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

COMARCH
Szkolenia

Bezpieczeństwo sieci i testy penetracyjne w wykorzystaniem Linuxa

Cele szkolenia

Celem szkolenia jest zapoznanie uczestników z metodami testowania zabezpieczeń systemów komputerowych oraz aplikacji webowych. Uczestnicy zdobędą praktyczne umiejętności w zakresie identyfikacji i eksploatacji podatności w systemach operacyjnych, sieciach komputerowych oraz aplikacjach webowych. Szkolenie pozwoli na lepsze zrozumienie technik stosowanych przez potencjalnych atakujących oraz sposobów zabezpieczania infrastruktury IT przed cyberzagrożeniami

Umiejętności

Dzięki szkoleniu uczestnik będzie:

- Potrafił konfigurować i tworzyć środowiska testowe do testów penetracyjnych.
- Umiał wykrywać i analizować podatności w usługach sieciowych.
- Znał metody ataków na aplikacje webowe i sposoby ich zabezpieczania.
- Rozumiał zagrożenia związane z bezpieczeństwem sieci bezprzewodowych oraz metody ich ochrony.
- Posiadał wiedzę na temat ataków na zdalny dostęp oraz znał techniki ich zapobiegania.
- Umiał przeprowadzać ataki na połączenia SSL oraz rozumiał ich konsekwencje.
- Znał techniki eskalacji uprawnień i ataków na system Windows oraz sposoby ich minimalizacji.

Profil uczestników

Szkolenie przeznaczone jest dla osób:

- Zajmujących się administracją systemów IT, bezpieczeństwem sieci oraz aplikacji webowych.
- Programistów i testerów aplikacji webowych, chcących lepiej zrozumieć zagrożenia związane z bezpieczeństwem oprogramowania.
- Specjalistów ds. bezpieczeństwa IT oraz analityków zagrożeń cybernetycznych.
- Studentów oraz entuzjastów bezpieczeństwa komputerowego, chcących zdobyć praktyczne umiejętności w zakresie testów penetracyjnych.

Przygotowanie uczestników

Podstawowa wiedza na temat system Linux oraz wirtualizacji.

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

COMARCH
Szkolenia

Szczegółowy program szkolenia

1. Tworzenie środowisk testowych do testów penetracyjnych
    - DVWA (Damn Vulnerable Web Application)
    - Metasploitable
2. Bezpieczeństwo usług sieciowych
    - nmap
    - podatności
    - Brute-force
    - MITM
    - Wireshark
    - DNS Spoofing
    - DDoS
3. Bezpieczeństwo aplikacji webowych
    - OWASP Top 10
    - Path Traversal
    - Local File Inclusion
    - Remote File Inclusion
    - SQL Injection
    - Command Injection
    - Cross-Site Scripting
    - Session hijacking
    - XSFR/CSRF
4. Ataki na infrastrukturę sieci WLAN
    - Atak na WPS
    - Atak na WEP
    - Atak na WPA/WPA2
5. Ataki na zdalny dostęp
    - VNC
    - SSH
    - Samba
    - RDP

6. Ataki na połączenia SSL
    - Protokół SSL/TLS
    - Certyfikat SSL
    - Bettercap
    - SSLStrip
    - HSTS
    - Decryptying SSL/TLS
7. Ataki na zabezpieczenia systemu Windows
    - Microsoft Security Response Center
    - Exploit Zero-Day
    - Privilege Escalation
    - Ataki na rejestr Windows
    - Ataki na pamięć

Metoda realizacji szkolenia

Szkolenie będzie prowadzone w formie zajęć praktycznych z wykorzystaniem środowiska wirtualnego do testów penetracyjnych. Uczestnicy będą pracować na specjalnie przygotowanych podatnych systemach oraz analizować rzeczywiste scenariusze ataków.

- Wykłady teoretyczne – omówienie zagadnień związanych z bezpieczeństwem IT oraz testami penetracyjnymi.
- Warsztaty praktyczne – samodzielne wykonywanie ćwiczeń w kontrolowanym środowisku.
- Analiza przypadków – omówienie rzeczywistych incydentów bezpieczeństwa.
- Dyskusje i konsultacje – wymiana doświadczeń oraz rozwiązywanie problemów zgłaszanych przez uczestników

Liczba dni, liczba godzin szkoleniowych

2 dni, 16 godzin szkoleniowych

Ścieżka rozwoju po szkoleniu

Ukończenie szkolenia otwiera przed uczestnikami możliwość dalszego rozwijania umiejętności w obszarze bezpieczeństwa IT oraz testów penetracyjnych. Po szkoleniu uczestnicy mogą:

1. Rozwój zawodowy
- Podjąć pracę jako Pentester, Analityk Bezpieczeństwa, Administrator Bezpieczeństwa IT lub Specjalista ds. Cyberbezpieczeństwa.
- Rozszerzyć swoje kompetencje i aplikować na stanowiska w działach SOC (Security Operations Center) oraz Red Team.

2. Certyfikacje

Szkolenie stanowi dobry fundament do przygotowania się do uzyskania certyfikatów branżowych, takich jak:

- CEH (Certified Ethical Hacker)
- OSCP (Offensive Security Certified Professional)
- Pentest+ (CompTIA)
- GPEN (GIAC Penetration Tester)