

Università degli Studi di Salerno



Dipartimento di Informatica

Penetration Testing & Ethical Hacking

Introduzione al Corso

Arcangelo Castiglione
arcastiglione@unisa.it

Outline

- Motivazioni del Corso
- Obiettivi e Scopi del Corso
- Contenuti del Corso
- Informazioni Generali

Outline

- **Motivazioni del Corso**
- Obiettivi e Scopi del Corso
- Contenuti del Corso
- Informazioni Generali

Motivazioni del Corso



Motivazioni del Corso

Investimenti Record

Report Insights

Market was valued at

 **\$219.04**
Billion

2023

Projected to reach

 **\$578.15**
Billion

2033

Growing at a CAGR

 **10.4% From**
2023-2032

CAGR 10.4%

**\$578.15
Billion**



Cyber Security Market
Report Code: A01442

Allied Market Research
© All right reserved

Fonte: [Allied Market Research](#)

Motivazioni del Corso

Investimenti Record

Cybersecurity, record per il mercato italiano: spesa a 2,15 miliardi

Il 62% delle grandi aziende ha investito di più in difesa digitale delle infrastrutture

di Enrico Netti

23 febbraio 2024

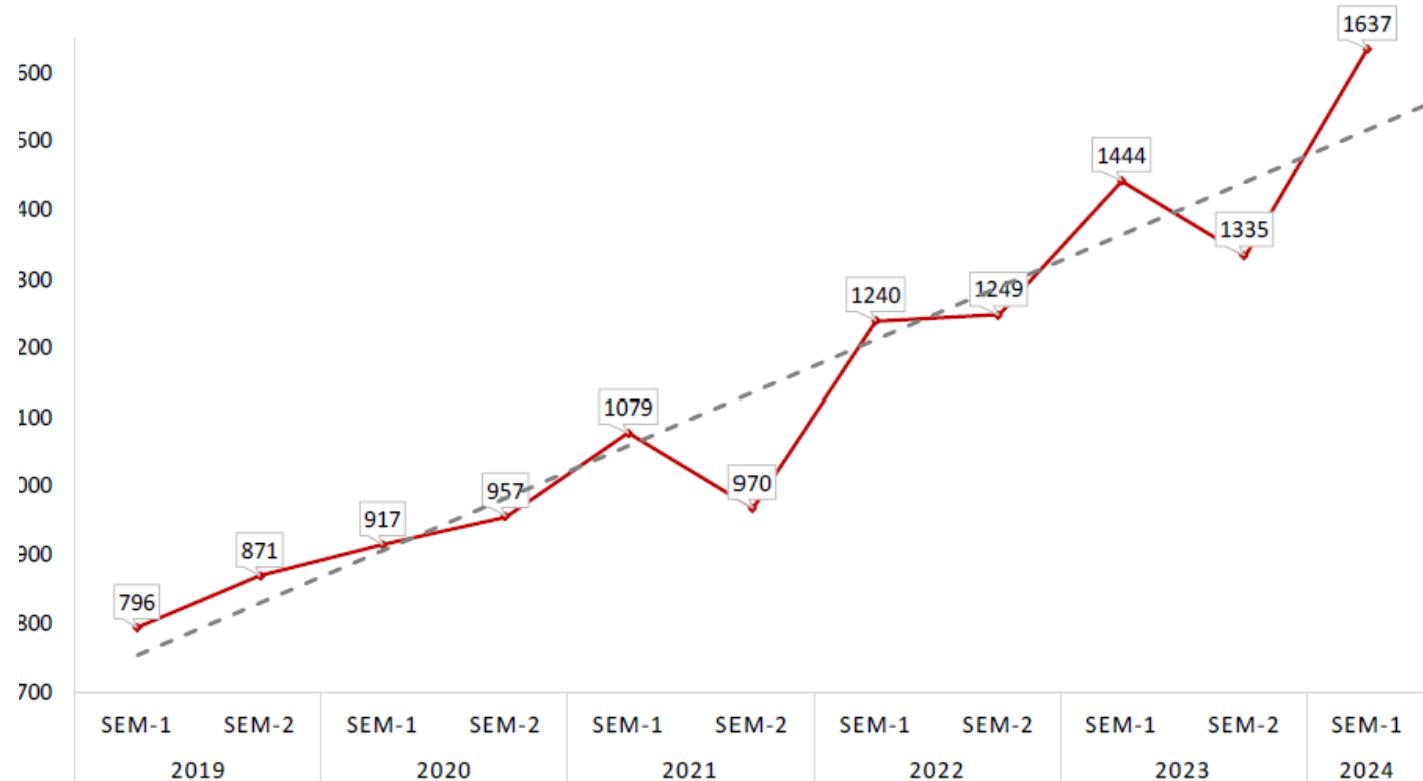


Fonte: [ilsole24ore](#)

Motivazioni del Corso

Forte Crescita degli Attacchi Informatici

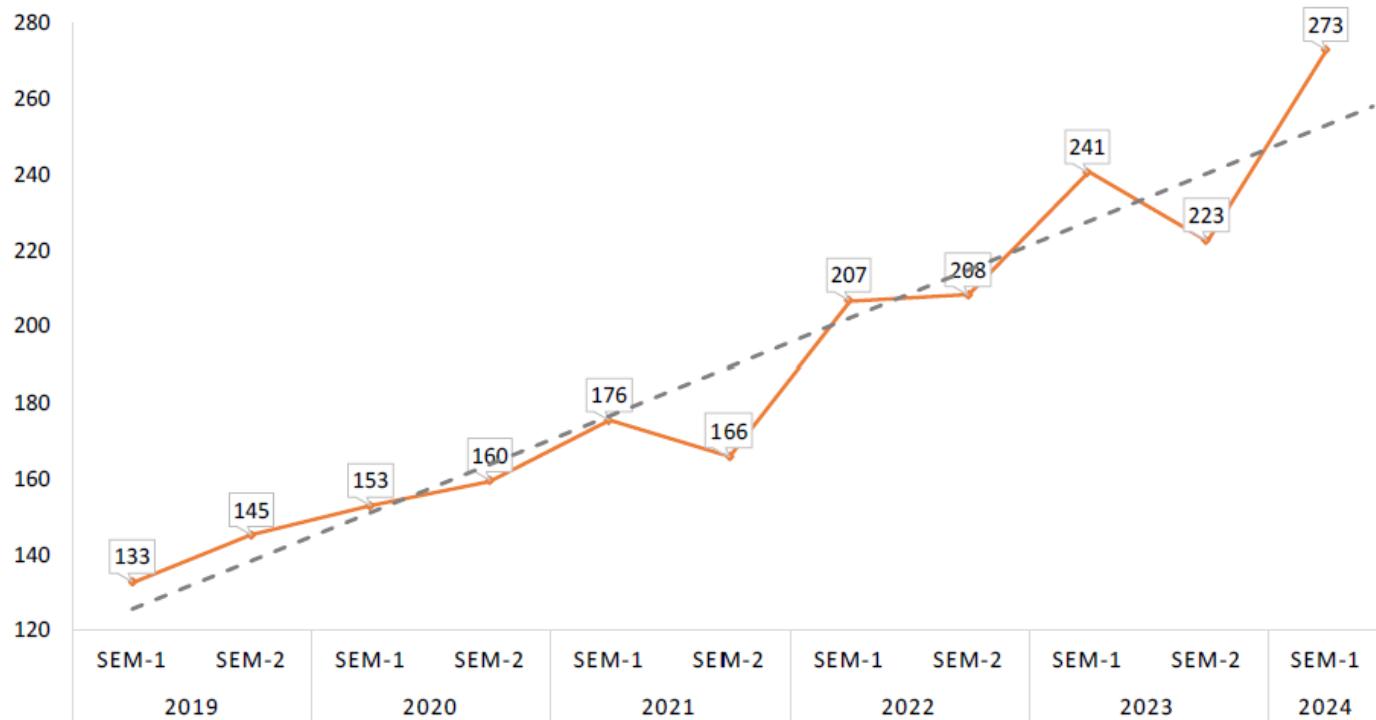
Incidenti per semestre H1 2019 - H1 2024



