Mestrado Próprio

Pentesting e Red Team

tech universidade tecnológica

tech universidade tecnológica

Mestrado Próprio
Pentesting e Red Team

- Modalidade: **online**
- Duração: **12 meses**
- Certificado: **TECH Universidade Tecnológica**
- Horário: **no seu próprio ritmo**
- Provas: **online**

Acesso ao site: www.techtitute.com/br/informatica/mestrado-proprio/mestrado-proprio-pentesting-red-team

Índice

01

Apresentação

A quantidade e a sofisticação dos ataques cibernéticos atingiram proporções alarmantes. Com o aumento exponencial das ameaças, desde ataques de *ransomware* até invasões avançadas, a necessidade de profissionais de segurança cibernética altamente capacitados é crucial. É nesse contexto que surge o presente programa, que não apenas proporcionará uma imersão total em técnicas avançadas de segurança, mas também abordará a realidade de um ambiente digital em constante evolução. Dessa forma, os alunos aprofundarão seus conhecimentos sobre técnicas de ataque e defesa, enfrentando os mais sofisticados desafios de segurança. Impulsionado pela necessidade de fortalecer as defesas cibernéticas, este plano de estudos se distingue por sua metodologia 100% online e pelo uso eficaz do *Relearning* para otimizar o aprendizado.

Você projetará protocolos de segurança impenetráveis graças a este programa pioneiro, com a garantia da TECH"

Manter-se atualizado é fundamental para preservar a eficácia da defesa contra ameaças atuais e emergentes. Nesse sentido, a rápida evolução da tecnologia e das táticas cibernéticas tornou imperativa a atualização constante. A proliferação de ameaças ressalta a urgência de contar com profissionais altamente capacitados.

Nesse contexto, esse programa universitário é uma resposta essencial, pois não só fornecerá uma compreensão aprofundada das técnicas mais avançadas de cibersegurança, mas também garantirá que os profissionais estejam na vanguarda das últimas tendências e tecnologias.

No programa de estudos deste Mestrado Próprio em Pentesting e Red Team, o aluno abordará de forma abrangente as demandas no campo da cibersegurança. A empresa implementará medidas eficazes de segurança de rede, incluindo firewalls, sistemas de detecção de intrusão (IDS) e segmentação de rede. Para isso, os especialistas aplicarão metodologias de investigação forense digital para solucionar casos, desde a identificação até a documentação das descobertas.

Além disso, eles desenvolverão habilidades em simulação de ameaças avançadas, replicando as táticas, técnicas e procedimentos mais comumente usados por agentes mal-intencionados. Além disso, a abordagem inovadora da TECH garantirá a aquisição de habilidades aplicáveis e valiosas no ambiente de trabalho de cibersegurança.

A metodologia do percurso acadêmico reforça seu caráter inovador, pois oferecerá um ambiente educacional 100% online. Esse programa será adaptado às necessidades de profissionais ocupados que buscam avançar em suas carreiras. Além disso, usará a metodologia *Relearning*, baseado na repetição de conceitos-chave para fixar o conhecimento e facilitar o aprendizado. Dessa forma, a combinação de flexibilidade e uma abordagem pedagógica robusta não só o tornará acessível, mas também altamente eficaz na preparação de cientistas da computação para os desafios dinâmicos da cibersegurança.

Este **Mestrado Próprio em Pentesting e Red Team** conta com o conteúdo mais completo e atualizado do mercado. Suas principais características são:

- O desenvolvimento de estudos de caso apresentados por especialistas em Pentesting e Red Team
- Os conteúdos gráficos, esquemáticos e extremamente práticos fornece informação atualizada e prática sobre aquelas disciplinas essenciais para o exercício da profissão
- Exercícios práticos onde o processo de autoavaliação é realizado para melhorar a aprendizagem
- Destaque especial para as metodologias inovadoras
- Lições teóricas, perguntas a especialistas, fóruns de discussão sobre temas controversos e trabalhos de reflexão individual
- Disponibilidade de acesso a todo o conteúdo a partir de qualquer dispositivo, fixo ou portátil, com conexão à Internet

Em apenas 12 meses, você dará à sua carreira o impulso de que ela precisa. Matricule-se agora e experimente o progresso imediato!"

Você quer experimentar um avanço de qualidade em sua carreira? Com a TECH, você será capacitado na implementação de estratégias para a execução eficaz de projetos de cibersegurança"

Você aprenderá mais sobre como identificar e avaliar vulnerabilidades em aplicativos da Web, graças à melhor universidade digital do mundo, de acordo com a Forbes.

Você dominará as técnicas forenses em ambientes de pentesting. Posicione-se como o especialista em cibersegurança que todas as empresas estão procurando!

A equipe de professores deste programa inclui profissionais desta área, cuja experiência é somada a esta capacitação, além de reconhecidos especialistas de conceituadas sociedades científicas e universidades de prestigio.

O conteúdo multimídia, desenvolvido com a mais recente tecnologia educacional, permitirá ao profissional uma aprendizagem contextualizada, ou seja, realizada através de um ambiente simulado, proporcionando uma capacitação imersiva e programada para praticar diante de situações reais.

A estrutura deste programa se concentra na Aprendizagem Baseada em Problemas, onde o profissional deverá tentar resolver as diferentes situações de prática profissional que surgirem ao longo do curso acadêmico. Para isso, contará com a ajuda de um inovador sistema de vídeo interativo realizado por especialistas reconhecidos.

02

Objetivos

O principal objetivo desse programa acadêmico é capacitar os alunos em testes de penetração e simulações de *Red Team*. Ao longo do programa, os cientistas da computação estarão imersos em uma abordagem prática e especializada, desenvolvendo habilidades para lidar com a identificação e a exploração de vulnerabilidades em sistemas e redes. Além disso, esse plano de estudos foi desenvolvido para oferecer uma compreensão aprofundada das táticas e estratégias de cibersegurança, preparando os alunos para enfrentar os desafios do mundo real e liderar a implementação eficaz de medidas de cibersegurança.

Você aprofundará seu conhecimento sobre análise e desenvolvimento de malware para se posicionar como um profissional líder. Alcance seus objetivos com a TECH!"

Objetivos gerais

- Adquirir habilidades avançadas em testes de penetração e simulações de *Red Team*, abordando a identificação e a exploração de vulnerabilidades em sistemas e redes
- Desenvolver habilidades de liderança para coordenar equipes especializadas em cibersegurança ofensiva, otimizando a execução de projetos de *Pentesting* e *Red Team*.
- Desenvolver habilidades na análise e no desenvolvimento de malware, compreendendo sua funcionalidade e aplicando estratégias defensivas e educacionais.
- Aperfeiçoar as habilidades de comunicação produzindo relatórios técnicos e executivos detalhados, apresentando as descobertas de forma eficaz para públicos técnicos e executivos.
- Promover a prática ética e responsável no campo da cibersegurança, considerando os princípios éticos e legais em todas as atividades.
- Manter os alunos atualizados com as tendências e tecnologias emergentes em cibersegurança.

Você alcançará seus objetivos graças às ferramentas didáticas da TECH, incluindo vídeos explicativos e resumos interativos"

Objetivos específicos

Módulo 1. Segurança ofensiva

- Familiarizar o aluno com as metodologias de teste de penetração, incluindo as principais fases, como coleta de informações, análise de vulnerabilidade, exploração e documentação
- Desenvolver habilidades práticas no uso de ferramentas especializadas de *pentesting* para identificar e avaliar vulnerabilidades em sistemas e redes
- Estudar e compreender as táticas, técnicas e procedimentos usados por agentes mal-intencionados, permitindo a identificação e a simulação de ameaças
- Aplicar os conhecimentos teóricos em cenários práticos e simulações, enfrentando desafios reais, a fim de fortalecer as habilidades de *Pentesting*
- Desenvolver habilidades eficazes de documentação, criando relatórios detalhados que reflitam as descobertas, as metodologias usadas e as recomendações para o aperfeiçoamento da segurança
- Praticar a colaboração eficaz em equipes de segurança ofensiva, otimizando a coordenação e a execução de atividades de *pentesting*

Módulo 2. Gerenciamento de Equipes de Cibersegurança

- Desenvolver habilidades de liderança específicas para equipes de cibersegurança, incluindo a capacidade de motivar, inspirar e coordenar esforços para atingir objetivos comuns
- Aprender a alocar recursos de forma eficiente em uma equipe de cibersegurança, levando em conta as habilidades individuais e maximizando a produtividade do projeto
- Aprimorar as habilidades de comunicação específicas de ambientes técnicos, facilitando a compreensão e a coordenação entre os membros da equipe
- Aprender estratégias para identificar e gerenciar conflitos na equipe de cibersegurança, promovendo um ambiente de trabalho colaborativo e eficiente

- Aprender como estabelecer métricas e sistemas de avaliação para medir o desempenho da equipe de cibersegurança e fazer ajustes conforme necessário
- Promover a integração de práticas éticas na gestão das equipes de cibersegurança, garantindo que todas as atividades sejam conduzidas de forma ética e legal
- Desenvolver competências para a preparação e a gestão eficiente de incidentes de cibersegurança, garantindo uma resposta rápida e eficaz às ameaças cibernéticas

