Master Privato

Penetration Test e Red Team

tech università tecnologica

tech università tecnologica

Master Privato
Penetration Test e Red Team

- Modalità: **online**
- Durata: **12 mesi**
- Titolo: **TECH Università Tecnologica**
- Orario: **a tua scelta**
- Esami: **online**

Accesso al sito web: www.techtitute.com/it/informatica/master/master-penetration-test-red-team

Indice

01

Presentazione

Il numero e la sofisticazione degli attacchi informatici hanno raggiunto proporzioni allarmanti. Con l'aumento esponenziale delle minacce, dagli attacchi *ransomware* alle intrusioni avanzate, la necessità di professionisti altamente qualificati nella sicurezza informatica è cruciale. In questo contesto emerge il presente programma, che non solo offrirà un'immersione completa in tecniche di sicurezza avanzate, ma affronterà anche la realtà di un ambiente digitale in continua evoluzione. In questo modo, gli studenti approfondiranno le tecniche di attacco e difesa, affrontando le sfide di sicurezza più sofisticate. Spinto dalla necessità di rafforzare le difese informatiche, questo programma si distingue per la sua metodologia 100% online e per l'uso efficace del metodo *Relearning* per ottimizzare l'apprendimento.

Progetta protocolli di sicurezza inespugnabili grazie a questo programma pionieristico, con la garanzia di TECH"

Rimanere aggiornati è fondamentale per preservare l'efficacia della difesa contro le minacce attuali ed emergenti. In questo senso, la rapida evoluzione della tecnologia e delle tattiche informatiche hanno reso l'aggiornamento costante un imperativo. La proliferazione delle minacce sottolinea l'urgenza di avere professionisti altamente qualificati.

In questo contesto, questo programma universitario si rivela come una risposta essenziale, in quanto non solo fornirà una profonda comprensione delle tecniche più avanzate nella sicurezza informatica, ma assicurerà anche che i professionisti siano all'avanguardia delle ultime tendenze e tecnologie.

Nel programma di questo Master Privato in Penetration Test e Red Team, lo studente affronterà in modo esaustivo le richieste nel campo della cibersicurezza. Implementerà efficaci misure di sicurezza nelle reti, inclusi firewall, sistemi di rilevamento delle intrusioni (IDS) e segmentazione della rete. A tal fine, gli specialisti applicheranno metodologie di indagine forense digitale per la risoluzione dei casi, dall'identificazione alla documentazione dei risultati.

Inoltre, svilupperanno competenze nella simulazione di minacce avanzate, replicando le tattiche, le tecniche e le procedure più utilizzate dai malintenzionati. L'approccio innovativo di TECH garantirà inoltre l'acquisizione di competenze pertinenti e preziose nell'ambiente di lavoro della cibersicurezza.

La metodologia del percorso accademico ne rafforza il carattere innovativo, offrendo un ambiente educativo online al 100%. Questo programma sarà adattato alle esigenze dei professionisti impegnati che cercano di avanzare nella loro carriera. Inoltre, utilizzerai la metodologia *Relearning*, basata sulla ripetizione di concetti chiave per fissare le conoscenze e facilitare l'apprendimento. In questo modo, la combinazione di flessibilità e robusto approccio pedagogico, non solo lo renderà accessibile, ma anche altamente efficace nella preparazione degli informatici alle sfide dinamiche della cibersicurezza.

Questo **Master Privato in Penetration Test e Red Team** possiede il programma educativo più completo e aggiornato del mercato. Le sue caratteristiche principali sono:

- Sviluppo di casi pratici presentati da esperti in Penetration Test e Red Team
- Contenuti grafici, schematici ed eminentemente pratici che forniscono informazioni aggiornate e pratiche sulle discipline essenziali per l'esercizio della professione
- Esercizi pratici che offrono un processo di autovalutazione per migliorare l'apprendimento
- Particolare enfasi è posta sulle metodologie innovative
- Lezioni teoriche, domande all'esperto e/o al tutor, forum di discussione su questioni controverse e compiti di riflessione individuale
- Contenuti disponibili da qualsiasi dispositivo fisso o mobile dotato di connessione a internet

In soli 12 mesi darai alla tua carriera l'impulso di cui ha bisogno. Iscriviti e sperimenta un progresso immediato!"

Desideri sperimentare un salto di qualità nella tua carriera? Con TECH ti preparerai nell'implementazione di strategie per l'esecuzione efficace di progetti di cibersicurezza"

Approfondirai l'identificazione e la valutazione delle vulnerabilità nelle applicazioni web, grazie alla migliore università digitale del mondo secondo Forbes.

Padroneggerai le tecniche forensi negli ambienti di Penetration test. Posizionati come l'esperto di cibersicurezza che tutte le aziende cercano!

Il personale docente del programma comprende rinomati professionisti e riconosciuti specialisti appartenenti a prestigiose società e università, che forniscono agli studenti le competenze necessarie a intraprendere un percorso di studio eccellente.

I contenuti multimediali, sviluppati in base alle ultime tecnologie educative, forniranno al professionista un apprendimento coinvolgente e localizzato, ovvero inserito in un contesto reale.

La creazione di questo programma è incentrata sull'Apprendimento Basato su Problemi, mediante il quale il professionista deve cercare di risolvere le diverse situazioni che gli si presentano durante il corso. Lo studente potrà usufruire di un innovativo sistema di video interattivi creati da esperti di rinomata fama.

02

Obiettivi

Questo percorso accademico mira principalmente a formare gli studenti nei penetration test e nelle simulazioni di *Red Team*. Nel corso del programma, gli informatici si immergeranno in un approccio pratico e specializzato, sviluppando competenze per affrontare l'identificazione e lo sfruttamento delle vulnerabilità nei sistemi e nelle reti. Inoltre, questo programma è stato progettato per fornire una comprensione approfondita delle tattiche e delle strategie di sicurezza informatica, preparando gli studenti ad affrontare le sfide del mondo reale e guidare l'implementazione efficace delle misure di sicurezza informatica.

Approfondirai l'analisi e lo sviluppo del malware per posizionarti come un eccezionale personale docente. Raggiungi i tuoi obiettivi grazie a TECH!"

Obiettivi generali

- Acquisire competenze avanzate nei penetration test e nelle simulazioni di *Red Team*, affrontando l'identificazione e lo sfruttamento delle vulnerabilità nei sistemi e nelle reti
- Sviluppare capacità di leadership per coordinare team specializzati nella sicurezza informatica offensiva, ottimizzando l'esecuzione dei progetti di *Penetration test* e *Red Team*
- Sviluppare competenze nell'analisi e nello sviluppo del malware, comprendendo la sua funzionalità e applicando strategie difensive ed educative
- Affinare le capacità di comunicazione producendo relazioni tecniche ed esecutive dettagliate, presentando i risultati in modo efficace a un pubblico tecnico ed esecutivo
- Promuovere una pratica etica e responsabile nel campo della sicurezza informatica, tenendo conto dei principi etici e legali in tutte le attività
- Mantenere studenti aggiornati sulle tendenze e le tecnologie emergenti nel campo della Cibersicurezza

Raggiungerai i tuoi obiettivi grazie agli strumenti didattici di TECH, tra cui video esplicativi e riassunti interattivi"

Obiettivi specifici

Modulo 1. Sicurezza Offensiva

- Familiarizzare con le metodologie di penetration testing, comprese le fasi chiave quali la raccolta di informazioni, l'analisi delle vulnerabilità, lo sfruttamento e la documentazione
- Sviluppare competenze pratiche nell'uso di strumenti di *Penetration test* per identificare e valutare le vulnerabilità di sistemi e reti
- Studiare e comprendere le tattiche, le tecniche e le procedure utilizzate dagli attori malintenzionati, consentendo l'identificazione e la simulazione delle minacce
- Applicare le conoscenze teoriche in scenari pratici e simulazioni, affrontando sfide reali per rafforzare le competenze di *Penetration test*
- Sviluppare un'efficace capacità di documentazione, creando relazioni dettagliate che riflettano i risultati, le metodologie utilizzate e le raccomandazioni per il miglioramento della sicurezza
- Praticare una collaborazione efficace nei team di sicurezza offensiva, ottimizzando il coordinamento e l'esecuzione delle attività di *Penetration test*

Modulo 2. Gestione delle Squadre di Cibersicurezza

- Sviluppare capacità di leadership specifiche per i team di sicurezza informatica, compresa la capacità di motivare, ispirare e coordinare gli sforzi per raggiungere obiettivi comuni
- Imparare a allocare in modo efficiente le risorse all'interno di un team di cibersicurezza, considerando le competenze individuali e massimizzando la produttività dei progetti

- Migliorare le capacità di comunicazione specifiche per gli ambienti tecnici, facilitando la comprensione e il coordinamento tra i membri del team
- Apprendere strategie per identificare e gestire i conflitti all'interno del team di cibersicurezza, promuovendo un ambiente di lavoro collaborativo ed efficiente
- Imparare a impostare metriche e sistemi di valutazione per misurare le prestazioni del team di sicurezza informatica e apportare modifiche se necessario
- Promuovere l'integrazione di pratiche etiche nella gestione dei team di sicurezza informatica, assicurando che tutte le attività siano condotte in modo etico e legale
- Sviluppare competenze per la preparazione e la gestione efficiente degli incidenti di cibersicurezza, garantendo una risposta rapida ed efficace alle minacce

