Cyberbezpieczeństwo – Zaawansowane techniki ochrony systemów, aplikacji mobilnych i sieci (kod: K-CYBERSECURITY)

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

Opis i cel kursu

Kurs „Cyberbezpieczeństwo – Zaawansowane techniki ochrony systemów, aplikacji mobilnych i sieci" to kompleksowe szkolenie składające się z trzech modułów, zaprojektowane z myślą o profesjonalistach IT pragnących zwiększyć swoje kompetencje w zakresie zabezpieczeń systemów Windows, aplikacji mobilnych oraz sieci komputerowych.

Zaawansowane techniki zabezpieczeń systemów Windows

W tym module uczestnicy zapoznają się z nowoczesnymi zagrożeniami atakującymi systemy Windows i nauczą się skutecznie je neutralizować. Kurs obejmuje szczegółową analizę modelu „Cyber Kill Chain" oraz wektory ataków, takie jak ataki lokalne, zdalne i socjotechniczne. Podczas warsztatów uczestnicy zdobędą umiejętności w zakresie ochrony poświadczeń, przejmowania kontroli nad kontami lokalnymi, eskalacji uprawnień oraz rozprzestrzeniania się po sieci (lateral movement).

Moduł obejmuje także zaawansowane techniki takie jak Pass-the-hash oraz zabezpieczenie krytycznych danych za pomocą narzędzi takich jak Bitlocker, TPM, Managed Service Accounts, Local Administrator Password Solution i modele Just Enough Administration oraz Just In-Time. Program kursu został wzbogacony o obsługę narzędzi takich jak Nmap, Wireshark, OpenVAS i Metasploit, co umożliwi uczestnikom skuteczną ochronę swoich systemów w sieci.

Bezpieczeństwo aplikacji mobilnych

Drugi moduł poświęcony jest zabezpieczeniom aplikacji mobilnych na platformach iOS i Android. Uczestnicy dowiedzą się, jak zaimplementować kluczowe mechanizmy bezpieczeństwa, takie jak systemy uprawnień, Data Protection i Keychain, aby skutecznie chronić dane użytkowników. Moduł obejmuje także praktyczne ćwiczenia z analizy zabezpieczeń systemowych oraz przełamywania szyfrowania danych w aplikacjach mobilnych. Uczestnicy nauczą się identyfikować próby eskalacji uprawnień oraz chronić wrażliwe informacje, takie jak SMS-y, dane GPS oraz e-maile.

Podczas szkolenia omówione zostaną metody bezpiecznego przechowywania loginów, haseł oraz kluczy kryptograficznych, a także implementacja szyfrowania i bezpiecznej komunikacji klient-serwer z wykorzystaniem protokołów SSL/TLS oraz PKI. Moduł kończy się analizą specyficznych dla platform zagrożeń, takich jak CSRF, framing, clickjacking, czy tapjacking.

Testowanie bezpieczeństwa sieci i testy penetracyjne

Ostatni moduł skupia się na testowaniu bezpieczeństwa sieci oraz przeprowadzaniu testów penetracyjnych. Uczestnicy zdobywają praktyczne umiejętności w symulowanych środowiskach testowych, co pozwala im na efektywne identyfikowanie i zarządzanie zagrożeniami w sieciach komputerowych. Kurs obejmuje analizę rzeczywistych przypadków ataków oraz najlepszych praktyk w branży, co pozwala lepiej zrozumieć wyzwania stojące przed specjalistami ds. bezpieczeństwa.

Cały kurs został zaprojektowany tak, aby dostarczyć uczestnikom wszechstronnej wiedzy teoretycznej i praktycznej z obszaru cyberbezpieczeństwa. Idealny dla

administratorów systemów, specjalistów ds. bezpieczeństwa IT oraz inżynierów sieciowych, którzy pragną podnieść swoje kompetencje i skutecznie chronić infrastrukturę IT przed współczesnymi zagrożeniami.

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

Program

Moduł 1 - Zaawansowane techniki zabezpieczeń systemów Windows:

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.

Moduł 2 - Bezpieczeństwo aplikacji mobilnych:

1. Wprowadzenie do Platform Mobilnych: iOS i Android
   — Podstawy funkcjonowania systemów operacyjnych iOS i Android.
   — Porównanie kluczowych cech bezpieczeństwa obu platform.
2. Bezpieczeństwo z Perspektywy Użytkownika Urządzenia
   — Domyślnie dostępne sposoby zabezpieczeń urządzeń w systemach iOS i Android.
   — Wpływ domyślnych zabezpieczeń urządzeń na bezpieczeństwo aplikacji.
   — Mechanizmy usuwania danych (data wiping) i ich znaczenie dla użytkownika.
3. Mechanizmy Bezpieczeństwa Dostarczane Developerom przez Producentów Systemów
   — System uprawnień w Androidzie: jak działa i jak go implementować.
   — Data Protection i Keychain w iOS: zabezpieczanie danych użytkowników.
   — Praktyczne zastosowanie tych mechanizmów w aplikacjach mobilnych.
4. Przełamywanie Zabezpieczeń Systemów
   — Eskalacja uprawnień w systemach mobilnych (jailbreak) i jej wpływ na bezpieczeństwo aplikacji.
   — Analiza przypadków dostępu do danych użytkowników (SMS, e-mail, dane GPS).
   — Techniki analizy systemu plików oraz przełamywania szyfrowania danych.
5. Bezpieczeństwo Danych
   — Zagrożenia związane z wykradaniem danych: studium przypadków.
   — Metody bezpiecznego przechowywania kluczowych danych (login, hasło, klucze, dane osobowe).
   — Implementowanie szyfrowania w aplikacjach mobilnych.
   — Zabezpieczanie aplikacji hasłem dostępowym.
   — Bezpieczna komunikacja pomiędzy aplikacjami i komponentami (Android: Activity, Service, Broadcast receiver, Content Resolver).
   — Szyfrowanie baz danych.
6. Bezpieczeństwo Komunikacji
   — Zagrożenia płynące z transportu danych i sposoby ich minimalizacji.
   — Poprawna, bezpieczna implementacja aplikacji klient-serwer.
   — Mechanizmy szyfrowania (SSL/TLS) i wykorzystanie PKI (Public Key Infrastructure).
7. Bezpieczeństwo Aplikacji
   — Analiza sposobów dystrybucji aplikacji i ryzyka z tym związane.
   — Analiza form binarnych aplikacji i ich dystrybucji (odex, Mach-O, ipa, apk).
   — Reverse Engineering aplikacji: narzędzia i techniki (Cycript, baksmali, apktool).
   — Metody utrudniania analizy kodu i modyfikacji działania aplikacji (blokowanie debuggerów, obfuskacja kodu, ASLR).
   — Wykrywanie środowisk z podwyższonymi uprawnieniami (jailbreak).
   — Narzędzia wspomagające analizę bezpieczeństwa aplikacji.
8. Istotne Mechanizmy Specyficzne dla Platform i Ataki z Nimi Związane
   — Multitasking i zarządzanie stanem aplikacji/GUI caching.
   — Wprowadzanie danych (input caching) i zagrożenia z tym związane.
   — Ataki na aplikacje webowe (CSRF, framing, clickjacking).
   — Identyfikacja urządzeń i użytkowników (UDID).
   — Bezpieczeństwo powiadomień push.
   — Tapjacking i zarządzanie logami.
9. Podsumowanie i Sesja Q&A;

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

— Praktyczne ćwiczenia z zakresu bezpieczeństwa aplikacji mobilnych.
— Sesja pytań i odpowiedzi, dyskusja nad najnowszymi zagrożeniami i technikami ochrony.

Moduł 3 - Testy penetracyjne i testowanie bezpieczeństwa sieci:

1. Wprowadzenie do testów penetracyjnych:
   — Omówienie różnych podejść i metod stosowanych w testach penetracyjnych.
   — Standardy OSSTMM i OWASP - przegląd standardów i wytycznych jako podstaw do prowadzenia testów.
   — Dobre praktyki opisane w dokumentach NIST i CIS - prezentacja dokumentów, które zawierają rekomendacje dotyczące zabezpieczeń.
   — Wyjaśnienie kluczowych różnic między testami penetracyjnymi a audytami bezpieczeństwa
2. Organizacja testów penetracyjnych:
   — Prawne aspekty przeprowadzania testów penetracyjnych
   — Tworzenie skutecznego i szczegółowego planu testów penetracyjnych.
   — Rozwiązywanie popularnych problemów napotykanych podczas testów
3. Fazy testu penetracyjnego:
   — Rekonesans i techniki zbierania informacji
   — Metody identyfikacji słabości i podatności w systemach
   — Praktyczne aspekty przeprowadzania ataków na cele testowe
   — Techniki ukrywania śladów po przeprowadzonych testach
   — Tworzenie kompleksowego raportu z przeprowadzonych testów, zawierającego rekomendacje
4. Metody ochrony przed atakami:
   — Zastosowanie i konfiguracja honeypotów jako narzędzi do wykrywania ataków.
   — Omówienie systemów detekcji i prewencji włamań (IDS/IPS)
   — Hardening systemów Windows i Linux - techniki wzmacniania zabezpieczeń systemów operacyjnych

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

Przeznaczenie i wymagania

Aby w pełni skorzystać z kursu, uczestnicy powinni posiadać podstawową wiedzę o systemach operacyjnych, szczególnie Windows, oraz rozumieć podstawy sieci komputerowych, takie jak adresacja IP i protokoły TCP/IP. Mile widziane jest doświadczenie w administracji IT, choć nie jest to warunek konieczny. Znajomość podstawowych narzędzi związanych z bezpieczeństwem, takich jak Nmap czy Wireshark, będzie dodatkowym atutem, ale nie jest wymagana. Dla modułu poświęconego aplikacjom mobilnym zalecana jest znajomość platform iOS oraz Android. Kluczowa jest również chęć nauki oraz gotowość do uczestnictwa w częściach praktycznych kursu. Spełnienie tych wymagań umożliwi pełne przyswojenie zaawansowanych technik omawianych podczas szkolenia.

Certyfikaty

Uczestnicy szkolenia otrzymują imienne certyfikaty sygnowane przez ALX.