Módulo 3. Gestão de Projetos de Segurança

- Desenvolver habilidades para planejar projetos de cibersegurança, definindo objetivos, escopo, recursos e cronogramas para implementação
- Aprender estratégias para a execução eficaz de projetos de segurança, garantindo a implementação bem-sucedida das medidas planejadas
- Desenvolver habilidades para a gestão eficiente de orçamentos e alocação de recursos em projetos de segurança, maximizando a eficácia e minimizando os custos
- Melhorar a comunicação eficaz com as partes *stakeholders*, fornecendo relatórios e atualizações claros e compreensíveis
- Aprender técnicas de monitoramento e controle de projetos, identificando desvios e tomando medidas corretivas conforme necessário
- Familiarizar os alunos com as metodologias ágeis de *pentesting*
- Desenvolver habilidades em documentação e relatórios detalhados, fornecendo uma visão clara do progresso do projeto e dos resultados alcançados
- Promover a colaboração eficaz entre diferentes equipes e disciplinas em projetos de segurança, garantindo uma abordagem integrada e coordenada
- Aprender estratégias para avaliar e medir a eficácia das medidas implementadas, garantindo a melhoria contínua da postura de segurança da organização

Módulo 4. Ataques a Redes e Sistemas Windows

- Desenvolver habilidades para identificar e avaliar vulnerabilidades específicas nos sistemas operacionais Windows
- Aprenda as táticas avançadas usadas pelos atacantes para se infiltrar e persistir em redes baseadas no Windows
- Adquirir habilidades em estratégias e ferramentas para atenuar ameaças específicas direcionadas aos sistemas operacionais Windows
- Familiarizar o aluno com as técnicas de análise forense aplicadas aos sistemas Windows, facilitando a identificação e a resposta a incidentes
- Aplicar o conhecimento teórico em ambientes simulados, participando de exercícios práticos para entender e combater ataques específicos a sistemas Windows
- Aprender estratégias específicas para proteger ambientes corporativos usando sistemas operacionais Windows, levando em consideração as complexidades das infraestruturas corporativas
- Desenvolver competências para avaliar e melhorar as configurações de segurança em sistemas Windows, garantindo a implementação de medidas eficazes
- Promover práticas éticas e legais na execução de ataques e testes em sistemas Windows, considerando os princípios éticos da cibersegurança
- Manter o aluno atualizado com as últimas tendências e ameaças em ataques a sistemas Windows, garantindo a relevância e a eficácia contínuas das habilidades adquiridas

Módulo 5. *Hacking* Web Avançado

- Desenvolver habilidades para identificar e avaliar vulnerabilidades em aplicativos da Web, incluindo injeções de SQL, *Cross-Site Scripting* (XSS) e outros vetores de ataque comuns
- Aprender como realizar testes de segurança em aplicativos modernos da Web
- Adquirir habilidades em técnicas avançadas de hacking na Web, explorando estratégias para contornar medidas de segurança e explorar vulnerabilidades sofisticadas
- Familiarizar o aluno com a avaliação da segurança em APIs e serviços da Web, identificando possíveis vulnerabilidades e reforçando a segurança em interfaces de programação
- Desenvolver habilidades para implementar medidas eficazes de atenuação em aplicativos da Web, reduzindo a exposição a ataques e reforçando a segurança
- Participar de simulações práticas para avaliar a segurança em ambientes complexos da Web, aplicando o conhecimento em situações do mundo real
- Desenvolver competências na formulação de estratégias de defesa eficazes para proteger os aplicativos da Web contra ameaças cibernéticas
- Aprender a alinhar as práticas avançadas de *hacking na Web* com as regulamentações e os padrões de segurança relevantes, garantindo a adesão a estruturas legais e éticas
- Promover a colaboração eficaz entre as equipes de desenvolvimento e segurança

Módulo 6. Arquitetura e Segurança em Redes

- Adquirir conhecimentos avançados de arquitetura de rede, incluindo topologias, protocolos e componentes principais
- Desenvolver habilidades para identificar e avaliar vulnerabilidades específicas em infraestruturas de rede, considerando as possíveis ameaças
- Aprender como implementar medidas eficazes de segurança de rede, incluindo *firewalls*, sistemas de detecção de intrusão (IDS) e segmentação de rede
- Familiarizar o aluno com as tecnologias de rede emergentes, como a rede definida por software (SDN), e entender seu impacto sobre a segurança
- Desenvolver habilidades para proteger as comunicações em redes, incluindo proteção contra ameaças, como *ataques de sniffing* e ataques de intermediários
- Aprender como avaliar e aprimorar as configurações de segurança em ambientes de rede corporativa, garantindo a proteção adequada
- Desenvolver habilidades para implementar medidas eficazes de atenuação contra ameaças às redes corporativas, desde ataques internos até ameaças externas
- Promover a colaboração eficaz com as equipes de segurança, integrando estratégias e esforços para proteger a infraestrutura de rede
- Promover práticas éticas e legais na implementação de medidas de segurança de rede, garantindo a adesão a princípios éticos em todas as atividades

Módulo 7. Análise e Desenvolvimento de *Malware*

- Adquirir conhecimentos avançados sobre a natureza, a funcionalidade e o comportamento do *malware*, compreender suas várias formas e objetivos
- Desenvolver habilidades em análise forense aplicadas ao *malware*, permitindo a identificação de indicadores de comprometimento (IoC) e padrões de ataque
- Aprender estratégias para detecção e prevenção eficazes de malware, incluindo a implementação de soluções avançadas de segurança
- Familiarizar o aluno com o desenvolvimento de *malware* para fins educacionais e defensivos, permitindo uma compreensão completa das táticas usadas pelos atacantes
- Promover práticas éticas e legais na análise e no desenvolvimento de *malware*, garantindo a integridade e a responsabilidade em todas as atividades
- Aplicar o conhecimento teórico em ambientes simulados, participar de exercícios práticos para entender e combater ataques maliciosos
- Desenvolver habilidades para avaliar e selecionar ferramentas de segurança *anti-malware*, considerando sua eficácia e adaptabilidade a ambientes específicos
- Aprender a implementar uma atenuação eficaz contra ameaças mal-intencionadas, reduzindo o impacto e a disseminação de ameaças de *malware* em sistemas e redes
- Promover a colaboração eficaz com as equipes de segurança, integrando estratégias e esforços para proteger contra ameaças de *Malware*
- Manter o aluno atualizado com as últimas tendências e técnicas usadas na análise e no desenvolvimento de *malware*, assegurando a relevância e a eficácia contínuas das habilidades adquiridas

Módulo 8. Fundamentos forenses e DFIR

- Adquirir uma sólida compreensão dos princípios fundamentais da Investigação Forense Digital (DFIR) e sua aplicação na resolução de incidentes cibernéticos
- Desenvolver habilidades na aquisição segura e forense de evidências digitais, garantindo a preservação da cadeia de custódia
- Aprender a realizar análise forense de sistemas de arquivos
- Familiarizar o aluno com técnicas avançadas para a análise de logs e registros, permitindo a reconstrução de eventos em ambientes digitais
- Aprender a aplicar metodologias de investigação forense digital na resolução de casos, desde a identificação até a documentação das descobertas
- Familiarizar o aluno com a análise de evidências digitais e a aplicação de técnicas forenses em *Pentesting*
- Desenvolver habilidades na preparação de relatórios forenses detalhados e claros, apresentando descobertas e conclusões de forma compreensível
- Promover a colaboração eficaz com as equipes de resposta a incidentes (IR), otimizando a coordenação na investigação e mitigação de ameaças
- Promover práticas éticas e legais em perícia digital, garantindo a adesão às normas de cibersegurança e aos padrões de conduta

Módulo 9. Exercícios de *Rede Team* Avançados

- Desenvolver habilidades em simulação de ameaças avançadas, replicando táticas, técnicas e procedimentos (TTPs) usados por agentes mal-intencionados atraentes
- Aprender a identificar pontos fracos e vulnerabilidades na infraestrutura por meio de exercícios realistas de *Red Team*, fortalecendo a postura de segurança
- Familiarizar o aluno com técnicas avançadas de evasão de segurança, permitindo a avaliação da resistência da infraestrutura a ataques desejáveis
- Desenvolver habilidades eficazes de coordenação e colaboração entre os membros da equipe de *Red Team*, otimizando a execução de táticas e estratégias para avaliar de forma abrangente a segurança da organização
- Aprender a simular cenários de ameaças atuais, como ataques de *ransomware* ou campanhas avançadas de phishing, para avaliar a capacidade da organização de responder a organização
- Familiarizar o aluno com as técnicas de análise pós-exercício, avaliando o desempenho da equipe de *Red Team* e extraindo as lições aprendidas para melhorias contínuas
- Desenvolver habilidades para avaliar a resiliência organizacional a ataques simulados, identificando áreas para aprimoramento de políticas e procedimentos
- Aprender a preparar relatórios detalhados que documentem as descobertas, as metodologias usadas e as recomendações derivadas de *Red Team* avançados
- Promover práticas éticas e legais na condução de exercícios de *Red Team*, assegurando a adesão às normas de cibersegurança e aos padrões éticos