Modulo 3. Gestione di Progetti di Sicurezza

- Sviluppare competenze per pianificare progetti di sicurezza informatica, definendo obiettivi, ambito, risorse e scadenze
- Apprendere le strategie per l'esecuzione efficace dei progetti di sicurezza, assicurando l'attuazione di successo delle misure pianificate
- Sviluppare competenze per la gestione efficiente del budget e l'allocazione delle risorse nei progetti di sicurezza, massimizzando l'efficienza e minimizzando i costi
- Migliorare la comunicazione efficace con gli *stakeholder*, presentando rapporti e aggiornamenti in modo chiaro e comprensibile
- Apprendere le tecniche di monitoraggio e controllo dei progetti, identificando le deviazioni e intraprendendo azioni correttive se necessario
- Familiarizzare gli studenti con le metodologie agili di *Penetration test*
- Sviluppare competenze nella documentazione dettagliata e nella produzione rapporti, fornendo una visione chiara dei progressi del progetto e i risultati ottenuti
- Promuovere una collaborazione efficace tra team e discipline diverse all'interno di progetti di sicurezza, assicurando una visione globale e coordinata
- Apprendere strategie per valutare e misurare l'efficacia delle misure implementate, garantendo il miglioramento continuo della postura di sicurezza dell'organizzazione

Modulo 4. Attacchi alla Rete e al Sistema Windows

- Sviluppare le competenze per identificare e valutare le vulnerabilità specifiche dei sistemi operativi Windows
- Imparare le tattiche avanzate utilizzate dagli aggressori per infiltrarsi e persistere nelle reti basate su Windows
- Acquisire competenze sulle strategie e sugli strumenti per mitigare le minacce specifiche che colpiscono i sistemi operativi Windows
- Familiarizzare con le tecniche di analisi forense applicate ai sistemi Windows, facilitando l'identificazione e la risposta agli incidenti
- Applicare le conoscenze teoriche in ambienti simulati, partecipando a esercitazioni pratiche per comprendere e contrastare attacchi specifici ai sistemi Windows
- Apprendere strategie specifiche per la sicurezza degli ambienti aziendali utilizzando i sistemi operativi Windows, tenendo conto della complessità delle infrastrutture aziendali
- Sviluppare competenze per valutare e migliorare le configurazioni di sicurezza dei sistemi Windows, garantendo l'implementazione di misure efficaci
- Promuovere pratiche etiche e legali nell'esecuzione di attacchi e test su sistemi Windows, tenendo conto dei principi etici della cibersicurezza
- Mantenere lo studente aggiornato sulle ultime tendenze e minacce in materia di attacchi ai sistemi Windows, garantendo la continuità della sicurezza

Modulo 5. *Hacking Web* Avanzato

- Sviluppare competenze per identificare e valutare le vulnerabilità nelle applicazioni web, tra cui SQL injection, *Cross-Site Scripting* (XSS) e altri vettori di attacco comuni
- Imparare a eseguire test di sicurezza sulle moderne applicazioni web
- Acquisire competenze in tecniche avanzate di hacking web, esplorando strategie di elusione di misure di sicurezza e sfruttamento di vulnerabilità sofisticate
- Familiarizzarsi con la valutazione della sicurezza in API e servizi web, identificando potenziali punti di vulnerabilità e rafforzando la sicurezza nelle interfacce di programmazione
- Sviluppare competenze per implementare misure di mitigazione efficaci nelle applicazioni web, riducendo l'esposizione agli attacchi e rafforzando la sicurezza
- Partecipare a simulazioni pratiche per valutare la sicurezza in ambienti web complessi, applicando le conoscenze in situazioni reali
- Sviluppare competenze nella formulazione di strategie di difesa efficaci per proteggere le applicazioni web dalle minacce informatiche
- Imparare a linearizzare le pratiche di *hacking web* avanzato con le normative e gli standard di sicurezza pertinenti, garantendo l'adesione a quadri legali ed etici
- Promuovere una collaborazione efficace tra i team di sviluppo e sicurezza

Modulo 6. Architettura e Sicurezza di Rete

- Acquisire conoscenze avanzate sull'architettura di rete, tra cui topologie, protocolli e componenti chiave
- Sviluppare competenze per identificare e valutare vulnerabilità specifiche nelle infrastrutture di rete, considerando le potenziali minacce
- Imparare a implementare misure di sicurezza efficaci nelle reti, inclusi *firewall*, sistemi di rilevamento delle intrusioni (IDS) e segmentazione della rete
- Familiarizzare lo studente con le tecnologie emergenti nelle reti, come le reti definite software (SDN) e comprenderne l'impatto sulla sicurezza
- Sviluppare competenze per proteggere le comunicazioni in rete, tra cui la protezione contro minacce quali *sniffing* e attacchi di intermediari
- Imparare a valutare e migliorare le configurazioni di sicurezza in ambienti di rete aziendali, garantendo una protezione adeguata
- Sviluppare competenze per implementare efficaci misure di mitigazione delle minacce alle reti aziendali, dagli attacchi interni alle minacce esterne
- Promuovere una collaborazione efficace con i team di sicurezza, integrando le strategie e sforzi per proteggere l'infrastruttura di rete
- Promuovere pratiche etiche e legali nell'attuazione delle misure di sicurezza in rete, assicurando il rispetto dei principi etici in tutte le attività

Modulo 7. Analisi e Sviluppo di *Malware*

- Acquisire una conoscenza avanzata della natura, della funzionalità e del comportamento del *malware*, comprendendone le varie forme e gli obiettivi
- Sviluppare competenze nell'analisi forense applicata al *malware*, consentendo l'identificazione degli indicatori di compromissione (IoC) e dei modelli di attacco
- Apprendere strategie per il rilevamento e la prevenzione efficace di *malware*, compresa l'implementazione di soluzioni di sicurezza avanzate

- Familiarizzare con lo sviluppo di *malware* a scopo educativo e difensivo, consentendo una comprensione approfondita delle tattiche utilizzate dagli hacker
- Promuovere pratiche etiche e legali nell'analisi e nello sviluppo di *malware*, garantendo integrità e responsabilità in tutte le attività
- Promuovere pratiche etiche e legali nell'analisi e nello sviluppo di malware, garantendo integrità e responsabilità in tutte le attività
- Sviluppare le competenze per valutare e selezionare gli strumenti di sicurezza *anti-malware*, considerando la loro efficacia e adattabilità ad ambienti specifici
- Imparare a implementare una mitigazione efficace contro le minacce dannose, riducendo l'impatto e la diffusione del *malware* su sistemi e reti
- Promuovere una collaborazione efficace con i team di sicurezza, integrando strategie e sforzi per la protezione dalle minacce *malware*
- Aggiornarsi sulle ultime tendenze e tecniche utilizzate nell'analisi e nello sviluppo di *malware*, assicurando la continua rilevanza ed efficacia delle competenze acquisite

Modulo 8. Fondamenti Forensi e DFIR

- Acquisiranno una solida conoscenza dei principi fondamentali dell'indagine forense digitale (DFIR), applicabili nella risoluzione degli incidenti informatici
- Sviluppare competenze nell'acquisizione sicura e forense di prove digitali, garantendo la conservazione della catena di custodia
- Imparare a eseguire analisi forensi dei file system
- Familiarizzare lo studente con tecniche avanzate per l'analisi di record e registri, consentendo la ricostruzione di eventi in ambienti digitali
- Imparare ad applicare le metodologie di indagine forense digitale nella risoluzione di casi, dall'identificazione alla documentazione dei risultati
- Familiarizzare lo studente con l'analisi delle prove digitali e l'applicazione di tecniche forensi in ambienti di *Penetration Test*
- Sviluppare competenze nella stesura di rapporti forensi dettagliati e chiari, presentando risultati e conclusioni in modo comprensibile
- Promuovere una collaborazione efficace con i team di risposta agli incidenti (IR), ottimizzando il coordinamento nella ricerca e nella mitigazione delle minacce
- Promuovere pratiche etiche e legali nelle indagini forensi digitali, garantendo il rispetto delle norme e degli standard di condotta in Cibersicurezza

Modulo 9. Esercizi di *Red Team* Avanzati

- Sviluppare competenze nella simulazione di minacce avanzate, replicando tattiche, tecniche e procedure (TTP) utilizzate da hacker
- Imparare a identificare i punti deboli e le vulnerabilità dell'infrastruttura con esercizi realistici di *Red Team*, rafforzando la posizione di sicurezza
- Familiarizzare il laureato con tecniche avanzate di evasione delle misure di sicurezza, consentendo di valutare la resilienza dell'infrastruttura alle attacchi desiderabili
- Sviluppare capacità di coordinamento e collaborazione efficace tra i membri del team di *Red Team*, ottimizzando l'esecuzione di tattiche e strategie per valutare in modo completo la sicurezza dell'organizzazione

- Imparare a simulare scenari di minacce attuali, come attacchi di *ransomware* o campagne di phishing avanzate, per valutare la capacità di risposta dell'organizzazione
- Familiarizzare lo studente con tecniche di analisi post-esercizio, valutando le prestazioni del team di *Red Team* ed estraendo le lezioni apprese per il miglioramento continuo
- Sviluppare competenze per valutare la resilienza organizzativa agli attacchi simulati, identificando le aree di miglioramento delle politiche e delle procedure
- Imparare a produrre rapporti dettagliati che documentano i risultati, le metodologie utilizzate e le raccomandazioni derivanti da esercizi di *Red Team* avanzati
- Promuovere pratiche etiche e legali nelle di da esercizi di *Red Team*, garantendo il rispetto delle norme e degli standard etici in Cibersicurezza

