

Spis treści

Przedmowa (9)

Podziękowania (15)

O autorze (17)

O korektorze merytorycznym (19)

Rozdział 1. Założenia analizy systemów komputerowych (21)

Wprowadzenie (21)

Założenia analizy systemów komputerowych (24)

Wersje systemu Windows (25)

Reguły i zasady przeprowadzania analizy (27)

Dokumentacja (40)

Konwergencja (42)

Wirtualizacja (44)

Konfiguracja środowiska śledczego (46)

Podsumowanie (50)

Rozdział 2. Szybka reakcja na incydenty (51)

Wprowadzenie (51)

Jak być przygotowanym do sprawnego reagowania na incydenty? (53)

Pytania (55)

Najważniejszy element - przygotowania (57)

Dzienniki zdarzeń (logi) (62)

Gromadzenie danych (68)

Szkolenia (72)

Podsumowanie (74)

Rozdział 3. Usługa VSS - kopiowanie woluminów w tle (75)

Wprowadzenie (75)

Czym jest usługa kopiowania woluminów w tle? (76)

Klucze w rejestrze (78)

Praca z kopiami VSS we włączonych systemach (79)

Pakiet ProDiscover (83)

Pakiet F-Response (83)

Praca z kopiami VSS w binarnych obrazach dysków (86)

Metoda z wykorzystaniem plików VHD (88)

Metoda z wykorzystaniem oprogramowania VMware (93)

Automatyzacja dostępu do kopii VSS (97)

ProDiscover (100)

Podsumowanie (103)

Literatura i inne źródła (103)

Rozdział 4. Analiza systemu plików (105)

Wprowadzenie (106)

Tablica MFT (107)

Mechanizm tunelowania w systemie plików (114)

Dzienniki zdarzeń systemowych (116)

Dziennik zdarzeń systemu Windows (121)

Folder Recycle Bin (125)

Pliki prefetch (129)

Zaplanowane zadania (134)

Listy szybkiego dostępu (138)

Pliki hibernacji (145)

Pliki aplikacji (146)

Logi programów antywirusowych (147)

Komunikator Skype (148)

Produkty firmy Apple (149)

Pliki graficzne (zdjęcia, obrazy) (151)

Podsumowanie (153)

Literatura i inne źródła (154)

Rozdział 5. Analiza rejestru systemu Windows (155)

Wprowadzenie (156)

Analiza rejestru (157)

Nomenklatura rejestru (158)

Rejestr jako plik dziennika (159)

Analiza historii urządzeń USB (160)

Gałąź System (175)

Gałąź Software (178)

Gałęzie rejestru związane z profilem użytkownika (188)

Dodatkowe źródła informacji (199)

Narzędzia (202)

Podsumowanie (204)

Literatura i inne źródła (204)

Rozdział 6. Wykrywanie złośliwego oprogramowania (205)

Wprowadzenie (206)

Typowe cechy złośliwego oprogramowania (207)

Początkowy wektor infekcji (209)

Mechanizm propagacji (212)

Mechanizm przetrwania (214)

Artefakty (219)

Wykrywanie złośliwego oprogramowania (222)

Analiza logów (223)

Skany antywirusowe (229)

Zagłębiamy głębiej (234)

Złośliwe strony internetowe (251)

Podsumowanie (254)

Literatura i inne źródła (254)

Rozdział 7. Analiza zdarzeń w osi czasu (255)

Wprowadzenie (256)

Zestawienie zdarzeń w osi czasu (256)

Źródła danych (259)

Formaty czasu (260)

Koncepcje (261)

Zalety analizy czasowej (263)

Format (267)

Tworzenie historii zdarzeń w osi czasu (273)

Metadane systemu plików (275)

Dzienniki zdarzeń (282)

Pliki prefetch (286)

Dane z rejestru (287)

Dodatkowe źródła danych (290)

Konwersja pliku zdarzeń na finalną postać (292)

Kilka uwag związanych z wizualizacją (294)

Studium przypadku (295)

Podsumowanie (299)

Rozdział 8. Analiza aplikacji (301)

Wprowadzenie (301)

Pliki logów (303)

Analiza dynamiczna (305)

Przechwytywanie ruchu sieciowego (310)

Analiza pamięci zajmowanej przez aplikację (312)

Podsumowanie (313)

Literatura i inne źródła (313)

Skorowidz (315)