Módulo 10. Relatório técnico e executivo

- Desenvolver habilidades para produzir relatórios técnicos detalhados, apresentando de forma clara e abrangente as descobertas, as metodologias usadas e as recomendações
- Aprender a se comunicar de forma eficaz com públicos técnicos, usando linguagem precisa e apropriada para transmitir informações técnicas complexas
- Desenvolver habilidades para formular recomendações práticas e acionáveis destinadas a atenuar as vulnerabilidades e melhorar a postura de segurança
- Aprender a avaliar o impacto potencial das vulnerabilidades identificadas, considerando aspectos técnicos, operacionais e estratégicos
- Familiarizar o aluno com as práticas recomendadas para relatórios executivos, adaptando informações técnicas para públicos não técnicos
- Desenvolver competências para alinhar as conclusões e recomendações com os objetivos estratégicos e operacionais da organização
- Aprender a usar ferramentas de visualização de dados para representar graficamente as informações contidas nos relatórios, facilitando a compreensão
- Promover a inclusão de informações relevantes sobre a conformidade com regulamentos e padrões nos relatórios, garantindo a adesão aos requisitos legais
- Promover a colaboração eficaz entre as equipes técnicas e executivas, garantindo a compreensão e o apoio às ações de melhoria propostas no relatório

03

Competências

Graças a este plano de estudos, os alunos serão capacitados com habilidades especializadas para implementar medidas de defesa ativa, fortalecendo a segurança de sistemas e redes com base nas práticas recomendadas de cibersegurança. Além disso, os alunos adquirirão competências avançadas em testes de penetração e simulação de *Red Team*, destacando-se na identificação proativa e na mitigação de vulnerabilidades. Nesse sentido, os profissionais dominarão as habilidades técnicas necessárias para lidar com ameaças do mundo real, preparando-os para liderar estratégias eficazes de avaliação e fortificação da segurança em ambientes cibernéticos dinâmicos. Além disso, a abordagem 100% online torna o aprendizado mais flexível.

Torne-se um especialista em cibersegurança por meio de 1.500 horas do melhor conteúdo multimídia, com o selo de qualidade da TECH"

Competências gerais

- Adquirir competências no planejamento, na execução e na gestão de projetos de cibersegurança, garantindo resultados eficazes e o cumprimento dos objetivos
- Adquirir conhecimentos avançados em arquitetura de rede e seus aspectos de segurança, avaliando as vulnerabilidades e aplicando estratégias para fortalecer a infraestrutura
- Desenvolver competências em perícia digital e resposta a incidentes, desde a coleta de evidências até a mitigação de ameaças e a restauração operacional
- Aplicar táticas avançadas no planejamento e na execução de exercícios de *Red Team*, simular cenários do mundo real para avaliar a resistência da infraestrutura, detectar pontos fracos e melhorar a preparação para ameaças cibernéticas

Atualize-se sobre o processo de identificação, avaliação e mitigação de riscos específicos para projetos de segurança cibernética. Estude na TECH!

Competências específicas

- Adquirir habilidades de coaching para o desenvolvimento profissional dos membros da equipe, promovendo o crescimento e o aprimoramento
- Desenvolver habilidades de tomada de decisões estratégicas em situações de cibersegurança, considerando o impacto de curto e longo prazo na segurança organizacional
- Adquirir competências na identificação, avaliação e atenuação de riscos específicos de projetos de cibersegurança
- Desenvolver habilidades para implementar medidas de defesa ativa, fortalecendo a segurança de sistemas e redes
- Aprender técnicas de análise de tráfego da Web para identificar padrões e comportamentos anômalos, facilitando a detecção de possíveis ameaças
- Adquirir habilidades em análise forense aplicada a ambientes de rede, permitindo a identificação e a resposta eficazes a incidentes cibernéticos
- Aprender estratégias para detecção e prevenção eficazes de malware, incluindo a implementação de soluções avançadas de segurança
- Desenvolver habilidades na identificação de indicadores de comprometimento (IoC) durante a investigação forense, facilitando a detecção e a resposta a incidentes
- Adquirir habilidades para o planejamento estratégico de exercícios de *Red Team*, considerando objetivos, escopo, recursos e cenários realistas
- Adquirir habilidades na identificação e priorização de vulnerabilidades, destacando aquelas que representam os maiores riscos à segurança

04

Direção do curso

Para a formação do corpo docente do Mestrado Próprio em Pentesting e Red Team, a TECH reuniu os melhores especialistas, que possuem uma extensa e reconhecida trajetória profissional em empresas líderes do setor. Nesse sentido, cada membro da equipe de professores contribuirá com sua experiência prática e conhecimento especializado, garantindo que os alunos se beneficiem do ensino de profissionais altamente qualificados. Além disso, a seleção cuidadosa desses especialistas garantirá não apenas a qualidade acadêmica, mas também a relevância e a aplicabilidade imediata do conteúdo no ambiente dinâmico da cibersegurança.

Os gigantes do setor de segurança cibernética lhe ajudarão a atingir o sucesso em apenas 12 meses com este programa universitário exclusivo da TECH"

Direção

Sr. Carlos Gómez Pintado

- Gerente de cibersegurança e Red Team Cipherbit no Grupo Oesía
- Gestor Advisor & Investor na Wesson App
- Formado em Engenharia de Software e Tecnologias da Sociedade da Informação pela Universidade Politécnica de Madri
- Colaboração com instituições educacionais para o desenvolvimento de ciclos de formação de nível superior em cibersegurança

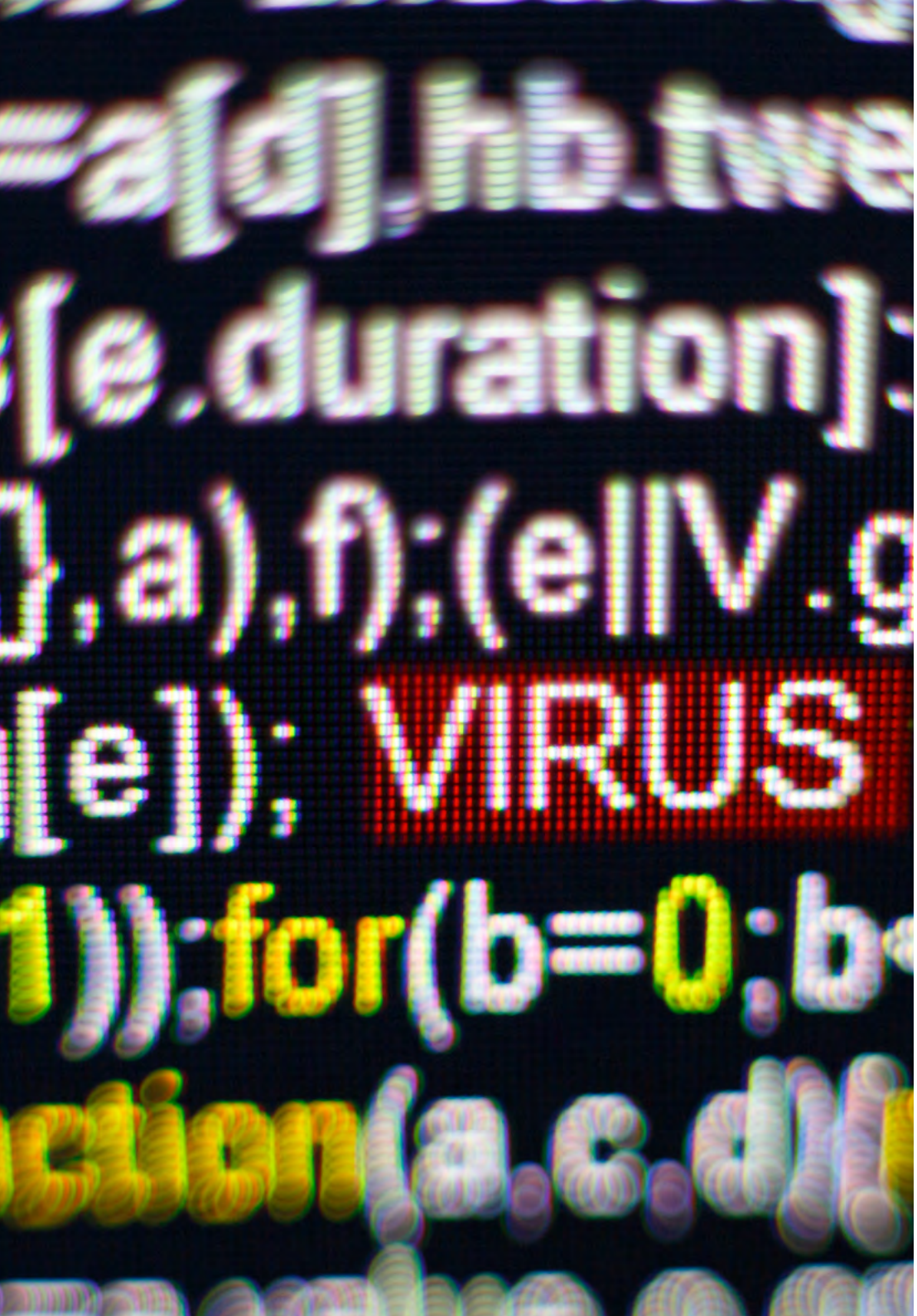
Professores

Sr. Marcelino Siles Rubia

- Cibersecurity Engineer
- Engenharia de Cibersegurança na Universidade Rey Juan Carlos
- Conhecimentos Programação Competitiva, *Hacking Web, Active Directory e Malware Development*
- Vencedor do concurso AdaByron

