Executive Master

Penetration Test e Red Team

MPTRT

tech università tecnologica

tech università tecnologica

Executive Master
Penetration Test e Red Team

- Modalità: **online**
- Durata: **12 mesi**
- Titolo: **TECH Università Tecnologica**
- Orario: **a tua scelta**
- Esami: **online**
- Rivolto a: **Diplomati e Laureati che abbiano precedentemente conseguito un qualsiasi titolo di studio nel campo delle Scienze Sociali e Giuridiche, Amministrative e Aziendali**

Accesso al sito web: **www.techtitute.com/business-school/master/master-penetration-test-red-team**

Indice

01 Benvenuto — pag. 4

02 Perché studiare in TECH? — pag. 6

03 Perché scegliere il nostro programma? — pag. 10

04 Obiettivi — pag. 14

05 Competenze — pag. 20

06 Struttura e contenuti — pag. 24

07 Metodologia — pag. 34

08 Profilo dei nostri studenti — pag. 42

09 Direzione del corso — pag. 46

10 Impatto sulla tua carriera — pag. 50

11 Benefici per la tua azienda — pag. 54

12 Titolo — pag. 58

01

Benvenuto

Attualmente, gli attacchi informatici hanno assunto un ruolo di primo piano e una forza considerevole, preoccupando la popolazione e le stesse aziende. In questo modo, le aziende hanno subito queste minacce in modo esponenziale, dovendo stabilire la massima protezione dei database e delle informazioni sensibili dei loro clienti. Pertanto, questo settore è alla costante ricerca di esperti altamente qualificati in sicurezza informatica, quindi TECH ha progettato questo programma accademico, con risorse tecnologiche e altre novità relative alle tattiche, tecniche e procedure utilizzate da attori malintenzionati. Tutto ciò mediante la metodologia *Relearning* e una completa piattaforma online al 100%, che offre flessibilità e comfort orario.

Executive Master in Penetration Test e Red Team
TECH Università Tecnologica

Grazie a questo programma online al 100%, sarai specializzato nella promozione di pratiche etiche e legali nell'esecuzione di attacchi e test su sistemi Windows”

02

Perché studiare in TECH?

TECH è la più grande business school del mondo che opera in modalità 100% online. Si tratta di una Business School d'élite, con un modello dotato dei più alti standard accademici. Un centro internazionale ad alto rendimento per la preparazione intensiva di competenze manageriali.

TECH è un'università all'avanguardia della tecnologia, che mette tutte le sue risorse a disposizione degli studenti per aiutarli a raggiungere il successo aziendale"

In TECH Università Tecnologica

Innovazione

L'Università offre un modello di apprendimento online che combina le ultime tecnologie educative con il massimo rigore pedagogico. Un metodo unico con il più alto riconoscimento internazionale che fornirà allo studente le chiavi per inserirsi in un mondo in costante cambiamento, in cui l'innovazione è concepita come la scommessa essenziale di ogni imprenditore.

"Caso di Successo Microsoft Europa" per aver incorporato l'innovativo sistema multivideo interattivo nei nostri programmi.

Massima esigenza

Il criterio di ammissione di TECH non si basa su criteri economici. Non è necessario effettuare un grande investimento per studiare in questa Università. Tuttavia, per ottenere una qualifica rilasciata da TECH, i limiti dell'intelligenza e della capacità dello studente saranno sottoposti a prova. I nostri standard accademici sono molto alti...

95% | **degli studenti di TECH termina i suoi studi con successo.**

Networking

In TECH partecipano professionisti provenienti da tutti i Paesi del mondo al fine di consentire allo studente di creare una vasta rete di contatti utile per il suo futuro.

+100000
manager specializzati ogni anno

+200
nazionalità differenti

Empowerment

Lo studente cresce di pari passo con le migliori aziende e con professionisti di grande prestigio e influenza. TECH ha sviluppato alleanze strategiche e una preziosa rete di contatti con i principali esponenti economici dei 7 continenti.