Modulo 10. Reporting Tecnico ed Esecutivo

- Sviluppare le competenze per produrre rapporti tecnici dettagliati, presentando in modo chiaro e completo i risultati, le metodologie utilizzate e le raccomandazioni
- Imparare a comunicare in modo efficace con il pubblico tecnico, utilizzando un linguaggio preciso e adeguato per trasmettere informazioni tecniche complesse
- Sviluppare competenze per formulare raccomandazioni pratiche e attuabili, orientate a mitigare le vulnerabilità e migliorare la postura di sicurezza
- Imparare a valutare il potenziale impatto delle vulnerabilità identificate, considerando gli aspetti tecnici, operativi e strategici
- Familiarizzare lo studente con le migliori pratiche per la presentazione esecutiva di relazioni, adeguando le informazioni tecniche per il pubblico non tecnico
- Sviluppare competenze per allineare risultati e raccomandazioni con gli obiettivi strategici e operativi dell'organizzazione
- Imparare a utilizzare strumenti di visualizzazione dei dati per rappresentare graficamente le informazioni contenute nei report, facilitando la comprensione
- Promuovere l'inclusione di informazioni pertinenti sulla conformità di norme e standard nei report, garantendo l'adesione a requisiti legali
- Promuovere un'efficace collaborazione tra team tecnici e dirigenti, assicurando la comprensione e il sostegno per le azioni di miglioramento proposte nella relazione

Un'esperienza educativa unica, cruciale e decisiva per crescere professionalmente"

03

Competenze

Grazie al presente programma, gli studenti saranno preparati con competenze specialistiche per implementare misure di difesa attiva, rafforzando la sicurezza dei sistemi e delle reti basate sulle migliori pratiche di cibersicurezza. Inoltre, gli studenti acquisiranno competenze avanzate nei test di penetrazione e nelle simulazioni di *Red Team*, evidenziando l'identificazione e la mitigazione proattiva delle vulnerabilità. In questo senso, i professionisti padroneggeranno le competenze tecniche necessarie per affrontare le minacce del mondo reale, preparandosi a condurre efficaci strategie di valutazione e fortificazione della sicurezza in ambienti informatici dinamici. Inoltre, l'approccio 100% online rende l'apprendimento più flessibile.

Diventa un esperto di sicurezza informatica attraverso 1.500 ore dei migliori contenuti multimediali, con il marchio di qualità di TECH"

Competenze generali

- Acquisire competenze nella pianificazione, esecuzione e gestione dei progetti di sicurezza informatica, garantendo risultati efficaci e il raggiungimento degli obiettivi
- Acquisire conoscenze avanzate nell'architettura di rete e nei suoi aspetti di sicurezza, valutando le vulnerabilità e attuando strategie per rafforzare l'infrastruttura
- Sviluppare competenze nella ricerca forense digitale e nella risposta agli incidenti, dalla raccolta delle prove alla mitigazione delle minacce e il ripristino operativo
- Applicare tattiche avanzate nella pianificazione e nell'esecuzione degli esercizi di *Red Team*, simulando scenari del mondo reale per valutare la resistenza dell'infrastruttura, rilevare le debolezze e migliorare la preparazione alle minacce informatiche

Aggiornati sul processo di identificazione, valutazione e mitigazione dei rischi specifici dei progetti di sicurezza informatica. Scegli TECH!"

Competenze specifiche

- Acquisire competenze di coaching per lo sviluppo professionale dei membri del team, promuovendo la crescita e il miglioramento
- Sviluppare capacità decisionali strategiche in situazioni di sicurezza informatica, considerando l'impatto a breve e lungo termine sulla sicurezza organizzativa
- Acquisire competenze in materia identificazione, valutazione e mitigazione dei rischi specifici dei progetti di sicurezza informatica
- Sviluppare le competenze per implementare misure di difesa attiva, rafforzando la sicurezza dei sistemi e delle reti basate
- Apprendere tecniche di analisi del traffico web per identificare modelli e comportamenti anomali, facilitando il rilevamento di potenziali minacce
- Acquisire competenze nell'analisi forense applicata agli ambienti di rete, consentendo l'identificazione e una risposta efficace agli incidenti informatici
- Apprendere strategie per il rilevamento e la prevenzione efficace di malware, compresa l'implementazione di soluzioni di sicurezza avanzate
- Sviluppare competenze nell'identificazione degli indicatori di coinvolgimento (IoC) durante le indagini forensi, facilitando l'individuazione e la risposta agli incidenti
- Acquisire competenze per la pianificazione strategica degli esercizi di *Red Team*, considerando obiettivi, ambito, risorse e scenari realistici
- Acquisire competenze nell'identificazione e nella prioritizzazione delle vulnerabilità, evidenziando quelle che rappresentano i maggiori rischi per la sicurezza

04

Direzione del corso

Nella scelta del personale docente del Master Privato in Penetration Test e Red Team, TECH ha riunito i migliori specialisti, che hanno un ampio e riconosciuto background professionale in aziende leader del settore. In questo senso, ogni membro del corpo insegnante apporterà la sua esperienza pratica e le sue conoscenze specialistiche, garantendo che gli alunni beneficino dell'insegnamento di professionisti altamente qualificati. Inoltre, un'attenta selezione di questi esperti garantirà non solo la qualità accademica, ma anche la rilevanza e l'applicabilità immediata dei contenuti nell'ambiente dinamico della cibersicurezza.

Giganti del settore della sicurezza informatica ti porteranno al successo in soli 12 mesi con questo esclusivo programma universitario di TECH"

Direzione

Dott. Gómez Pintado, Carlos

- Responsabile di Cibersicurezza e Rete Cipherbit presso Grupo Oesía
- Responsabile Advisor & Investor presso Wesson App
- Laurea in Ingegneria del Software e Tecnologie della Società dell'Informazione, Università Politecnica di Madrid
- Collabora con istituzioni educative per la preparazione di cicli di formazione di livello superiore in materia di cibersicurezza

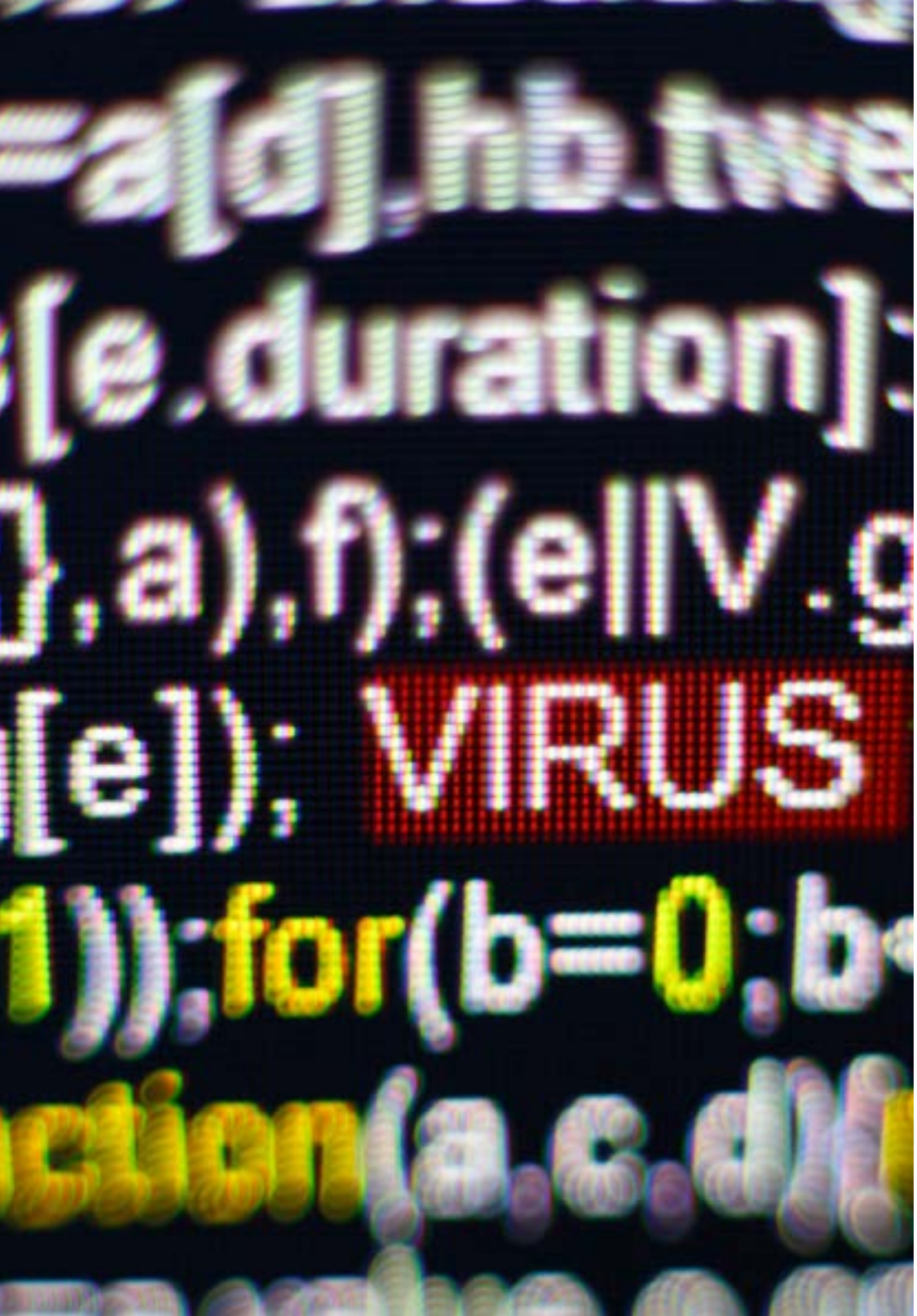
Personale docente

Dott. Siles Rubia, Marcelino

- Cibersecurity Engineer
- Ingegneria della Cibersicurezza presso l'Università Rey Juan Carlos
- Conoscenze: Programmazione Competitiva, *Hacking Web, Active Directory e Malware Development*
- Vincitore del Concorso AdaByron