Sr. Pablo Redondo Castro

- Pentester no Grupo Oesía
- Engenheiro de cibersegurança, Universidade Rey Juan Carlos, Madri
- Ampla experiência como *Cibersecurity Evaluator Traineev*
- Ele acumula experiência de ensino, ministrando capacitações relacionadas a torneios de Capture The Flag



Sr. Alejandro Gallego Sánchez

- Consultor de Cibersegurança na Integración Tecnológica Empresarial, S.L.
- Técnico Audiovisual na Ingeniería Audiovisual S.A.
- Formado em Engenharia de Cibersegurança pela Universidade Rey Juan Carlos

Sr. Marcos González Sanz

- Cybersecurity Consultant-Red Teamer Cipherbit no Grupo Oesía
- Engenheiro de Software pela Universidade Politécnica de Madri
- Especialista em Cybersecurity Tutor e Core Dumped

Sr. Sergio Mora Navas

- Consultor de Cibersegurança no Grupo Oesía
- Engenheiro de Cibersegurança, Universidade Rey Juan Carlos, Madri.
  Engenheiro da Computação pela Universidade de Burgos

Sr. Yuba González Parrilla

- Coordenador da linha de segurança ofensiva e red team
- Especialista em gestão de projetos *Predictive* no Project Management Institute
- Especialista em *SmartDefense*
- Especialista em *Web Application Penetration Tester* no eLearnSecurity
- *Junior Penetration Tester* no eLearnSecurity
- Graduado em Engenharia da Computação pela Universidade Politécnica de Madri

05

Estrutura e conteúdo

Esse programa universitário oferece uma imersão completa nas disciplinas cruciais de testes de penetração e simulações de *Red Team*. Ao longo do curso, os alunos desenvolverão habilidades avançadas para identificar e explorar vulnerabilidades em sistemas e redes, usando técnicas e ferramentas modernas. Essa capacitação, projetada com um enfoque prático, este programa equipará os profissionais de cibersegurança para enfrentar os desafios do mundo real. Nesse sentido, os alunos se beneficiarão de uma combinação exclusiva de teoria e prática, orientada por especialistas do setor, para fortalecer seu entendimento e implementar com eficácia estratégias de avaliação de segurança em ambientes cibernéticos.

Você obterá uma compreensão profunda das diferentes funções e responsabilidades da equipe de cibersegurança. Matricule-se já!"

Módulo 1. Segurança ofensiva

1.1. Definição e contexto
- 1.1.1. Conceitos fundamentais de segurança ofensiva
- 1.1.2. A importância da cibersegurança na atualidade
- 1.1.3. Desafios e oportunidades na segurança ofensiva

1.2. Fundamentos da cibersegurança
- 1.2.1. Desafios iniciais e evolução das ameaças
- 1.2.2. Marcos tecnológicos e seu impacto na cibersegurança
- 1.2.3. Cibersegurança na era moderna

1.3. Base da segurança ofensiva
- 1.3.1. Principais conceitos e terminologia
- 1.3.2. *Think Outside the Box*
- 1.3.3. Diferenças entre hacking ofensivo e defensivo

1.4. Metodologias de segurança ofensivas
- 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. Funções e responsabilidades na segurança ofensiva
- 1.5.1. Principais perfis
- 1.5.2. *Bug Bounty Hunters*
- 1.5.3. *Researching:* A arte da pesquisa

1.6. Arsenal do auditor ofensivo
- 1.6.1. Sistemas operacionais de *Hacking*
- 1.6.2. Introdução ao C2
- 1.6.3. *Metasploit*: Fundamentos e uso
- 1.6.4. Recursos úteis

1.7. OSINT Inteligência em Fontes Abertas
- 1.7.1. Fundamentos da OSINT
- 1.7.2. Técnicas e ferramentas de OSINT
- 1.7.3. Aplicativos OSINT em segurança ofensiva

1.8. *Scripting*: Introdução à automatização
- 1.8.1. Fundamentos de scripting
- 1.8.2. *Scripting* em Bash
- 1.8.3. *Scripting* em Python

1.9. Categorização de vulnerabilidades
- 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. Ética e *hacking*
- 1.10.1. Princípios de ética *hacker*
- 1.10.2. A linha entre *hacking* ético e *hacking* malicioso
- 1.10.3. Implicações e consequências legais
- 1.10.4. Estudos de caso: Situações éticas na cibersegurança

Módulo 2. Gerenciamento de Equipes de Cibersegurança

2.1. Gestão de equipes
- 2.1.1. Quem é quem
- 2.1.2. O gestor
- 2.1.3. Conclusões

2.2. Funções e responsabilidades
- 2.2.1. Identificação de função
- 2.2.2. Delegação eficaz
- 2.2.3. Gestão de expectativas

2.3. Formação e desenvolvimento de equipes
- 2.3.1. Estágios da formação de equipes
- 2.3.2. Dinâmicas de grupo
- 2.3.3. Avaliação e retroalimentação

2.4. Gestão de Talentos
  2.4.1. Identificação de talentos
  2.4.2. Desenvolvimento de capacidades
  2.4.3. Retenção de talentos
2.5. Liderança e motivação de equipes
  2.5.1. Estilos de liderança
  2.5.2. Teorias da motivação
  2.5.3. Reconhecimento de conquistas
2.6. Comunicação e coordenação
  2.6.1. Ferramentas de comunicação
  2.6.2. Obstáculos à comunicação
  2.6.3. Estratégias de coordenação
2.7. Planejamento estratégico de desenvolvimento de pessoal
  2.7.1. Identificação das necessidades de capacitação
  2.7.2. Planos de desenvolvimento individual
  2.7.3. Monitoramento e avaliação
2.8. Resolução de conflitos
  2.8.1. Identificação de conflitos
  2.8.2. Métodos de medição
  2.8.3. Prevenção de conflitos
2.9. Gestão de qualidade e melhoria contínua
  2.9.1. Princípios de qualidade
  2.9.2. Técnicas de aprimoramento contínuo
  2.9.3. *Feedback* e retroalimentação
2.10. Ferramentas e tecnologias
  2.10.1. Plataformas colaborativas
  2.10.2. Gerenciamento de projetos
  2.10.3. Conclusões

Módulo 3. Gestão de Projetos de Segurança

3.1. Gestão de projetos de segurança
  3.1.1. Definição e propósito da gestão de projetos de cibersegurança
  3.1.2. Principais desafios
  3.1.3. Considerações
3.2. Ciclo de vida de um projeto de segurança
  3.2.1. Estágios iniciais e definição de objetivos
  3.2.2. Implementação e execução
  3.2.3. Avaliação e revisão
3.3. Planejamento e estimativa de recursos
  3.3.1. Conceitos básicos de gestão econômica
  3.3.2. Determinação de recursos humanos e e técnicos
  3.3.3. Orçamento e custos associados
3.4. Implementação e monitoramento de projetos
  3.4.1. Monitoramento e acompanhamento
  3.4.2. Adaptação e mudanças no projeto
  3.4.3. Avaliação intermediária e revisões
3.5. Comunicação e relatórios do projeto
  3.5.1. Estratégias efetivas de comunicação
  3.5.2. Preparação de relatórios e apresentações
  3.5.3. Comunicação com o cliente e a gestão
3.6. Ferramentas e tecnologias
  3.6.1. Ferramentas de planejamento e organização
  3.6.2. Ferramentas de colaboração e comunicação
  3.6.3. Ferramentas de documentação e armazenamento
3.7. Documentação e protocolos
  3.7.1. Estruturação e criação de documentação
  3.7.2. Protocolos de ação
  3.7.3. Guias
3.8. Regulamentos e conformidade em projetos de cibersegurança
  3.8.1. Leis e regulamentos internacionais
  3.8.2. Conformidade
  3.8.3. Auditorias

3.9. Gerenciamento de risco do projeto de segurança
- 3.9.1. Identificação e análise de riscos
- 3.9.2. Estratégias de mitigação
- 3.9.3. Monitoramento e revisão de riscos

3.10. Encerramento do projeto
- 3.10.1. Revisão e avaliação
- 3.10.2. Documentação final
- 3.10.3. Feedback

Módulo 4. Ataques a Redes e Sistemas Windows

4.1. Windows e Diretório Ativo
- 4.1.1. História e evolução do Windows
- 4.1.2. Noções básicas sobre o Diretório Ativo
- 4.1.3. Funções e serviços do Diretório Ativo
- 4.1.4. Arquitetura geral do Diretório Ativo