+500 | **accordi di collaborazione con le migliori aziende**

Talento

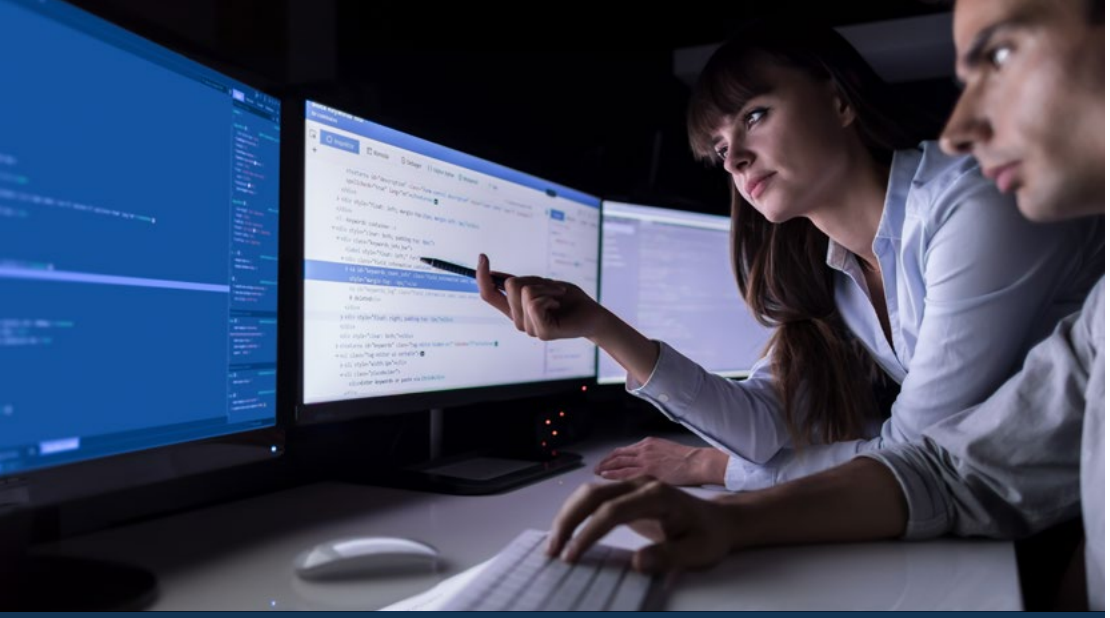
Il nostro programma è una proposta unica per far emergere il talento dello studente nel mondo imprenditoriale. Un'opportunità unica di affrontare i timori e la propria visione relativi al business.

TECH si propone di aiutare gli studenti a mostrare al mondo il proprio talento grazie a questo programma.

Contesto Multiculturale

Gli studenti che intraprendono un percorso con TECH possono godere di un'esperienza unica. Studierai in un contesto multiculturale. Lo studente, inserito in un contesto globale, potrà addentrarsi nella conoscenza dell'ambito lavorativo multiculturale mediante una raccolta di informazioni innovativa e che si adatta al proprio concetto di business.

Gli studenti di TECH provengono da oltre 200 nazioni differenti.



Impara con i migliori

Il personale docente di TECH contribuisce a mostrare agli studenti il proprio bagaglio di esperienze attraverso un contesto reale, vivo e dinamico. Si tratta di docenti impegnati a offrire una specializzazione di qualità che permette allo studente di avanzare nella sua carriera e distinguersi in ambito imprenditoriale.

Professori provenienti da 20 nazionalità differenti.

In TECH avrai accesso ai casi di studio più rigorosi e aggiornati del mondo accademico"

TECH punta all'eccellenza e dispone di una serie di caratteristiche che la rendono unica:

Analisi

In TECH esploriamo il lato critico dello studente, la sua capacità di mettere in dubbio le cose, la sua competenza nel risolvere i problemi e le sue capacità interpersonali.

Eccellenza accademica

TECH offre agli studenti la migliore metodologia di apprendimento online. L'università combina il metodo Relearning (la metodologia di apprendimento post-laurea meglio valutata a livello internazionale), con i casi di studio. Tradizione e avanguardia in un difficile equilibrio e nel contesto del più esigente itinerario educativo.

Economia di scala

TECH è la più grande università online del mondo. Dispone di oltre 10.000 corsi universitari di specializzazione universitaria. Nella nuova economia, **volume + tecnologia = prezzo dirompente**. In questo modo, garantiamo che lo studio non sia così costoso come in altre università.

03

Perché scegliere il nostro programma?

Studiare con TECH significa moltiplicare le tue possibilità di raggiungere il successo professionale nell'ambito del Senior Management.

È una sfida che comporta sforzo e dedizione, ma che apre le porte a un futuro promettente. Lo studente imparerà dai migliori insegnanti e con la metodologia educativa più flessibile e innovativa.

Disponiamo del personale docente più prestigioso e del programma più completo del mercato, il che ci permette di offrire una preparazione di altissimo livello accademico"

Questo programma fornirà molteplici vantaggi professionali e personali, tra i seguenti:

01 Dare una spinta decisiva alla carriera di studente

Studiando in TECH, lo studente può prendere le redini del suo futuro e sviluppare tutto il suo potenziale. Completando il nostro programma acquisirà le competenze necessarie per ottenere un cambio positivo nella sua carriera in poco tempo.

Il 70% dei partecipanti a questa specializzazione ottiene un cambiamento di carriera positivo in meno di 2 anni.

02 Svilupperai una visione strategica e globale dell'azienda

TECH offre una visione approfondita della gestione generale per comprendere come ogni decisione influenzi le diverse aree funzionali dell'azienda.

La nostra visione globale di azienda migliorerà la tua visione strategica.

03 Consolidare lo studente nella gestione aziendale superiore

Studiare in TECH significa avere accesso ad un panorama professionale di grande rilevanza, che permette agli studenti di ottenere un ruolo di manager di alto livello e di possedere un'ampia visione dell'ambiente internazionale.

Lavorerai con più di 100 casi reali di alta direzione.

04 Assumerai nuove responsabilità

Durante il programma vengono mostrate le ultime tendenze, gli sviluppi e le strategie per svolgere il lavoro professionale in un contesto in continuo cambiamento.

Il 45% degli studenti ottiene una promozione interna nel proprio lavoro.

05

Accesso a un'importante rete di contatti

TECH crea reti di contatti tra i suoi studenti per massimizzare le opportunità. Studenti con le stesse preoccupazioni e il desiderio di crescere. Così, sarà possibile condividere soci, clienti o fornitori.

