Esperto Universitario
Red Team nella Cibersicurezza

tech global university

tech global university

Esperto Universitario
Red Team nella Cibersicurezza

- Modalità: **online**
- Durata: **6 mesi**
- Titolo: **TECH Global University**
- Accreditamento: **18 ECTS**
- Orario: **a scelta**
- Esami: **online**

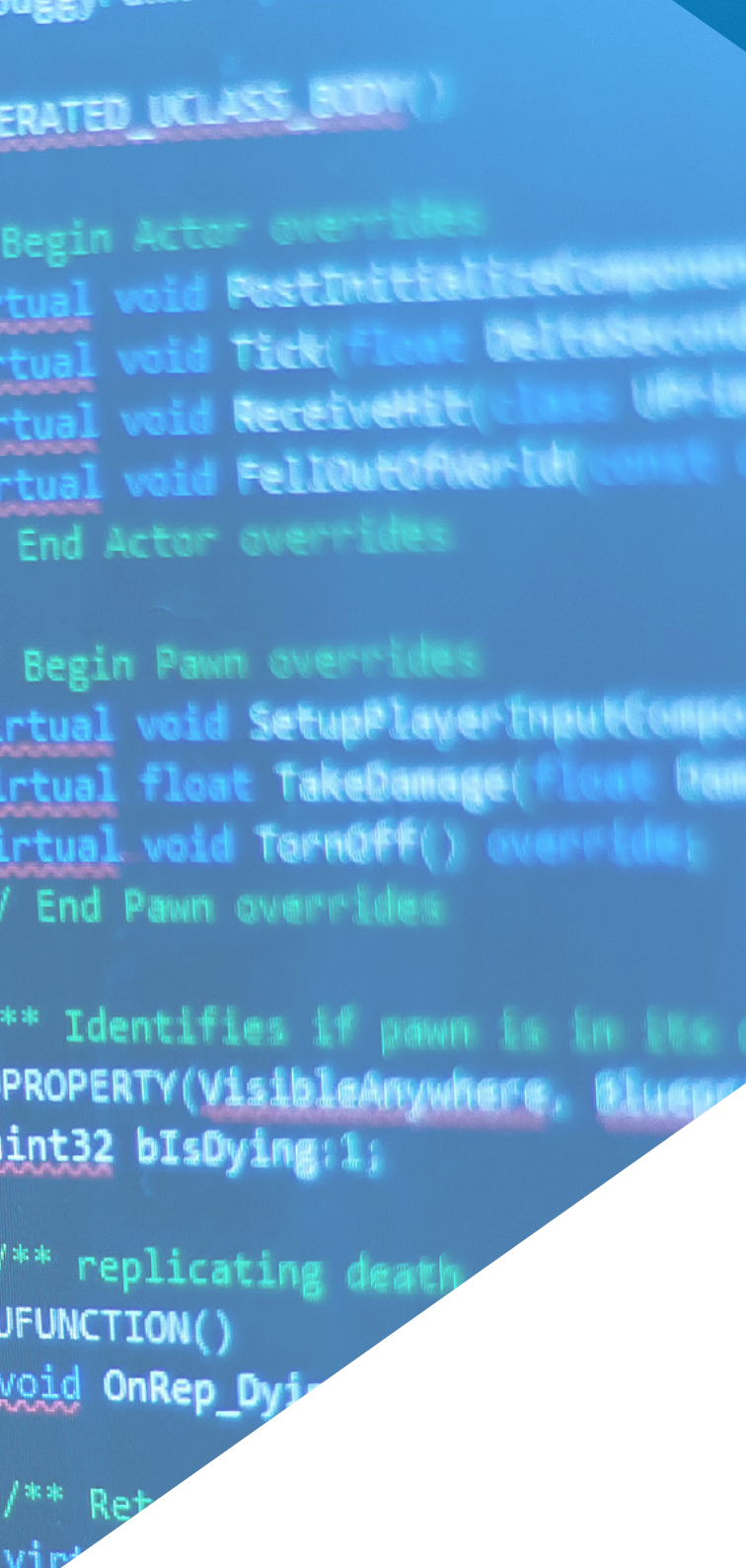
Accesso al sito web: www.techtitute.com/it/informatica/specializzazione/specializzazione-red-team-cibersicurezza