4.2. Redes em ambientes de Diretório Ativo
- 4.2.1. Protocolos de rede no Windows
- 4.2.2. DNS e seu funcionamento no Diretório Ativo
- 4.2.3. Ferramentas de diagnóstico de rede
- 4.2.4. Implementação de redes no Diretório Ativo

4.3. Autenticação e autorização no Diretório Ativo
- 4.3.1. Processo e fluxo de autenticação
- 4.3.2. Tipos de credenciais
- 4.3.3. Armazenamento e gestão de credenciais
- 4.3.4. Segurança de autenticação

4.4. Permissões e políticas no Diretório Ativo
- 4.4.1. GPOs
- 4.4.2. Implementação e gestão de GPOs
- 4.4.3. Gestão de licenças no Diretório Ativo
- 4.4.4. Vulnerabilidades e mitigações em licenças

4.5. Noções básicas do Kerberos
- 4.5.1. O que é o Kerberos?
- 4.5.2. Componentes e funcionamento
- 4.5.3. Tickets no Kerberos
- 4.5.4. Kerberos no contexto do Diretório Ativo

4.6. Técnicas avançadas do Kerberos
- 4.6.1. Ataques comuns do Kerberos
- 4.6.2. Mitigações e proteções
- 4.6.3. Monitoramento de tráfego Kerberos
- 4.6.4. Ataques avançados do Kerberos

4.7. *Active Directory Certificate Services* (ADCS)
- 4.7.1. Noções básicas de PKI
- 4.7.2. Funções e componentes do ADCS
- 4.7.3. Configuração e implantação do ADCS
- 4.7.4. Segurança em ADCS

4.8. Ataques e defesas em *Active Directori Certificate Services* (ADCS)
- 4.8.1. Vulnerabilidades comuns no ADCS
- 4.8.2. Ataques e técnicas de exploração
- 4.8.3. Defesas e mitigações
- 4.8.4. Monitoramento e auditoria de ADCS

4.9. Auditoria do Diretório Ativo
- 4.9.1. Importância da auditoria no Diretório Ativo
- 4.9.2. Ferramentas de auditoria
- 4.9.3. Detecção de anomalias e comportamentos suspeitos
- 4.9.4. Resposta a incidentes e recuperação

4.10. Azure AD.
- 4.10.1. Fundamentos do Azure AD
- 4.10.2. Sincronização com o diretório ativo local
- 4.10.3. Gestão de identidades no Azure AD
- 4.10.4. Integração com aplicativos e serviços

Módulo 5. *Hacking* Web Avançado

5.1. Funcionamento de um site
- 5.1.1. O URL e suas partes
- 5.1.2. Métodos HTTP
- 5.1.3. Os cabeçalhos
- 5.1.4. Como visualizar solicitações da Web com o Burp Suite

5.2. Sessões
- 5.2.1. Os *cookies*
- 5.2.2. *Tokens* JWT
- 5.2.3. Ataques de sequestro de sessão
- 5.2.4. Ataques a JWT

5.3. *Cross Site Scripting* (XSS)
- 5.3.1. O que é um XSS
- 5.3.2. Tipos de XSS
- 5.3.3. Exploração de um XSS
- 5.3.4. Introdução ao *XSLeaks*

5.4. Injeções de banco de dados
- 5.4.1. O que é um *SQL Injection*
- 5.4.2. Extração de informações com *SQLi*
- 5.4.3. *SQLi Blind, Time-Based* e *Error-Based*
- 5.4.4. Injeções de NoSQLi

5.5. *Path Traversal* e *Local File Inclusion*
- 5.5.1. O que são e suas diferenças
- 5.5.2. Filtros comuns e como contorná-los
- 5.5.3. *Log Poisoning*
- 5.5.4. LFIs em PHP

5.6. *Broken Authentication*
- 5.6.1. *User Enumeration*
- 5.6.2. *Password Bruteforce*
- 5.6.3. *2FA Bypass*
- 5.6.4. *Cookies* com informações sensíveis e modificáveis

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 em uploads de arquivos
- 5.8.3. XML *External Entity* (XXE) *Injection*
- 5.8.4. *Path traversal* em uploads de arquivos

5.9. *Broken Acess Control*
- 5.9.1. Acesso aos painéis sem restrição
- 5.9.2. *Insecure Direct Object References* (IDOR)
- 5.9.3. Bypass de filtros
- 5.9.4. Métodos de autorização insuficientes

5.10. Vulnerabilidades do DOM e ataques mais avançados
- 5.10.1. *Regex Denial of Service*
- 5.10.2. DOM *Clobbering*
- 5.10.3. *Prototype Pollution*
- 5.10.4. HTTP *Request Smuggling*

Módulo 6. Arquitetura e Segurança em Redes

6.1. Redes de computadores
- 6.1.1. Conceitos básicos Protocolos LAN, WAN, CP, CC
- 6.1.2. Modelo OSI TCP/IP
- 6.1.3. *Switching:* Conceitos básicos
- 6.1.4. *Routing:* Conceitos básicos

6.2. *Switching:*
- 6.2.1. Introdução às VLANs
- 6.2.2. STP
- 6.2.3. *EtherChannel*
- 6.2.4. Ataques à camada 2

6.3. VLAN´s
- 6.3.1. Importância das VLANs
- 6.3.2. Vulnerabilidades em VLANs
- 6.3.3. Ataques comuns a VLANs
- 6.3.4. Mitigações

6.4. *Routing*
- 6.4.1. Endereçamento IP - IPv4 e IPv6
- 6.4.2. Roteamento: Conceitos fundamentais
- 6.4.3. Roteamento estático
- 6.4.4. Roteamento dinâmico: Introdução

6.5. Protocolos IGP
- 6.5.1. RIP
- 6.5.2. OSPF
- 6.5.3. RIP vs OSPF
- 6.5.4. Análise das necessidades de topologia

6.6. Proteção do perímetro
- 6.6.1. DMZs
- 6.6.2. *Firewalls*
- 6.6.3. Arquiteturas comuns
- 6.6.4. *Zero Trust Network Access*

6.7. IDS e IPS
- 6.7.1. Características
- 6.7.2. Implementação
- 6.7.3. SIEM e SIEM CLOUDS
- 6.7.4. Detecção baseada em *HoneyPots*

6.8. TLS e VPN´s
- 6.8.1. SSL/ TLS
- 6.8.2. TLS: Ataques comuns
- 6.8.3. VPNs com TLS
- 6.8.4. VPNs com IPSEC

6.9. Segurança em redes sem fio
- 6.9.1. Introdução às redes sem fio
- 6.9.2. Protocolos
- 6.9.3. Elementos fundamentais
- 6.9.4. Ataques comuns

6.10. Redes empresariais e como lidar com elas
- 6.10.1. Segmentação lógica
- 6.10.2. Segmentação física
- 6.10.3. Controle de acesso
- 6.10.4. Outras considerações

Módulo 7. Análise e Desenvolvimento de *Malware*

7.1. Análise e Desenvolvimento de *Malware*
- 7.1.1. História e evolução do *malware*
- 7.1.2. Classificação e tipos de *Malware*
- 7.1.3. Análises de *malware*
- 7.1.4. Desenvolvimento de *malware*

7.2. Preparação do ambiente
- 7.2.1. Configuração de máquina virtual e *Snapshots*
- 7.2.2. Ferramentas de análise de *malware*
- 7.2.3. Ferramentas de desenvolvimento de *malware*

7.3. Fundamentos do Windows
- 7.3.1. Formato do arquivo PE (*Portable Executable*)
- 7.3.2. Processos e *Threads*
- 7.3.3. Sistema de arquivos e registro
- 7.3.4. *Windows Defender*

7.4. Técnicas de Malware básicas
- 7.4.1. Geração de *shellcode*
- 7.4.2. Execução de *shellcode* no disco
- 7.4.3. Disco vs memória
- 7.4.4. Execução de shellcode na memória

7.5. Técnicas de malware intermediárias
- 7.5.1. Persistência no Windows
- 7.5.2. Pasta inicial
- 7.5.3. Chaves de registro
- 7.5.4. Protetores de tela

7.6. Técnicas de *malware* avançadas
- 7.6.1. Cifrado de *shellcode* (XOR)
- 7.6.2. Cifrado de *shellcode* (RSA)
- 7.6.3. Ofuscação de *strings*
- 7.6.4. Injeção de processos

7.7. Análise estática de ***malware***
- 7.7.1. Analisando *packers* com DIE (Detect It Easy)
- 7.7.2. Analisando seções com o PE-Bear
- 7.7.3. Descompilação com Ghidra

7.8. Análise dinâmica de ***malware***
- 7.8.1. Observando o comportamento com o Process Hacker
- 7.8.2. Análise de chamadas com o API Monitor
- 7.8.3. Análise de alterações no registro com o Regshot
- 7.8.4. Observação de solicitações de rede com o TCPView