Troverai una rete di contatti essenziali per la tua crescita professionale.

06

Svilupperai il progetto di business in modo rigoroso

Lo studente acquisirà una profonda visione strategica che lo aiuterà a sviluppare il proprio progetto, tenendo conto delle diverse aree dell'azienda.

Il 20% dei nostri studenti sviluppa la propria idea di business.

07

Migliorare le *soft skills* e le competenze direttive

TECH aiuta lo studente ad applicare e sviluppare le conoscenze acquisite e migliorare le capacità interpersonali per diventare un leader che faccia la differenza.

Migliora le tue capacità di comunicazione e di leadership e dai una spinta alla tua professione.

08

Farai parte di una comunità esclusiva

Lo studente farà parte di una comunità di manager d'élite, grandi aziende, istituzioni rinomate e professori qualificati delle università più prestigiose del mondo: la comunità di TECH Università Tecnologica.

Ti diamo l'opportunità di specializzarti grazie a un personale docente di reputazione internazionale.

04

Obiettivi

Questo corso fornirà agli studenti aggiornamenti innovativi sulle normative e la conformità nei progetti di cibersicurezza nell'area del *Penetration test*, apportando più valore alla sua carriera professionale. In questo senso, TECH fornirà risorse didattiche durante l'intero sviluppo del programma, potenziando le competenze relative al rilevamento delle anomalie e i comportamenti sospetti. Così, alla fine di questo programma, lo studente avrà ampliato le sue conoscenze su *Penetration test e Red Team*. Tutto questo, in 12 mesi di formazione online.

Grazie a questo Executive Master, ti aggiornerai sull'utilità della Digital Forensic Investigation (DFIR) per risolvere i crimini informatici"

TECH fa suoi gli obiettivi dei suoi studenti
Lavoriamo insieme per raggiungerli

Il **Executive Master in Penetration Test e Red Team** specializza lo studente per:

01 Studiare e comprendere le tattiche, le tecniche e le procedure utilizzate dagli attori malintenzionati, consentendo l'identificazione e la simulazione delle minacce

02 Applicare le conoscenze teoriche in scenari pratici e simulazioni, affrontando sfide reali per rafforzare le competenze di *Penetration test*

03 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

04 Migliorare le capacità di comunicazione specifiche per gli ambienti tecnici, facilitando la comprensione e il coordinamento tra i membri del team

05 Apprendere le tecniche di monitoraggio e controllo dei progetti, identificando le deviazioni e intraprendendo azioni correttive se necessario

06 Sviluppare competenze per valutare e migliorare le configurazioni di sicurezza dei sistemi Windows, garantendo l'implementazione di misure efficaci

07 Promuovere pratiche etiche e legali nell'esecuzione di attacchi e test su sistemi Windows, tenendo conto dei principi etici della cibersicurezza

08 Familiarizzarsi con la valutazione della sicurezza in API e servizi web, identificando potenziali punti di vulnerabilità e rafforzando la sicurezza nelle interfacce di programmazione

09 Promuovere una collaborazione efficace con i team di sicurezza, integrando le strategie e sforzi per proteggere l'infrastruttura di rete

10 Promuovere pratiche etiche e legali nell'analisi e nello sviluppo di malware, garantendo integrità e responsabilità in tutte le attività

11 Applicare le conoscenze teoriche in contesti simulati, partecipare ad esercizi pratici per comprendere e contrastare gli attacchi dannosi

12 Acquisire una solida conoscenza dei principi fondamentali dell'indagine forense digitale (DFIR), applicabili nella risoluzione degli incidenti informatici

13 Imparare a produrre rapporti dettagliati che documentano i risultati, le metodologie utilizzate e le raccomandazioni derivanti da esercizi di *Red Team* avanzati

14 Sviluppare competenze per formulare raccomandazioni pratiche e attuabili, orientate a mitigare le vulnerabilità e migliorare la postura di sicurezza

15 Familiarizzare lo studente con le migliori pratiche per la presentazione esecutiva di relazioni, adeguando le informazioni tecniche per il pubblico non tecnico

05

Competenze

Questa proposta accademica fornirà al laureato una visione attuale sul *Penetration test*. Questo ti darà l'opportunità di aumentare le tue abilità, assumendo ruoli di gestione, affrontando situazioni impegnative e mutevoli, e anche lavorando a stretto contatto e in modo efficace con altre aziende del settore IT. In questo modo, il professionista avrà a disposizione molteplici strumenti, come infografiche e video, che presenteranno una prospettiva più pratica in questo campo di studio.