Indice

01

Presentazione

La Cibersicurezza è diventata un pilastro fondamentale nell'era digitale, mentre la crescente interconnessione dei sistemi ha intensificato la minaccia di attacchi informatici. La domanda di professionisti altamente qualificati in questo campo è più evidente che mai, soprattutto considerando l'aumento esponenziale della criminalità informatica e degli attacchi sofisticati. In questo contesto, questo programma è presentato come una risposta strategica per fornire ai professionisti le competenze necessarie per affrontare le minacce informatiche. Durante il corso, gli studenti saranno immersi nella simulazione di minacce avanzate. La metodologia del curriculum, 100% online, offre flessibilità e accessibilità, con una grande varietà di contenuti multimediali e l'applicazione del metodo *Relearning*.



Contribuirai a migliorare la Cibersicurezza ed eviterai il verificarsi di grandi crimini digitali. Non perdere quest'opportunità, iscriviti subito!"

Nel complesso scenario della sicurezza informatica, avere un esperto in questo campo si presenta come una necessità imperante per le organizzazioni che cercano di rafforzare le loro difese contro le minacce in continua evoluzione. Questo approccio proattivo, fondamentale per migliorare continuamente la posizione di sicurezza, sottolinea la necessità critica di esperti.

L'implementazione di misure proattive è essenziale e la formazione specializzata in Red Team offre ai professionisti la capacità di anticipare, identificare e mitigare attivamente le vulnerabilità nei sistemi e nelle reti. In questo Esperto Universitario, lo studente acquisirà competenze in test di penetrazione e simulazioni, affrontando l'identificazione e lo sfruttamento delle vulnerabilità. In questo senso, non solo svilupperai competenze tecniche avanzate, ma incoraggerai anche una collaborazione efficace con i team di sicurezza, integrando strategie contro le minacce *malware*.

Inoltre, gli studenti acquisiranno una solida conoscenza dei principi fondamentali dell'indagine forense digitale (DFIR), applicabili nella risoluzione degli incidenti informatici. Inoltre, questo approccio olistico garantirà che i professionisti siano dotati di competenze all'avanguardia nel campo della Cibersicurezza.

Questo percorso accademico si distingue non solo per il suo contenuto, ma anche per la sua metodologia avanzata. Sarà a disposizione degli studenti in modo completamente online, garantendo la flessibilità di cui hanno bisogno per avanzare nella loro carriera senza compromettere le loro responsabilità lavorative.

Inoltre, l'applicazione del *Relearning*, consistente nella ripetizione di concetti chiave, è utilizzato per fissare le conoscenze e facilitare un apprendimento efficace. Questa combinazione di accessibilità e solido approccio pedagogico rende questo Esperto Universitario non solo un'opzione educativa avanzata, ma anche un impulso significativo per coloro che cercano di eccellere nel campo della Cibersicurezza.

Questo **Esperto Universitario in Red Team nella Cibersicurezza** possiede il programma più completo e aggiornato del mercato. Le caratteristiche principali del programma sono:

- Sviluppo di casi pratici presentati da esperti in Red Team nella Cibersicurezza
- 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 sulle metodologie innovative
- Lezioni teoriche, domande all'esperto e/o al tutor, forum di discussione su questioni controverse e compiti di riflessione individuale
- Disponibilità di accesso ai contenuti da qualsiasi dispositivo fisso o portatile dotato di connessione a Internet

Ti distinguerai in un settore con grandi proiezioni grazie a questo esclusivo programma universitario di TECH"

Approfondirai la stesura di rapporti forensi dettagliati presso l'università meglio valutata al mondo dai suoi studenti, secondo la piattaforma Trustpilot (4,9/5)"

Svilupperai competenze per valutare e selezionare strumenti di sicurezza anti-malware.

Dimenticati di memorizzare! Con il sistema Relearning integrerai i concetti in modo naturale e progressivo.

Il personale docente del programma comprende rinomati specialisti del settore e altre aree correlate, che forniscono agli studenti le competenze necessarie a intraprendere un percorso di studio eccellente.

