Spis treści książki

        - TaHiTI - polowanie ukierunkowane integrujące informatykę wywiadowczą
    - Tworzenie hipotezy
    - Podsumowanie

Rozdział 3. Z jakich źródeł pozyskujemy dane?

- Wymogi merytoryczne i techniczne
- Zrozumienie zebranych danych
    - Podstawy systemów operacyjnych
    - Podstawy działania sieci komputerowych
- Narzędzia dostępne w systemie Windows
    - Podgląd zdarzeń w systemie Windows
    - Instrumentacja zarządzania systemem Windows (WMI)
    - Śledzenie zdarzeń dla Windows (ETW)
- Źródła danych
    - Dane z punktów końcowych
    - Dane sieciowe
    - Dane zabezpieczeń
- Podsumowanie

Część II. Zrozumieć przeciwnika

Rozdział 4. Jak mapować przeciwnika

- Wymogi merytoryczne
- Framework ATT&CK
    - Taktyki, techniki, subtechniki i procedury
    - Macierz ATT&CK
    - Nawigator ATT&CK
- Mapowanie za pomocą frameworka ATT&CK
- Przetestuj się!
    - Odpowiedzi
- Podsumowanie

Rozdział 5. Praca z danymi

- Wymogi merytoryczne i techniczne
- Używanie słowników danych
    - Metadane zdarzeń zagrażających bezpieczeństwu typu open source
- Używanie narzędzia MITRE CAR
    - CARET
- Używanie Sigmy
- Podsumowanie

Rozdział 6. Jak emulować przeciwnika

- Stworzenie planu emulacji przeciwnika
    - Czym jest emulacja przeciwnika?
    - Plan emulacji zespołu MITRE ATT&CK

- Jak emulować zagrożenie
  - Atomic Red Team
  - Mordor (Security Datasets)
  - CALDERA
  - Pozostałe narzędzia
- Przetestuj się!
  - Odpowiedzi
- Podsumowanie

Część III. Jak pracować z wykorzystaniem środowiska badawczego

Rozdział 7. Jak stworzyć środowisko badawcze

- Wymogi merytoryczne i techniczne
- Konfigurowanie środowiska badawczego
- Instalowanie środowiska wirtualnego VMware ESXI
  - Tworzenie sieci VLAN
  - Konfigurowanie zapory (firewalla)
- Instalowanie systemu operacyjnego Windows Server
- Konfigurowanie systemu operacyjnego Windows Server w roli kontrolera domeny
  - Zrozumienie struktury usługi katalogowej Active Directory
  - Nadanie serwerowi statusu kontrolera domeny
  - Konfigurowanie serwera DHCP
  - Tworzenie jednostek organizacyjnych
  - Tworzenie użytkowników
  - Tworzenie grup
  - Obiekty zasad grupy
  - Konfigurowanie zasad inspekcji
  - Dodawanie nowych klientów
- Konfigurowanie stosu ELK
  - Konfigurowanie usługi systemowej Sysmon
  - Pobieranie certyfikatu
- Konfigurowanie aplikacji Winlogbeat
  - Szukanie naszych danych w instancji stosu ELK
- Bonus - dodawanie zbiorów danych Mordor do naszej instancji stosu ELK
- HELK - narzędzie open source autorstwa Roberto Rodrigueza
  - Rozpoczęcie pracy z platformą HELK
- Podsumowanie

Rozdział 8. Jak przeprowadzać kwerendę danych

- Wymogi merytoryczne i techniczne
- Atomowe polowanie z użyciem bibliotek Atomic Red Team
- Cykl testowy bibliotek Atomic Red Team
  - Testowanie dostępu początkowego
  - Testowanie wykonania
  - Testowanie zdolności do przetrwania
  - Testy nadużywania przywilejów
  - Testowanie unikania systemów obronnych

        - Testowanie pod kątem wykrywania przez atakującego zasobów ofiary
        - Testowanie taktyki wysyłania poleceń i sterowania (C2)
        - Invoke-AtomicRedTeam
    - Quasar RAT
        - Przypadki użycia trojana Quasar RAT w świecie rzeczywistym
        - Uruchamianie i wykrywanie trojana Quasar RAT
        - Testowanie zdolności do przetrwania
        - Testowanie dostępu do danych uwierzytelniających
        - Badanie ruchów poprzecznych
    - Podsumowanie

Rozdział 9. Jak polować na przeciwnika

- Wymogi merytoryczne i techniczne
- Oceny przeprowadzone przez MITRE
    - Importowanie zbiorów danych APT29 do bazy HELK
    - Polowanie na APT29
- Używanie frameworka MITRE CALDERA
    - Konfigurowanie programu CALDERA
    - Wykonanie planu emulacji za pomocą programu CALDERA
- Reguły pisane w języku Sigma
- Podsumowanie

Rozdział 10. Znaczenie dokumentowania i automatyzowania procesu

- Znaczenie dokumentacji
    - Klucz do pisania dobrej dokumentacji
    - Dokumentowanie polowań
- Threat Hunter Playbook
- Jupyter Notebook
- Aktualizowanie procesu polowania
- Znaczenie automatyzacji
- Podsumowanie

Część IV. Wymiana informacji kluczem do sukcesu

Rozdział 11. Jak oceniać jakość danych

- Wymogi merytoryczne i techniczne
- Jak odróżnić dane dobrej jakości od danych złej jakości
    - Wymiary danych
- Jak poprawić jakość danych
    - OSSEM Power-up
    - DeTT&CT
    - Sysmon-Modular
- Podsumowanie

Rozdział 12. Jak zrozumieć dane wyjściowe

- Jak zrozumieć wyniki polowania