Potenzia le tue abilità per il rilevamento e la prevenzione efficaci dei malware, risolvendo le situazioni più impegnative nel settore informatico"

01 Acquisire competenze di *coaching* per lo sviluppo professionale dei membri del team, promuovendo la crescita e il miglioramento

02 Sviluppare capacità decisionali strategiche in situazioni di sicurezza informatica, considerando l'impatto a breve e lungo termine sulla sicurezza organizzativa

03 Acquisire competenze in materia identificazione, valutazione e mitigazione dei rischi specifici dei progetti di sicurezza informatica

04 Sviluppare le competenze per implementare misure di difesa attiva, rafforzando la sicurezza dei sistemi e delle reti basate

05 Apprendere tecniche di analisi del traffico web per identificare modelli e comportamenti anomali, facilitando il rilevamento di potenziali minacce

06 Acquisire competenze nell'analisi forense applicata agli ambienti di rete, consentendo l'identificazione e una risposta efficace agli incidenti informatici

07 Apprendere strategie per il rilevamento e la prevenzione efficace di malware, compresa l'implementazione di soluzioni di sicurezza avanzate

08 Sviluppare competenze nell'identificazione degli indicatori di coinvolgimento (IoC) durante le indagini forensi, facilitando l'individuazione e la risposta agli incidenti

09 Acquisire competenze per la pianificazione strategica degli esercizi di *Red Team*, considerando obiettivi, ambito, risorse e scenari realistici

10 Acquisire competenze nell'identificazione e nella prioritizzazione delle vulnerabilità, evidenziando quelle che rappresentano i maggiori rischi per la sicurezza

06

Struttura e contenuti

Il programma in Penetration Test e Red Team è un programma incentrato essenzialmente affinché lo studente acquisisca le competenze relative all'informatica forense nella cibersicurezza. In questo modo, questa qualifica accademica è orientata verso una struttura teorico-pratica, accompagnata dall'ampia esperienza e dal grande bagaglio di un team di esperti altamente specializzati.

Nessun programma predefinito o valutazioni continue: TECH ti garantisce l'accesso più rapido e flessibile ai suoi contenuti accademici"

Piano di studi

Questo Executive Master consiste di 1.500 ore di apprendimento continuo, attraverso un insegnamento dei più alti standard, grazie al quale lo studente otterrà le migliori posizioni nel settore informatico e aziendale. In questo modo, gli studenti supereranno i vari ostacoli posti dall'ambiente di lavoro. Questa qualifica faciliterà molteplici competenze che affrontano tecniche avanzate di Kerberos, mitigazioni e protezioni.

D'altra parte, il personale docente ha sviluppato un programma esclusivo, che incorpora 10 moduli, con lo scopo di consentire allo studente di acquisire competenze fondamentali relative alla valutazione della sicurezza in API e servizi web, identificando possibili punti di vulnerabilità.

Inoltre, il professionista approfondirà le raccomandazioni pratiche e attuabili, volte a mitigare le vulnerabilità e migliorare la posizione di sicurezza. In questo senso, diventeranno importanti specialisti in materia di metodi di misurazione e prevenzione dei conflitti.

Per questo programma accademico, i datori di lavoro si baseranno sull'esclusiva metodologia *Relearning*, attraverso la quale potranno esaminare concetti complessi e assimilare la loro applicazione quotidiana in modo fluido. Allo stesso tempo, il corso viene impartito da un'innovativa piattaforma di apprendimento 100% online, non è soggetta a orari fissi o a programmi di valutazione continua.

Questo Executive Master ha una durata di 12 mesi ed è suddiviso in 10 moduli:

Modulo 1	Sicurezza Offensiva
Modulo 2	Gestione delle Squadre di Cibersicurezza
Modulo 3	Gestione di Progetti di Sicurezza
Modulo 4	Attacchi a Reti e Sistemi Windows
Modulo 5	*Hacking Web* Avanzato
Modulo 6	Architettura e Sicurezza di Rete
Modulo 7	Analisi e Sviluppo di *Malware*
Modulo 8	Fondamenti Forensi e DFIR
Modulo 9	Esercizi di *Red Team Avanzati*
Modulo 10	Reporting Tecnico ed Esecutivo

Dove, quando e come si svolge?

TECH ti offre la possibilità di svolgere questo Executive Master in Penetration Test e Red Team in modalità completamente online. Durante i 12 mesi di durata della specializzazione, gli studenti potranno accedere in qualsiasi momento a tutti i contenuti di questo programma, che consentirà loro di autogestire il proprio tempo di studio.

Un'esperienza educativa unica, chiave e decisiva per potenziare la tua crescita professionale e dare una svolta definitiva.

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 a Reti e Sistemi 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. Reti 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 *cookie*
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

07

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"

La Business School di TECH utilizza il 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"

Il nostro programma ti prepara ad affrontare sfide in ambienti incerti e a raggiungere il successo nel tuo business.

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

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 aziendale più attuali.

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

Il metodo casistico è stato il sistema di apprendimento più usato nelle migliori business school 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 ci confrontiamo nel metodo casistico, un metodo di apprendimento orientato all'azione. Durante il programma, 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