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

L'Esperto Universitario in *Red Team* nella Cibersicurezza ha l'obiettivo principale di formare gli studenti nello sviluppo di competenze nella simulazione di minacce avanzate. Durante il programma, gli studenti saranno immersi nella replica di tattiche, tecniche e procedure (TTP), utilizzate da attori malintenzionati. In questo contesto, l'approccio specializzato non solo rafforzerà le competenze tecniche di i professionisti, ma li formerà anche per affrontare le sfide del mondo reale in questo settore. Inoltre, l'uso della metodologia *Relearning* faciliterà l'apprendimento, fissando concetti chiave con poco sforzo.

Identificherai i punti deboli e le vulnerabilità nelle infrastrutture informatiche delle aziende. Raggiungi i tuoi obiettivi con TECH!"

Obiettivi generali

- Acquisire competenze avanzate nei test di penetrazione e nelle simulazioni di *Red Team*, affrontando l'identificazione e lo sfruttamento delle vulnerabilità di sistemi e reti
- Sviluppare capacità di leadership per coordinare team specializzati nella Cibersicurezza offensiva, ottimizzando l'esecuzione di progetti di *Penetration Test* e *Red Team*
- Sviluppare competenze nell'analisi e nello sviluppo di *malware*, comprendendone le funzionalità e applicando misure 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 Cibersicurezza, tenendo conto dei principi etici e legali in tutte le attività
- Mantenere gli 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. 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 2. 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 3. 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

03

Direzione del corso

Per questo programma universitario, TECH ha riunito un distinto personale docente, composto dai migliori specialisti del settore. In questo senso, ogni membro del personale docente possiede un ampio e riconosciuto background professionale, forgiato in aziende leader del settore della Cibersicurezza. Inoltre, selezionati con cura per la loro esperienza e competenza, questi professionisti non solo garantiranno la qualità accademica del piano di studi, ma forniranno anche una prospettiva pratica e aggiornata, arricchendo la formazione degli studenti con insight preziosi provenienti dalla loro esperienza reale nell'ambito del Red Team.

Aggiornati sulle più recenti tecniche di crittografia Shellcode (XQR) grazie ai migliori esperti di Cibersicurezza. Dai uno slancio alla tua carriera con 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

04

Struttura e contenuti

Questo programma offrirà allo studente un'immersione specializzata nell'analisi forense applicata al *malware*, evidenziando lo sviluppo di competenze chiave per l'identificazione di indicatori di compromissione (IoC) e modelli di attacco. Durante il corso, gli studenti si immergeranno in metodologie avanzate, fornendo loro gli strumenti e le conoscenze necessarie per affrontare sofisticate minacce informatiche. Inoltre, questo programma, strutturato in modo rigoroso, garantirà una formazione integrale nell'ambito del *Red Team*, preparando i professionisti ad analizzare e contrastare le complesse strategie utilizzate da attori malintenzionati.

Approfondirai le tecniche avanzate di post-sfruttamento e ti posizionerai come un eccezionale Red Teamer"

Modulo 1. Analisi e Sviluppo di *Malware*

1.1. Analisi e sviluppo di *Malware*
- 1.1.1. Storia ed evoluzione di *malware*
- 1.1.2. Classificazione e tipi di *malware*
- 1.1.3. Analisi dei *malware*
- 1.1.4. Sviluppo di *malware*

1.2. Preparazione dell'ambiente
- 1.2.1. Configurazione di Macchine Virtuali e *Snapshots*
- 1.2.2. Strumenti di analisi del *malware*
- 1.2.3. Strumenti di sviluppo del *malware*