7.9. Análise em .NET
- 7.9.1. Introdução ao .NET
- 7.9.2. Descompilação com o dnSpy
- 7.9.3. Depuração com o dnSpy

7.10. Analizando um *malware* real
- 7.10.1. Preparação do ambiente
- 7.10.2. Análise estática do *malware*
- 7.10.3. Análise dinâmica do *malware*
- 7.10.4. Criação de regras YARA

Módulo 8. Fundamentos forenses e DFIR

8.1. Forense digital
- 8.1.1. História e evolução da computação forense
- 8.1.2. Importância da computação forense na cibersegurança
- 8.1.3. História e evolução da computação forense

8.2. Fundamentos de informática forense
- 8.2.1. Cadeia de custódia e sua implementação
- 8.2.2. Tipos de evidência digital
- 8.2.3. Processos de aquisição de evidências

8.3. Sistemas de arquivos e estrutura de dados
- 8.3.1. Principais sistemas de arquivos
- 8.3.2. Métodos de ocultação de dados
- 8.3.3. Análise de metadados e atributos de arquivos

8.4. Análise de sistemas operacionais
- 8.4.1. Análise forense de sistemas Windows
- 8.4.2. Análise forense de sistemas Linux
- 8.4.3. Análise forense de sistemas macOS

8.5. Recuperação de dados e análise de disco
- 8.5.1. Recuperação de dados de mídias danificadas
- 8.5.2. Ferramentas de análise de disco
- 8.5.3. Interpretação de tabelas de alocação de arquivos

8.6. Análise de rede e tráfego
- 8.6.1. Captura e análise de pacotes de rede
- 8.6.2. Análise de registros de *firewall*
- 8.6.3. Detecção de intrusão de rede

8.7. Malware e análise de código malicioso
- 8.7.1. Classificação de *Malware* e suas características
- 8.7.2. Análise estática e dinâmica de *malware*
- 8.7.3. Técnicas de desmontagem e depuração

8.8. Análise de registros e eventos
- 8.8.1. Tipos de registros em sistemas e aplicativos
- 8.8.2. Interpretação de eventos relevantes
- 8.8.3. Ferramentas de análise de registros

8.9. Resposta a incidentes de segurança
- 8.9.1. Processo de resposta a incidentes
- 8.9.2. Criação de um plano de resposta a incidentes
- 8.9.3. Coordenação com equipes de segurança

8.10. Apresentação de evidências e questões legais
- 8.10.1. Regras de evidência digital no campo jurídico
- 8.10.2. Preparação de relatórios forenses
- 8.10.3. Comparecimento ao julgamento como testemunha especializada

Módulo 9. Exercícios de *Rede Team* Avançados

9.1. Técnicas avançadas de reconhecimento
- 9.1.1. Enumeração avançada de subdomínios
- 9.1.2. *Google Dorking* avançado
- 9.1.3. Redes Sociais e theHarvester

9.2. Campanhas de *phishing* avançadas
- 9.2.1. O que é *Reverse-Proxy Phishing*
- 9.2.2. *2FA Bypass* com Evilginx
- 9.2.3. Exfiltração de dados

9.3. Técnicas avançadas de persistência
- 9.3.1. *Golden Tickets*
- 9.3.2. *Silver Tickets*
- 9.3.3. Técnica *DCShadow*

9.4. Técnicas avançadas de evasão
- 9.4.1. Bypass de AMSI
- 9.4.2. Modificação de ferramentas existentes
- 9.4.3. Ofuscação de *Powershell*

9.5. Técnicas avançadas de movimento lateral
- 9.5.1. *Pass-the-Ticket* (PtT)
- 9.5.2. *Overpass-the-Hash* (Pass-the-Key)
- 9.5.3. NTLM Relay

9.6. Técnicas avançadas de pós-exploração
- 9.6.1. *Dump* de LSASS
- 9.6.2. *Dump* de SAM
- 9.6.3. Ataque *DCSync*

9.7. Técnicas avançadas de *pivoting*
- 9.7.1. O que él *pivoting*
- 9.7.2. Túneis com SSH
- 9.7.3. Pivoting com Chisel

9.8. Intrusões físicas
- 9.8.1. Vigilância e reconhecimento
- 9.8.2. *Tailgating* e *Piggybacking*
- 9.8.3. *Lock-Picking*

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

9.10. Ataques RFID
- 9.10.1. Leitura de cartões RFID
- 9.10.2. Manuseio de cartões RFID
- 9.10.3. Criação de cartões clonados

Módulo 10. Relatório técnico e executivo

10.1. Processo de relatório
- 10.1.1. Estrutura de um relatório
- 10.1.2. Processo de relatório
- 10.1.3. Conceitos fundamentais
- 10.1.4. Executivo x Técnico

10.2. Guias
- 10.2.1. Introdução
- 10.2.2. Tipos de guias
- 10.2.3. Guias nacionais
- 10.2.4. Casos de uso

10.3. Metodologias
- 10.3.1. Avaliação
- 10.3.2. *Pentesting*
- 10.3.3. Revisão de metodologias comuns
- 10.3.4. Introdução às metodologias nacionais

10.4. Abordagem técnica para a fase de relatório
- 10.4.1. Entendendo os limites do *pentester*
- 10.4.2. Uso e dicas de linguagem
- 10.4.3. Apresentação de informações
- 10.4.4. Erros mais comuns

10.5. Abordagem executiva para a fase de relatório
- 10.5.1. Ajustando o relatório ao contexto
- 10.5.2. Uso e dicas de linguagem
- 10.5.3. Padronização
- 10.5.4. Erros mais comuns

10.6. OSSTMM
- 10.6.1. Entendendo a metodologia
- 10.6.2. Reconhecimento
- 10.6.3. Documentação
- 10.6.4. Elaboração do relatório

10.7. LINCE
- 10.7.1. Entendendo a metodologia
- 10.7.2. Reconhecimento
- 10.7.3. Documentação
- 10.7.4. Elaboração do relatório

10.8. Relatório de vulnerabilidades
- 10.8.1. Conceitos fundamentais
- 10.8.2. Quantificação do escopo
- 10.8.3. Vulnerabilidades e evidências
- 10.8.4. Erros mais comuns

10.9. Focando o relatório no cliente
- 10.9.1. Importância da evidência do trabalho
- 10.9.2. Soluções e mitigações
- 10.9.3. Dados sensíveis e relevantes
- 10.9.4. Exemplos práticos e casos

10.10. Reportando *retakes*
- 10.10.1. Conceitos fundamentais
- 10.10.2. Compreensão das informações legadas
- 10.10.3. Verificação de erros
- 10.10.4. Adicionando informações

06

Metodologia

Este curso oferece uma maneira diferente de aprender. Nossa metodologia é desenvolvida através de um modo de aprendizagem cíclico: ***o Relearning***. Este sistema de ensino é utilizado, por exemplo, nas faculdades de medicina mais prestigiadas do mundo e foi considerado um dos mais eficazes pelas principais publicações científicas, como o ***New England Journal of Medicine.***

Descubra o Relearning, um sistema que abandona a aprendizagem linear convencional para realizá-la através de sistemas de ensino cíclicos: uma forma de aprendizagem que se mostrou extremamente eficaz, especialmente em disciplinas que requerem memorização"

Estudo de caso para contextualizar todo o conteúdo

Nosso programa oferece um método revolucionário para desenvolver as habilidades e o conhecimento. Nosso objetivo é fortalecer as competências em um contexto de mudança, competitivo e altamente exigente.

Com a TECH você irá experimentar uma forma de aprender que está revolucionando as bases das universidades tradicionais em todo o mundo"

Você terá acesso a um sistema de aprendizagem baseado na repetição, por meio de um ensino natural e progressivo ao longo de todo o programa.

Através de atividades de colaboração e casos reais, o aluno aprenderá a resolver situações complexas em ambientes reais de negócios.

Um método de aprendizagem inovador e diferente

Este curso da TECH é um programa de ensino intensivo, criado do zero, que propõe os desafios e decisões mais exigentes nesta área, em âmbito nacional ou internacional. Através desta metodologia, o crescimento pessoal e profissional é impulsionado em direção ao sucesso. O método do caso, técnica que constitui a base deste conteúdo, garante que a realidade econômica, social e profissional mais atual seja adotada.

> *Nosso programa prepara você para enfrentar novos desafios em ambientes incertos e alcançar o sucesso na sua carreira"*

O método do caso é o sistema de aprendizagem mais utilizado nas principais escolas de Informática do mundo, desde que elas existem. Desenvolvido em 1912 para que os estudantes de Direito não aprendessem a lei apenas com base no conteúdo teórico, o método do caso consistia em apresentar-lhes situações realmente complexas para que tomassem decisões conscientes e julgassem a melhor forma de resolvê-las. Em 1924 foi estabelecido como o método de ensino padrão em Harvard.

