Certified Ethical Hacker

PRZEZNACZENIE SZKOLENIA

Szkolenie skierowane do administratorów sieci, osób odpowiedzialnych za infrastrukturę informatyczną, administratorów witryn oraz każdego, kto planuje podniesienie poziomu bezpieczeństwa informatycznego swojej organizacji. Osoby nie będące specjalistami z zakresu bezpieczeństwa IT zwiększą świadomość dotyczącą zagrożeń oraz poznają różne technologie ataków powszechnie stosowane przez hakerów. Specjaliści ds. bezpieczeństwa informatycznego, audytorzy i tzw. security officers będą mogli ugruntować, usystematyzować bądź uzupełnić swoją wiedzę.

KORZYŚCI WYNIKAJĄCE Z UKOŃCZENIA SZKOLENIA

Celem pracy etycznych hakerów jest identyfikacja słabych punktów organizacji oraz pomaganie w znalezieniu skutecznej metody obrony przed atakami na firmowe systemy. Uczestnicy dokonują kontrolowanych włamań do systemu „ofiary" i zdobywają praktyczne umiejętności efektywnej ochrony sieci. Podczas gdy konwencjonalne środki bezpieczeństwa są niezbędne, ważne jest, aby uzyskać perspektywę ludzi, którzy mogą potencjalnie zagrozić systemom.

W ramach szkolenia **Uczestnicy otrzymują voucher na egzamin CEHv10.0 weryfikujący zdobytą wiedzę i umiejętności.**

Uczestnicy szkolenia nauczą się:

- definiować i charakteryzować najważniejsze techniki ataków stosowanych przez hakerów
- skanować, testować i przełamywać zabezpieczenia systemów
- identyfikować i analizować podatności w organizacji
- rozpoznawać i zapobiegać metodom eskalacji uprawnień w systemach
- tworzyć lepsze polityki na urządzeniach IDS/IPS dotyczące wykrywania włamań
- rozpoznawać socjotechniki wykorzystywane przez przestępców
- tworzyć wirusy, hakować urządzenia mobilne, smartfony
- identyfikować potencjał zagrożeń płynących z "Internetu Rzeczy" (IoT) i jak się przed nimi zabezpieczyć
- rozpoznawać subtelne różnice między backdoor'ami, trojanami oraz innymi zagrożeniami
- docelowo, będą mogli skuteczniej uświadamiać pracowników firmy w kwestiach bezpieczeństwa informacji

METODA EGZAMINOWANIA

Uwaga: zdając egzamin CEH w formule online, obowiązuje dodatkowa opłata 100 USD netto. Koszt obejmuje wynajęcie osoby nadzorującej egzamin (tzw. proktora), zakupu dokonujemy indywidulanie na stronie vendora: https://store.eccouncil.org/product/voucher-upgrade-rps-to-vue/

OCZEKIWANE PRZYGOTOWANIE SŁUCHACZY

Wymagana podstawowa znajomość systemów operacyjnych Windows oraz Linux. Zalecane przynajmniej dwuletnie doświadczenie w branży IT, znajomość protokołu TCP / IP (w tym usług takich jak DNS czy DHCP, znajomość koncepcji routingu IP, przełączania w sieciach LAN).

Metoda szkolenia

- wykład
- warsztaty

PRZYGOTOWANIE DO SZKOLENIA

Wirtualna Klasa

- Poznanie trenera i grupy
- Sprawdzanie wiedzy - testy i quizy
- Wprowadzenie w temat zajęć

WYKŁADY I WARSZTATY

Sala szkoleniowa

1. Wprowadzenie do „Etycznego Hakingu"
2. Footprinting i Rekonesans - wstępne zbieranie informacji o celu ataku
3. Skanowanie sieci - identyfikacja systemów, portów, usług działających w sieci
4. Enumeracja – aktywne odpytywanie usług/systemów w celu rozpoznania słabych punktów w infrastrukturze
5. Analiza podatności - omówienie narzędzi do wykonywania skanowania oraz kryteriów ich doboru
6. Włamywanie się do systemów („Hakowanie” systemów)
7. Zagrożenia malware – rodzaje niebezpiecznego oprogramowania i mechanizmy działania
8. Podsłuchiwanie (Sniffing) sieci – przechwytywanie danych
9. Socjotechniki (Inżynieria społeczna)
10. Ataki na odmowę dostępu do usługi (Denial-of-Service)
11. Przechwytywanie sesji – przejęcie komunikacji między ofiarą a systemem docelowym
12. Omijanie systemów IDS, firewall’i, honeypot’ów
13. Atakowanie serwerów webowych
14. Atakowanie aplikacji webowych
15. SQL Injection – ataki z wykorzystaniem braku odpowiedniego filtrowania zapytań baz danych SQL
16. Włamywanie się do sieci bezprzewodowych
17. Hakowanie platform i urządzeń mobilnych
18. Hakowanie "Internetu Rzeczy" (IoT)
19. Koncepcje i bezpieczeństwo rozwiązań chmurowych (cloud computing)
20. Kryptografia

WSPARCIE I ROZWÓJ PO SZKOLENIU

Portal Altkom Akademii

- Dostęp do materiałów szkoleniowych i uzupełniających
- Opieka trenera
- Kontakt ze społecznością

Kod szkolenia	CEHv10 / PL AA 5d
Czas trwania	5 dni
Poziom	Średnio zaawansowany
Autoryzacja	EC-Council