Poligon Cybernetyczny Windows Backdooring

Warsztaty na bazie scenariusza Windows Backdooring są skierowane do administratorów bezpieczeństwa systemów z rodziny Windows i mają na celu zapoznanie uczestnika treningu z praktycznym podejściem do zagadnienia backdooringu. Trening skupia się przede wszystkim na identyfikacji różnych sposobów na jakie atakujący może uzyskiwać nieautoryzowany dostęp do systemu operacyjnego Windows.

PRZEZNACZENIE SZKOLENIA

Zadaniem trenującego jest identyfikacja i usunięcie, bądź unieszkodliwienie znalezionych backdoorów przy jednoczesnym utrzymaniu dostępności usług serwowanych przez maszyny zlokalizowane w sieci emulującej sieć Internet.

KORZYŚCI WYNIKAJĄCE Z UKOŃCZENIA SZKOLENIA

Biorąc udział w treningu uczestnik :

- Poznaje i uczy się jak wykorzystywać w praktyce narzędzia służące analizie systemów rodziny Windows, takie jak: Wireshark, RegShot, MS Message Analyzer, Process Hacker, narzędzia pakietu Sysinternals oraz natywne narzędzia dostępne w samym systemie,
- Buduje „mindset" nastawiony na poszukiwanie w nadzorowanych przez siebie systemach anomalii, mogących świadczyć o wrogich działaniach skierowanych na utrzymanie dostępu do przejętych wcześniej systemów lub wskazujących na mogącą mieć miejsce exfiltrację danych z tychże systemów,.
- Uczy się jak unieszkodliwiać / usuwać zidentyfikowane wcześniej backdoory oraz nabywa wiedzę i doświadczenie w zakresie hardenigu systemów Windows

OCZEKIWANE PRZYGOTOWANIE SŁUCHACZY

- Bardzo dobra znajomość systemów desktopowych oraz serwerowych z rodziny Windows (zalecane posiadanie certyfikatu MCSE)
- Znajomość narzędzi z pakietu SysInternal
- Podstawowa znajomość protokołów TCP/IP oraz narzędzi do analizy ruchu sieciowego (np. Wireshark)
- W przypadku osób chętnych tylko na drugi dzień warsztatowy (poligon) wymagana znajomość podstaw utwardzania systemów oraz narzędzi do analizy i zapobiegania atakom.

PRZYGOTOWANIE DO SZKOLENIA

Wirtualna Klasa

- Poznanie trenera i grupy
- Sprawdzanie wiedzy - testy i quizy
- Wprowadzenie w temat zajęć

WYKŁADY I WARSZTATY

Sala szkoleniowa

Omówienie założeń oraz topologii sieciowej środowiska

Poligon cybernetyczny (4 h)

Podsumowanie i omówienie uzyskanych podczas treningu wyników.

WSPARCIE I ROZWÓJ PO SZKOLENIU

Portal Altkom Akademii

- Dostęp do materiałów szkoleniowych i uzupełniających
- Opieka trenera
- Kontakt ze społecznością

Kod szkolenia	BS-P-SWB / PL AA 1d
Czas trwania	1 dni
Poziom	Zaawansowany
Autoryzacja	Vector Synergy