kod szkolenia: CEHv12 Pro / PL AA 5d

Certified Ethical Hacker

Autoryzowane szkolenie **EC-Council - CEHv12 - Certified Ethical Hacker** realizowane w formie wykładu oraz praktycznych warsztatów. Firma EC-Council, by sprostać rosnącemu zapotrzebowaniu na nowe umiejętności i wiedzę o cyberbezpieczeństwie, opracowała szkolenie Certified Ethical Hacker. Niekonwencjonalne podejście do myślenia o infrastrukturze firmowej z punktu widzenia intruza jest niezwykle efektywnym mechanizmem nauczania, który otwiera oczy na wiele często zaniedbywanych obszarów naszej pracy. Szkolenie, mimo iż od podstaw omawia technologię oraz techniki wykorzystywane przez hackerów, porusza również bardzo zaawansowane zagadnienia. Kurs zawiera ogrom materiału i ćwiczeń znacznie wykraczający poza zakres typowego 5-dniowego szkolenia i część zagadnień przeznaczona jest do praktykowania w trybie self-study. Po ukończeniu szkolenia kursanci będą mieli okazję zapisać się na egzamin CEH. Certyfikat CEH jest jednym z najbardziej pożądanych na rynku pracy i pomaga zwiększyć szanse zatrudnienia na stanowiskach związanych z cyberbezpieczeństwem na całym świecie.

Przeznaczenie szkolenia

Szkolenie skierowane jest do:

- administratorów sieci,
- osób odpowiedzialnych za infrastrukturę informatyczną,
- inżynierów systemowych,
- osób planujących podniesienie poziomu bezpieczeństwa informatycznego swojej organizacji,
- pracowników SOC,
- administratorów witryn www,
- pracowników IT planujących podniesienie poziomu bezpieczeństwa informatycznego swojej

organizacji,

Dla osób nie będących specjalistami z zakresu bezpieczeństwa IT szkolenie może być zbyt intensywne ale pozwoli zwiększyć świadomość dotyczącą zagrożeń oraz pokazuje różne techniki ataków powszechnie stosowane przez hakerów.

Specjaliści ds. bezpieczeństwa informatycznego, audytorzy i analitycy bezpieczeństwa oraz pentesterzy 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 trakcie ćwiczeń studenci będą pracowali na takich systemach jak Parrot Security OS, Windows 11, Windows Server 2019, Windows Server2022, Android czy Ubuntu Linux 22.04. Podczas laboratoriów każdy zapozna się z wieloma narzędziami wykorzystywanymi przez specjalistów od cyberbezpieczeństwa.

W ramach szkolenia uczestnicy otrzymują voucher na egzamin CEH weryfikujący zdobytą wiedzę i umiejętności.

Uczestnicy szkolenia nauczą się:

- definiować i charakteryzować najważniejsze techniki ataków stosowanych przez hakerów,
- przeprowadzać rekonesans dotyczący własnej firmy czy konkurencji,
- 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,
- generować wirusy, hakować urządzenia mobilne, smartfony,
- analizować złośliwe oprogramowanie,
- identyfikować potencjał zagrożeń płynących z "Internetu Rzeczy" (IoT) i jak się przed nimi zabezpieczyć,
- określić wyzwania dla sieci przemysłowych i wpływ cyberbezpieczeństwa na koncepcje OT (Operational Technology),
- charakteryzować najważniejsze elementy systemów kontenerowych (Docker, Kubernetes),
- weryfikować bezpieczeństwo rozwiązań chmurowych takich jak AWS,
- rozpoznawać subtelne różnice między backdoor’ami, trojanami oraz innymi zagrożeniami,
- docelowo, będą mogli skuteczniej uświadamiać pracowników firmy w kwestiach bezpieczeństwa informacji,

Metoda egzaminowania

Do egzaminu można przystąpić w autoryzowanych ośrodkach egzaminacyjnych EC-Council.
Informacje o egzaminie CEH (ANSI)
Tytuł – Certified Ethical Hacker
Format testu: Pytania wielokrotnego wyboru
Ilość pytań – 125
Czas trwania – 4 godz.
Uwaga: zdając egzamin CEH w formule online z tzw. ochroną zdalną, 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 adresacji IP, routingu, przełączania w sieciach LAN).
Metoda szkolenia

- wykład
- warsztaty

Język szkolenia

- Szkolenie: polski
- Materiały: angielski

Szkolenie obejmuje

Czas trwania

5 dni / 40 godzin

Agenda szkolenia

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" oraz "Technologii Operacyjnych" (IoT i OT)
19. Koncepcje i bezpieczeństwo rozwiązań chmurowych (cloud computing)
20. Kryptografia