Em uma determinada situação, o que um profissional deveria fazer? Esta é a pergunta que abordamos no método do caso, um método de aprendizagem orientado para a ação. Ao longo do curso, os alunos vão se deparar com múltiplos casos reais. Terão que integrar todo o conhecimento, pesquisar, argumentar e defender suas ideias e decisões.

Metodologia Relearning

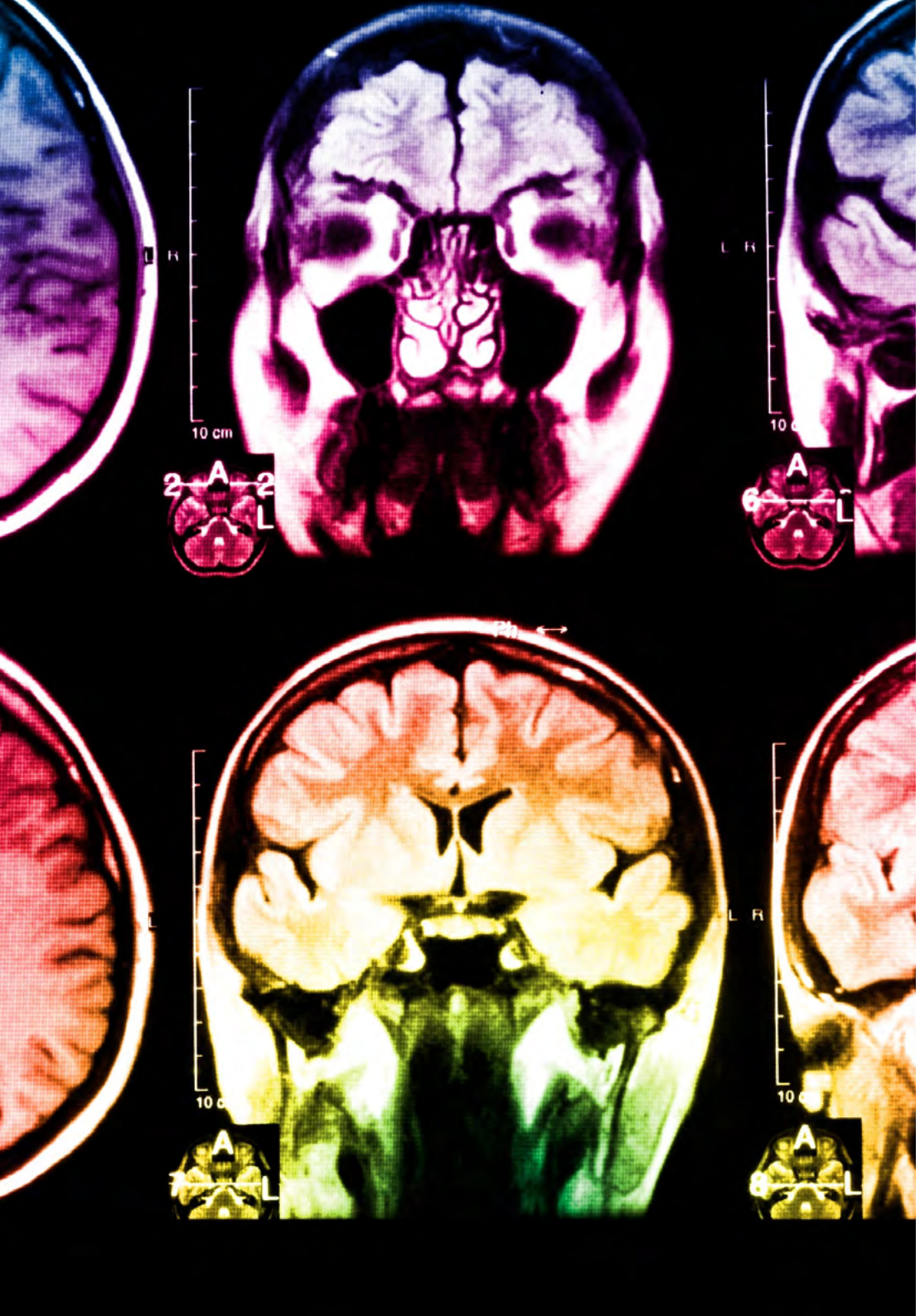
A TECH utiliza de maneira eficaz a metodologia do estudo de caso com um sistema de aprendizagem 100% online, baseado na repetição, combinando elementos didáticos diferentes em cada aula.

Potencializamos o Estudo de Caso com o melhor método de ensino 100% online: o Relearning.

Em 2019 alcançamos os melhores resultados de aprendizagem entre todas as universidades online do mundo.

Na TECH você aprenderá através de uma metodologia de vanguarda, desenvolvida para capacitar os profissionais do futuro. Este método, na vanguarda da pedagogia mundial, se chama Relearning.

Nossa universidade é uma das únicas que possui a licença para usar este método de sucesso. Em 2019 conseguimos melhorar os níveis de satisfação geral dos nossos alunos (qualidade de ensino, qualidade dos materiais, estrutura dos curso, objetivos, entre outros) com relação aos indicadores da melhor universidade online.



No nosso programa, a aprendizagem não é um processo linear, ela acontece em espiral (aprender, desaprender, esquecer e reaprender). Portanto, combinamos cada um desses elementos de forma concêntrica. Esta metodologia já capacitou mais de 650 mil universitários com um sucesso sem precedentes em campos tão diversos como a bioquímica, a genética, a cirurgia, o direito internacional, habilidades administrativas, ciência do esporte, filosofia, direito, engenharia, jornalismo, história, mercados e instrumentos financeiros. Tudo isso em um ambiente altamente exigente, com um corpo discente com um perfil socioeconômico médio-alto e uma média de idade de 43,5 anos.

O Relearning permitirá uma aprendizagem com menos esforço e mais desempenho, fazendo com que você se envolva mais em sua especialização, desenvolvendo o espírito crítico e sua capacidade de defender argumentos e contrastar opiniões: uma equação de sucesso.

A partir das últimas evidências científicas no campo da neurociência, sabemos como organizar informações, ideias, imagens, memórias, mas sabemos também que o lugar e o contexto onde aprendemos algo é fundamental para nossa capacidade de lembrá-lo e armazená-lo no hipocampo, para mantê-lo em nossa memória a longo prazo.

Desta forma, no que se denomina Neurocognitive context-dependent e-learning, os diferentes elementos do nosso programa estão ligados ao contexto onde o aluno desenvolve sua prática profissional.

Neste programa, oferecemos o melhor material educacional, preparado especialmente para os profissionais:

Material de estudo

Todo o conteúdo foi criado especialmente para o curso pelos especialistas que irão ministrá-lo, o que faz com que o desenvolvimento didático seja realmente específico e concreto.

Posteriormente, esse conteúdo é adaptado ao formato audiovisual, para criar o método de trabalho online da TECH. Tudo isso, com as técnicas mais inovadoras que proporcionam alta qualidade em todo o material que é colocado à disposição do aluno.

Masterclasses

Há evidências científicas sobre a utilidade da observação de terceiros especialistas.

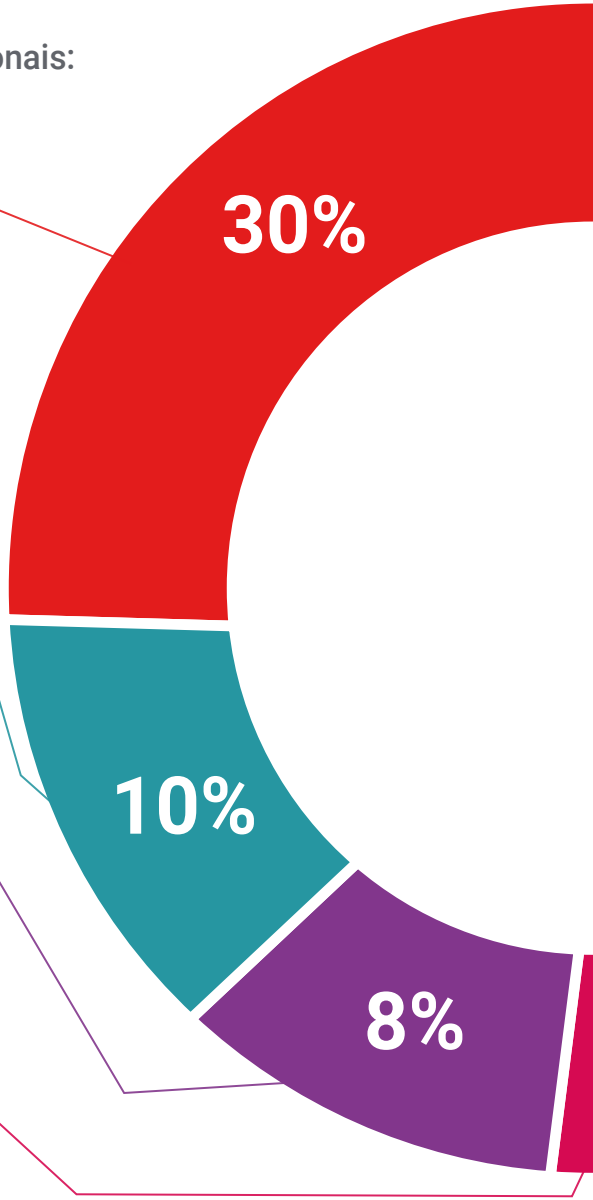
O "Learning from an expert" fortalece o conhecimento e a memória, além de gerar segurança para a tomada de decisões difíceis no futuro.