Motivazioni del Corso

Forte Crescita degli Attacchi Informatici

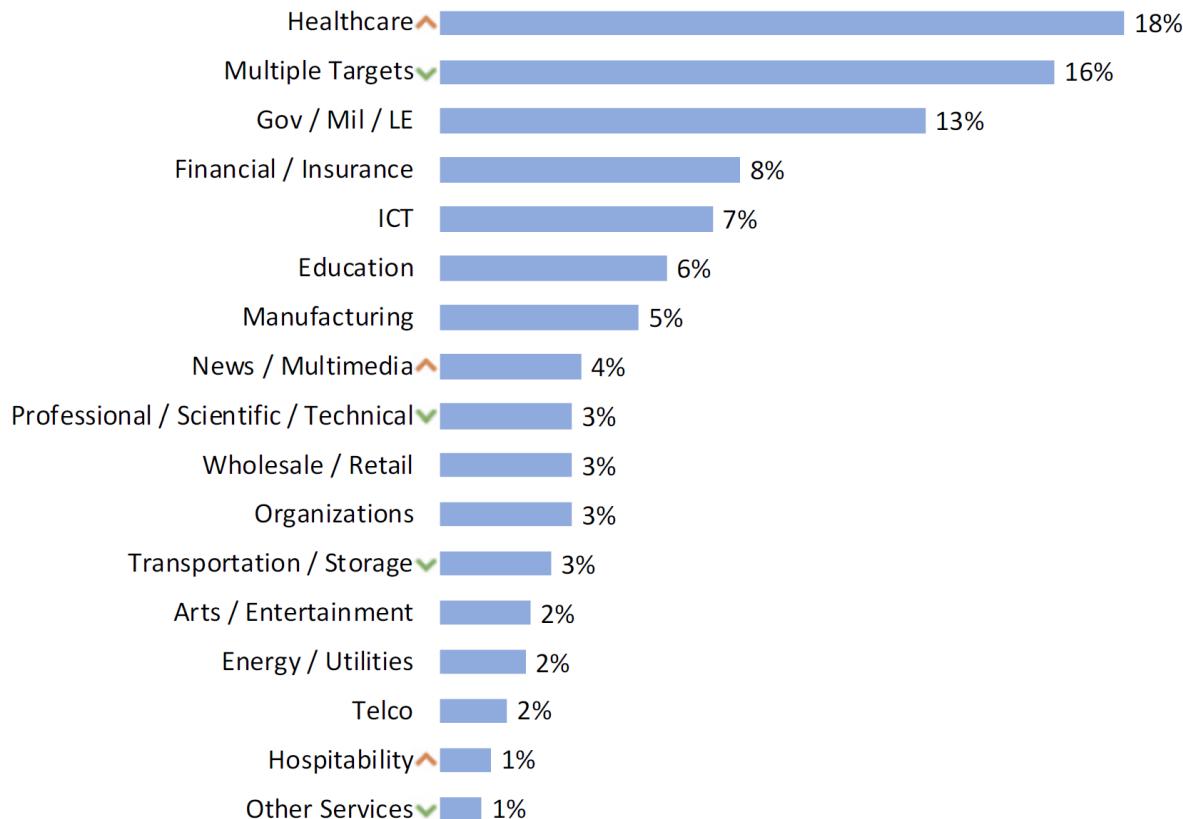
Media mensile per semestre H1 2019 - H1 2024



Motivazioni del Corso

Forte Crescita degli Attacchi Informatici

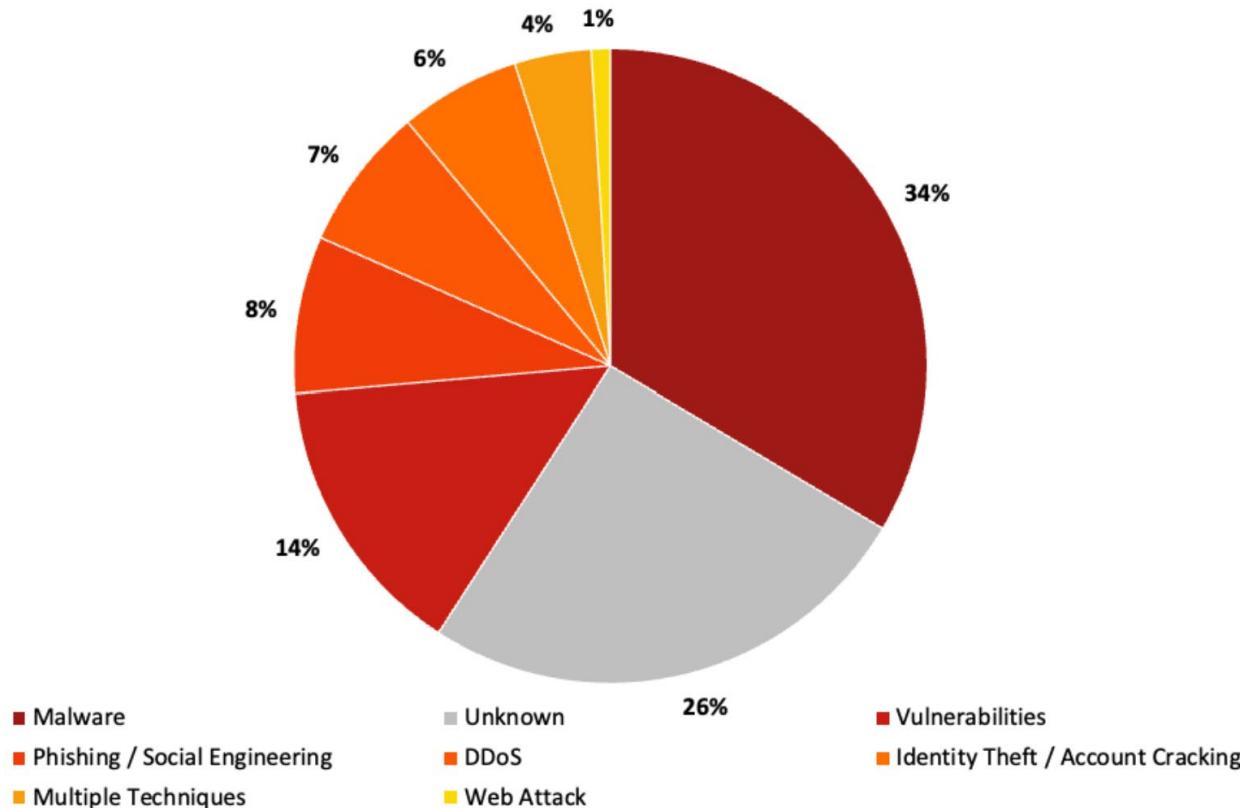
Distribuzione delle vittime H1 2024



Motivazioni del Corso

Forte Crescita degli Attacchi Informatici

Distribuzione delle tecniche H1 2024



© Clusit - Rapporto 2024 sulla Sicurezza ICT in Italia - Aggiornamento giugno 2024

Motivazioni del Corso

Informatizzazione implica Necessità di Protezione



Motivazioni del Corso

General Data Protection Regulation (EU GDPR)



Link

Motivazioni del Corso

The EU Cybersecurity Act



Link

Motivazioni del Corso

Network and Information Security (NIS 2)



<https://nis2directive.eu/>

Motivazioni del Corso

Network and Information Security (NIS 2)

- «...effettuare valutazioni coordinate dei rischi per la sicurezza...»
- «...audit sulla sicurezza periodici e mirati effettuati da un organismo indipendente o da un'autorità competente...»
- «...attuazione di politiche di cibersicurezza, quali i risultati di audit sulla sicurezza effettuati da un controllore qualificato...»
- «...imporre ai soggetti interessati di attuare le raccomandazioni fornite in seguito a un audit sulla sicurezza entro un termine ragionevole...»
- «...scansioni di sicurezza basate su criteri di valutazione dei rischi obiettivi, non discriminatori, equi e trasparenti, se necessario, con la cooperazione del soggetto interessato...»
- «...scansione proattiva dei sistemi informativi e di rete del soggetto interessato per rilevare le vulnerabilità con potenziale impatto significativo...»
- «...scansione è effettuata per individuare sistemi informativi e di rete vulnerabili o configurati in modo non sicuro e per informare i soggetti interessati...»



Motivazioni del Corso

Cyberwarfare and Cyber Defence

- La NATO ha più volte ribadito che «un attacco cyber rivolto ad una Nazione è un'aggressione a tutti i paesi membri»
- L'Articolo 5 del trattato NATO sancisce che «il diritto alla difesa collettiva scatterebbe immediatamente, poiché la NATO considera lo spazio cibernetico una nuova dimensione degli scontri armati al pari di terra, cielo, aria e spazio...»