Dott. Redondo Castro, Pablo

- Pentester presso Grupo Oesía
- Ingegnere di Cibersicurezza presso l'Università Rey Juan Carlos
- Ampia esperienza come *Cibersecurity Evaluator Traineev*
- Esperienza di insegnamento, fornendo formazioni relative ai tornei di Capture The Flag



Dott. Gallego Sánchez, Alejandro

- Consulente di Cibersicurezza presso Integración Tecnológica Empresarial, S.L.
- Tecnico audiovisivo presso Ingeniería Audiovisual S.A.
- Laurea in Ingegneria dei della Cibersicurezza presso l'Università Rey Juan Carlos

Dott. González Sanz, Marcos

- Cybersecurity Consultant-Red Teamer Cipherbit presso Grupo Oesía
- Ingegnere Software presso l'Università Politecnica di Madrid
- Specialista in Cybersecurity Tutor e Core Dumped

Dott. Mora Navas, Sergio

- Consulente in Cibersicurezza presso Grupo Oesia
- Ingegnere di Cibersicurezza presso l'Università Rey Juan Carlos
  Ingegnere Informatico presso l'Università di Burgos

Dott. González Parrilla, Yuba

- Coordinatore della linea di sicurezza offensiva e del team di rete
- Specialista in Gestione di Progetti *Predictive* nel Project Management Institute
- Specialista in *SmartDefense*
- Esperto in *Web Application Penetration Tester* presso eLearnSecurity
- *Junior Penetration Tester* presso eLearnSecurity
- Laurea in Ingegneria Computazionale presso l'Università Politecnica di Madrid

05

Struttura e contenuti

Questo programma universitario offre un'immersione completa nelle discipline cruciali dei Penetration test e delle simulazioni di *Red Team*. Durante il corso, gli studenti svilupperanno competenze avanzate per identificare e sfruttare le vulnerabilità nei sistemi e nelle reti, utilizzando tecniche e strumenti moderni. Questa qualifica, progettata con un approccio pratico, consentirà ai professionisti della cibersicurezza di affrontare le sfide del mondo reale. A questo proposito, gli studenti beneficeranno di una combinazione unica di teoria e pratica, guidati da esperti del settore, per rafforzare la loro comprensione e applicare efficacemente strategie di valutazione della sicurezza in ambienti informatici.

Approfondirai i diversi ruoli e responsabilità del team di cibersicurezza. Iscriviti subito!"

Modulo 1. Sicurezza Offensiva

1.1. Definizione e contesto
- 1.1.1. Concetti fondamentali della sicurezza offensiva
- 1.1.2. Importanza della cibersicurezza nell'attualità
- 1.1.3. Sfide e opportunità della sicurezza offensiva

1.2. Basi della cibersicurezza
- 1.2.1. Sfide iniziali e minacce in evoluzione
- 1.2.2. Pietre miliari della tecnologia e loro impatto sulla cibersicurezza
- 1.2.3. Cibersicurezza nell'era moderna

1.3. Basi della sicurezza offensiva
- 1.3.1. Concetti chiave e terminologia
- 1.3.2. *Think Outside the Box*
- 1.3.3. Differenze tra hacking offensivo e difensivo

1.4. Metodologie di sicurezza offensiva
- 1.4.1. PTES (*Penetration Testing Execution Standard*)
- 1.4.2. OWASP (*Open Web Application Security Project*)
- 1.4.3. *Cyber Security Kill Chain*

1.5. Ruoli e responsabilità nella sicurezza offensiva
- 1.5.1. Profili principali
- 1.5.2. *Bug Bounty Hunters*
- 1.5.3. *Researching:* L'arte della ricerca

1.6. Arsenale del revisore offensivo
- 1.6.1. Sistemi operativi di *hacking*
- 1.6.2. Introduzione al C2
- 1.6.3. *Metasploit*: Fondamenti e uso
- 1.6.4. Risorse utili

1.7. OSINT: Intelligenza open source
- 1.7.1. Fondamenti di OSINT
- 1.7.2. Tecniche e strumenti OSINT
- 1.7.3. Applicazioni OSINT nella sicurezza offensiva

1.8. *Scripting*: Introduzione all'automatizzazione
- 1.8.1. Fondamenti di scripting
- 1.8.2. *Scripting* in Bash
- 1.8.3. *Scripting* in Python

1.9. Categorizzazione delle vulnerabilità
- 1.9.1. CVE (*Common Vulnerabilities and Exposure*)
- 1.9.2. CWE (*Common Weakness Enumeration*)
- 1.9.3. CAPEC (*Common Attack Pattern Enumeration and Classification*)
- 1.9.4. CVSS (*Common Vulnerability Scoring System*)
- 1.9.5. MITRE ATT & CK

1.10. Etica e *hacking*
- 1.10.1. Principi di etica *hacker*
- 1.10.2. La linea tra *hacking* etico e *hacking* malevolo
- 1.10.3. Implicazioni e conseguenze legali
- 1.10.4. Casi di studio: Situazioni etiche nella cibersicurezza

Modulo 2. Gestione delle Squadre di Cibersicurezza

2.1. Gestione di squadre
- 2.1.1. Chi è chi
- 2.1.2. Il direttore
- 2.1.3. Conclusioni

2.2. Ruoli e responsabilità
- 2.2.1. Identificazione dei ruoli
- 2.2.2. Delega effettiva
- 2.2.3. Gestione delle aspettative

2.3. Formazione e sviluppo di squadre
- 2.3.1. Fasi della costruzione di una squadra
- 2.3.2. Dinamiche di gruppo
- 2.3.3. Valutazione e feedback

2.4. Gestione del talento
- 2.4.1. Identificazione del talento
- 2.4.2. Sviluppo delle capacità
- 2.4.3. Conservazione dei talenti

2.5. Leadership e motivazione della squadra
- 2.5.1. Stili di leadership
- 2.5.2. Teorie di motivazione
- 2.5.3. Riconoscimento dei risultati conseguiti

2.6. Comunicazione e coordinamento
- 2.6.1. Strumenti di comunicazione
- 2.6.2. Barriere nella comunicazione
- 2.6.3. Strategie di coordinamento

2.7. Pianificazione strategica dello sviluppo professionale del personale
- 2.7.1. Identificazione dei bisogni formativi
- 2.7.2. Piano di sviluppo individuale
- 2.7.3. Monitoraggio e valutazione

2.8. Risoluzione di conflitti
- 2.8.1. Identificazione dei conflitti
- 2.8.2. Metodi di misurazione
- 2.8.3. Prevenzione dei conflitti

2.9. Gestione della qualità e miglioramento continuo
- 2.9.1. Principi di qualità
- 2.9.2. Tecniche per il miglioramento continuo
- 2.9.3. *Feedback*

2.10. Strumenti e tecnologie
- 2.10.1. Piattaforme di collaborazione
- 2.10.2. Gestione dei progetti
- 2.10.3. Conclusioni

Modulo 3. Gestione di Progetti di Sicurezza

3.1. Gestione di progetti di sicurezza
- 3.1.1. Definizione e scopo della gestione dei progetti in cibersicurezza
- 3.1.2. Principali sfide
- 3.1.3. Considerazioni

3.2. Ciclo di vita di un progetto di sicurezza
- 3.2.1. Fasi iniziali e definizione degli obiettivi
- 3.2.2. Implementazione ed esecuzione
- 3.2.3. Valutazione e revisione

3.3. Pianificazione e stima di risorse
- 3.3.1. Concetti base di gestione economia
- 3.3.2. Individuazione delle risorse umane e tecniche
- 3.3.3. Budget e costi associati

3.4. Esecuzione e controllo del progetto
- 3.4.1. Monitoraggio e follow-up
- 3.4.2. Adattamento e cambiamenti nel progetto
- 3.4.3. Valutazione intermedia e revisioni

3.5. Comunicazione e promozione del progetto
- 3.5.1. Strategie di comunicazione efficaci
- 3.5.2. Preparazione di report e presentazioni
- 3.5.3. Comunicazione con il cliente e la direzione

3.6. Strumenti e tecnologie
- 3.6.1. Strumenti di pianificazione e organizzazione
- 3.6.2. Strumenti di collaborazione e comunicazione
- 3.6.3. Strumenti di documentazione e archiviazione

3.7. Documentazione e protocolli
- 3.7.1. Strutturazione e creazione di documentazione
- 3.7.2. Protocolli di attuazione
- 3.7.3. Le guide

3.8. Normativa e conformità nei progetti di cibersicurezza
- 3.8.1. Leggi e regolamenti internazionali
- 3.8.2. Conformità
- 3.8.3. Audit

3.9. Gestione dei rischi di progetti di sicurezza
- 3.9.1. Identificazione e analisi dei rischi
- 3.9.2. Strategie di mitigazione
- 3.9.3. Monitoraggio e revisione dei rischi