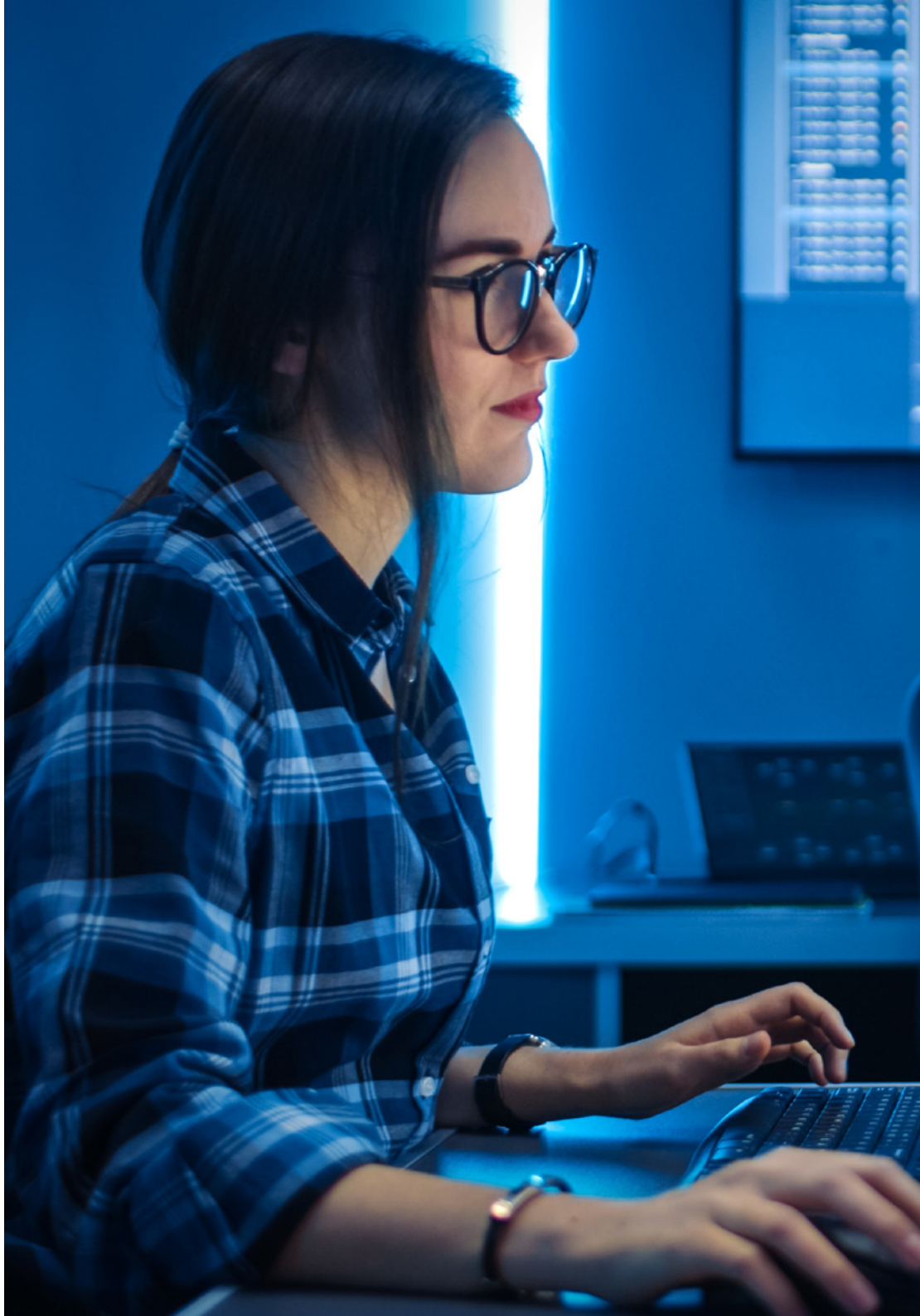
1.3. Fondamenti di Windows
- 1.3.1. Formato dei file PE (*Portable Executable*)
- 1.3.2. Processo e *Threads*
- 1.3.3. Sistemi di archivio e registro
- 1.3.4. *Windows Defender*

1.4. Tecniche di *malware* di base
- 1.4.1. Generazione di *shellcode*
- 1.4.2. Esecuzione di *shellcode* su disco
- 1.4.3. Disco vs memoria
- 1.4.4. Esecuzione di *shellcode* su memoria

1.5. Tecniche di *malware* intermedie
- 1.5.1. Persistenza di Windows
- 1.5.2. Cartella Home
- 1.5.3. Chiavi di registro
- 1.5.4. Screensaver

1.6. Tecniche di *malware* avanzate
- 1.6.1. Crittografia di *shellcode* (XOR)
- 1.6.2. Crittografia di *shellcode* (RSA)
- 1.6.3. Offuscamento di *strings*
- 1.6.4. Iniezione di processi

1.7. Analisi statica dei *malware*
- 1.7.1. Analisi dei *packers* con DIE (*Detect It Easy*)
- 1.7.2. Analisi delle sezioni con PE-Bear
- 1.7.3. Decompilazione con Ghidra



