

### Il Ruolo dell'Ethical Hacker in azienda

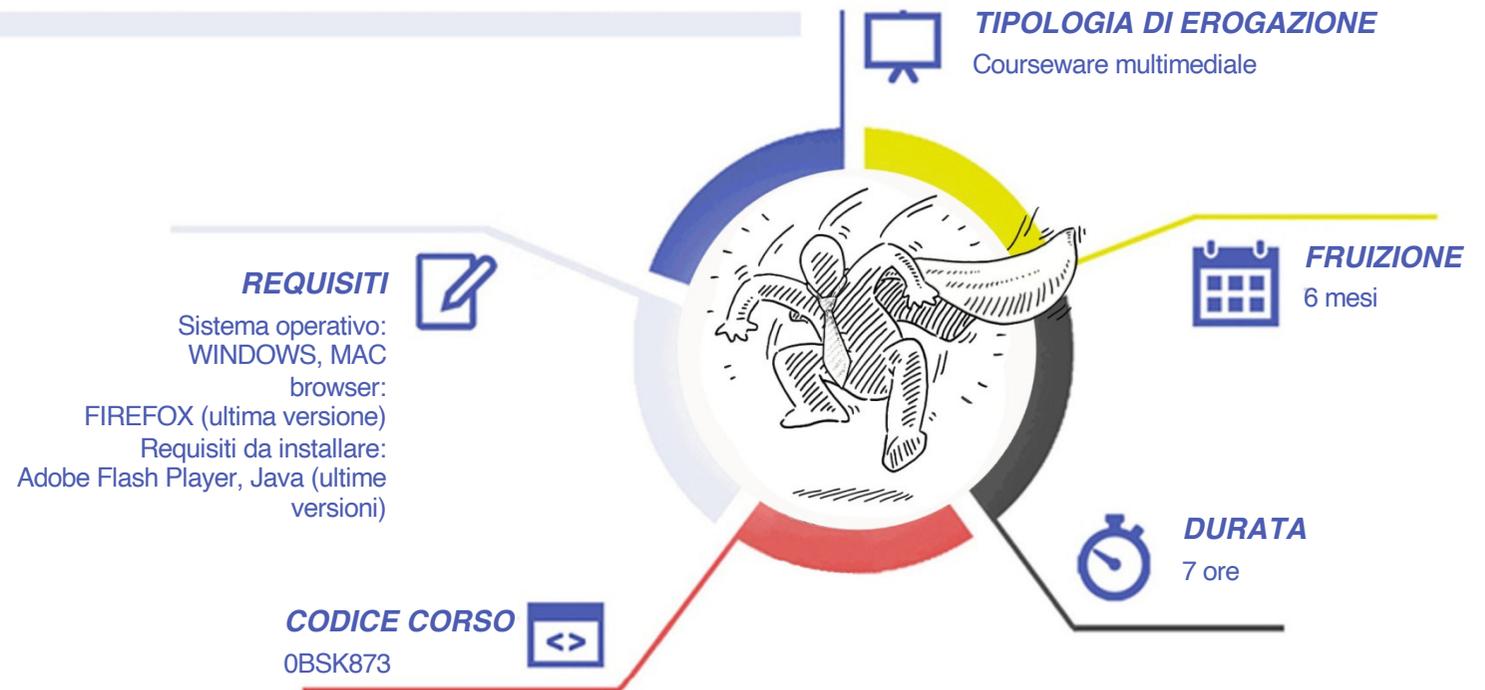
#### A CHI SI RIVOLGE

Il corso è rivolto a tutti coloro che vogliono approfondire le proprie conoscenze nell'ambito della Cybersecurity.

#### OBIETTIVI

Il corso presenta gli strumenti principali utilizzati da un ethical hacker. Dopo ogni lezione teorica viene descritto il funzionamento degli strumenti con esempi pratici, in modo tale da indirizzare lo studente fin da subito verso il mondo della cyber security. Ad esempio, come eseguire dei penetration test manuali con burp e come evidenziare le tipologie di attacco più frequenti (sql injection, xss, xxe ed altre).