3.10. Chiusura del progetto
- 3.10.1. Revisione e valutazione
- 3.10.2. Documenti finali
- 3.10.3. Feedback

Modulo 4. Attacchi alla Rete e al Sistema Windows

4.1. Windows e Active Directory
- 4.1.1. Storia ed evoluzione di Windows
- 4.1.2. Nozioni di base di Active Directory
- 4.1.3. Ruoli e servizi di Active Directory
- 4.1.4. Architettura generale di Active Directory

4.2. Networking in ambienti Active Directory
- 4.2.1. Protocolli di rete in Windows
- 4.2.2. DNS e il suo funzionamento in Active Directory
- 4.2.3. Strumenti di siagnosi di rete
- 4.2.4. Implementazione della rete in Active Directory

4.3. Autenticazione e autorizzazione in Active Directory
- 4.3.1. Processo e flusso di autenticazione
- 4.3.2. Tipi di credenziali
- 4.3.3. Archiviazione e gestione dei credenziali
- 4.3.4. Sicurezza nell'autenticazione

4.4. Permessi e Politica in Active Directory
- 4.4.1. GPO
- 4.4.2. Applicazione e gestione delle GPO
- 4.4.3. Gestione dei permessi di Active Directory
- 4.4.4. Vulnerabilità e mitigazioni dei permessi

4.5. Fondamenti di Kerberos
- 4.5.1. Che cos'è Kerberos?
- 4.5.2. Componenti e funzionamento
- 4.5.3. Ticket in Kerberos
- 4.5.4. Kerberos nel contesto di Active Directory

4.6. Tecniche avanzate in Kerberos
- 4.6.1. Attacchi comuni a Kerberos
- 4.6.2. Mitigazioni e protezioni
- 4.6.3. Monitoraggio del traffico Kerberos
- 4.6.4. Attacchi avanzati a Kerberos

4.7. *Active Directory Certificate Services* (ADCS)
- 4.7.1. Nozioni di base sulla PKI
- 4.7.2. Ruoli e componenti di ADCS
- 4.7.3. Configurazione e distribuzione dell'ADCS
- 4.7.4. Sicurezza dell'ADCS

4.8. Attacchi e difese in *Active Directory Certificate Services* (ADCS)
- 4.8.1. Vulnerabilità comuni in ADCS
- 4.8.2. Attacchi e tecniche di utilizzo
- 4.8.3. Difese e mitigazioni
- 4.8.4. Monitoraggio e auditing dell'ADCS

4.9. Audit di Active Directory
- 4.9.1. Importanza dell'audit di Active Directory
- 4.9.2. Strumenti di audit
- 4.9.3. Rilevamento di anomalie e comportamenti sospetti
- 4.9.4. Risposta agli incidenti e recupero

4.10. Azure AD
- 4.10.1. Concetti base di Azure AD
- 4.10.2. Sincronizzazione con Active Directory locale
- 4.10.3. Gestione delle identità in Azure AD
- 4.10.4. Integrazione con applicazioni e servizi

Modulo 5. *Hacking* Web Avanzato

5.1. Funzionamento di un sito web
- 5.1.1. L'URL e le sue parti
- 5.1.2. Metodi HTTP
- 5.1.3. Le testate
- 5.1.4. Come visualizzare le richieste web con Burp Suite

5.2. Sessioni
- 5.2.1. I *cookies*
- 5.2.2. *Tokens* JWT
- 5.2.3. Attacchi di furto di sessione
- 5.2.4. Attacchi JWT

5.3. *Cross Site Scripting* (XSS)
- 5.3.1. Cos'è un XSS
- 5.3.2. Tipologie di XSS
- 5.3.3. Utilizzo di un XSS
- 5.3.4. Introduzione agli *XSLeaks*

5.4. Iniezione ai database
- 5.4.1. Cos'è una *SQL Injection*
- 5.4.2. Filtrare le informazioni con *SQLi*
- 5.4.3. *SQLi Blind, Time-Based e Error-Based*
- 5.4.4. Iniezioni NoSQLi

5.5. *Path Traversal* e *Local File Inclusion*
- 5.5.1. Cosa sono e le loro differenze
- 5.5.2. Filtri comuni e come saltarli
- 5.5.3. *Log Poisoning*
- 5.5.4. LFIs in PHP

5.6. *Broken Authentication*
- 5.6.1. *User Enumeration*
- 5.6.2. *Password Bruteforce*
- 5.6.3. *2FA Bypass*
- 5.6.4. *Cookie* con informazioni sensibili e modificabili

5.7. *Remote Command Execution*
- 5.7.1. *Command Injection*
- 5.7.2. *Blind Command Injection*
- 5.7.3. *Insecure Deserialization PHP*
- 5.7.4. *Insecure Deserialization Java*

5.8. *File Uploads*
- 5.8.1. RCE mediante *webshells*
- 5.8.2. XSS nei caricamenti di file
- 5.8.3. XML *External Entity* (XXE) *Injection*
- 5.8.4. *Path traversal* nei caricamenti di file

5.9. *Broken Acess Control*
- 5.9.1. Accesso ai pannelli senza restrizioni
- 5.9.2. *Insecure Direct Object References* (IDOR)
- 5.9.3. Bypass dei filtri
- 5.9.4. Metodi di autorizzazione insufficienti

5.10. Vulnerabilità DOM e attacchi più avanzati
- 5.10.1. *Regex Denial of Service*
- 5.10.2. DOM *Clobbering*
- 5.10.3. *Prototype Pollution*
- 5.10.4. HTTP *Request Smuggling*

Modulo 6. Architettura e Sicurezza di Rete

6.1. Le reti informatiche
- 6.1.1. Concetti di base: Protocolli LAN, WAN, CP, CC
- 6.1.2. Modello OSI e TCP/IP
- 6.1.3. *Switching:* Concetti di base
- 6.1.4. *Routing:* Concetti di base

6.2. *Switching*
- 6.2.1. Introduzione a VLAN
- 6.2.2. STP
- 6.2.3. *EtherChannel*
- 6.2.4. Attacchi allo strato 2

6.3. VLAN
- 6.3.1. Importanza delle VLAN
- 6.3.2. Vulnerabilità delle VLAN
- 6.3.3. Attacchi comuni nelle VLAN
- 6.3.4. Mitigazioni

6.4. *Routing*
- 6.4.1. Indirizzamento IP- IPv4 e IPv6
- 6.4.2. Routing: Concetti di base
- 6.4.3. Routing statico
- 6.4.4. Routing dinamico: Introduzione

6.5. Protocolli IGP
- 6.5.1. RIP
- 6.5.2. OSPF
- 6.5.3. RIP vs OSPF
- 6.5.4. Analisi dei bisogni della topologia

6.6. Protezione perimetrale
- 6.6.1. DMZ
- 6.6.2. *Firewall*
- 6.6.3. Architetture comuni
- 6.6.4. *Zero Trust Network Access*

6.7. IDS e IPS
- 6.7.1. Caratteristiche
- 6.7.2. Implementazione
- 6.7.3. SIEM e SIEM CLOUDS
- 6.7.4. Rilevamento basato su *HoneyPots*

6.8. TLS e VPN
- 6.8.1. SSL/TLS
- 6.8.2. TLS: Attacchi comuni
- 6.8.3. VPN con TLS
- 6.8.4. VPN con IPSEC

6.9. Sicurezza nelle reti wireless
- 6.9.1. Introduzione alle reti wireless
- 6.9.2. Protocolli
- 6.9.3. Elementi chiave
- 6.9.4. Attacchi comuni

6.10. Reti aziendali e come affrontarle
- 6.10.1. Segmentazione logica
- 6.10.2. Segmentazione fisica
- 6.10.3. Controllo degli accessi
- 6.10.4. Altre misure da prendere in considerazione

Modulo 7. Analisi e Sviluppo di *Malware*

7.1. Analisi e sviluppo di *Malware*
- 7.1.1. Storia ed evoluzione di *malware*
- 7.1.2. Classificazione e tipi di *malware*
- 7.1.3. Analisi dei *malware*
- 7.1.4. Sviluppo di *malware*

7.2. Preparazione dell'ambiente
- 7.2.1. Configurazione di Macchine Virtuali e *Snapshots*
- 7.2.2. Strumenti di analisi del *malware*
- 7.2.3. Strumenti di sviluppo del *malware*

7.3. Fondamenti di Windows
- 7.3.1. Formato dei file PE (*Portable Executable*)
- 7.3.2. Processo e *Threads*
- 7.3.3. Sistemi di archivio e registro
- 7.3.4. *Windows Defender*

7.4. Tecniche di malware di base
- 7.4.1. Generazione di *shellcode*
- 7.4.2. Esecuzione di *shellcode* su disco
- 7.4.3. Disco vs memoria
- 7.4.4. Esecuzione di shellcode su memoria

7.5. Tecniche di malware intermedie
- 7.5.1. Persistenza di Windows
- 7.5.2. Cartella Home
- 7.5.3. Chiavi di registro
- 7.5.4. Screensaver

7.6. Tecniche di *malware* avanzate
- 7.6.1. Crittografia di *shellcode* (XOR)
- 7.6.2. Crittografia di *shellcode* (RSA)
- 7.6.3. Offuscamento di *strings*
- 7.6.4. Iniezione di processi

7.7. Analisi statica dei *malware*
- 7.7.1. Analisi dei *packers* con DIE (Detect It Easy)
- 7.7.2. Analisi delle sezioni con PE-Bear
- 7.7.3. Decompilazione con Ghidra

