Social Engineering - techniki inżynierii społecznej (kod: Social Engineering)

Zapytaj o szczegóły
tel. 22 63 64 164
akademia@alx.pl

Opis i cel szkolenia

Szkolenie z zakresu technik inżynierii społecznej. Zajęcia rozpoczynamy od wprowadzenia do pojęcia social engineering, definiując jego znaczenie oraz przedstawiając przykłady ataków i znanych wydarzeń tego rodzaju. Następnie, uczestnicy poznają podstawowe istniejące rodzaje złośliwego oprogramowania, takie jak wirusy, trojany, ransomware i spyware, oraz ich historię i ewolucję. Przegląd wybranych ataków z użyciem różnych rodzajów złośliwego oprogramowania pozwala na zrozumienie aktualnych zagrożeń. Dalej, omawiamy metody rozprzestrzeniania złośliwego oprogramowania, w tym techniki rozmnażania oraz zagrożenia nierozprzestrzeniające się.

Wyposażeni w powyższą wiedzę, kursanci nauczą się różnych technik zbierania informacji, w tym pozyskiwania danych o domenach i kontach networkingowych, oraz korzystania z narzędzia Maltego. Przygotowanie laboratorium testów penetracyjnych oraz instalacja i konfiguracja niezbędnych narzędzi, takich jak maszyna wirtualna i Maltego, umożliwiają nam praktyczne generowanie złośliwych plików.

Ostatnim etapem jest tworzenie i wdrażanie złośliwego oprogramowania. Uczestnicy dowiadują się, jak zainstalować i skonfigurować program BeeLogger, wdrażać skrypty wiersza poleceń, tworzyć zaawansowane backdoory i niestandardowe keyloggery, rejestrować hasła oraz wykonywać złośliwe ładunki. Omówione zostają techniki dostarczania złośliwego oprogramowania, takie jak inicjowanie serwera SMTP, fałszowanie e-maili, replikowanie stron logowania i kierowanie do złośliwych adresów URL. Szkolenie kończy się omówieniem metod zapobiegania social engineering, w tym rozpoznawania fałszywych e-maili, ochrony przed exploitami przeglądarki oraz wykrywania złośliwego oprogramowania. Całość uzupełniają praktyczne ćwiczenia, scenariusze ataków oraz dyskusja na temat najnowszych trendów i zagrożeń.

Czas trwania

3 dni

Program

1. Wprowadzenie do Social Engineering
   - Definicja i znaczenie Social Engineering
   - Przykłady ataków opartych na Social Engineering
2. Rodzaje i Ewolucja Złośliwego Oprogramowania
   - Podstawowe rodzaje złośliwego oprogramowania (wirusy, trojany, ransomware, spyware itp.)
   - Historia i ewolucja złośliwego oprogramowania
   - Przegląd najnowszych ataków złośliwego oprogramowania
3. Metody Rozprzestrzeniania Złośliwego Oprogramowania
   - Techniki rozmnażania złośliwego oprogramowania
   - Nierozprzestrzeniające się zagrożenia
   - Gromadzenie informacji przez złośliwe oprogramowanie
4. Techniki Zbierania Informacji
   - Informacje o domenie
   - Konta networkingowe
   - Przegląd narzędzia Maltego

   — Przygotowanie laboratorium testów penetracyjnych
5. Instalacja i Konfiguracja Narzędzi
   — Instalowanie i konfigurowanie maszyny wirtualnej
   — Instalowanie i konfigurowanie Maltego
   — Generowanie złośliwych plików
6. Tworzenie i Wdrażanie Złośliwego Oprogramowania
   — Instalacja i konfiguracja programu BeeLogger
   — Wdrażanie skryptów wiersza poleceń do uzyskiwania dostępu do systemu operacyjnego
   — Tworzenie zaawansowanego backdoora
   — Tworzenie niestandardowego zdalnego keyloggera
   — Rejestrowanie zapisanych haseł
   — Wykonywanie złośliwego ładunku
   — Raportowanie wykonania ładunku
   — Opcje dostawy złośliwego oprogramowania
7. Techniki Dostarczania Złośliwego Oprogramowania
   — Inicjowanie serwera SMTP
   — Fałszowanie wiadomości e-mail
   — Replikowanie dowolnej legalnej strony logowania
   — Kierowanie celów do złośliwego adresu URL
8. Zapobieganie Social Engineering
   — Rozpoznawanie fałszywych wiadomości e-mail
   — Ochrona przed exploitami przeglądarki
   — Ręczne wykrywanie złośliwego oprogramowania
   — Korzystanie z piaskownicy do analizy złośliwego oprogramowania
9. Podsumowanie
   — Praktyczne ćwiczenia i scenariusze ataków
   — Dyskusja na temat najnowszych trendów i zagrożeń

Zapytaj o szczegóły
tel. 22 63 64 164
akademia@alx.pl

Przeznaczenie i wymagania

Brak szczegółowych wymagań wobec uczestników szkolenia.

Certyfikaty

Uczestnicy szkolenia otrzymują imienne certyfikaty sygnowane przez ALX.

Lokalizacje

— Warszawa – ul. Jasna 14/16A
— Zdalnie – zajęcia realizowane poprzez platformę Zoom
— Kraków – ul. św. Filipa 23
— Katowice – ul. Stawowa 10
— Wrocław – ul. Rynek 35
— Gdańsk – ul. Toruńska 12
— Warsaw (English) – Jasna 14/16A
— Online (English) – your home, office or wherever you want
— na życzenie dowolne miejsce w Polsce, lub UE (zajęcia prowadzone w języku angielskim)

Cena szkolenia

2490 PLN netto (VAT 23%)

W cenę szkoleń organizowanych w naszej siedzibie wliczone są:

— autorskie materiały szkoleniowe,
— indywidualne stanowisko komputerowe do pracy podczas zajęć,
— certyfikaty ukończenia szkolenia,
— drobny poczęstunek oraz ciepłe i zimne napoje,
— możliwość jednorazowego kontaktu z instruktorem (instruktorami) po szkoleniu i zadawania pytań dotyczących materiału szkolenia.

Cena szkolenia nie zawiera obiadów. Można je dokupić w cenie 35 zł netto za obiad.

Zapytaj o szczegóły
tel. 22 63 64 164
akademia@alx.pl