Ethical Hacker (CEH) (kod: CEH)

Opis i cel szkolenia

Szkolenie z etycznego hackingu wprowadza uczestników w świat cyberbezpieczeństwa, ucząc ich technik stosowanych przez etycznych hakerów. Program obejmuje podstawy ethical hacking, w tym definicję, rolę w organizacji i zasady etyczne. Uczestnicy poznają metody zbierania informacji, techniki skanowania sieci i enumeracji oraz analizę podatności za pomocą narzędzi takich jak Nmap i Nessus.

Szkolenie obejmuje również etapy hackowania systemów, w tym zawładnięcie, eskalację uprawnień i backdooring, a także analizę złośliwego oprogramowania. Uczestnicy nauczą się monitorowania i przechwytywania danych, technik inżynierii społecznej, ochrony przed atakami DDoS, przejmowania sesji oraz omijania systemów wykrywania intruzów i zapór ogniowych. Dalsze tematy to hackowanie serwerów sieciowych i aplikacji internetowych, hackowanie sieci bezprzewodowych, mobilnych platform, bezpieczeństwo chmury i Internetu Rzeczy (IoT).

Program kończy się podstawami kryptografii i jej praktycznym zastosowaniem w zabezpieczaniu informacji. Szkolenie łączy wykłady teoretyczne z praktycznymi ćwiczeniami, umożliwiając uczestnikom zdobycie kompleksowej wiedzy i umiejętności w dziedzinie etycznego hackingu.

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

Czas trwania

5 dni

Program

1. Wprowadzenie do etycznego hackingu
   - Omówienie pojęcia etycznego hackingu
   - Rola etycznego hakera w organizacji
   - Podstawowe zasady i kodeks etyczny
   - Przegląd najnowszych trendów i zagrożeń w cyberbezpieczeństwie
2. Zbieranie informacji o ataku
   - Metody i narzędzia wykorzystywane do zbierania informacji (OSINT)
   - Techniki footprintingu i fingerprintingu
   - Analiza dostępnych źródeł informacji
3. Skanowanie sieci
   - Przegląd narzędzi do skanowania sieci (Nmap, Nessus)
   - Techniki skanowania portów i identyfikacja usług
   - Wykrywanie topologii sieci i urządzeń
4. Enumeracja
   - Różnice między skanowaniem a enumeracją
   - Narzędzia i techniki enumeracji
   - Analiza i interpretacja wyników
5. Analiza podatności
   - Metody identyfikacji podatności
   - Przegląd narzędzi do analizy podatności (OpenVAS, Nessus)
   - Ocena ryzyka i priorytetyzacja podatności
6. Hackowanie systemu
   - Etapy ataku na system (zawładnięcie, eskalacja uprawnień, backdooring)
   - Techniki wykorzystywane do atakowania systemów operacyjnych
   - Praktyczne przykłady i demonstracje ataków

7. Złośliwe oprogramowanie
   — Rodzaje złośliwego oprogramowania (wirusy, robaki, ransomware)
   — Metody infekcji i propagacji
   — Analiza przypadków złośliwego oprogramowania
8. Monitorowanie i przechwytywanie danych
   — Narzędzia do monitorowania sieci i przechwytywania pakietów (Wireshark, tcpdump)
   — Analiza przechwyconych danych
   — Wykrywanie nieautoryzowanej aktywności
9. Inżynieria społeczna – socjotechniki
   — Techniki manipulacji i phishingu
   — Przykłady ataków socjotechnicznych
   — Strategie obrony przed atakami socjotechnicznymi
10. Ataki DDoS
   — Rodzaje ataków DDoS
   — Narzędzia i techniki przeprowadzania ataków DDoS
   — Strategie ochrony przed atakami DDoS
11. Przejęcie/przechwytywanie sesji
   — Mechanizmy uwierzytelniania sesji
   — Techniki przechwytywania i przejmowania sesji
   — Metody zabezpieczania sesji
12. Omijanie IDS, zapór Firewall i Honeypots
   — Techniki omijania systemów wykrywania intruzów (IDS)
   — Strategie przełamywania zapór ogniowych (Firewall)
   — Omijanie honeypots i systemów pułapek
13. Hackowanie serwerów sieciowych
   — Przegląd metod atakowania serwerów sieciowych
   — Narzędzia do testowania bezpieczeństwa serwerów (Metasploit, Burp Suite)
   — Praktyczne przykłady i demonstracje ataków
14. Hackowanie aplikacji internetowych
   — Wprowadzenie do OWASP Top 10
   — Techniki atakowania aplikacji internetowych (XSS, CSRF, RCE)
   — Narzędzia do testowania aplikacji (Burp Suite, OWASP ZAP)
15. Ataki przez zapytania w SQL
   — Wprowadzenie do SQL Injection
   — Techniki wykonywania ataków SQLi
   — Narzędzia do wykrywania i eksploatacji SQLi
16. Hackowanie sieci bezprzewodowych
   — Przegląd protokołów i zabezpieczeń sieci bezprzewodowych
   — Techniki łamania zabezpieczeń Wi-Fi (WEP, WPA/WPA2)
   — Narzędzia do atakowania sieci bezprzewodowych (Aircrack-ng, Wireshark)
17. Hackowanie mobilnych platform
   — Specyfika bezpieczeństwa urządzeń mobilnych
   — Techniki atakowania systemów Android i iOS
   — Narzędzia do testowania bezpieczeństwa aplikacji mobilnych
18. Bezpieczeństwo chmury
   — Wyzwania i zagrożenia związane z bezpieczeństwem chmury
   — Techniki zabezpieczania środowisk chmurowych
   — Przykłady narzędzi i rozwiązań do zabezpieczania chmury
19. Hackowanie Internetu Rzeczy
   — Wprowadzenie do bezpieczeństwa IoT
   — Typowe zagrożenia i luki w zabezpieczeniach urządzeń IoT
   — Narzędzia i techniki testowania bezpieczeństwa IoT
20. Kryptografia

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

- Podstawowe pojęcia kryptografii
- Techniki szyfrowania i deszyfrowania
- Praktyczne zastosowania kryptografii w bezpieczeństwie informacji

Przeznaczenie i wymagania

Szkolenie skierowane do Specjalistów IT, Administratorów sieci i systemów, Inżynierów i Analityków bezpieczeństwa, chcących poznać aspekty ofensywnego bezpieczeństwa oraz wykrywać i zapobiegać zagrożenia.

Podstawa znajomość systemów operacyjnych od strony administracyjnej (np. Linux, Windows), podstawowa znajomość sieci komputerowych (protokoły sieciowe, narzędzia diagnostyczne). Mile widziana umiejętność programowania w języku skryptowym.

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

5790 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