7.8. Analisi dinamica dei *malware*
- 7.8.1. Analisi del comportamento con Process Hacker
- 7.8.2. Analisi delle chiamate con API Monitor
- 7.8.3. Analisi delle modifiche al registro di sistema con Regshot
- 7.8.4. Analisi delle richieste di rete con TCPView

7.9. Analisi in .NET
- 7.9.1. Introduzione a .NET
- 7.9.2. Decompilazione con dnSpy
- 7.9.3. Debug con dnSpy

7.10. Analisi di *malware* reali
- 7.10.1. Preparazione dell'ambiente
- 7.10.2. Analisi statica dei *malware*
- 7.10.3. Analisi dinamica dei *malware*
- 7.10.4. Creazione di regole YARA

Modulo 8. Fondamenti Forensi e DFIR

8.1. Forense digitale
- 8.1.1. Storia ed evoluzione dell'informatica forense
- 8.1.2. Importanza dell'informatica forense nella cibersicurezza
- 8.1.3. Storia ed evoluzione dell'informatica forense

8.2. Fondamenti di informatica forense
- 8.2.1. Catena di custodia e sua applicazione
- 8.2.2. Tipi di evidenza digitale
- 8.2.3. Processo di acquisizione delle evidenze

8.3. File system e struttura dei dati
- 8.3.1. Principali file system
- 8.3.2. Metodi di occultamento dei dati
- 8.3.3. Analisi dei metadati e degli attributi dei file

8.4. Analisi dei sistemi operativi
- 8.4.1. Analisi forense dei sistemi Windows
- 8.4.2. Analisi dei sistemi operativi
- 8.4.3. Analisi forense dei sistemi macOS

8.5. Recupero dati e analisi del disco
- 8.5.1. Recupero dati da supporti danneggiati
- 8.5.2. Strumenti di analisi del disco
- 8.5.3. Interpretazione delle tabelle di allocazione dei file

8.6. Analisi della rete e del traffico
- 8.6.1. Acquisizione e analisi dei pacchetti di rete
- 8.6.2. Analisi dei registri del *firewall*
- 8.6.3. Rilevamento delle intrusioni di rete

8.7. Malware e analisi di codice dannoso
- 8.7.1. Classificazione di *malware* e caratteristiche
- 8.7.2. Analisi statica e dinamica dei *malware*
- 8.7.3. Tecniche di smontaggio e debug

8.8. Analisi di log ed eventi
- 8.8.1. Tipi di registri nei sistemi e nelle applicazioni
- 8.8.2. Interpretazione degli eventi rilevanti
- 8.8.3. Strumenti di analisi dei registri

8.9. Rispondere agli incidenti di sicurezza
- 8.9.1. Processo di risposta agli incidenti
- 8.9.2. Creazione di un piano di risposta agli incidenti
- 8.9.3. Coordinamento con le squadre di sicurezza

8.10. Presentazione di prove e legali
- 8.10.1. Regole di evidenza digitale in ambito legale
- 8.10.2. Preparazione di rapporti forensi
- 8.10.3. Audizione in qualità di testimone esperto

Modulo 9. Esercizi di *Red Team* Avanzati

9.1. Tecniche avanzate di osservazione
- 9.1.1. Elenco avanzato di sottodomini
- 9.1.2. *Google Dorking* avanzato
- 9.1.3. Social network e theHarvester

9.2. Campagne di *phishing* avanzate
- 9.2.1. Cos'è *Reverse-Proxy Phishing*
- 9.2.2. *2FA Bypass* con Evilginx
- 9.2.3. Infiltrazione di dati

9.3. Tecniche avanzate di persistenza
- 9.3.1. *Golden Tickets*
- 9.3.2. *Silver Tickets*
- 9.3.3. Tecnica *DCShadow*

9.4. Tecniche avanzate di evasione
- 9.4.1. Bypass di AMSI
- 9.4.2. Modifica degli strumenti esistenti
- 9.4.3. Offuscamento di *Powershell*

9.5. Tecniche avanzate di movimento laterale
- 9.5.1. *Pass-the-Ticket* (PtT)
- 9.5.2. *Overpass-the-Hash* (Pass-the-Key)
- 9.5.3. NTLM Relay

9.6. Tecniche avanzate di post-sfruttamento
- 9.6.1. *Dump* di LSASS
- 9.6.2. *Dump* di SAM
- 9.6.3. Attacco *DCSync*

9.7. Tecniche avanzate di *pivoting*
- 9.7.1. Cos'è il *pivoting*
- 9.7.2. Gallerie con SSH
- 9.7.3. Pivoting con Chisel

9.8. Intrusioni fisiche
- 9.8.1. Sorveglianza e riconoscimento
- 9.8.2. *Tailgating* e *Piggybacking*
- 9.8.3. *Lock-Picking*

9.9. Attacchi Wi-Fi
- 9.9.1. Attacchi a WPA/WPA2 PSK
- 9.9.2. Attacchi di Rogue AP
- 9.9.3. Attacchi a WPA2 *Enterprise*

9.10. Attacchi RFID
- 9.10.1. Lettura di schede RFID
- 9.10.2. Gestione di schede RFID
- 9.10.3. Creazione di schede clonate

Modulo 10. Reporting Tecnico ed Esecutivo

10.1. Processo di reporting
- 10.1.1. Struttura di un report
- 10.1.2. Processo di reporting
- 10.1.3. Concetti principali
- 10.1.4. Esecutivo vs Tecnico

10.2. Le guide
- 10.2.1. Introduzione
- 10.2.2. Tipi di Guide
- 10.2.3. Guide
- 10.2.4. Casi d'uso

10.3. Metodologie
- 10.3.1. Valutazione
- 10.3.2. *Penetration Test*
- 10.3.3. Panoramica delle metodologie comuni
- 10.3.4. Introduzione alle metodologie

10.4. Approccio tecnico alla fase di reporting
- 10.4.1. Capire i limiti del *Penetration Test*
- 10.4.2. Uso e chiavi del linguaggio
- 10.4.3. Presentazione delle informazioni
- 10.4.4. Errori più comuni

10.5. Approccio esecutivo alla fase di reporting
- 10.5.1. Adattare il report al contesto
- 10.5.2. Uso e chiavi del linguaggio
- 10.5.3. Standardizzazione
- 10.5.4. Errori più comuni

10.6. OSSTMM
- 10.6.1. Comprendere la metodologia
- 10.6.2. Riconoscimento
- 10.6.3. Documentazione
- 10.6.4. Preparazione del report

10.7. LINCE
- 10.7.1. Comprendere la metodologia
- 10.7.2. Riconoscimento
- 10.7.3. Documentazione
- 10.7.4. Preparazione del report

10.8. Segnalare le vulnerabilità
- 10.8.1. Concetti principali
- 10.8.2. Quantificazione della portata
- 10.8.3. Vulnerabilità e prove
- 10.8.4. Errori più comuni

10.9. Focalizzare il report sul cliente
- 10.9.1. Importanza delle prove di lavoro
- 10.9.2. Soluzioni e mitigazioni
- 10.9.3. Dati sensibili e rilevanti
- 10.9.4. Esempi pratici e casi

10.10. Segnalare *retakes*
- 10.10.1. Concetti chiave
- 10.10.2. Comprendere le informazioni ereditate
- 10.10.3. Controllo degli errori
- 10.10.4. Aggiungendo informazioni

05

Metodologia

Questo programma ti offre un modo differente di imparare. La nostra metodologia si sviluppa in una modalità di apprendimento ciclico: ***il Relearning***.

Questo sistema di insegnamento viene applicato nelle più prestigiose facoltà di medicina del mondo ed è considerato uno dei più efficaci da importanti pubblicazioni come il ***New England Journal of Medicine.***

Scopri il Relearning, un sistema che abbandona l'apprendimento lineare convenzionale, per guidarti attraverso dei sistemi di insegnamento ciclici: una modalità di apprendimento che ha dimostrato la sua enorme efficacia, soprattutto nelle materie che richiedono la memorizzazione"

Caso di Studio per contestualizzare tutti i contenuti

Il nostro programma offre un metodo rivoluzionario per sviluppare le abilità e le conoscenze. Il nostro obiettivo è quello di rafforzare le competenze in un contesto mutevole, competitivo e altamente esigente.

Con TECH potrai sperimentare un modo di imparare che sta scuotendo le fondamenta delle università tradizionali in tutto il mondo"

Avrai accesso a un sistema di apprendimento basato sulla ripetizione, con un insegnamento naturale e progressivo durante tutto il programma.

Imparerai, attraverso attività collaborative e casi reali, la risoluzione di situazioni complesse in ambienti aziendali reali.

Un metodo di apprendimento innovativo e differente

Questo programma di TECH consiste in un insegnamento intensivo, creato ex novo, che propone le sfide e le decisioni più impegnative in questo campo, sia a livello nazionale che internazionale. Grazie a questa metodologia, la crescita personale e professionale viene potenziata, effettuando un passo decisivo verso il successo. Il metodo casistico, la tecnica che sta alla base di questi contenuti, garantisce il rispetto della realtà economica, sociale e professionale più attuali.

