



Corso di

# Ethical Hacking

SLAS//SCHOCI

— alta formazione —

# \* Partner e certificazioni \*



APP DEVELOPMENT  
WITH SWIFT  
LEVEL 1



EC-Council Associate

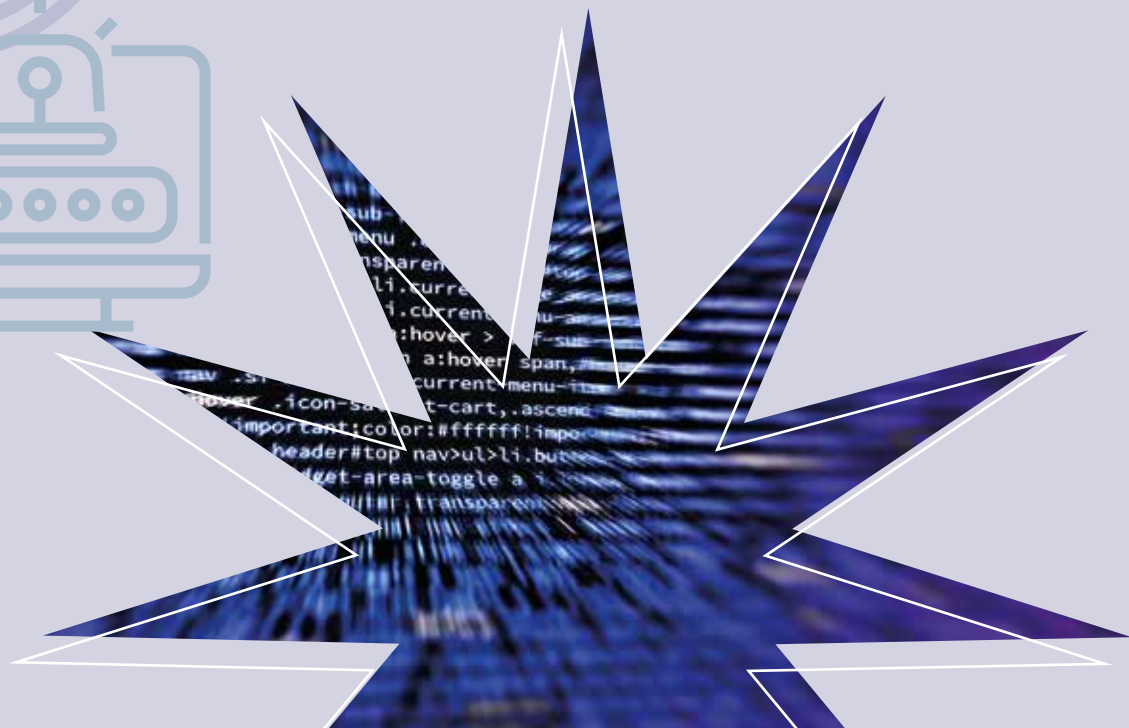


# \* Cosa fa un Ethical Hacker? \*



L'Ethical Hacker è un professionista della sicurezza informatica che, con il permesso delle aziende, utilizza le proprie competenze per individuare e correggere vulnerabilità nei sistemi. Il suo obiettivo è migliorare la sicurezza dei dati, impiegando "in maniera etica" le tecniche usate dai criminali informatici.

Il corso di Ethical Hacking include una combinazione di teoria e pratica ed offre scenari realistici per simulare attacchi e difese in un ambiente sicuro e identificare e mitigare le vulnerabilità dei sistemi, utilizzando approcci etici e conformi alle normative.



# \* Lavorare come Ethical Hacker \*



Ecco un esempio dei profili che è possibile ricoprire al termine del percorso formativo:



**ETHICAL HACKER JUNIOR • PENETRATION TESTER  
VULNERABILITY ASSESSOR • SECURITY CONSULTANT  
SPECIALISTA IN SICUREZZA RETI • INCIDENT RESPONDER**



## Destinatari

Studenti, neolaureati, diplomati, sistemisti IT, aspiranti ethical hacker, penetration tester, amministratori di rete.



