

Security/Testy Penetracyjne

- wprowadzenie



Przeznaczenie szkolenia

Szkolenie skierowane do osób, które zajmują się bezpieczeństwem systemów informatycznych w firmie w ramach swoich obowiązków, jednak nie tylko bezpośrednio w zespołach bezpieczeństwa, a w szczególności dla:

- administratorów systemów,
- administratorów bezpieczeństwa,
- osób wprost zajmujących się testami bezpieczeństwa – zlecających je, wykonujących lub weryfikujących ich jakość, tj.
 - Oficerowie IT Security,
 - Pentesterzy,
 - Członkowie zespołów Red-Team, Blue-Team oraz Compliance.



Korzyści wynikające z ukończenia szkolenia

- Poznanie i zrozumienie zależności pomiędzy podmiotami i przedmiotami bezpieczeństwa informacyjnego i cyberbezpieczeństwa.
- Zdobycie wiedzy z zakresu najczęściej stosowanych metod ataków cybernetycznych.
- Umiejętność doboru i właściwego wykorzystania zaawansowanych metod, narzędzi i technik informacyjno-komunikacyjnych.



Oczekiwane przygotowanie słuchaczy

Obsługa systemów Linux, Windows na średnim poziomie, znajomość sieci oraz budowy komputera.



Język szkolenia

Język: polski

Materiały: polski



Szkolenie obejmuje

Metoda szkolenia:

- Wykłady (40%) – model akademicki
- Warsztaty – ćwiczenia koncepcyjne, prezentacje praktycznych ataków



Czas trwania

2 dni / 14 godzin

Agenda szkolenia

1. Wstęp

- Co to jest cyberbezpieczeństwo – definicja cyberprzestrzeni i cyberbezpieczeństwa, dlaczego to jest ważne, aktualne trendy na świecie.
- Rodzaje testów bezpieczeństwa.
- Analiza ryzyka w kontekście testów bezpieczeństwa.

2. Testy bezpieczeństwa.

- Strategie Red-Team oraz zespołów penetracyjnych.
- Baza testów bezpieczeństwa – projekty, standardy, wzorce.
- Narzędzia przy testach bezpieczeństwa (omówienie i prezentacja).
- Etapy wykonywania testów penetracyjnych.
- Raportowanie oraz prezentacja wyników – co zespół penetracyjny powinien przekazywać, a czego z osoba zlecająca musi oczekiwać.

3. Praktyczne ataki w testach penetracyjnych (na bazie taktyk i technik Mitre Attack) – pokaz

i ćwiczenia:

- Exploitation
- Data Exfiltration

- Lateral Movement
- Persistence
- Privilege Escalation

4. Ogólne inne typy ataków hackerskich – prezentacja.

- Przegląd aktualnych ataków komputerowych wykorzystywanych przez cyberprzestępców, typowe błędy zabezpieczeń wykorzystywane przez atakujących.
- Ścieżka ataku (kill-chain) zasady- rozpoznanie i zasady postępowania .
- Ataki przez sieci bezprzewodowe (WiFi, Bluetooth, NFC).
- Ataki przez pocztę e-mail (fałszywe e-maile).
- Ataki przez strony WWW – jak nie dać się zainfekować, fałszywe strony.
- Ataki APT, phishing, smishing, spear-phishing, pharming, spoofing, spam, spim, scam.

5. Dobre praktyki, formy obrony przed atakami.

6. Rozwój Kompetencji z zakresu bezpieczeństwa.