> *Il nostro programma ti prepara ad affrontare nuove sfide in ambienti incerti e a raggiungere il successo nella tua carriera"*

Il Metodo Casistico è stato il sistema di apprendimento più usato nelle migliori Scuole di Informatica del mondo da quando esistono. Sviluppato nel 1912 affinché gli studenti di Diritto non imparassero la legge solo sulla base del contenuto teorico, il metodo casistico consisteva nel presentare loro situazioni reali e complesse per prendere decisioni informate e giudizi di valore su come risolverle. Nel 1924 fu stabilito come metodo di insegnamento standard ad Harvard.

Cosa dovrebbe fare un professionista per affrontare una determinata situazione? Questa è la domanda con cui ti confrontiamo nel metodo dei casi, un metodo di apprendimento orientato all'azione. Durante il corso, gli studenti si confronteranno con diversi casi di vita reale. Dovranno integrare tutte le loro conoscenze, effettuare ricerche, argomentare e difendere le proprie idee e decisioni.

Metodologia Relearning

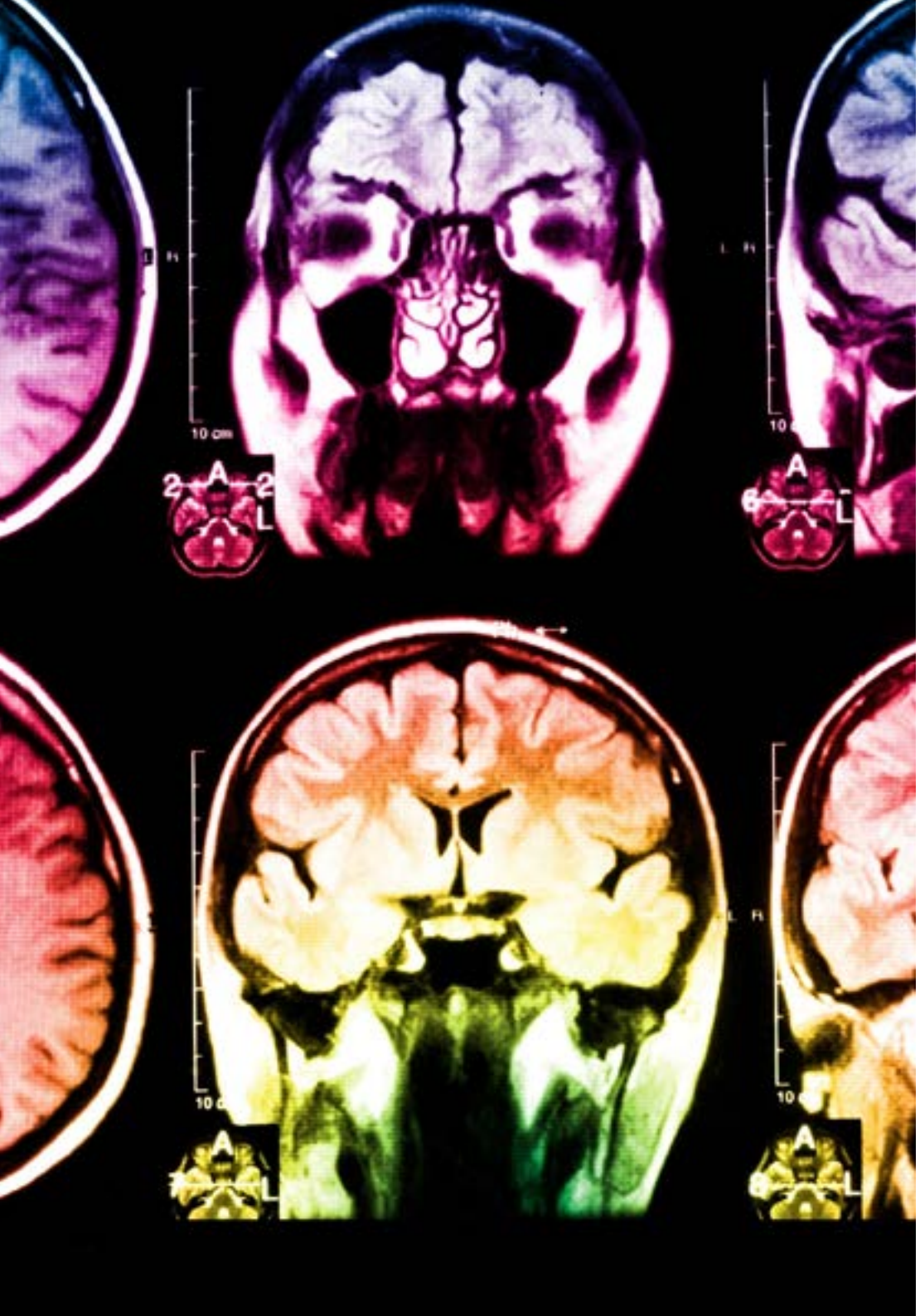
TECH coniuga efficacemente la metodologia del Caso di Studio con un sistema di apprendimento 100% online basato sulla ripetizione, che combina diversi elementi didattici in ogni lezione.

Potenziamo il Caso di Studio con il miglior metodo di insegnamento 100% online: il Relearning.

Nel 2019 abbiamo ottenuto i migliori risultati di apprendimento di tutte le università online del mondo.

In TECH imparerai con una metodologia all'avanguardia progettata per formare i manager del futuro. Questo metodo, all'avanguardia della pedagogia mondiale, si chiama Relearning.

La nostra università è l'unica autorizzata a utilizzare questo metodo di successo. Nel 2019, siamo riusciti a migliorare il livello di soddisfazione generale dei nostri studenti (qualità dell'insegnamento, qualità dei materiali, struttura del corso, obiettivi...) rispetto agli indicatori della migliore università online.



Nel nostro programma, l'apprendimento non è un processo lineare, ma avviene in una spirale (impariamo, disimpariamo, dimentichiamo e re-impariamo). Pertanto, combiniamo ciascuno di questi elementi in modo concentrico. Questa metodologia ha formato più di 650.000 laureati con un successo senza precedenti in campi diversi come la biochimica, la genetica, la chirurgia, il diritto internazionale, le competenze manageriali, le scienze sportive, la filosofia, il diritto, l'ingegneria, il giornalismo, la storia, i mercati e gli strumenti finanziari. Tutto questo in un ambiente molto esigente, con un corpo di studenti universitari con un alto profilo socio-economico e un'età media di 43,5 anni.

Il Relearning ti permetterà di apprendere con meno sforzo e più performance, impegnandoti maggiormente nella tua specializzazione, sviluppando uno spirito critico, difendendo gli argomenti e contrastando le opinioni: un'equazione diretta al successo.

Dalle ultime evidenze scientifiche nel campo delle neuroscienze, non solo sappiamo come organizzare le informazioni, le idee, le immagini e i ricordi, ma sappiamo che il luogo e il contesto in cui abbiamo imparato qualcosa è fondamentale per la nostra capacità di ricordarlo e immagazzinarlo nell'ippocampo, per conservarlo nella nostra memoria a lungo termine.

In questo modo, e in quello che si chiama Neurocognitive Context-dependent E-learning, i diversi elementi del nostro programma sono collegati al contesto in cui il partecipante sviluppa la sua pratica professionale.

Questo programma offre i migliori materiali didattici, preparati appositamente per i professionisti:

Materiale di studio

Tutti i contenuti didattici sono creati appositamente per il corso dagli specialisti che lo impartiranno, per fare in modo che lo sviluppo didattico sia davvero specifico e concreto.

Questi contenuti sono poi applicati al formato audiovisivo che supporterà la modalità di lavoro online di TECH. Tutto questo, con le ultime tecniche che offrono componenti di alta qualità in ognuno dei materiali che vengono messi a disposizione dello studente.

Master class

Esistono evidenze scientifiche sull'utilità dell'osservazione di esperti terzi.

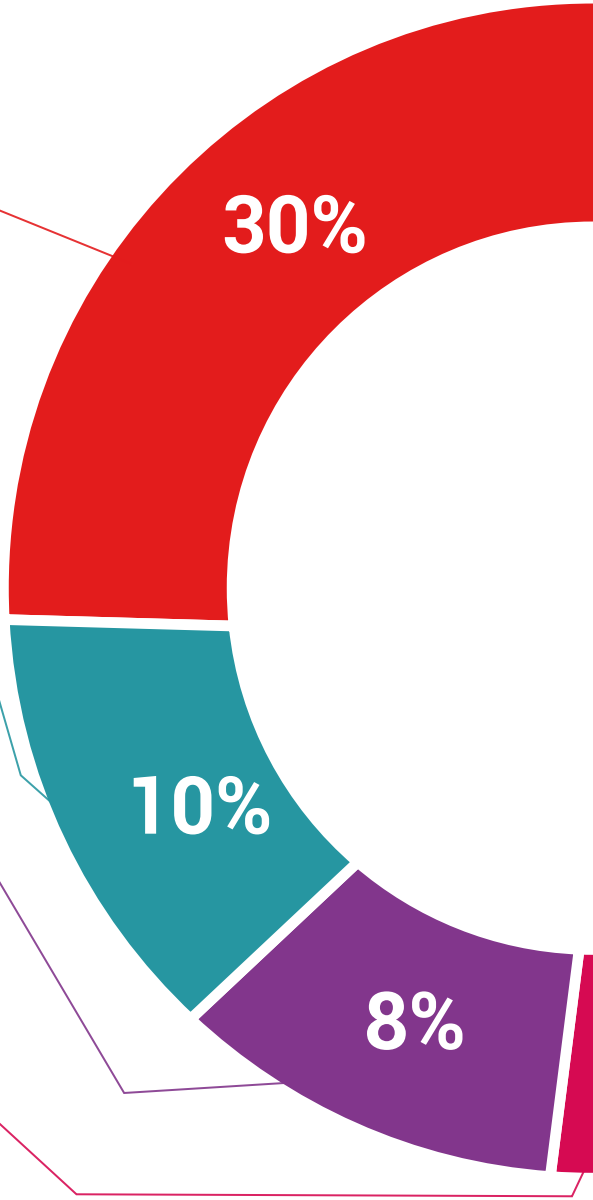
Imparare da un esperto rafforza la conoscenza e la memoria, costruisce la fiducia nelle nostre future decisioni difficili.