1.8. Analisi dinamica dei *malware*
- 1.8.1. Analisi del comportamento con Process Hacker
- 1.8.2. Analisi delle chiamate con API Monitor
- 1.8.3. Analisi delle modifiche al registro di sistema con Regshot
- 1.8.4. Analisi delle richieste di rete con TCPView

1.9. Analisi in .NET
- 1.9.1. Introduzione a .NET
- 1.9.2. Decompilazione con dnSpy
- 1.9.3. Debug con dnSpy

1.10. Analisi di *malware* reali
- 1.10.1. Preparazione dell'ambiente
- 1.10.2. Analisi statica dei *malware*
- 1.10.3. Analisi dinamica dei *malware*
- 1.10.4. Creazione di regole YARA

Modulo 2. Fondamenti Forensi e DFIR

2.1. Forense digitale
- 2.1.1. Storia ed evoluzione dell'informatica forense
- 2.1.2. Importanza dell'informatica forense nella cibersicurezza
- 2.1.3. Storia ed evoluzione dell'informatica forense

2.2. Fondamenti di informatica forense
- 2.2.1. Catena di custodia e sua applicazione
- 2.2.2. Tipi di evidenza digitale
- 2.2.3. Processo di acquisizione delle evidenze

2.3. File system e struttura dei dati
- 2.3.1. Principali file system
- 2.3.2. Metodi di occultamento dei dati
- 2.3.3. Analisi dei metadati e degli attributi dei file

2.4. Analisi dei sistemi operativi
- 2.4.1. Analisi forense dei sistemi Windows
- 2.4.2. Analisi dei sistemi operativi
- 2.4.3. Analisi forense dei sistemi macOS

2.5. Recupero dati e analisi del disco
- 2.5.1. Recupero dati da supporti danneggiati
- 2.5.2. Strumenti di analisi del disco
- 2.5.3. Interpretazione delle tabelle di allocazione dei file

2.6. Analisi della rete e del traffico
- 2.6.1. Acquisizione e analisi dei pacchetti di rete
- 2.6.2. Analisi dei registri del *firewall*
- 2.6.3. Rilevamento delle intrusioni di rete

2.7. *Malware* e analisi di codice dannoso
- 2.7.1. Classificazione di *malware* e caratteristiche
- 2.7.2. Analisi statica e dinamica dei *malware*
- 2.7.3. Tecniche di smontaggio e debug

2.8. Analisi di log ed eventi
- 2.8.1. Tipi di registri nei sistemi e nelle applicazioni
- 2.8.2. Interpretazione degli eventi rilevanti
- 2.8.3. Strumenti di analisi dei registri

2.9. Rispondere agli incidenti di sicurezza
- 2.9.1. Processo di risposta agli incidenti
- 2.9.2. Creazione di un piano di risposta agli incidenti
- 2.9.3. Coordinamento con le squadre di sicurezza

2.10. Presentazione di prove e legali
- 2.10.1. Regole di evidenza digitale in ambito legale
- 2.10.2. Preparazione di rapporti forensi
- 2.10.3. Audizione in qualità di testimone esperto

Modulo 3. Esercizi di *Red Team* Avanzati

3.1. Tecniche avanzate di osservazione
- 3.1.1. Elenco avanzato di sottodomini
- 3.1.2. *Google Dorking* avanzato
- 3.1.3. Social network e theHarvester

3.2. Campagne di *phishing* avanzate
- 3.2.1. Cos'è *Reverse-Proxy Phishing*
- 3.2.2. *2FA Bypass* con Evilginx
- 3.2.3. Infiltrazione di dati

3.3. Tecniche avanzate di persistenza
- 3.3.1. *Golden Tickets*
- 3.3.2. *Silver Tickets*
- 3.3.3. Tecnica *DCShadow*

3.4. Tecniche avanzate di evasione
- 3.4.1. *Bypass* di AMSI
- 3.4.2. Modifica degli strumenti esistenti
- 3.4.3. Offuscamento di *Powershell*

3.5. Tecniche avanzate di movimento laterale
- 3.5.1. *Pass-the-Ticket* (PtT)
- 3.5.2. *Overpass-the-Hash (Pass-the-Key)*
- 3.5.3. NTLM Relay