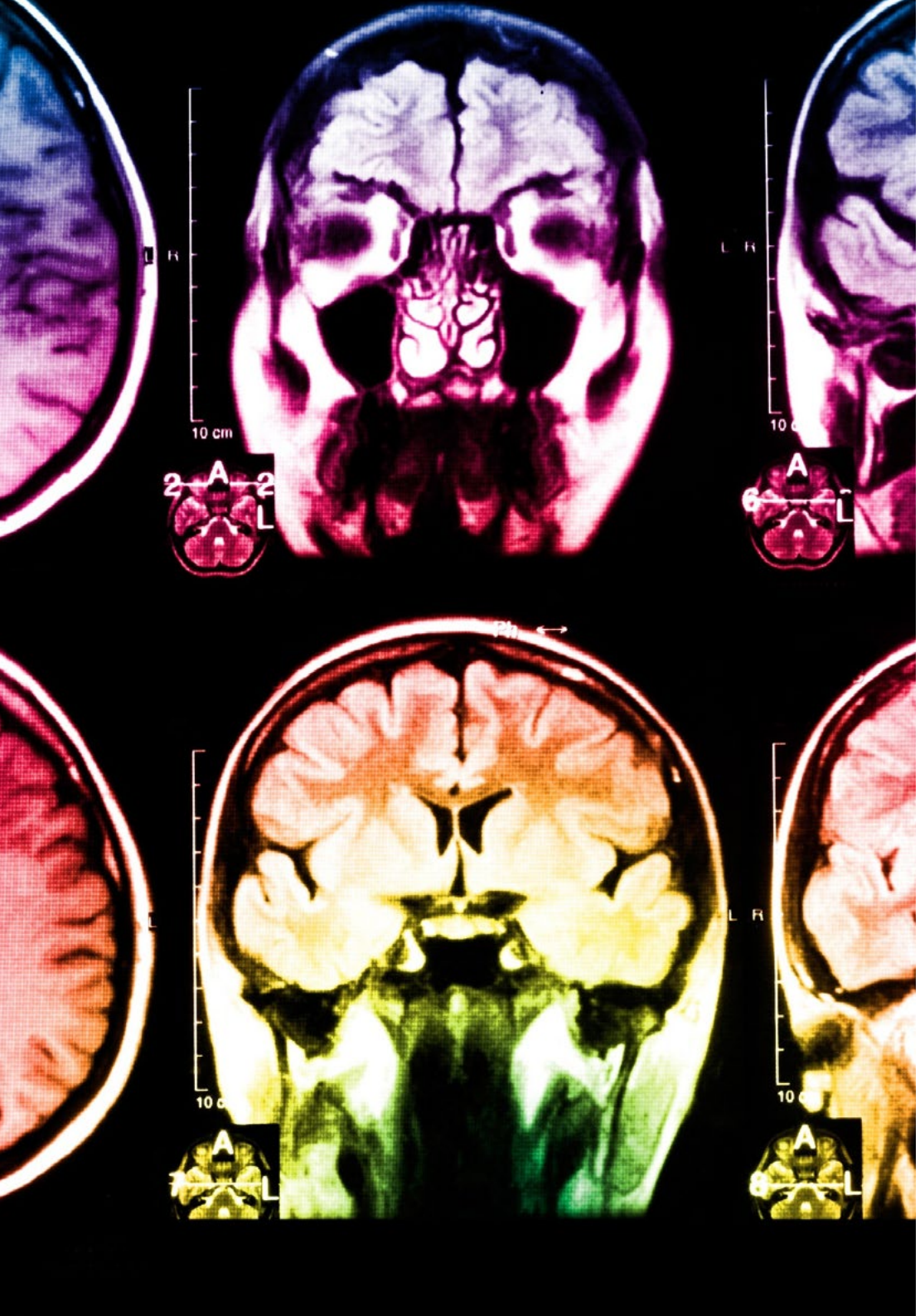
TECH coniuga efficacemente la metodologia del Caso di Studio con un sistema di apprendimento 100% online basato sulla ripetizione, che combina diversi elementi didattici in ogni lezione.

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

Il nostro sistema online ti permetterà di organizzare il tuo tempo e il tuo ritmo di apprendimento, adattandolo ai tuoi impegni. Sarai in grado di accedere ai contenuti da qualsiasi dispositivo fisso o mobile con una connessione internet.

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 scuola di business 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). Di conseguenza, combiniamo ciascuno di questi elementi in modo concentrico. Con questa metodologia abbiamo formato oltre 650.000 laureati con un successo senza precedenti, in ambiti molto 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 che punta direttamente 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.

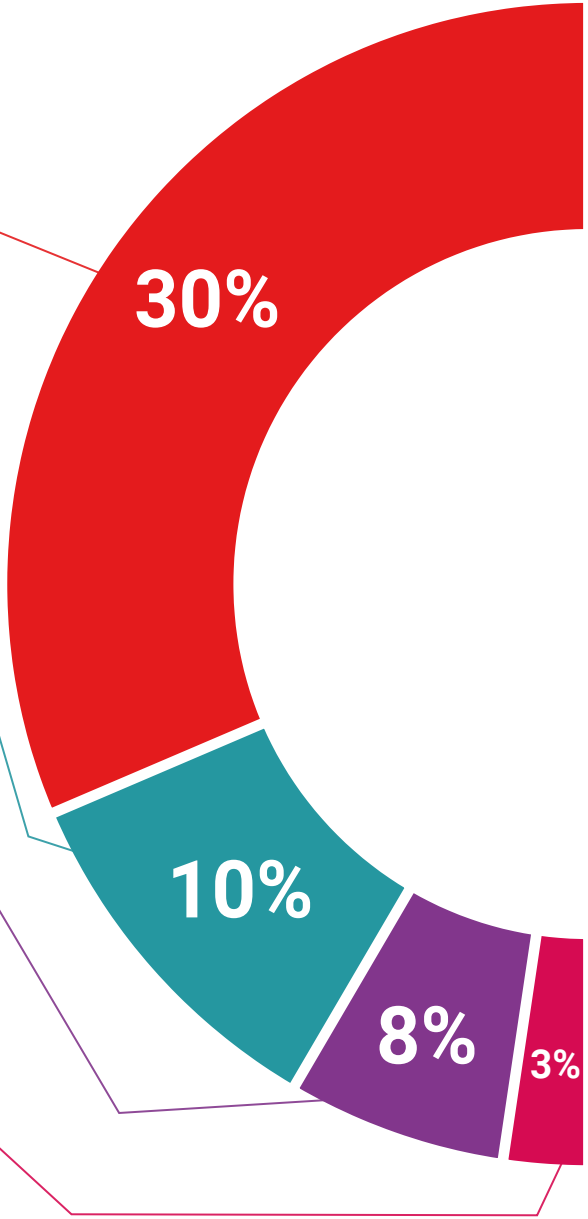
Imparare da un esperto rafforza la conoscenza e la memoria, costruisce la fiducia nelle nostre future decisioni difficili.