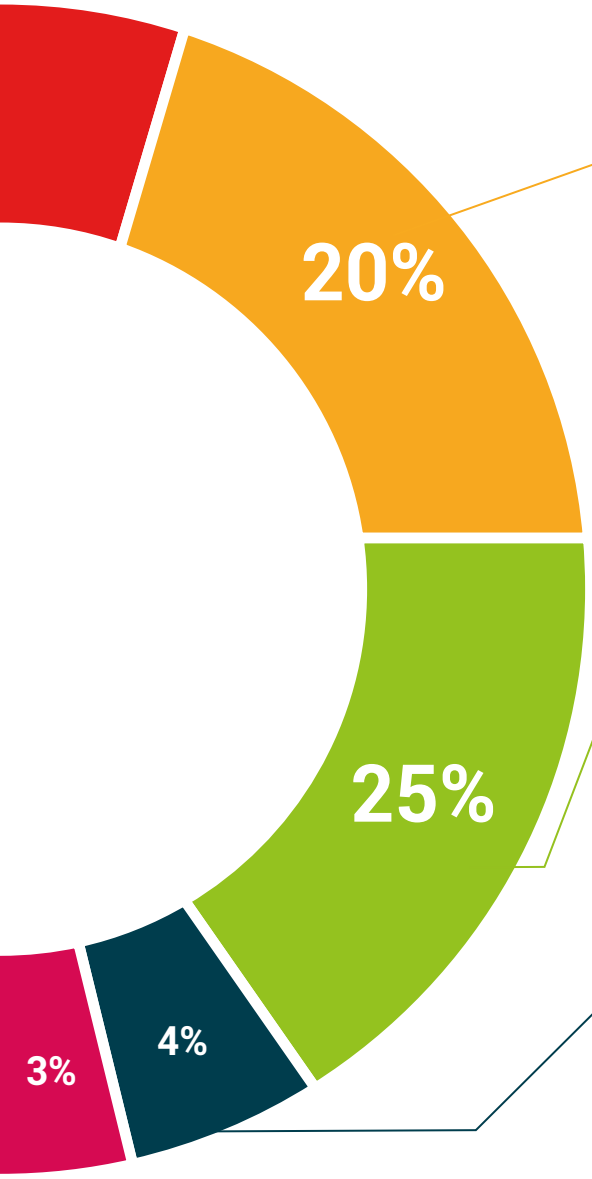
Pratiche di competenze e competenze

Svolgerai attività per sviluppare competenze e capacità specifiche in ogni area tematica. Pratiche e dinamiche per acquisire e sviluppare le competenze e le abilità che uno specialista deve sviluppare nel quadro della globalizzazione in cui viviamo.

Letture complementari

Articoli recenti, documenti di consenso e linee guida internazionali, tra gli altri. Nella biblioteca virtuale di TECH potrai accedere a tutto il materiale necessario per completare la tua specializzazione.





Casi di Studio

Completerai una selezione dei migliori casi di studio scelti appositamente per questo corso. Casi presentati, analizzati e monitorati dai migliori specialisti del panorama internazionale.

Riepiloghi interattivi

Il team di TECH presenta i contenuti in modo accattivante e dinamico in pillole multimediali che includono audio, video, immagini, diagrammi e mappe concettuali per consolidare la conoscenza.

Questo esclusivo sistema di specializzazione per la presentazione di contenuti multimediali è stato premiato da Microsoft come "Caso di successo in Europa".

Testing & Retesting

Valutiamo e rivalutiamo periodicamente le tue conoscenze durante tutto il programma con attività ed esercizi di valutazione e autovalutazione, affinché tu possa verificare come raggiungi progressivamente i tuoi obiettivi.

07

Titolo

Il Master Privato in Penetration Test e Red Team garantisce, oltre alla preparazione più rigorosa e aggiornata, il conseguimento di una qualifica di Master Privato rilasciata da TECH Università Tecnologica.

Porta a termine questo programma e ricevi la tua qualifica universitaria senza spostamenti o fastidiose formalità"

Questo **Master Privato in Penetration Test e Red Team** possiede il programma più completo e aggiornato del mercato.

Dopo aver superato la valutazione, lo studente riceverà mediante lettera certificata* con ricevuta di ritorno, la sua corrispondente qualifica di **Esperto Universitario** rilasciata da **TECH Università Tecnologica.**

Il titolo rilasciato da **TECH Università Tecnologica** esprime la qualifica ottenuta nell'Esperto Universitario, e riunisce tutti i requisiti comunemente richiesti da borse di lavoro, concorsi e commissioni di valutazione di carriere professionali.

Titolo: **Esperto Universitario in Tecniche Avanzate di Visione Artificiale Web**

Modalità: **online**

Durata: **12 mesi**


tech università tecnologica

Conferisce il presente

DIPLOMA

a

Dott./Dott.ssa _____, con documento d'identità n°_____

Per aver completato con esito positivo e accreditato il programma di

MASTER PRIVATO

in

Penetration Test e Red Team

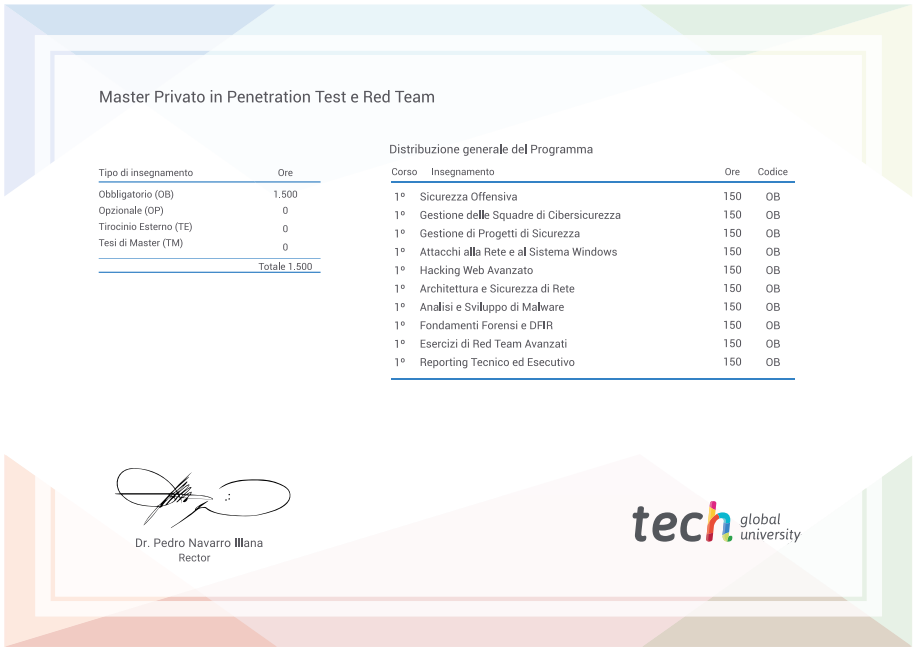
Si tratta di un titolo rilasciato da questa Università ed equivalente a 1.500 ore, con data di inizio gg/mm/aaaa e con data di fine gg/mm/aaaa.

TECH è un Istituto Privato di Istruzione Superiore riconosciuto dal Ministero della Pubblica Istruzione a partire dal 28 giugno 2018.

In data 17 Giugno 2020

Tere Guevara Navarro
Rettrice

codice unico TECH: AFWORD23S techtitute.com/titulos


Master Privato in Penetration Test e Red Team

Tipo di insegnamento	Ore
Obbligatorio (OB)	1.500
Opzionale (OP)	0
Tirocinio Esterno (TE)	0
Tesi di Master (TM)	0
	Totale 1.500

Distribuzione generale del Programma

Corso	Insegnamento	Ore	Codice
1°	Sicurezza Offensiva	150	OB
1°	Gestione delle Squadre di Cibersicurezza	150	OB
1°	Gestione di Progetti di Sicurezza	150	OB
1°	Attacchi alla Rete e al Sistema Windows	150	OB
1°	Hacking Web Avanzato	150	OB
1°	Architettura e Sicurezza di Rete	150	OB
1°	Analisi e Sviluppo di Malware	150	OB
1°	Fondamenti Forensi e DFIR	150	OB
1°	Esercizi di Red Team Avanzati	150	OB
1°	Reporting Tecnico ed Esecutivo	150	OB

Dr. Pedro Navarro Illana
Rector

tech global university

*Apostille dell'Aia. Se lo studente dovesse richiedere che il suo diploma cartaceo sia provvisto di Apostille dell'Aia, TECH EDUCATION effettuerà le gestioni opportune per ottenerla pagando un costo aggiuntivo.

tech università tecnologica

Master Privato
Penetration Test e Red Team

- Modalità: **online**
- Durata: **12 mesi**
- Titolo: **TECH Università Tecnologica**
- Orario: **a tua scelta**
- Esami: **online**

Master Privato

Penetration Test e Red Team

tech università tecnologica