Motivazioni del Corso

Cyberwarfare and Cyber Defence

NATO will defend itself

Article by NATO Secretary General Jens Stoltenberg published in Prospect's new cyber resilience supplement

27 Aug. 2019 - | Last updated: 29 Aug. 2019 16:38

[English](#) | [French](#) | [Russian](#) | [Ukrainian](#)

The alliance will guard its cyber domain—and invoke collective defence if required.

f

X

in



Fonte: nato.int

Motivazioni del Corso

Cyberwarfare and Cyber Defence

Cyber defence

Last updated: 30 Jul. 2024 16:59

[English](#) | [French](#) | [Russian](#) | [Ukrainian](#)

f Cyber threats to the security of the Alliance are complex, destructive and coercive, and are becoming ever more frequent. Cyberspace is contested at all times and malicious cyber events occur every day, from low-level to technologically sophisticated attacks. NATO and Allies are responding by strengthening the Alliance's ability to detect, prevent and respond to malicious cyber activities. NATO and its Allies rely on strong and resilient cyber defences to fulfil the Alliance's three core tasks of deterrence and defence, crisis prevention and management, and cooperative security. The Alliance needs to be prepared to defend its networks and operations against the growing sophistication of the cyber threats it faces.

X

in



Fonte: [nato.int](https://www.nato.int)

Motivazioni del Corso

NATO Cooperative Cyber Defence Centre of Excellence



The NATO Cooperative Cyber Defence Centre of Excellence is a multinational and interdisciplinary cyber defence hub

We do research, training and exercises in four core areas: technology, strategy, operations and law

Fonte: <https://ccdcOE.org/>

Motivazioni del Corso

Agenzia per la Cybersicurezza Nazionale (ACN)



**AGENZIA PER LA
CYBERSICUREZZA NAZIONALE**

[Agenzia](#) ▾

[Strategia](#) ▾

[PNRR](#)

[Comunicazione](#)

[Lavora con noi](#)

RESILIENZA, PROTEZIONE E INNOVAZIONE

L'ACN è l'Autorità nazionale per la cybersicurezza a tutela degli interessi nazionali nel campo della sicurezza e resilienza cibernetiche. Garantisce l'implementazione della **Strategia Nazionale di Cybersicurezza** adottata dal Presidente del Consiglio dei ministri.

[CHI SIAMO](#)

<https://www.acn.gov.it/>

Motivazioni del Corso

Agenzia per la Cybersicurezza Nazionale (ACN)



**AGENZIA PER LA
CYBERSICUREZZA NAZIONALE**

[Agenzia](#) ▾

[Strategia](#) ▾

PNRR

Comunicazione

[Lavora con noi](#)

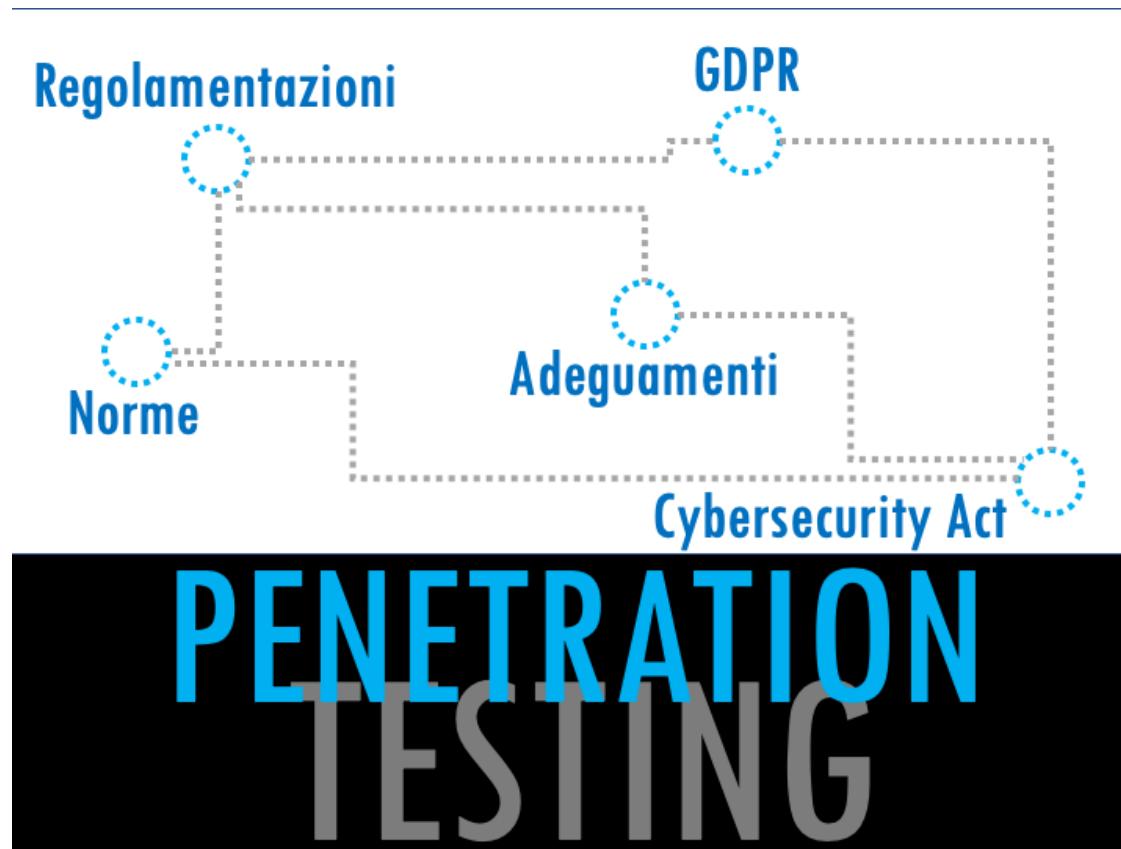
[Home](#) / [Lavora con noi](#)