3.6. Tecniche avanzate di post-sfruttamento
- 3.6.1. *Dump* di LSASS
- 3.6.2. *Dump* di SAM
- 3.6.3. Attacco *DCSync*

3.7. Tecniche avanzate di *pivoting*
- 3.7.1. Cos'è il *pivoting*
- 3.7.2. Gallerie con SSH
- 3.7.3. *Pivoting* con Chisel

3.8. Intrusioni fisiche
- 3.8.1. Sorveglianza e riconoscimento
- 3.8.2. *Tailgating e Piggybacking*
- 3.8.3. *Lock-Picking*

3.9. Attacchi Wi-Fi
- 3.9.1. Attacchi a WPA/WPA2 PSK
- 3.9.2. Attacchi di Rogue AP
- 3.9.3. Attacchi a WPA2 *Enterprise*

3.10. Attacchi RFID
- 3.10.1. Lettura di schede RFID
- 3.10.2. Gestione di schede RFID
- 3.10.3. Creazione di schede clonate

Non perdere questa opportunità per dare impulso alla tua carriera con questo programma innovativo. Diventa un esperto in Cibersicurezza"

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

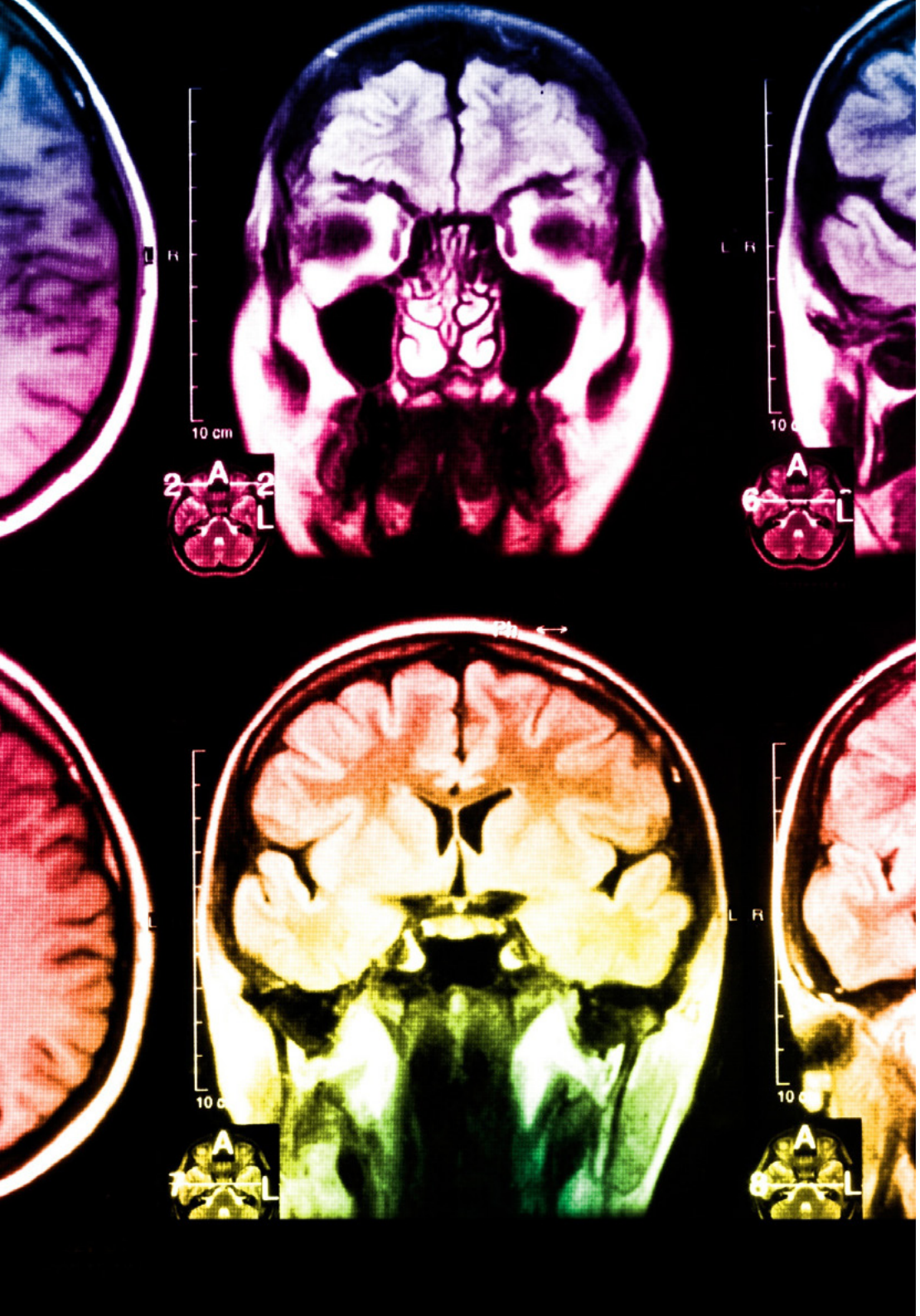
TECH coniuga efficacemente la metodologia del Caso di Studio con un sistema di apprendimento 100% online basato sulla ripetizione, che combina diversi elementi didattici in ogni lezione.

