzeń	393
6.3.2. Bombardowanie e-mailami	395
6.4. Inne	398
6.4.1. Zdalna instalacja VNC	398
6.4.2. Blokowanie dostępu do określonych stron	401
6.4.2.1. Blokowanie na podstawie adresu domenowego	401
6.4.2.2. Blokowanie na podstawie adresu IP	402
6.4.3. Omijanie blokady dostępu do określonych stron	403
6.4.4. Uzyskiwanie dostępu do wiersza poleceń i uruchamianie zablokowanych programów	403