Lavora con noi

**Unisciti all'Agenzia per la cybersicurezza
nazionale**

Motivazioni del Corso

Professionisti della Sicurezza



Motivazioni del Corso

Professionisti della Sicurezza



Motivazioni del Corso

Nuove Opportunità

NUOVE OPPORTUNITÀ



Motivazioni del Corso

Nuove Opportunità



Motivazioni del Corso

Nuove Opportunità

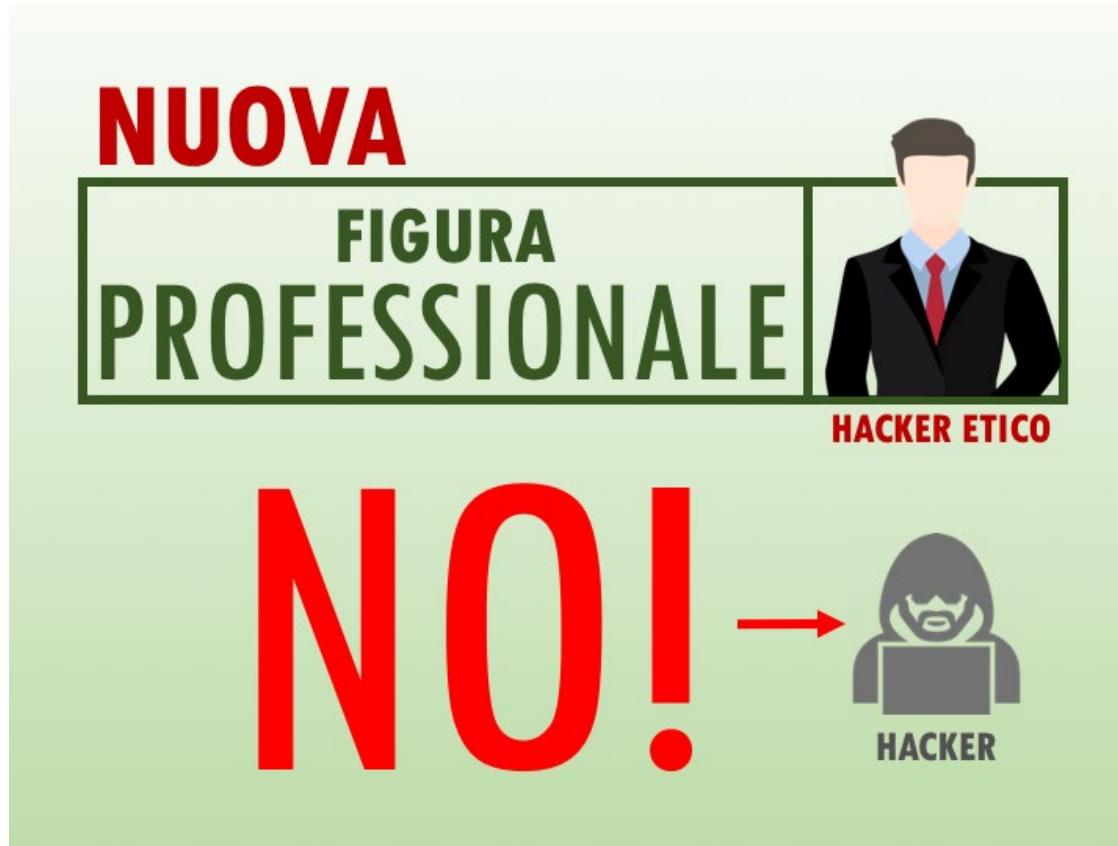
BUSINESS
LAVORO
RICERCA

NUOVE OPPORTUNITÀ



Motivazioni del Corso

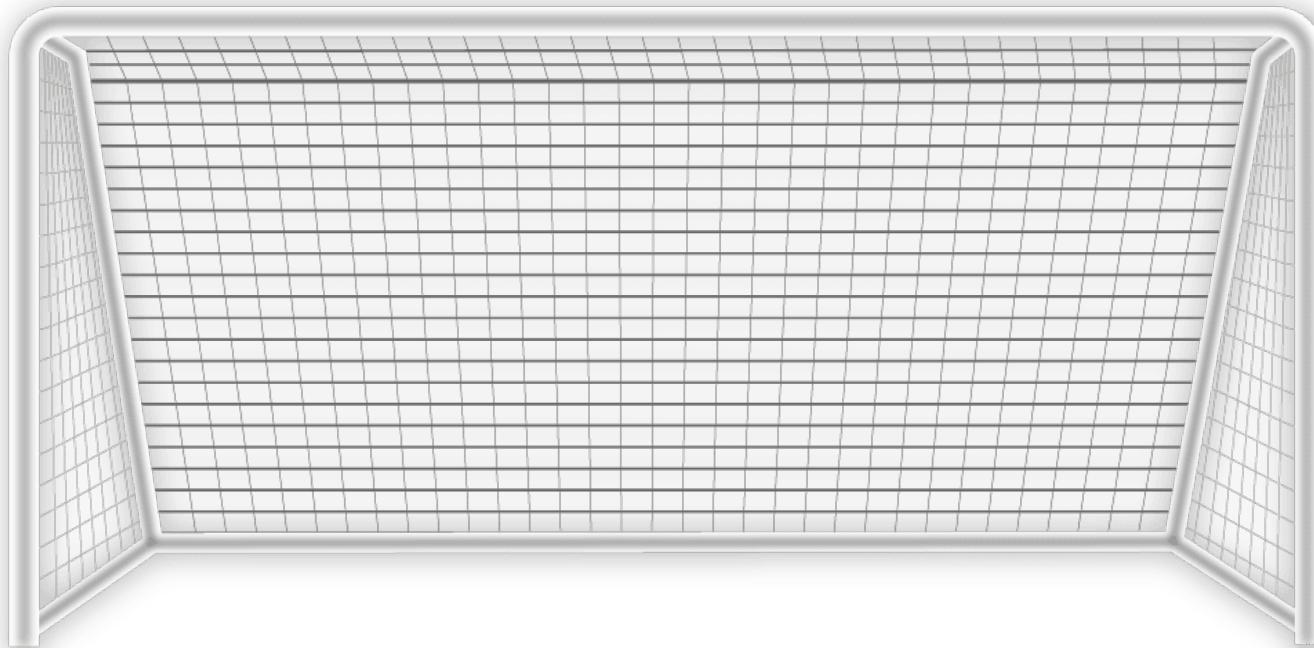
Nuova Figura Professionale – Hacker Etico



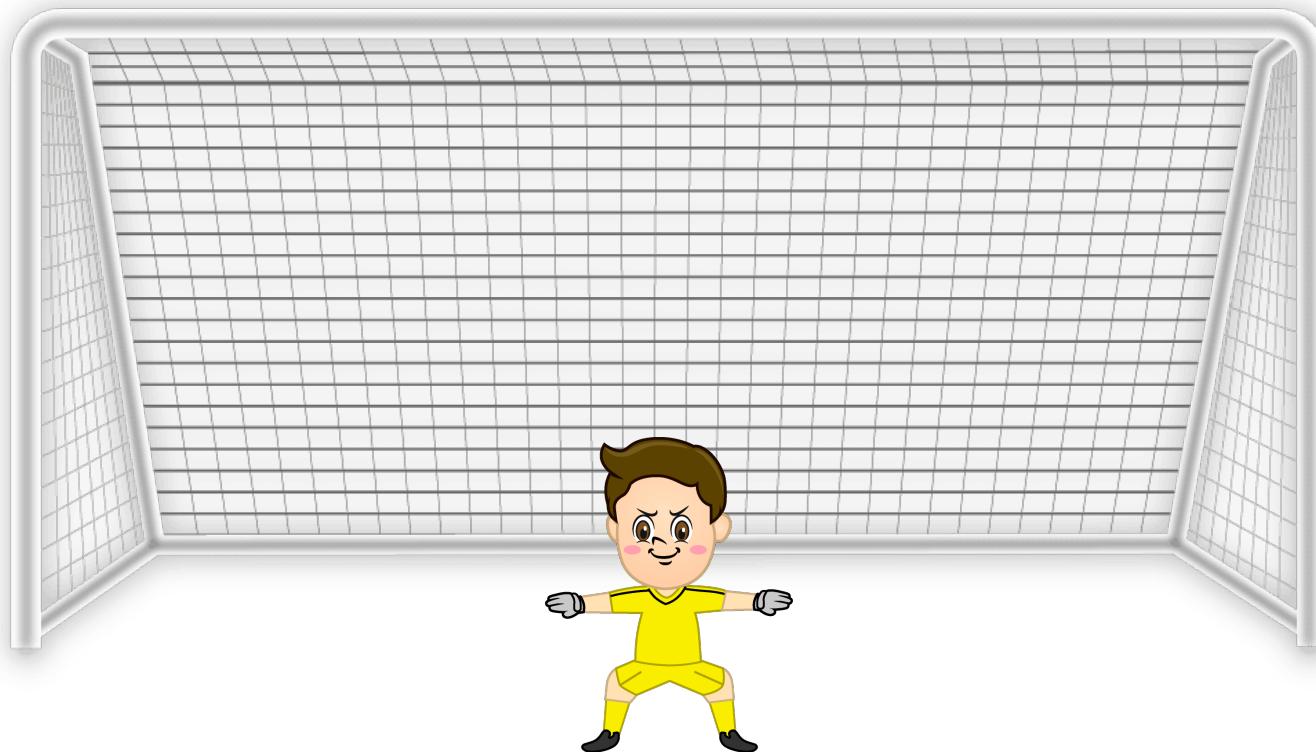
Outline

- Motivazioni del Corso
- **Obiettivi e Scopi del Corso**
- Contenuti del Corso
- Informazioni Generali

