



3 ore. Un obiettivo. Una competenza chiave.

Corso Kali Linux per Ethical Hacker





Corso Kali Linux per Ethical Hacker

Simulazione d'attacco con Kali Linux

In 3 ore vedrai dall'interno una simulazione d'attacco condotta con Kali Linux: demo pratiche, scansione, exploitation e post-exploit in laboratorio isolato. Capirai come gli attaccanti trovano e sfruttano debolezze e quali contromisure applicare per migliorare le difese.

ISCRIVITI

Dettagli del corso

-  10 giugno 2026 dalle 9.30 - 12.30
-  Online Live
-  €99+IVA a partecipante
-  Posti limitati

Cosa è incluso nel corso

-  Open Badge
-  Registrazione per 3 mesi
-  Materiale didattico

La tua skill in 3 ore

L'obiettivo è capire come si svolge un penetration test pratico e saper interpretare risultati e rischi per potenziare le difese.

Alla fine del corso sarai in grado di:

- Eseguire scansioni e interpretare i risultati (host, porte, servizi, fingerprint OS)
- Capire il funzionamento base di Metasploit e come costruire/gestire payload e sessioni
- Valutare vulnerabilità comuni (es. SMB/EternalBlue) e le contromisure pratiche
- Interpretare output di cracking e brute-force e applicare mitigazioni operative

Corso Kali Linux per Ethical Hacker

Simulazione d'attacco con Kali Linux

Prerequisiti di partecipazione

- Conoscenze base di Linux, concetti di rete (IP, TCP/UDP) e familiarità con VM.

Programma del corso

Modulo 1: Approccio etico & panoramica Kali Linux

- Cos'è Kali Linux e a cosa serve
- Le fasi del penetration testing
- Strumenti preinstallati: come è strutturato Kali
- Etica, legalità e come allestire un lab sicuro (VM isolate, firewall, snapshot)

Modulo 2: Scansione della rete e discovery

- Rilevamento host e mapping di rete (principi e interpretazione risultati)
- Identificazione servizi e porte (TCP/UDP) e fingerprinting OS (concetti, output tipici)
- Scansioni "aggressive" e cosa significano le flag più usate (-A, -sV ecc.)
- Esempio live su VM vulnerabile: mappa servizi e rischi emersi

Modulo 3: Exploitation con Metasploit e attacchi alle password

- Introduzione a Metasploit: exploit, payload, sessioni
- Brute-force su RDP/SSH/SMB e cracking password (dizionari, rainbow tables)
- Esempio exploit SMB (EternalBlue o equivalente) e post-exploit pratico
- Dump e cracking di hash da SAM/NTDS (demo controllata)