SZKOLENIE ŚREDNIO ZAAWANSOWANE

Analiza oraz zabezpieczanie przed szkodliwym kodem w praktyce

MALWARE/ANA

Czas trwania: 2 dni

Cele szkolenia

- Przedstawienie narzędzi i podejścia przy analizie szkodliwego oprogramowania oraz technik zabezpieczania sieci komputerowej przed malware
- Wykorzystanie REMnux (dystrybucja Linux) oraz FLARE VM (Windows) - dystrybucje narzędzi dedykowane do analizy malware

Zalety

- Kameralne grupy - szkolenia technologiczne prowadzimy w grupach liczących do 8 osób. Pozwala to na indywidualne podejście oraz aktywizację każdego uczestnika
- Praktyka przed teorią - wszystkie szkolenia technologiczne prowadzone są w formie warsztatowej. Konieczna teoria jest wyjaśniana na przykładzie praktycznych zadań
- Konkretne umiejętności - w ramach każdego szkolenia rozwijamy praktyczne umiejętności związane z daną technologią i tematyką
- Nauka z praktykami - wszyscy trenerzy na co dzień pracują w projektach, gwarantuje to dostęp do eksperckiej wiedzy i praktycznego know-how

Dla kogo?

- Szkolenie kierowane jest do administratorów, inżynierów sieci oraz ludzi zajmujących się obsługą incydentów bezpieczeństwa

Wymagania

- Biegłe posługiwanie się systemem Windows i Linux, podstawowa znajomość asemblera i umiejętność czytania kodu programów w języku C

Program

1. Rodzaje szkodliwego oprogramowania: backdoory, keyloggery, trojany bankowe, ransomware
2. Sposoby infekcji systemu
   a. Phishing, wodopój, supply chain attacks, 0-day, grupy APT
3. Analiza stron WWW
   a. Analiza skryptów JavaScript
4. Analiza plików PDF
5. Analiza plików Office
   a. Analiza i deobfuskacja Makr
6. Analiza złośliwych skryptów PowerShell
   a. Techniki ataku z użyciem WMI
   b. Zaawansowana obfuskacja kodu
7. Analiza plików wykonywalnych
   a. Podstawy formatu plików wykonywalnych (PE, PE64)
   b. Analiza plików natywnych, Delphi, .NET, AutoIt, Java
   c. Rozpoznanie
      -API Virustotal
      -Wykrywanie zmian w systemie: rejestr, autostart, pliki systemowe, mechanizm Prefetch
   d. Analiza statyczna
      -Magiczne stałe i ciągi
      -Sygnatury (Yara rules)
      -Dezasemblacja i dekompilacja, analiza kodu asemblerowego
      -Przykłady kodu asemblerowego
   e. Analiza dynamiczna
      -Monitorowanie aktywności w systemie: Regmonitor, Filemonitor, API monitor
      -Analiza z użyciem Debuggera
      -Monitorowanie komunikacji w fałszywej sieci
   f. Zabezpieczenia malware przed analizą
      -Wykrywanie maszyn wirtualnych typu VMWare
      -Obfuskacja kodu
      -Pakery i protektory, ręczne i automatyczne rozpakowywanie plików
      -Implementacja z użyciem maszyny wirtualnej
8. Wykrywanie szkodliwego oprogramowania w systemie (rootkity)
   a. Metody ukrywania w systemach Windows i Linux
   b. Metody wykrywania modyfikacji w systemie
      -Struktury systemowe
   c. Ukrywanie procesów
9. Zautomatyzowana analiza malware za pomocą Cuckoo Sandbox
10. Metody zabezpieczania
    a. Antywirusy - dobre czy złe?
    b. Whitelisting
11. Pułapki dla szkodliwego oprogramowania
    a. Honeypots i Honeytraps