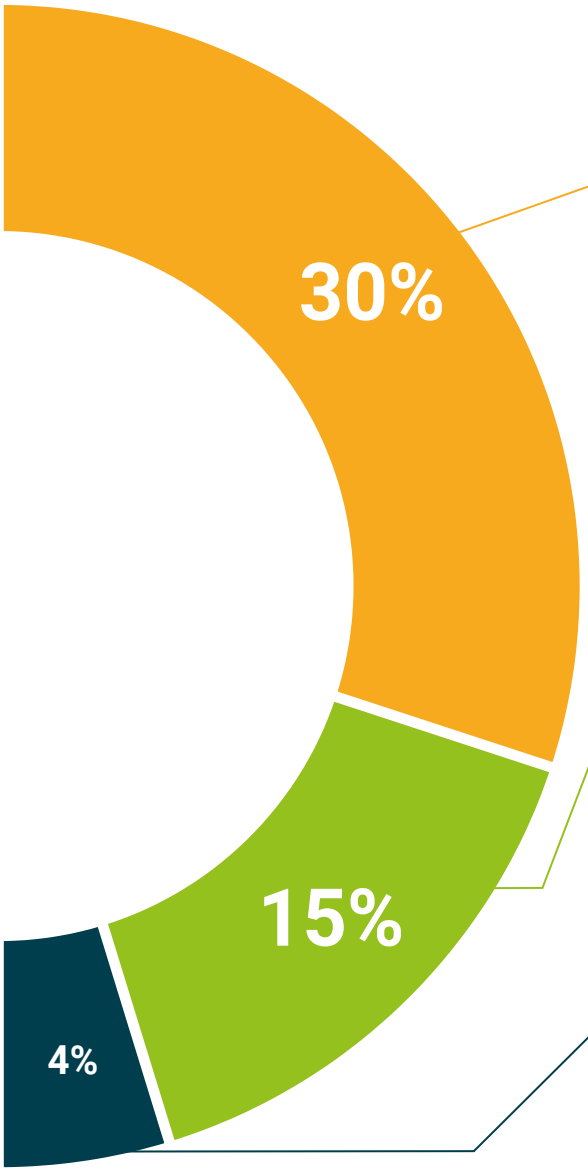
Stage di competenze manageriali

Svolgerai attività per sviluppare competenze manageriali specifiche in ogni area tematica. Pratiche e dinamiche per acquisire e sviluppare le competenze e le abilità che un senior manager 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 tutorati dai migliori specialisti in senior management 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.

08

Profilo dei nostri studenti

Il programma è rivolto a laureati e diplomati che hanno precedentemente completato una qualsiasi delle successive qualifiche nel campo delle Scienze Sociali, Giuridiche, Amministrative e dell'Economia.

La diversità dei partecipanti, con diversi profili accademici e di varie nazionalità, costituisce l'approccio multidisciplinare di questo programma.

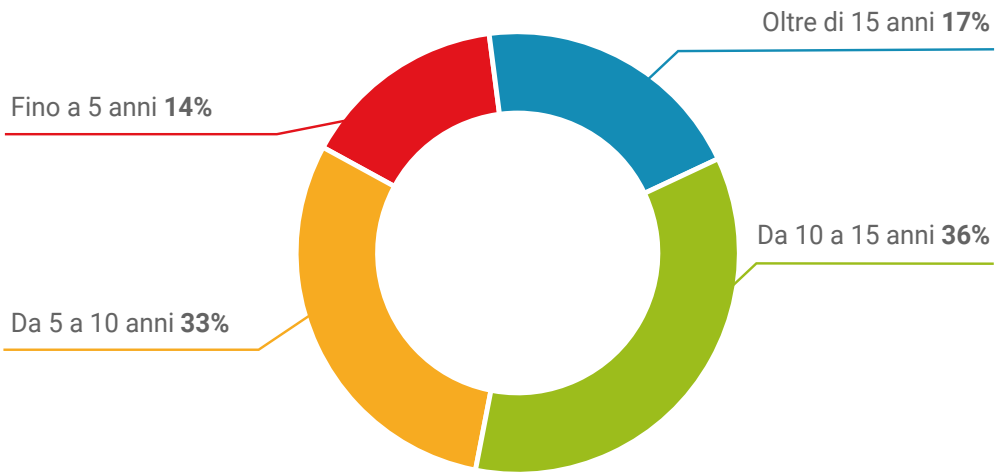
Il programma può essere conseguito anche da professionisti con una laurea in qualsiasi settore e due anni di esperienza lavorativa nel campo dell'Informatica.

