Zaawansowane techniki zabezpieczeń systemów Windows (kod: Windows Security)

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

Opis i cel szkolenia

Szkolenie "Zaawansowane techniki zabezpieczeń systemów Windows" to kompleksowe i praktyczne warsztaty, które przygotowują uczestników do skutecznej ochrony infrastruktury IT przed współczesnymi zagrożeniami. Uczestnicy poznają szczegółowo model "Cyber Kill Chain" oraz różnorodne wektory ataków na system Windows, w tym ataki lokalne, zdalne oraz socjotechniczne. Program obejmuje zaawansowane techniki przejmowania kontroli nad kontem lokalnym, eskalacji uprawnień, ustanawiania persystencji oraz lateral movement w sieci.

Szkolenie kładzie duży nacisk na ochronę poświadczeń i wykrywanie oraz łamanie skrótów haseł. Uczestnicy nauczą się również, jak używać narzędzi takich jak Nmap, Wireshark, OpenVAS i Metasploit do ochrony systemu w sieci. W dalszej części warsztatów omówione zostaną techniki rozszerzania wpływu, takie jak Pass-the-hash, oraz metody zabezpieczania krytycznych danych i uprawnień użytkowników.

Dzięki modułom poświęconym ochronie lokalnej i sieciowej, uczestnicy zdobędą wiedzę na temat implementacji i zarządzania technologiami zabezpieczeń takimi jak Bitlocker, TPM, firewall systemowy, a także Managed Service Accounts, Local Administrator Password Solution oraz modele Just Enough Administration i Just In-Time.

Szkolenie jest skierowane przede wszystkiem dla administratorów systemów, specjalistów ds. bezpieczeństwa IT oraz inżynierów sieciowych, którzy chcą podnieść poziom zabezpieczeń swoich systemów Windows i skutecznie chronić je przed współczesnymi zagrożeniami.

Czas trwania

3 dni

Program

1. Model "Cyber Kill Chain"
   - Wprowadzenie do koncepcji Cyber Kill Chain i jej zastosowania w analizie cyberataków.
   - Omówienie różnych wektorów ataków na system Windows:
     - Ataki lokalne: metody i techniki.
     - Ataki zdalne: wykorzystanie luk w zabezpieczeniach.
     - Ataki socjotechniczne: manipulacja użytkownikami i wykorzystanie błędów ludzkich.
2. Ogólny Model Ataków na Infrastrukturę Opartą na Windows
   - Przejęcie kontroli nad kontem lokalnym: techniki i narzędzia.
   - Lokalna eskalacja uprawnień: sposoby uzyskania dostępu do zasobów systemu.
   - Ustanowienie persystencji: techniki utrzymania dostępu po włamaniu.
   - Rekonesans i ruch boczny („lateral movement”): zbieranie informacji i przemieszczanie się w sieci.
   - Eskalacja uprawnień w strukturze Active Directory: zaawansowane metody uzyskiwania wyższych uprawnień.

3. Ochrona Poświadczeń w Systemie Windows
   — Przegląd krytycznych plików i procesów: SAM, NTDS.DIT, rejestr, proces lsass.exe.
   — Mechanizmy ochrony haseł: LM Hash i NTLM Hash.
   — Techniki łamania skrótów haseł: narzędzia i metody.
4. Ochrona Systemu w Sieci
   — Użycie skanera Network Mapper („Nmap”): identyfikacja i analiza sieci.
   — Analizator komunikacji sieciowej Wireshark: monitorowanie i diagnostyka ruchu sieciowego.
   — Skaner podatności OpenVAS: wykrywanie luk bezpieczeństwa.
   — Platforma Metasploit: wykorzystanie wykrytych podatności (np. EternalBlue, PrintNightmare, Zerologon).
5. Rozszerzanie Wpływu
   — Pass-the-hash (PtH): techniki i środki zaradcze.
   — Local System impersonation: metody przejęcia tożsamości systemowej.
   — Ochrona sekretów LSA: zabezpieczanie krytycznych danych.
   — Przywileje i prawa użytkowników: zarządzanie uprawnieniami.
6. Ochrona Lokalna
   — Bitlocker, TPM, PIN, klucz startowy: zaawansowane techniki szyfrowania i ochrony danych.
   — Firewall systemowy: konfiguracja i zarządzanie zaporą ogniową.
   — Aktualizacje: polityki i praktyki.
   — Ochrona kont wysoceuprzywilejowanych: zarządzanie i monitorowanie.
7. Ochrona w Sieci
   — Managed Service Accounts (MSA) i Group Managed Service Accounts (gMSA): zarządzanie kontami serwisowymi.
   — Local Administrator Password Solution (LAPS): zabezpieczanie lokalnych haseł administratora.
   — Bastion Forest: architektura i zastosowanie.
   — Modele Just Enough Administration (JEA) oraz Just In-Time (JIT): minimalizacja uprawnień i kontrola dostępu.

Przeznaczenie i wymagania

Szkolenie jest przeznaczone dla administratorów systemów, specjalistów ds. bezpieczeństwa IT, inżynierów sieciowych oraz wszystkich osób odpowiedzialnych za ochronę infrastruktury opartej na Windows.

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
— 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

2790 PLN netto (VAT 23%)

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

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