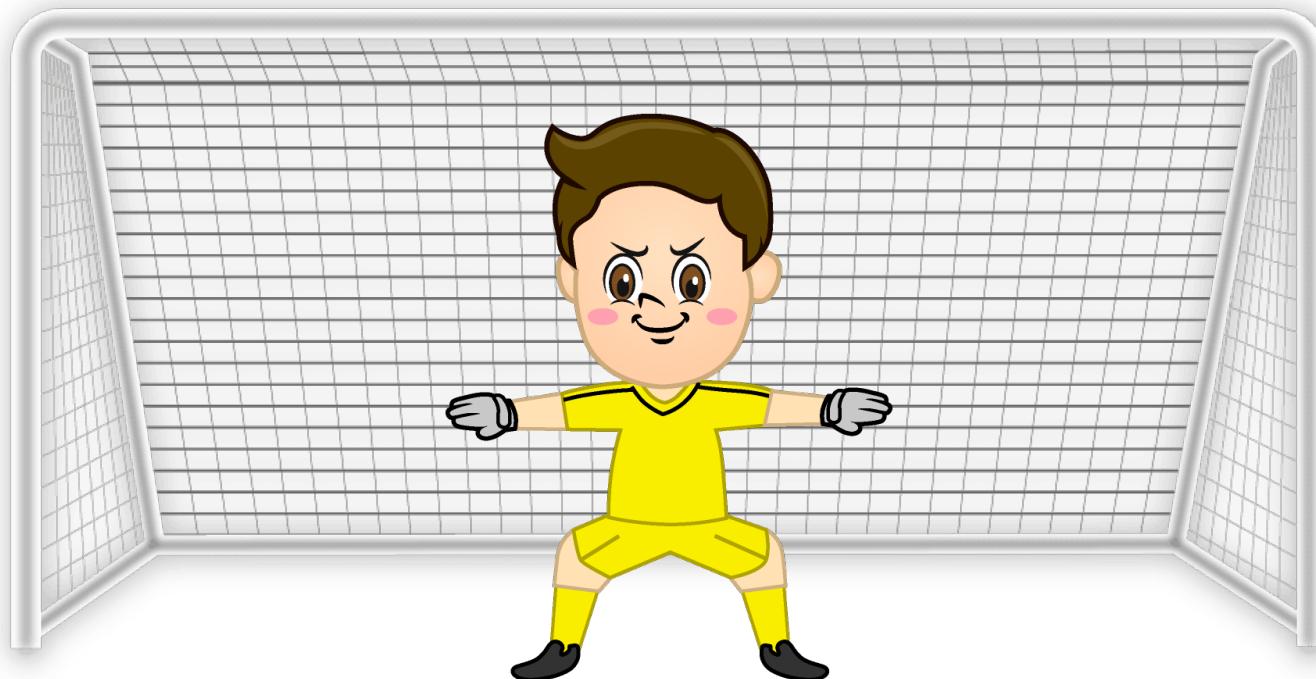
Obiettivi del Corso



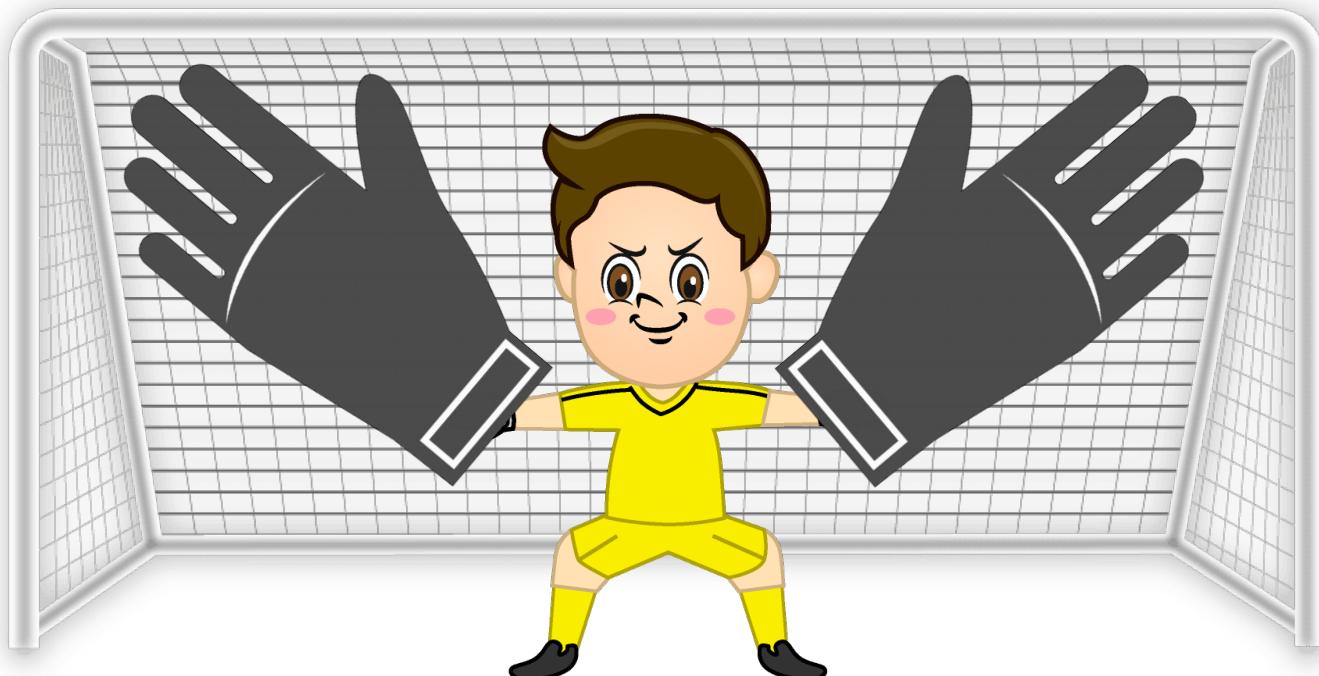
Obiettivi del Corso



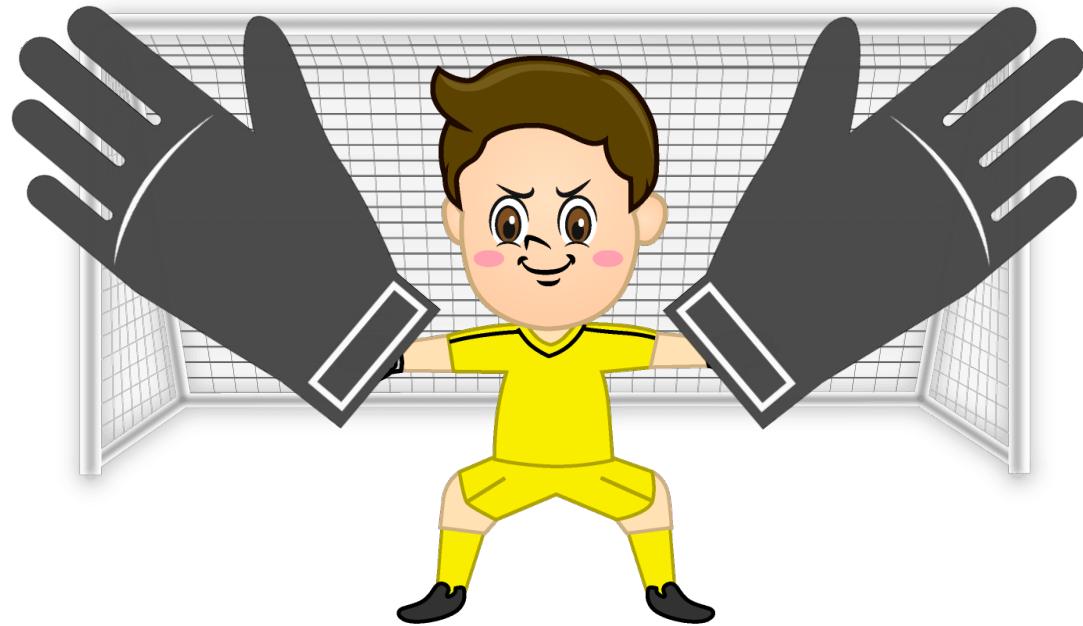
Obiettivi del Corso



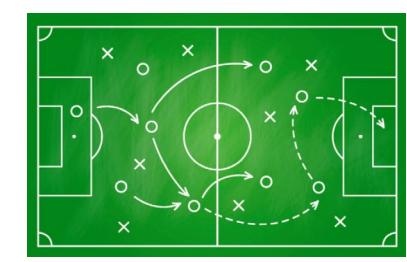
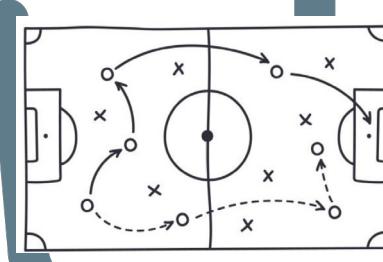
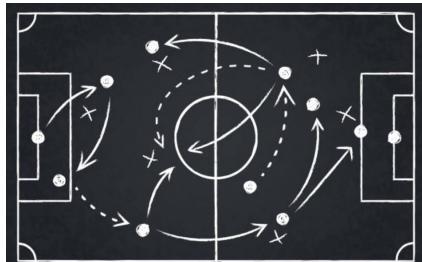
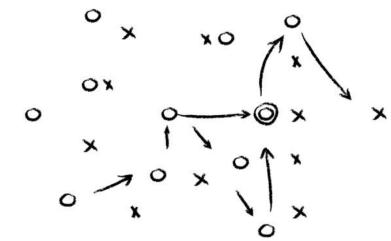
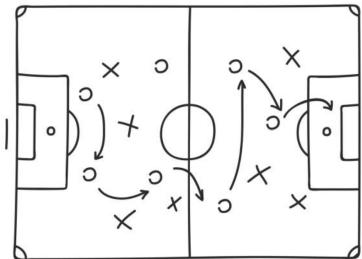
Obiettivi del Corso



Obiettivi del Corso



Obiettivi del Corso



Introduzione al Corso

Obiettivi del Corso

Obiettivi del Corso



Mostrare **come agiscono gli hacker** e come si possono utilizzare gli stessi metodi e strumenti **per proteggere i sistemi informatici** contro attacchi provenienti dagli stessi hacker

“Hackers Needed To Defeat Hackers”

COMMUNICATIONS
OF THE
ACM 

Obiettivi del Corso

Obiettivi del Corso



 Acquisire il necessario **background tecnico e metodologico** per valutare la sicurezza di sistemi complessi attraverso la comprensione delle **vulnerabilità esistenti**