Se hai esperienza in Penetration Test e Red Team, e sei alla ricerca di un'interessante miglioramento della tua carriera pur continuando a lavorare, questo è il programma adatto a te"

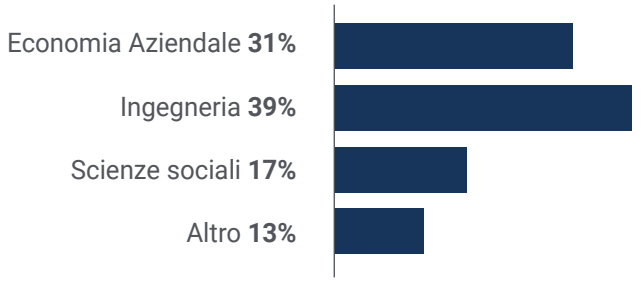
Età media

Da **35** e **45** anni

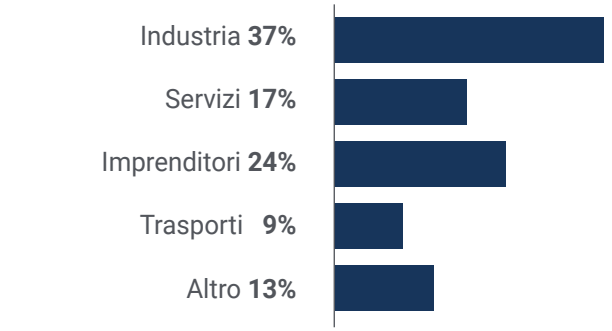
Anni di esperienza



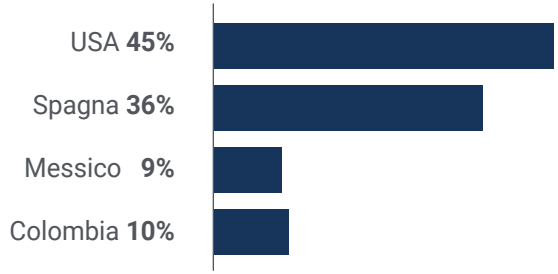
Educazione



Profilo accademico



Distribuzione geografica



Salomón Galvis

Analista di Sicurezza dell'Informazione

"Da questa qualifica ho evidenziato che sono riuscito ad approfondire l'importanza delle valutazioni regolari e l'essenziale per misurare la cibersicurezza. Un grande investimento che si rifletterà in futuro, grazie agli strumenti chiave che il personale docente implementa nello sviluppo del programma"

09

Direzione del corso

Questo Executive Master ha a disposizione un team di insegnanti di grande riconoscimento internazionale e con importanti conoscenze specialistiche in Software e Tecnologie della Società dell'Informazione e Cibersicurezza in Integrazione Tecnologica Aziendale. Così, l'educazione d'élite si riflette in un approccio dinamico e innovativo al programma, implementando le ultime tendenze nella cibersicurezza. In questo modo vengono accoppiati casi simulati e l'analisi di situazioni reali per consentire agli studenti di ottenere una prassi di alto livello, consentendo loro di affrontare le diverse sfide professionali nel mondo del lavoro.

Grandi esperti di Penetration Test e Red Team terranno questo programma innovativo e rigoroso"

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 Developmen*t
- Vincitore del Concorso AdaByron

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. 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

- Pentester presso Grupo Oesía
- 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. Mora Navas, Sergio

- Consulente in Cibersicurezza presso Grupo Oesia
- Ingegnere in 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

Un'esperienza formativa unica, fondamentale e decisiva per promuovere il tuo sviluppo professionale"

10

Impatto sulla tua carriera

Questo programma universitario è stato progettato con l'intenzione di guidare il laureato sulle conoscenze che lo porteranno ad affrontare qualsiasi situazione nel campo della cibersicurezza. In questo modo, TECH si addentrerà specificamente nell'insegnamento della massima qualità, cercando efficienza in ciascuna delle sue qualifiche. In questo modo, al professionista sarà garantito un apprendimento specializzato in *Penetration Test* e *Red Team*.

Red Team e altri aspetti informatici della cibersicurezza possono essere integrati nel Penetration Test attraverso questa intensa titolazione"

L'ottimizzazione delle campagne di marketing è un'altra delle competenze che avrai a disposizione dopo questo Executive Master completo di 12 mesi.

Sei pronto a dare una svolta? Un eccellente miglioramento professionale ti aspetta

Il Executive Master in Penetration Test e Red Team di TECH è un programma intensivo che ti prepara ad affrontare sfide e decisioni aziendali nell'ambito della Informatica. Il suo obiettivo principale è quello di promuovere la tua crescita personale e professionale. Aiutarti a raggiungere il successo.