In questo corso, oltre alla descrizione passo passo di come procedere alla configurazione dei sistemi, verranno anche spiegati tool e strumenti hardware e software utilizzati spesso nel campo della sicurezza.



## BUSINESS SKILLS

### CONTENUTI

#### Introduzione

- Introduzione all'installazione dei sistemi
- Installazione di Parrot Security

#### Privacy e crittografia

- Il concetto di anonimato
- La cancellazione sicura dei dati
- Cancellazione dei Dati con Shred: teoria e pratica
- Analisi Metadati: teoria e pratica
- Teoria - La crittografia
- Pratica - Strumenti di crittografia – SiriKali
- Teoria - La crittografia con GPG
- Pratica - Strumenti di crittografia GPG – GPA

#### Footprinting

- Teoria Information Gathering
- Configurazione Metasploitable 2 – Target
- Analisi Nmap
- Dig & Whois
- Recon-ng
- Traceroute
- Shodan
- Spiderfoot
- Maltego

#### Analisi dei certificati TLS/SSL

- SSLscan Command line
- SSLscan GUI version

#### Vulnerability Assessment

- Teoria Vulnerability Assessment
- Openvas Setup
- Openvas su Parrot – Setup
- Openvas Utilizzo
- Openvas Reportistica
- Nikto
- Nmap e Vulscan

#### WAPT

- Intro WAPT
- SQL Injection Teoria
- SQL Injection- Enumerazione Numero di Colonne
- SQL Injection - Enumerazione Type
- SQL Injection- Dati da altre tabelle
- SQL Injection- Più valori da una colonna
- SQL Injection- Versione DB Oracle
- SQL Injection - Version DB Microsoft e MySql
- SQL Injection - Listing DB non Oracle
- SQL Injection - Listing DB Oracle
- SQL Injection - Server Response
- Dictionary Attack – Teoria
- BROK AUTHENTICATION - Enumerazione user e password
- Teoria – XSS
- Reflected XSS
- Stored XSS
- Teoria – XML
- XXE - XML injection entità esterne
- Generazione Report

#### PENTEST

- Teoria Pentest
- Metasploit
- Armitage
- Metasploit - Backdoor Persistente
- Beef
- Penetration Test Windows – Enumerazione
- Penetration Test Windows - Enumerazione e utilizzo di Visual Basic
- Penetration Test Windows - Presa utente e ulteriore analisi
- Penetration Test Windows - Presa utente root
- Penetration Test con Lua
- Penetration Test con GTFO Bins
- Penetration Test con Metasploit e John the Ripper

### I VANTAGGI DELL'E-LEARNING

- Risparmio in termini di tempi/costi - Piattaforma AICC/SCORM 1.2 conforme agli standard internazionali - Accessibilità ovunque e in ogni momento
- Possibilità di rivedere le lezioni anche dopo aver terminato il corso

## BUSINESS SKILLS

### **ESERCITAZIONI**

All'interno del corso vi saranno momenti di verifica aventi come oggetto domande attinenti all'argomento appena trattato. In caso di risposta errata, l'utente non potrà proseguire o concludere la formazione se non affrontando nuovamente il momento di verifica.

### **SUPERAMENTO**

Una volta seguite tutte le lezioni proposte nella loro interezza di tempo è possibile ottenere l'attestato di superamento del corso.

Gli attestati conseguibili sono nominali per singolo corso ed è possibile ottenerli solo al corretto completamento del momento formativo finale.

### **CERTIFICAZIONI**

Gli attestati rilasciati permettono di acquisire competenze secondo quanto indicato dal Framework DigComp 2.1 e, quindi, sono in grado di attestare in maniera oggettiva le competenze digitali necessarie per operare correttamente a livello professionalizzante nel lavoro in Europa.

### **I VANTAGGI DELL'E-LEARNING**

- Risparmio in termini di tempi/costi - Piattaforma AICC/SCORM 1.2 conforme agli standard internazionali
- Accessibilità ovunque e in ogni momento - Possibilità di rivedere le lezioni anche dopo aver terminato il corso