Obiettivi del Corso

Dettagli

Arcangelo CASTIGLIONE | PENETRATION TESTING AND ETHICAL HACKING

PENETRATION TESTING AND ETHICAL HACKING	
	DIPARTIMENTO DI INFORMATICA
	CORSO DI LAUREA MAGISTRALE
	INFORMATICA
	2024/2025

cod. 0522500081

INSEGNAMENTO SU PIÙ CURRICULA 2

CURRICULUM SICUREZZA INFORMATICA

MODULI

DOCENTI

SCHEDA

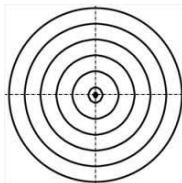


Obiettivi e Scopi del Corso

➤ Lo studente

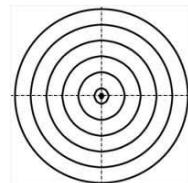
- acquisirà il necessario background, tecnico e metodologico, per valutare lo stato ed i fabbisogni di sicurezza di sistemi complessi
- In accordo a specifici requisiti di conformità e certificazione
- Attraverso la comprensione delle vulnerabilità esistenti

- apprenderà quanto necessario per rendere sicuri tali sistemi, prevenendo le principali minacce e malfunzionamenti che potrebbero influenzarne la corretta operatività



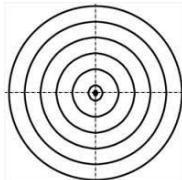
Obiettivi e Scopi del Corso

- Al termine del corso lo studente sarà in grado di
 - 1) Valutare debolezze e potenziali vulnerabilità all'interno di sistemi ed infrastrutture ICT
 - Valutazione ed analisi critica dei servizi oggetto di protezione
 - Individuazione dei possibili scenari di incidente, per prevedere eventuali contromisure e strategie di aggiornamento periodico e protezione



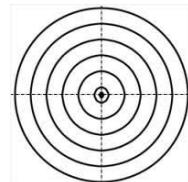
Obiettivi e Scopi del Corso

- Al termine del corso lo studente sarà in grado di
- 2) Spiegare ed utilizzare le metodologie standard per l'esecuzione delle verifiche di sicurezza della rete e dei penetration test
 - 3) Utilizzare strumenti comuni usati dai professionisti per lo svolgimento di verifiche di sicurezza della rete e dei penetration test
 - 4) Identificare e spiegare minacce alla sicurezza presenti in rete mediante relativi exploit e vulnerabilità



Obiettivi e Scopi del Corso

- Al termine del corso lo studente sarà in grado di
 - 5) Eseguire penetration test conformi ai principali standard internazionali
 - 6) Sviluppare documentazione mirata, da fornire alle controparti tecniche e gestionali
 - Illustrando tutti gli aspetti dei controlli di sicurezza effettuati mediante i penetration test che sono stati eseguiti



Outline

- Motivazioni del Corso
- Obiettivi e Scopi del Corso
- **Contenuti del Corso**
- Informazioni Generali

Principali Contenuti del Corso

- Fondamenti di Ethical Hacking
- Tipi e Metodologie di Penetration Testing
- Fasi del Processo di Penetration Testing
 - Target Scoping
 - Information Gathering
 - Target Discovery ed Enumerating Target
 - Vulnerability Mapping
 - Target Exploitation e Social Engineering
 - Target Post-Exploitation
 - Documentazione e Reporting
- Wireless Penetration Testing



Principali Contenuti del Corso

Fondamenti di Ethical Hacking

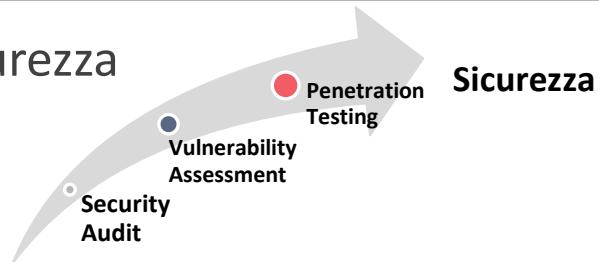
- Sicurezza e Caratterizzazione degli Attacchi
- Storia dell'Hacking
- Caratterizzazione degli Hacker
- Ethical Hacking Plan
- I Dieci Comandamenti dell'Ethical Hacking



Principali Contenuti del Corso

Tipi e Metodologie di Penetration Testing

➤ Tipologie di Test di Sicurezza



➤ Tipi di Penetration Testing



➤ Metodologie di Testing



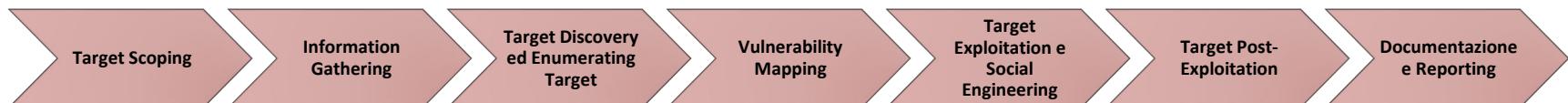
OWASP
Open Web Application
Security Project



Principali Contenuti del Corso

Fasi del Processo di Penetration Testing

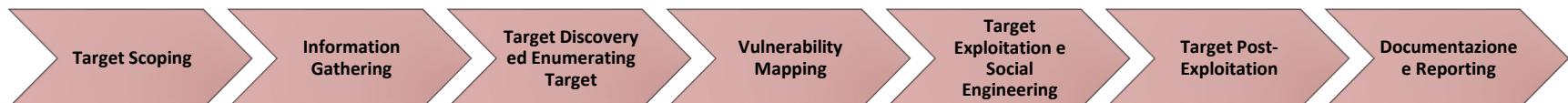
1. Target Scoping
2. Information Gathering
3. Target Discovery ed Enumerating Target
4. Vulnerability Mapping
5. Target Exploitation e Social Engineering
6. Target Post-Exploitation
7. Documentazione e Reporting



Principali Contenuti del Corso

Fasi del Processo di Penetration Testing

1. Target Scoping
2. Information Gathering
3. Target Discovery ed Enumerating Target
4. Vulnerability Mapping
5. Target Exploitation e Social Engineering
6. Target Post-Exploitation
7. Documentazione e Reporting

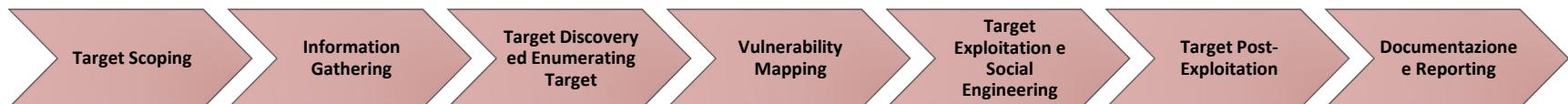


Principali Contenuti del Corso

Fasi del Processo di Penetration Testing

1. Target Scoping
2. Information Gathering
3. Target Discovery ed Enumerating Target
4. Vulnerability Mapping
5. Target Exploitation e Social Engineering
6. Target Post-Exploitation
7. Documentazione e Reporting

Fasi condotte in modo sequenziale su un'infrastruttura di rete, talvolta complessa, nota come «Asset»

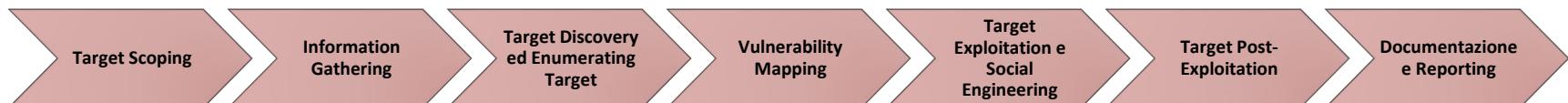


Principali Contenuti del Corso

Fasi del Processo di Penetration Testing

1. Target Scoping
2. Information Gathering
3. Target Discovery ed Enumerating Target
4. Vulnerability Mapping
5. Target Exploitation e Social Engineering
6. Target Post-Exploitation
7. Documentazione e Reporting

Fasi condotte in modo sequenziale da uno o più esperti di Penetration Testing, noti come «Penetration Tester» (o «Pentester»)



Principali Contenuti del Corso

Target Scoping

- Definisce gli **obiettivi** e le **limitazioni** del penetration testing



- Risponde alle seguenti domande
 - Cosa sarà valutato dal penetration testing?
 - Come avverrà il penetration testing?
 - Quali risorse saranno allocate per il penetration testing?
 - Quali limitazioni saranno applicate durante il penetration testing?
 - Quali obiettivi di business saranno raggiunti dopo il penetration testing?
 - Come verrà pianificata e schedulata l'attività di penetration testing?