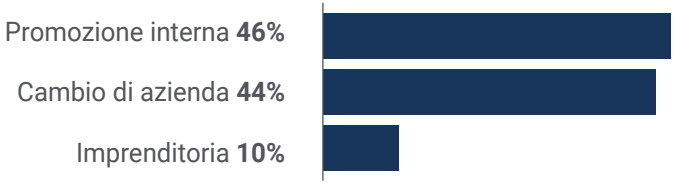
Se vuoi migliorare te stesso, ottenere un cambiamento positivo a livello professionale e creare una rete di contatti con i migliori, questo è il posto che fa per te.

Approfitta di questa opportunità rigorosa e completa per ampliare le tue competenze nel Penetration Test grazie a TECH, la migliore università online al mondo secondo Forbes.

Momento del cambiamento

Durante il programma	Durante il primo anno	Due anni dopo
13%	64%	23%

Tipo di cambiamento



Miglioramento salariale

La realizzazione di questo programma prevede per i nostri studenti un incremento salariale superiore al **25,55%**

Salario precedente	Incremento salariale	Salario posteriore
55.465 €	**25,55%**	**74.500 €**

11

Benefici per la tua azienda

Questo programma contribuisce a elevare il talento dell'organizzazione al suo massimo potenziale attraverso la didattica di leader di alto livello.

Inoltre, partecipare a questo programma è un'opportunità unica per accedere a una rete di contatti dove si possono trovare futuri partner professionali, clienti o fornitori.

Nell'era digitale, i manager devono integrare nuovi processi e strategie che comportano cambiamenti significativi e uno sviluppo organizzativo. Questo è possibile solo attraverso la preparazione e l'aggiornamento universitario"

Sviluppare e mantenere il talento nelle aziende è il miglior investimento a lungo termine.

01

Crescita del talento e del capitale intellettuale

Il professionista apporterà all'azienda nuovi concetti, strategie e prospettive che possono portare cambiamenti significativi nell'organizzazione.

02

Trattenere i manager ad alto potenziale ed evitare la fuga di cervelli

Questo programma rafforza il legame tra l'azienda e il professionista e apre nuove vie di crescita professionale all'interno.

03

Creare agenti di cambiamento

Sarai in grado di prendere decisioni in tempi di incertezza e di crisi, aiutando l'organizzazione a superare gli ostacoli.

04

Incremento delle possibilità di espansione internazionale

Grazie a questo programma, l'azienda entrerà a contatto con i principali mercati dell'economia mondiale.

05

Sviluppo di progetti propri

Il professionista può lavorare su un progetto esistente o sviluppare nuovi progetti nell'ambito di R&S o del Business Development della sua azienda.

06

Aumento della competitività

Questo programma fornirà ai rispettivi professionisti le competenze per affrontare nuove sfide e far crescere l'organizzazione

12

Titolo

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

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

Questo **Executive Master 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 **Executive Master** rilasciata da **TECH Università Tecnologica.**

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

Titolo: **Executive Master in Penetration Test e Red Team**

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

EXECUTIVE MASTER

in

Penetration Test e Red Team

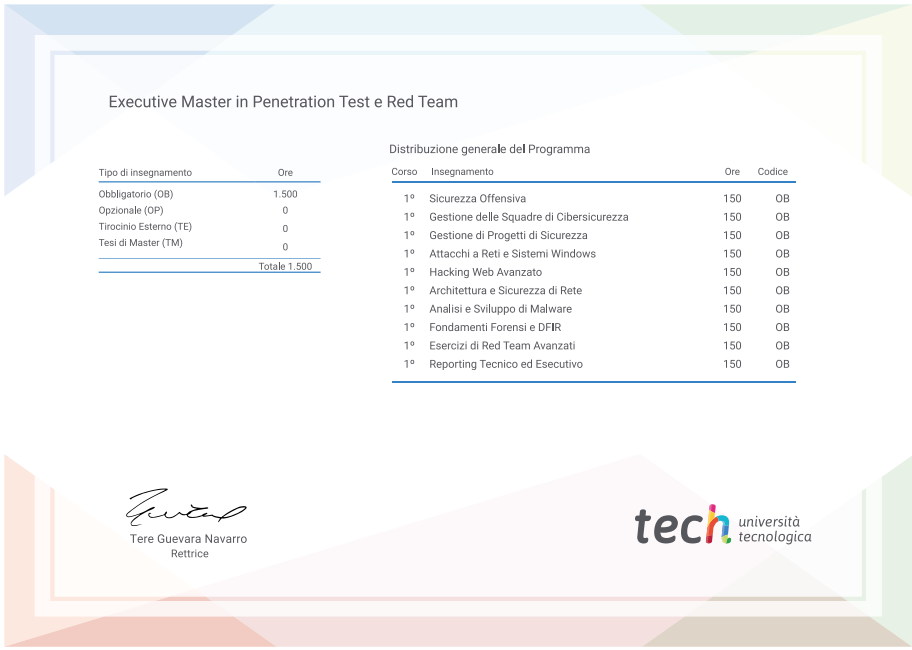
Si tratta di un titolo rilasciato da questa Università ed equivalente a 1.500 ore, con data di inizio gg/mm/aaaa e con data di fine gg/mm/aaaa.

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


Executive Master in Penetration Test e Red Team

Distribuzione generale del Programma

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

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

Tere Guevara Navarro
Rettrice

tech università tecnologica

*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

Executive Master
Penetration Test e Red Team

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

Executive Master

Penetration Test e Red Team

tech università tecnologica