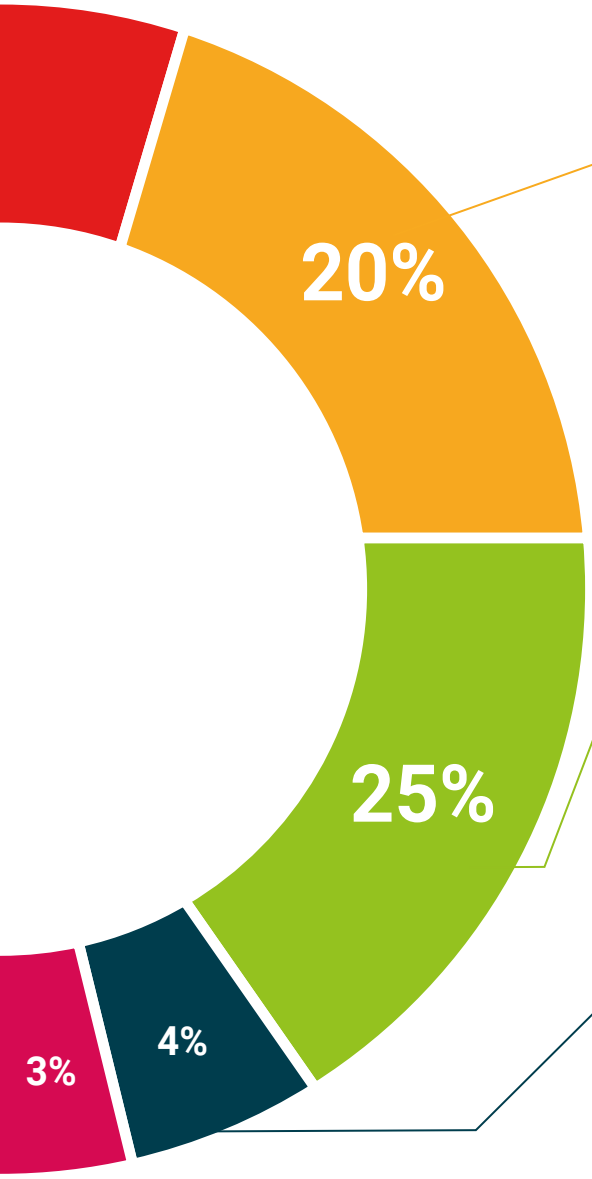
Práticas de habilidades e competências

Serão realizadas atividades para desenvolver competências e habilidades específicas em cada área temática. Práticas e dinâmicas para adquirir e ampliar as competências e habilidades que um especialista precisa desenvolver no contexto globalizado em que vivemos.

Leituras complementares

Artigos recentes, documentos de consenso e diretrizes internacionais, entre outros. Na biblioteca virtual da TECH o aluno terá acesso a tudo o que for necessário para complementar a sua capacitação.





Estudos de caso

Os alunos irão completar uma seleção dos melhores estudos de caso escolhidos especialmente para esta capacitação. Casos apresentados, analisados e orientados pelos melhores especialistas do cenário internacional.

Resumos interativos

A equipe da TECH apresenta o conteúdo de forma atraente e dinâmica através de pílulas multimídia que incluem áudios, vídeos, imagens, gráficos e mapas conceituais para consolidar o conhecimento.

Este sistema exclusivo de capacitação por meio da apresentação de conteúdo multimídia foi premiado pela Microsoft como "Caso de sucesso na Europa".

Testing & Retesting

Avaliamos e reavaliamos periodicamente o conhecimento do aluno ao longo do programa, através de atividades e exercícios de avaliação e autoavaliação, para que possa comprovar que está alcançando seus objetivos.

07

Certificado

O Mestrado Próprio em Pentesting e Red Team garante, além da capacitação mais rigorosa e atualizada, o acesso a um título de Mestrado Próprio emitido pela TECH Universidade Tecnológica.

Conclua este programa de estudos com sucesso e receba o seu certificado sem sair de casa e sem burocracias”

Este **Mestrado Próprio em Pentesting e Red Team** conta com o conteúdo mais completo e atualizado do mercado.

Uma vez aprovadas as avaliações, o aluno receberá por correio o certificado* do **Mestrado Próprio** emitido pela **TECH Universidade Tecnológica.**

O certificado emitido pela **TECH Universidade Tecnológica** expressará a qualificação obtida no Mestrado Próprio, atendendo aos requisitos normalmente exigidos pelas bolsas de empregos, concursos públicos e avaliação de carreira profissional.

Título: **Mestrado Próprio em Pentesting e Red Team**

Modalidade: **online**

Duração: **12 meses**


tech universidade tecnológica

Outorga o presente

CERTIFICADO

a

Sr./Sra. _____, com documento de identidade nº_____

por ter concluído e aprovado com sucesso o programa de

MESTRADO PRÓPRIO

em

Pentesting e Red Team

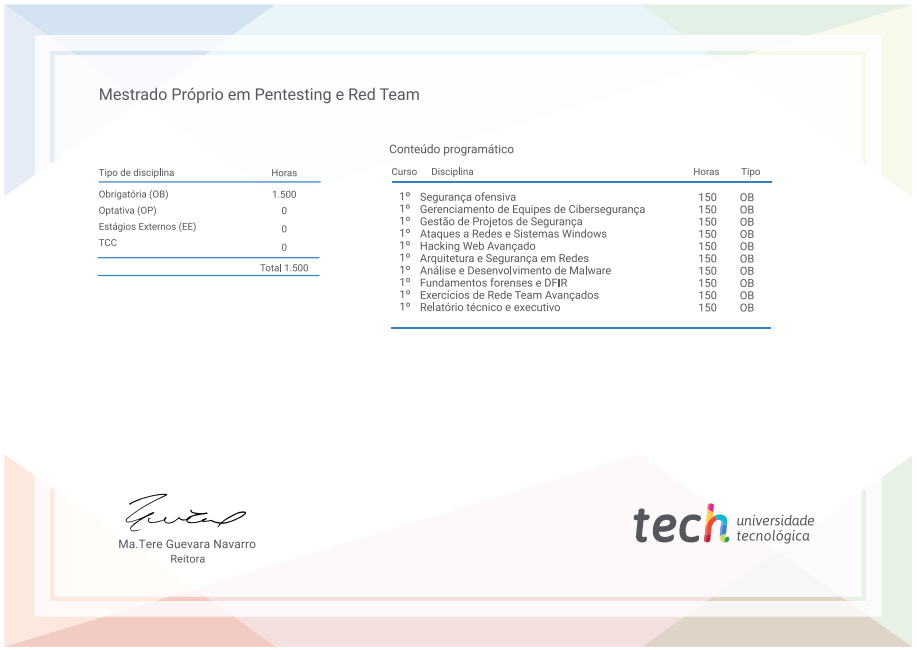
Este é um curso próprio desta Universidade, com duração de 1.500 horas, com data de início dd/mm/aaaa e data final dd/mm/aaaaa.

A TECH é uma Instituição Privada de Ensino Superior reconhecida pelo Ministério da Educação Pública em 28 de junho de 2018.

Em 17 de junho de 2020

Ma.Tere Guevara Navarro
Reitora

código único TECH: AFWOR23S techtitute.com/titulos


Mestrado Próprio em Pentesting e Red Team

Tipo de disciplina	Horas
Obrigatória (OB)	1.500
Optativa (OP)	0
Estágios Externos (EE)	0
TCC	0
	Total 1.500

Conteúdo programático

Curso	Disciplina	Horas	Tipo
1º	Segurança ofensiva	150	OB
1º	Gerenciamento de Equipes de Cibersegurança	150	OB
1º	Gestão de Projetos de Segurança	150	OB
1º	Ataques a Redes e Sistemas Windows	150	OB
1º	Hacking Web Avançado	150	OB
1º	Arquitetura e Segurança em Redes	150	OB
1º	Análise e Desenvolvimento de Malware	150	OB
1º	Fundamentos forenses e DFIR	150	OB
1º	Exercícios de Rede Team Avançados	150	OB
1º	Relatório técnico e executivo	150	OB

Ma.Tere Guevara Navarro
Reitora

tech universidade tecnológica

*Apostila de Haia: Caso o aluno solicite que seu certificado seja apostilado, a TECH EDUCATION providenciará a obtenção do mesmo a um custo adicional.

tech universidade tecnológica

Mestrado Próprio
Pentesting e Red Team

- Modalidade: **online**
- Duração: **12 meses**
- Certificado: **TECH Universidade Tecnológica**
- Horário: **no seu próprio ritmo**
- Provas: **online**

Mestrado Próprio
Pentesting e Red Team

tech universidade tecnológica