## Pre-requisiti

- **Conoscenza di base dei sistemi operativi**
- **Comprensione generale dei concetti IT**
- **Interesse per la sicurezza informatica**

# \* Cosa ti offriamo \*



## LEZIONI ONLINE IN DIRETTA

con registrazioni accessibili  
in qualsiasi momento



## CORSO PRATICO CON SFIDE REALI

e simulazioni degli scenari  
del contesto professionale



## PROJECT WORK FINALE

da far valere come  
tuo portfolio



## NESSUN REQUISITO DI ACCESSO

se non la volontà di  
conseguire il risultato!



## ORARI FLESSIBILI

concordati in base  
ai tuoi impegni



## AREA RISERVATA ALLO STUDENTE

con materiale didattico, test  
e simulatori esami



## SUPPORTO COSTANTE DEI DOCENTI

per facilitare  
l'apprendimento



## CERTIFICAZIONI INTERNAZIONALI

per le tue opportunità  
di carriera



## COACHING DI CARRIERA

Servizio opzionale per facilitare  
l'accesso al mondo del lavoro

# \* Il nostro piano di studi \*



## 12 MODULI DIDATTICI PER DIVENTARE ETHICAL HACKER

+2 SPECIALIZZAZIONI OPZIONALI

1. INTRODUZIONE ALL'ETHICAL HACKING
2. STRUTTURA E FUNZIONAMENTO DELLE RETI
3. FOOTPRINTING E RICOGNIZIONE
4. SCANSIONE E ANALISI DELLE VULNERABILITÀ
5. HACKING DELLE RETI
6. HACKING DEI SISTEMI
7. HACKING DELLE APPLICAZIONI WEB
8. SICUREZZA E PROTEZIONE DATI
9. INGEGNERIA SOCIALE E PHISHING
10. REPORTISTICA E DOCUMENTAZIONE
11. PORTFOLIO E PROGETTO FINALE
12. PREPARAZIONE ALL'ESAME DI CERTIFICAZIONE



**Computer  
Forensics Expert**



**Chief Information  
Security Officer  
(CISO)**

✦ Scopri il nostro ✦

# Piano di studi

nel dettaglio



# \* Piano di studi \*

## 1 > INTRODUZIONE ALL'ETHICAL HACKING

Esplorare i principi fondamentali dell'ethical hacking, il suo ruolo nella sicurezza informatica e le differenze tra hacking etico e non etico.

### Unità didattiche

- Ethical hacking e hacking non etico
  - Definizione di vulnerabilità, exploit e minaccia
  - Ruolo dell'ethical hacker e ciclo di vita della sicurezza
  - Normative ed etica professionale
- 

## 2 > STRUTTURA E FUNZIONAMENTO DELLE RETI

Acquisire le nozioni di base sul funzionamento delle reti informatiche, essenziali per comprendere come gli attaccanti sfruttano le vulnerabilità di rete.

### Unità didattiche

- Protocolli di rete (TCP/IP, UDP, HTTP, DNS)
  - Topologie e infrastrutture di rete
  - Firewall, NAT e segmentazione della rete
  - Introduzione alla sicurezza delle reti wireless
- 

## 3 > FOOTPRINTING E RICOGNIZIONE

Apprendere le tecniche per raccogliere informazioni su un obiettivo (come indirizzi IP, infrastrutture etc.), per identificare possibili punti deboli da proteggere prima di pianificare un attacco etico.

### Unità didattiche

- Footprinting e open-source intelligence (OSINT)
- Strumenti di ricognizione (Nmap, Maltego, Recon-ng)
- Identificazione di servizi e versioni dei sistemi
- Tecniche di social engineering e reconnaissance online

## 4 > SCANSIONE E ANALISI DELLE VULNERABILITÀ

Identificare e valutare le vulnerabilità nei sistemi informatici, utilizzando strumenti specifici per analizzare potenziali rischi e punti deboli da correggere.