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.

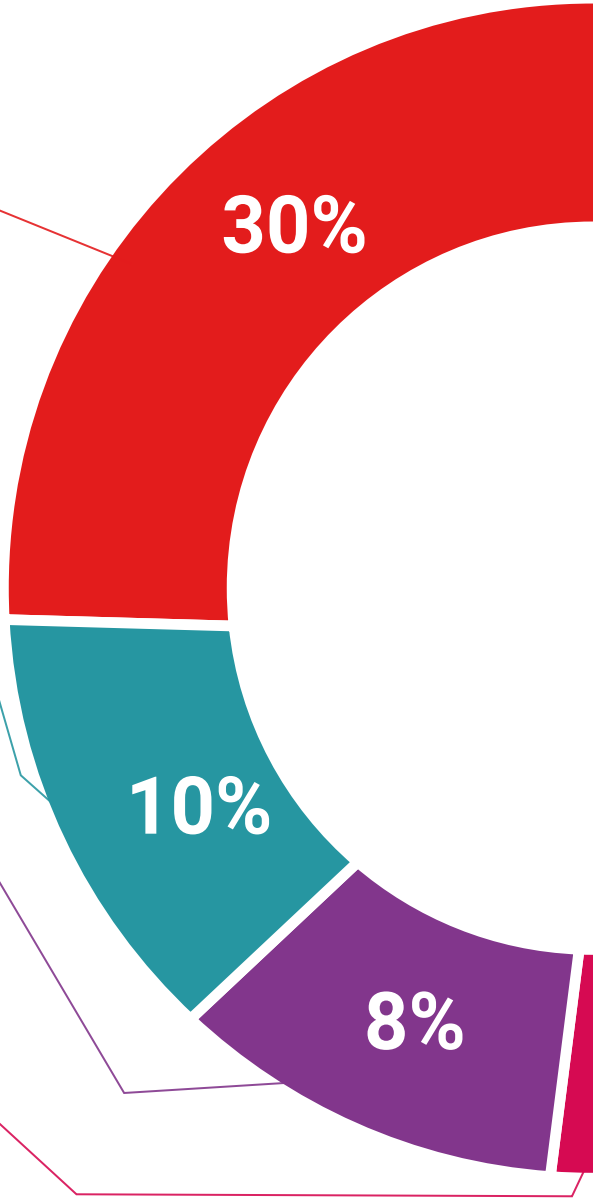
Imparare da un esperto rafforza la conoscenza e la memoria, costruisce la fiducia nelle nostre future decisioni difficili.

