Centrum Szkoleniowe Comarch
ul. Prof. Michała Życzkowskiego 33
31-864 Kraków

COMARCH
Szkolenia

Linux dla Pentesterów

Cele szkolenia

Celem szkolenia jest zdobycie praktycznych umiejętności w zakresie administracji systemem Linux w kontekście testów penetracyjnych. Uczestnicy nauczą się korzystać z systemu Linux jako narzędzia do analizy bezpieczeństwa, eksploracji podatności oraz wykonywania ataków w kontrolowanym środowisku testowym.

Umiejętności

Dzięki szkoleniu uczestnik będzie:

- Znał strukturę i dystrybucje systemu Linux ze szczególnym uwzględnieniem Kali Linux.
- Korzystał z powłoki systemowej do automatyzacji zadań i eksploracji systemu.
- Obsługiwał kluczowe polecenia związane z zarządzaniem plikami, użytkownikami oraz uprawnieniami.
- Analizował konfigurację i bezpieczeństwo sieci w systemach Linux.
- Rozumiał mechanizmy zabezpieczeń systemu i sposoby ich omijania

Profil uczestników

Szkolenie przeznaczone jest dla:

- Pentesterów oraz osób planujących karierę w testach penetracyjnych.
- Administratorów systemów i sieci, którzy chcą poznać zagrożenia w środowiskach Linux.
- Specjalistów ds. cyberbezpieczeństwa, którzy chcą poszerzyć swoją wiedzę o bezpieczeństwie systemu Linux.
- Osób zainteresowanych etycznym hakowaniem i analizą podatności.

Przygotowanie uczestników

- Podstawowa znajomość systemu Linux.
- Ogólna wiedza o sieciach komputerowych i zagadnieniach związanych z cyberbezpieczeństwem

Centrum Szkoleniowe Comarch
ul. Prof. Michała Życzkowskiego 33
31-864 Kraków

COMARCH
Szkolenia

Szczegółowy program szkolenia

1. Wstęp do systemu Linux
    - dystrybucje
    - Kali Linux
    - kategorie narzędzi Kali Linux
    - powłoka ZSH
    - powłoka systemowa
2. Polecenia systemu Linux
    - strumienie wejścia/wyjścia
    - metaznaki
    - repozytorium
    - pliki pomocy
    - zarządzanie pakietami
    - menadżer pakietów
    - zarządzanie procesami
    - poszukiwania plików z wzorcem
    - wyszukiwanie plików rekursywnie
    - wyrażenia regularne
    - wyszukiwanie i przetwarzanie wzorców w plikach lub strumieniach danych
    - strumieniowe przetwarzanie tekstu znak po znaku
    - wyszukanie linii z pasującymi słowami
    - wyświetlanie wskazanej liczby wierszy oraz w trybie ciągłym
    - historii wydawanych poleceń
3. Zarządzanie użytkownikami
    - dodanie, usuwanie, modyfikacja użytkownika
    - przełączenie się na innego użytkownika
    - zmiana hasła
    - id użytkownika
    - zarządzanie grupami
    - pliki konfiguracyjne

4. Zarządzanie plikami i katalogami
    - wyświetlanie nazwy katalogu w którym się znajdujemy
    - poruszanie się po strukturze katalogów
    - tworzenie katalogu
    - wyświetlenie zawartości
    - przeglądanie zawartości pliku
    - kopiowanie pliku/katalogu
    - usuwanie plików/katalogów
    - wyświetlanie wielkości plików/katalogów
    - wyświetlenie zajętości przez system plików
    - edytor tekstu vi
5. Zarządzanie uprawnieniami
    - obliczenia praw dostępu
    - ustawienie bitu SUID
    - ustawienie bitu GUID
    - Sticky Bit
    - zmiana uprawnień do pliku/katalogu
    - wyświetlenie listy kontroli dla pliku/katalogu
    - ustawienie listy kontroli dla pliku/katalogu
6. Zarządzanie ustawieniami sieciowymi
    - pliki konfiguracyjne ustawień sieciowych
    - wyświetlanie/modyfikacja ustawień sieciowych
    - wyświetlanie listy wszystkich interfejsów sieciowych i powiązanych z nimi adresami IP
    - konfiguracja adresacji IP
    - tablica routingu
    - dodawanie nowej trasy do podsieci
    - narzędzie diagnostyczne połączeń sieciowych
    - narzędzie służące do zdalnego połączenia
    - statystyki połączeń sieciowych

Centrum Szkoleniowe Comarch
ul. Prof. Michała Życzkowskiego 33
31-864 Kraków

Metoda realizacji szkolenia

- Zajęcia praktyczne – większość ćwiczeń będzie wykonywana w środowisku Kali Linux.
- Wykłady teoretyczne – omówienie kluczowych koncepcji związanych z bezpieczeństwem systemu Linux.
- Analiza przypadków – rzeczywiste scenariusze ataków i podatności.
- Dyskusje i konsultacje – możliwość omówienia problemów zgłaszanych przez uczestników.

Liczba dni, liczba godzin szkoleniowych

2 dni, 16 godzin szkoleniowych

Ścieżka rozwoju po szkoleniu

Po ukończeniu szkolenia uczestnicy mogą kontynuować rozwój w kierunkach:

1. Rozwój zawodowy
   - Specjalista ds. testów penetracyjnych (Pentester)
   - Analityk bezpieczeństwa IT
   - Administrator systemów Linux z naciskiem na bezpieczeństwo

2. Certyfikacje
   - OSCP (Offensive Security Certified Professional)
   - CEH (Certified Ethical Hacker)
   - GPEN (GIAC Penetration Tester)