### Unità didattiche

- Tipologie di scansione (attiva, passiva, approfondita)
  - Uso di scanner di vulnerabilità (Nessus, OpenVAS)
  - Identificazione di porte aperte e servizi vulnerabili
  - Analisi dei risultati e valutazione dei rischi
- 

## 5 > HACKING DELLE RETI

Fornire le tecniche per compromettere "eticamente" la sicurezza delle reti, simulando attacchi reali ai protocolli di comunicazione e alle configurazioni di rete, al fine di rafforzare la protezione contro minacce esterne.

### Unità didattiche

- Tecniche di attacco man-in-the-middle (MITM)
  - Sniffing e intercettazione del traffico di rete
  - Sfruttamento di vulnerabilità in protocolli e reti wireless
  - Attacchi DDoS e prevenzione
- 

## 6 > HACKING DEI SISTEMI

Utilizzare metodologie e tecniche per compromettere "eticamente" i sistemi operativi e le applicazioni, esplorando vulnerabilità nei software, per fornire soluzioni per migliorare la sicurezza informatica.

### Unità didattiche

- Strumenti di attacco a sistemi Windows e Linux
  - Privilege escalation e mantenimento dell'accesso
  - Metasploit Framework: introduzione e utilizzo
  - Tecniche di post-exploitation
- 

## 7 > HACKING DELLE APPLICAZIONI WEB

Apprendere le tecniche per identificare e sfruttare le vulnerabilità nelle applicazioni web, al fine di migliorare la sicurezza e proteggere i dati sensibili da attacchi informatici.

### Unità didattiche

- Vulnerabilità OWASP Top 10
- Attacchi SQL injection e XSS
- Analisi delle configurazioni errate
- Testing delle app web (Burp Suite, OWASP ZAP)

## 8 > SICUREZZA E PROTEZIONE DATI

Proteggere i dati sensibili attraverso l'implementazione di tecniche di sicurezza avanzate, comprendendo i rischi associati alla perdita di dati, come la violazione della privacy e i danni alla reputazione aziendale.

### Unità didattiche

- Principi di crittografia e cifratura
  - Tecniche di protezione dei dati sensibili
  - Analisi dei rischi legati ai ransomware
  - Best practice per la gestione sicura dei dati
- 

## 9 > INGEGNERIA SOCIALE E PHISHING

Apprendere le tecniche di manipolazione psicologica, come l'inganno, l'intimidazione e la persuasione, utilizzate da malintenzionati per sfruttare la fiducia umana e compromettere i sistemi informatici.

### Unità didattiche

- Fondamenti di ingegneria sociale
  - Tecniche di phishing e spear phishing
  - Pretexting e baiting
  - Strategie di difesa contro attacchi sociali
- 

## 10 > REPORTISTICA E DOCUMENTAZIONE

Documentare accuratamente le attività di hacking etico, strutturare e redigere report professionali di sicurezza dettagliati, che includano le vulnerabilità identificate e le metodologie utilizzate.

### Unità didattiche

- Report tecnico di penetration testing
  - Analisi dei risultati e raccomandazioni
  - Comunicazione dei rischi a clienti e team di sviluppo
  - Gestione della compliance normativa
- 

## 11 > PORTFOLIO E PROGETTO FINALE

Sviluppare un progetto pratico da far valere come portfolio per mostrare le proprie competenze e la capacità di applicarle in contesti reali. Affrontare scenari e studi di caso per consolidare le abilità tecniche.

### Unità didattiche

- Sviluppo di un penetration test completo
- Documentazione e presentazione dei risultati
- Preparazione del portfolio professionale

## 12 > PREPARAZIONE ALL'ESAME DI CERTIFICAZIONE

Certificare le conoscenze e le competenze per aumentare la credibilità professionale, ottenere un vantaggio competitivo nel mondo del lavoro e migliorare le opportunità di carriera.