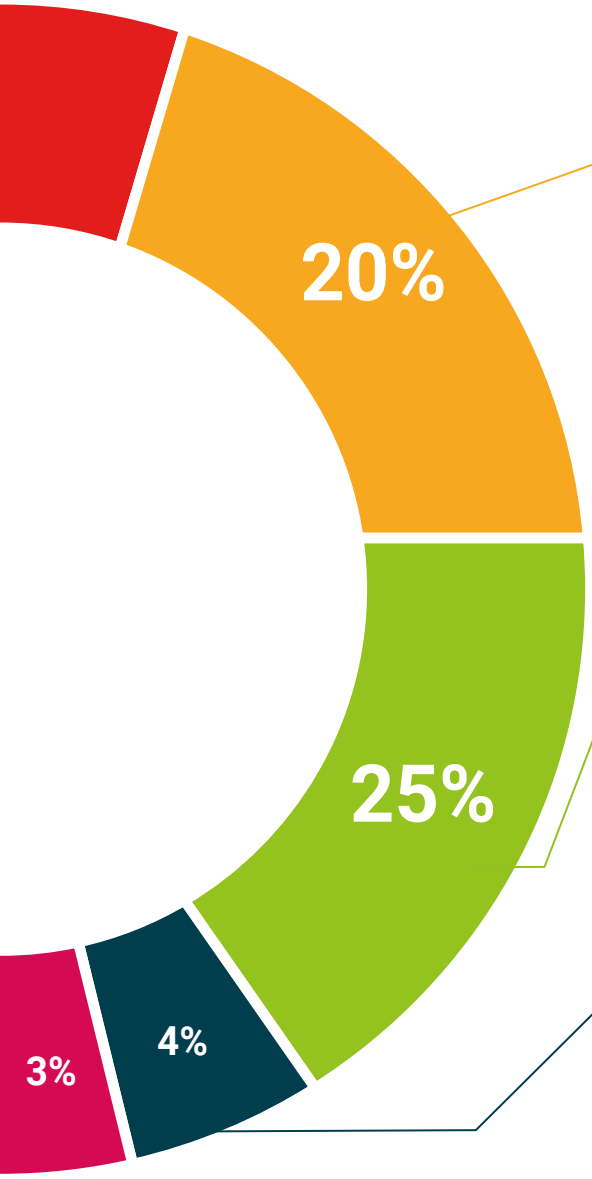
Pratiche di competenze e competenze

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.

06

Titolo

Questo programma ti consentirà di ottenere il titolo di studio di Esperto Universitario in Red Team nella Cibersicurezza rilasciato da TECH Global University, la più grande università digitale del mondo.

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

Questo programma ti consentirà di ottenere il titolo di studio di **ESTUDIO in Red Team nella Cibersicurezza** rilasciato da **TECH Global University**, la più grande università digitale del mondo.

TECH Global University è un'Università Ufficiale Europea riconosciuta pubblicamente dal Governo di Andorra ***(bollettino ufficiale)***. Andorra fa parte dello Spazio Europeo dell'Istruzione Superiore (EHEA) dal 2003. L'EHEA è un'iniziativa promossa dall'Unione Europea che mira a organizzare il quadro formativo internazionale e ad armonizzare i sistemi di istruzione superiore dei Paesi membri di questo spazio. Il progetto promuove valori comuni, l'implementazione di strumenti congiunti e il rafforzamento dei meccanismi di garanzia della qualità per migliorare la collaborazione e la mobilità tra studenti, ricercatori e accademici.

Questo titolo privato di **TECH Global Universtity** è un programma europeo di formazione continua e aggiornamento professionale che garantisce l'acquisizione di competenze nella propria area di conoscenza, conferendo allo studente che supera il programma un elevato valore curriculare.

Titolo: **Esperto Universitario in Red Team nella Cibersicurezza**

ECTS: **18**

Nº Ore Ufficiali: **450 o.**


tech global university

Dott _____, con documento d'identità _____ ha superat o con successo e ottenuto il titolo di:

Esperto Universitario in Red Team nella Cibersicurezza

Si tratta di un titolo di studio privato corrispondente a 450 horas di durata equivalente a 18 ECTS, con data di inizio dd/mm/aaaa e data di fine dd/mm/aaaa.

TECH Global University è un'università riconosciuta ufficialmente dal Governo di Andorra il 31 de gennaio 2024, appartenente allo Spazio Europeo dell'Istruzione Superiore (EHEA).

In Andorra la Vella, 28 febbraio 2024

Dott. Pedro Navarro Illa na
Rettore

código único TECH: AFWDR23S techtitute.com/titulos

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

tech global university

Esperto Universitario
Red Team nella Cibersicurezza

- Modalità: **online**
- Durata: **6 mesi**
- Titolo: **TECH Global University**
- Accreditamento: **18 ECTS**
- Orario: **a scelta**
- Esami: **online**

Esperto Universitario
Red Team nella Cibersicurezza

tech global university