Principali Contenuti del Corso

Information Gathering

- Fase nota anche come «**ricognizione**» o «**footprinting**»
- Raccoglie quante più **informazioni** possibili sull'obiettivo da analizzare (*asset*)
 - Informazioni riguardanti l'infrastruttura ICT
 - Domain Name System (DNS), indirizzi IP, hostname, autonomous systems
 - Tecnologie e configurazioni usate
 - Etc
 - Informazioni riguardanti le persone «appartenenti» all'infrastruttura
 - Informazioni di contatto, lavoro, posizione, credenziali, documenti
 - Metadati
 - Etc



Principali Contenuti del Corso

Target Discovery ed Enumerating Target

- Tali fasi permettono di individuare
- Le **macchine attive** all'interno dell'asset analizzato
 - **N.B.** Se una macchina non è attiva, non è possibile effettuarne il penetration testing
 - Alcune macchine potrebbero essere «filtrate»
- Il **sistema operativo** utilizzato da ciascuna macchina
- I **servizi di rete** erogati da ciascuna macchina



Principali Contenuti del Corso

Vulnerability Mapping

- Permette di
 - Individuare ed analizzare i **problemi di sicurezza** («**vulnerabilità**») in un dato asset
 - Analizzare i controlli di sicurezza di un asset rispetto a **vulnerabilità note** (ma anche, eventualmente, **Zero-day**)



Principali Contenuti del Corso

Target Exploitation e Social Engineering

- Cerca di **sfruttare le vulnerabilità rilevate** e di trarne vantaggio



- Gli obiettivi principali di questa fase sono
 - Ottenere il controllo (totale o parziale) dell'asset analizzato
 - Ottenere ulteriori informazioni e visibilità su tale asset
 - Causare malfunzionamenti all'asset
- Il *Social Engineering* sfrutta «vulnerabilità» umane
 - Fondamentale per un pentester quando non ci sono vulnerabilità tecniche da sfruttare nell'asset analizzato



Principali Contenuti del Corso

Web Penetration Testing

- Strumenti e metodologie per identificare, analizzare e sfruttare vulnerabilità delle Web Application (o Web App), tra le quali
 - Information Leakage
 - File Upload
 - Local e Remote File Inclusion
 - Command Injection
 - SQL Injection
 - Cross-Site Scripting (XSS)
 - Cross-Site Request Forgery (CSRF)
 - Etc



Principali Contenuti del Corso

Target Post-Exploitation

- Gli obiettivi di questa fase sono
 - Provare ad «elevare» i permessi di accesso del pentester (**Privilege Escalation**) in un sistema violato tramite la fase di Target Exploitation o accedere ad altri sistemi (**Pivoting**)
 - Provare ad installare meccanismi di persistenza sul sistema violato (**Maintaining Access**), quali *backdoor*, etc



Principali Contenuti del Corso

Documentazione e Reporting

- Documentazione e Verifica dei Risultati
- Tipi di Report
- Penetration Testing Report
- Preparazione della Presentazione
- Procedure di Post Testing



Principali Contenuti del Corso

Wireless Penetration Testing

- Wireless Sniffing
- Ricognizione ed Intrusione in Reti Wireless
- Post Cracking



Outline

- Motivazioni del Corso
- Obiettivi e Scopi del Corso
- Contenuti del Corso
- Informazioni Generali

Informazioni Generali

- **9 CFU**
 - **72 ore di lezione**
 - **Lezioni frontali**
 - **Eventuali Seminari di esperti**
 - **Periodo didattico: Lun 24 febbraio 2025 – ven 30 maggio 2025 (con interruzione per festività della Pasqua dal 17 aprile al 22 aprile)**



Informazioni Generali

Orario ed Aula delle Lezioni

- **Orario ed Aula delle Lezioni**
 - **Martedì: 14:30 – 17:30 (Aula F5)**
 - **Giovedì: 14:30 – 17:30 (Aula F5)**
- **N.B. Controllate costantemente la pagina web relativa agli orari del corso**

Orario del corso di PTEH - Link EasyCourse



Informazioni Generali

Contatti

➤ Contatti



arcastiglione@unisa.it



Specificare sempre l'Oggetto
dell'e-mail

A:

Oggetto:

Domande, dubbi, chiarimenti...

Informazioni Generali

Comunicazioni

- **Controllare costantemente l'e-mail studenti**
- **Le comunicazioni avverranno via e-mail, tramite la piattaforma ESSE3 di Ateneo e la piattaforma e-Learning del Dipartimento di Informatica**



Informazioni Generali

Ricevimento

- **Ricevimento**
- Fissare un appuntamento tramite e-mail
- arcastiglione@unisa.it

Informazioni Generali

Condivisione Contenuti

- **Piattaforma e-Learning del Dipartimento di Informatica**
- <http://elearning.informatica.unisa.it/el-platform/>

The screenshot shows the homepage of the eLearning platform. At the top, a blue header bar displays the text "Secondo Semestre - Secondo Anno Magistrale 2024/2025 - LM18". Below the header, there is a large graphic featuring a red and blue 3D-style arrow pointing upwards and to the right, set against a background of a brick wall and a white surface. To the right of the arrow is a small blue square icon with a white double-headed arrow symbol. Below the graphic, the course title "Penetration Testing And Ethical Hacking 2024/2025" is displayed in blue text. Underneath the title, it says "Home page del Corso di Penetration Testing and Ethical Hacking (PTEH), A.A. 2024/2025.". Below that, the teacher's information is provided: "Docente: Prof. Arcangelo Castiglione (E-mail: arcastiglione@unisa.it)". On the left side of the main content area, there is a circular profile picture placeholder and the name "Arcangelo Castiglione" followed by the word "Docente". On the right side, there is a graphic of a hand holding a piece of paper with horizontal lines, representing a document or assignment. Below this graphic is a small ellipsis (...).

Informazioni Generali

Condivisione Contenuti

- **Piattaforma e-Learning del Dipartimento di Informatica**
- <http://elearning.informatica.unisa.it/el-platform/>

The screenshot shows a portion of the eLearning platform. At the top, there is a navigation bar with a dropdown menu and the text "Introduzione". Below this, a section titled "Annunci" (Announcements) is visible. The main content area displays three course weeks:

- 24 febbraio - 2 marzo (Settimana corrente)
- 3 marzo - 9 marzo
- 10 marzo - 16 marzo

Each week entry includes a small edit icon (pencil symbol) next to the date range.



Informazioni Generali

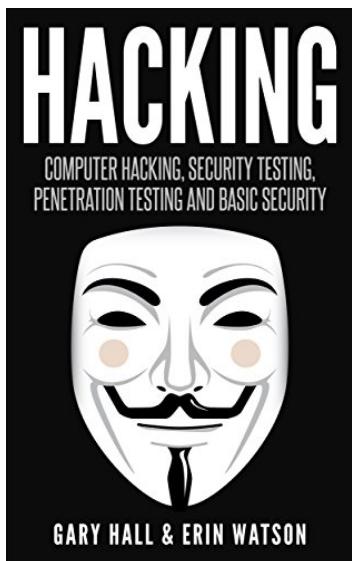
Condivisione Contenuti

- **Varie Tipologie di Contenuti**
 - Slide
 - Materiale Integrativo
 - Approfondimenti
 - Informazioni
 - Comunicazioni
 - Avvisi
 - Etc.

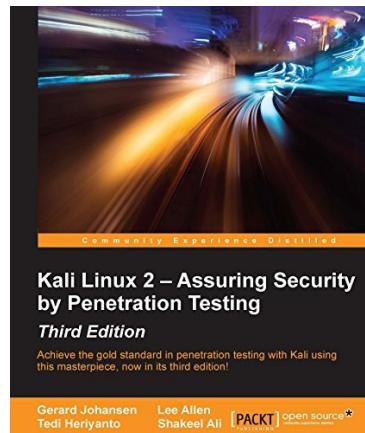
Informazioni Generali

Testi di Riferimento

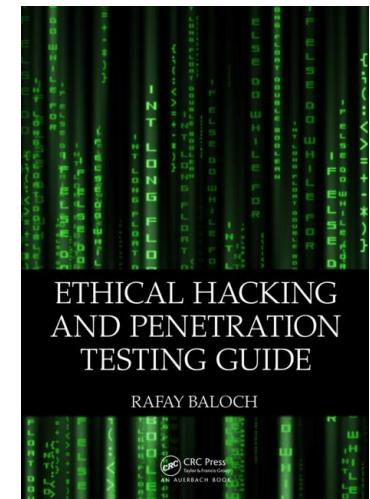
➤ **Hacking: Computer Hacking, Security Testing, Penetration Testing, and Basic Security.** Gary Hall & Erin Watson. 2016



➤ **Kali Linux 2 - Assuring Security by Penetration Testing. Third Edition.** Gerard Johansen, Lee Allen, Tedi Heriyanto, Shakeel Ali. Packt Publishing. 2016