### Unità didattiche

- Analisi del syllabus delle competenze
- Svolgimento delle prove di simulazione
- Strategie e tecniche per affrontare l'esame

# \* Specializzazione \*

Al termine del percorso sarà possibile specializzarsi ulteriormente partecipando a focus di approfondimento che consentiranno di diventare più competitivi nel mercato del lavoro, grazie ad una preparazione più approfondita per affrontare sfide specifiche nel settore. I due percorsi di specializzazione:

## Computer Forensics Expert



## Chief Information Security Officer (CISO)



## SPECIALIST 1

# COMPUTER FORENSICS EXPERT

Il Computer Forensics Expert, noto anche come Digital Forensics Expert, è un professionista che opera nell'ambito dei reati informatici o computer crime. Si occupa di preservare, identificare, analizzare e interpretare i dati contenuti all'interno di qualsiasi supporto digitale o dispositivo di memorizzazione.

### Unità didattiche

- Responsabilità dell'esperto in forensics
- Attendibilità dei dati informatici
- Acquisizione e conservazione dei dati
- Crimini informatici e network forensics
- Tutela della reputazione online



## SPECIALIST 2

# CHIEF INFORMATION SECURITY OFFICER (CISO)

Il CISO è un dirigente responsabile della gestione della sicurezza informatica aziendale e della protezione delle informazioni sensibili. Il suo compito è definire strategie di cybersecurity, valutare i rischi informatici e garantire la conformità alle normative di sicurezza.

### Unità didattiche

- Governance e Strategie di Cybersecurity
- Risk Management e Business Continuity
- Compliance e Normative di Sicurezza
- Incident Response e Gestione delle Minacce
- Leadership e Gestione del Budget per la Sicurezza



# \* Certificazione \*

## EC-COUNCIL ETHICAL HACKING ESSENTIALS

La certificazione Ethical Hacking Essentials (EHE) è:

– Approvata dal Dipartimento dell'Istruzione (DOE) della Florida degli Stati Uniti come titolo riconosciuto dal settore nell'ambito del Florida Career and Professional Education Act (CAPE) per l'istruzione secondaria.

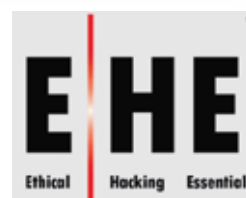
– Approvata dal Dipartimento dell'Istruzione dello Stato della Virginia, istruzione professionale e tecnica come credenziali riconosciute dal settore.

– Approvato dall'Ohio DOE (Dipartimento dell'Istruzione) e da Workforce come elenco di credenziali riconosciute dal settore e approvato dalla divisione Career and Technical Education dell'Arkansas DOE come titolo riconosciuto dal settore.



### Syllabus e obiettivi esame:

1. Information Security Fundamentals
2. Ethical Hacking Fundamentals
3. Threats and Vulnerability Assessment
4. Password Cracking Techniques
5. Social Engineering Techniques
6. Networks, Web, Wireless, IOT & OT attacks
7. Cloud computing threats
8. Penetration testing



\* Esame presso centro autorizzato

Superato l'esame previsto sarà possibile ottenere la copia elettronica del Certificato accedendo con le credenziali (user name e password) al proprio profilo sul sito: [www.certiport.com](http://www.certiport.com)

**MILANO** Via Caldera, 21

**ROMA** Via Vittorio Veneto, 54 b

**NAPOLI** Centro Direzionale, Isola E/2, 1° piano, int. 4

**AVELLINO** Piazza Libertà, 45

**MISTERBIANCO (CT)** Via A.B. Sabin angolo via Milicia, sn

Tel. 02 30 35 76 98

Fax 02 30 35 76 00

[info@slashschool.it](mailto:info@slashschool.it)

**SLAS//SCHOO/**  
— alta formazione —

[www.slashschool.it](http://www.slashschool.it)