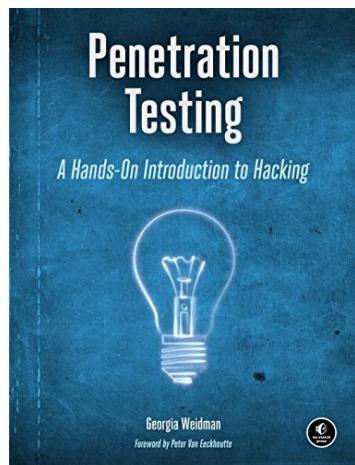
➤ **Ethical Hacking and Penetration Testing Guide.** Rafay Baloch. CRC Press. 2014



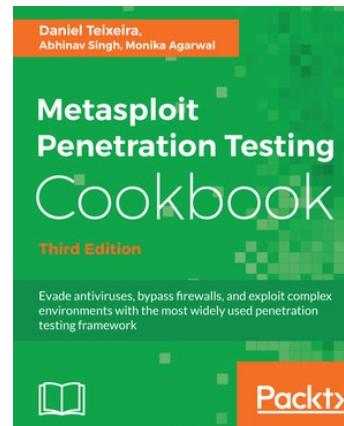
Informazioni Generali

Testi Consigliati

➤ **Penetration Testing: A Hands-On Introduction to Hacking.** Georgia Weidman. No Starch Press. 2014



➤ **Metasploit Penetration Testing Cookbook - Third Edition.** Daniel Teixeira, Abhinav Singh, Monika Agarwal. Packt Publishing. 2016



Informazioni Generali

Prerequisiti

- Reti di Calcolatori (Richiesto)
- Sistemi Operativi (Fortemente Consigliato)
- Sicurezza (Consigliato)



Informazioni Generali

Date d'Esame

- **2 Appelli Straordinari**, riservato agli studenti fuori corso ed a quelli che abbiano conseguito almeno 65 CFU
 - 26 Marzo 2025
 - 7 Maggio 2025
- **4 Appelli Ordinari**
 - Preappello: 17 giugno 2025
 - I appello: 8 luglio 2025
 - II appello: 22 luglio 2025
 - III appello: 19 settembre 2025
- Per ulteriori informazioni, consultare il **Calendario Didattico**
 - <https://corsi.unisa.it/informatica/didattica/calendari>

Informazioni Generali

Prenotazione all'Esame

➤ Per poter sostenere l'esame è **NECESSARIA** la **prenotazione on-line mediante la piattaforma ESSE3**



Area Struttura Didattica

DA QUESTA PAGINA E' POSSIBILE ACCEDERE ALL'AREA RISERVATA.

GLI STUDENTI CHE ACCEDONO PER LA PRIMA VOLTA ALL'AREA RISERVATA DEVONO REGISTRARSI AL SITO SELEZIONANDO 'REGISTRAZIONE' DAL MENU' IN ALTO A DESTRA, PER OTTENERE I CODICI DI ACCESSO 'NOME UTENTE' E 'PASSWORD'

GLI STUDENTI CHE SONO GIA' REGISTRATI POSSONO ACCEDERE ALL'AREA RISERVATA SELEZIONANDO 'LOGIN' DAL MENU' IN ALTO A DESTRA

I DOCENTI NON DEVONO REGISTRARSI; BISOGNA UTILIZZARE LE CREDENZIALI CAU PER ACCEDERE ALL'AREA RISERVATA, SELEZIONANDO 'LOGIN' DAL MENU' IN ALTO A DESTRA



Informazioni Generali

Modalità D'Esame

- La modalità d'esame prevede un **colloquio orale**

- Tale colloquio verterà su
 - Gli argomenti trattati durante il corso ED
 - Un'attività progettuale concordata con il docente via e-mail
 - L'attività progettuale dovrà essere svolta individualmente (salvo talune eccezioni)



Informazioni Generali

Modalità D'Esame – Attività Progettuale

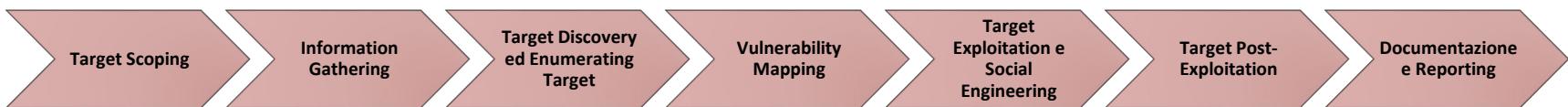
- **L'attività progettuale potrà essere di due tipologie**
 - **Tipologia 1:** Penetration testing su un caso di studio scelto dallo studente
 - **Tipologia 2:** Approfondimento di un argomento trattato al corso o di argomenti relati



Informazioni Generali

Attività Progettuale – Tipologia 1

- Applicazione e documentazione di tutte le fasi del processo di penetration testing su un caso di studio (concordato con il docente) a scelta dello studente



Penetration Testing ≠ Capture the Flag (CTF)

Informazioni Generali

Attività Progettuale – Tipologia 1

- Possibili casi di studio da analizzare
 - Sistemi Operativi vulnerabili «by design» (ad es., scelti da <https://www.vulnhub.com/> o similari);
 - Sistemi Operativi/Applicativi con vulnerabilità presenti nativamente o installate dallo studente
- La lista aggiornata dei casi di studio già analizzati sarà resa disponibile mediante la piattaforma e-Learning del Dipartimento di Informatica
 - **N.B. I casi di studio già analizzati non potranno essere scelti nuovamente**

Informazioni Generali

Attività Progettuale – Tipologia 1

- Lo studente dovrà produrre e consegnare al docente
 1. Documentazione relativa all'attività progettuale svolta. Tale documentazione sarà composta da:
 - **Documento 1:** Contenente l'approccio, le metodologie e gli strumenti utilizzati per portare a termine il processo di penetration testing
 - **N.B.** Il Documento 1 dovrà contenere tutte le informazioni necessarie alla replicabilità del processo di penetration testing che è stato condotto
 - Si consiglia di strutturare tale documento in capitoli, uno per ciascuna fase del processo di penetration testing che è stato affrontato
 - **Documento 2:** *Penetration Testing Report* (maggiori dettagli in seguito)
 2. Presentazione in formato digitale dell'attività progettuale svolta

Per maggiori informazioni, consultare il documento **Informazioni_per_Esame_23-24.pdf**, che sarà presente sulla piattaforma e-Learning del Dipartimento di Informatica

Informazioni Generali

Attività Progettuale – Tipologia 2

- Lo studente dovrà produrre e consegnare al docente una dettagliata documentazione e presentazione digitale relativa all'attività svolta
 - La documentazione e la presentazione digitale dovranno necessariamente includere tutti i riferimenti bibliografici utilizzati
- Tutto il materiale prodotto nell'ambito dell'attività progettuale, compresi eventuale codice sorgente e file di configurazione, dovrà essere integralmente inviato al docente prima del colloquio orale
 - Dovranno essere inviati al docente anche tutti i file e le informazioni necessarie a replicare quanto svolto nell'attività progettuale

Per maggiori informazioni, consultare il documento che sarà reso disponibile sulla piattaforma e-Learning del Dipartimento di Informatica

Informazioni Generali

Strumenti Necessari

- **Virtual Box** (Ambiente di Virtualizzazione)
 - <https://www.virtualbox.org/wiki/Downloads>



- **Kali Linux** (Distribuzione per il pentesting)
 - Installazione tramite Virtual Box (Consigliata)
 - <https://www.kali.org/get-kali/#kali-virtual-machines>



Informazioni Generali

Strumenti Necessari (Sistemi Operativi «Vulnerabili»)

- **Metasploitable 1** (Distribuzione Linux Vulnerabile)
 - <https://www.dropbox.com/s/2pccqfcy9eq8ajg/Metasploitable1.ova?dl=0>
- **Metasploitable 2** (Distribuzione Linux Vulnerabile)
 - <https://www.dropbox.com/s/bo3api8egevxxt8/Metasploitable2.ova?dl=0>
- **Metasploitable 3** (Sistema Windows Vulnerabile)
 - <https://www.dropbox.com/s/vhn9i41i2r51axe/metasploitable3.ova?dl=0>
- **Microsoft Windows XP**
 - <https://www.dropbox.com/s/g768oa5wchjsmw5/Windows%20XP%2064%20Bit%20ENG.ova?dl=0>

Informazioni Generali

Strumenti Consigliati

➤ **Parrot Security**

➤ <https://parrotsec.org/>



➤ **BackBox Linux**

➤ <https://www.backbox.org/>



➤ **BlackArch Linux**

➤ <https://blackarch.org/>



Informazioni Generali

Altri Strumenti Consigliati

- **Microsoft Windows 10**
 - <https://developer.microsoft.com/en-us/microsoft-edge/tools/vms/>
- **OWASP Broken Web Apps**
 - https://www.dropbox.com/s/ja1923vm0ghwth7/OWASP_BWA.ova?dl=0