Máster Título Propio
Pentesting y Red Team

tech universidad tecnológica

tech universidad tecnológica

Máster Título Propio
Pentesting y Red Team

- Modalidad: **online**
- Duración: **12 meses**
- Titulación: **TECH Universidad Tecnológica**
- Horario: **a tu ritmo**
- Exámenes: **online**

Acceso web: **www.techtitute.com/informatica/master/master-pentesting-red-team**

Índice

01

Presentación

La cantidad y la sofisticación de los ciberataques han alcanzado proporciones alarmantes. Con el aumento exponencial de amenazas, desde ataques de *ransomware* hasta intrusiones avanzadas, la necesidad de profesionales altamente capacitados en ciberseguridad es crucial. En este contexto, surge el presente programa, que no solo ofrecerá una inmersión completa en técnicas avanzadas de seguridad, sino que también abordará la realidad de un entorno digital en constante evolución. De esta manera, los alumnos profundizarán en técnicas de ataque y defensa, enfrentándose a los desafíos de seguridad más sofisticados. Impulsado por la necesidad de fortalecer las defensas cibernéticas, este plan de estudios se distingue por su metodología 100% online y por el uso efectivo del método *Relearning* para optimizar el aprendizaje.

Diseñarás protocolos de seguridad inexpugnables gracias a este pionero programa, con la garantía de TECH”

Mantenerse actualizado es vital para preservar la eficacia en la defensa contra amenazas actuales y emergentes. En este sentido, la rápida evolución de la tecnología y las tácticas cibernéticas han convertido la actualización constante en un imperativo. La proliferación de amenazas subraya la urgencia de contar con profesionales altamente capacitados.

En este contexto, este programa universitario se revela como una respuesta esencial, ya que no solo proporcionará una comprensión profunda de las técnicas más avanzadas en ciberseguridad, sino que también asegurará que los profesionales estén a la vanguardia de las últimas tendencias y tecnologías.

En el temario de este Máster Título Propio en Pentesting y Red Team, el egresado abordará de manera exhaustiva las demandas en el ámbito de la ciberseguridad. Así, implementará medidas de seguridad efectivas en redes, incluyendo firewalls, sistemas de detección de intrusiones (IDS) y segmentación de red. Para ello, los especialistas aplicarán metodologías de investigación forense digital para la resolución de casos, desde la identificación hasta la documentación de hallazgos.

Además, desarrollarán competencias en la simulación de amenazas avanzadas, replicando las tácticas, las técnicas y los procedimientos más utilizados por actores malintencionados. Asimismo, el innovador enfoque de TECH garantizará la adquisición de habilidades aplicables y valiosas en el entorno laboral de la ciberseguridad.

La metodología del itinerario académico refuerza su carácter innovador, pues ofrecerá un entorno educativo 100% online. Este programa se adaptará a las necesidades de los profesionales ocupados que buscan avanzar en sus carreras. Además, empleará la metodología *Relearning*, basada en la repetición de conceptos clave para fijar conocimientos y facilitar el aprendizaje. De esta manera, la combinación de flexibilidad y enfoque pedagógico robusto, no solo lo hará accesible, sino también altamente efectivo en la preparación de los informáticos para los desafíos dinámicos de la ciberseguridad.

Este **Máster Título Propio en Pentesting y Red Team** contiene el programa educativo más completo y actualizado del mercado. Sus características más destacadas son:

- El desarrollo de casos prácticos presentados por expertos en Pentesting y Red Team
- Los contenidos gráficos, esquemáticos y eminentemente prácticos con los que está concebido recogen una información actualizada y práctica sobre aquellas disciplinas indispensables para el ejercicio profesional
- Los ejercicios prácticos donde realizar el proceso de autoevaluación para mejorar el aprendizaje
- Su especial hincapié en metodologías innovadoras
- Las lecciones teóricas, preguntas al experto, foros de discusión de temas controvertidos y trabajos de reflexión individual
- La disponibilidad de acceso a los contenidos desde cualquier dispositivo fijo o portátil con conexión a internet

En solo 12 meses le darás a tu carrera el impulso que necesita. ¡Matricúlate ahora y experimenta un progreso inmediato!"

¿Deseas experimentar un salto de calidad en tu carrera? Con TECH te capacitarás en la implementación de estrategias para la ejecución efectiva de proyectos de ciberseguridad"

Profundizarás en la identificación y evaluación de vulnerabilidades en aplicaciones web, gracias a la mejor universidad digital del mundo según Forbes.

Dominarás técnicas forenses en entornos de Pentesting. ¡Posiciónate como el experto en ciberseguridad que todas las empresas buscan!

El programa incluye en su cuadro docente a profesionales del sector que vierten en esta capacitación la experiencia de su trabajo, además de reconocidos especialistas de sociedades de referencia y universidades de prestigio.

Su contenido multimedia, elaborado con la última tecnología educativa, permitirá al profesional un aprendizaje situado y contextual, es decir, un entorno simulado que proporcionará una capacitación inmersiva programada para entrenarse ante situaciones reales.

El diseño de este programa se centra en el Aprendizaje Basado en Problemas, mediante el cual el profesional deberá tratar de resolver las distintas situaciones de práctica profesional que se le planteen a lo largo del curso académico. Para ello, contará con la ayuda de un novedoso sistema de vídeo interactivo realizado por reconocidos expertos.

02

Objetivos

Este itinerario académico tiene como objetivo principal capacitar a los egresados en pruebas de penetración y simulaciones de *Red Team*. A lo largo del programa, los informáticos se sumergirán en un enfoque práctico y especializado, desarrollando competencias para abordar la identificación y explotación de vulnerabilidades en sistemas y redes. Asimismo, este plan de estudios se ha diseñado para proporcionar una comprensión profunda de las tácticas y estrategias en ciberseguridad, preparando a los alumnos para enfrentar los desafíos del mundo real y liderar en la implementación efectiva de medidas de seguridad cibernética.

Profundizarás en el análisis y el desarrollo de malware para posicionarte como un destacado profesional. ¡Alcanza tus metas de la mano de TECH!"

Objetivos generales

- Adquirir habilidades avanzadas en pruebas de penetración y simulaciones de *Red Team*, abordando la identificación y explotación de vulnerabilidades en sistemas y redes
- Desarrollar capacidades de liderazgo para coordinar equipos especializados en ciberseguridad ofensiva, optimizando la ejecución de proyectos de *Pentesting* y *Red Team*
- Desarrollar habilidades en el análisis y desarrollo de malware, comprendiendo su funcionalidad y aplicando estrategias defensivas y educativas
- Perfeccionar habilidades de comunicación mediante la elaboración de informes técnicos y ejecutivos detallados, presentando hallazgos de manera efectiva a audiencias técnicas y ejecutivas
- Promover una práctica ética y responsable en el ámbito de la ciberseguridad, considerando los principios éticos y legales en todas las actividades
- Mantener actualizado al alumnado con las tendencias y tecnologías emergentes en ciberseguridad

Conseguirás tus objetivos gracias a las herramientas didácticas de TECH, entre las que destacan los vídeos explicativos y los resúmenes interactivos"

Objetivos específicos

Módulo 1. La Seguridad Ofensiva

- Familiarizar al egresado con las metodologías de pruebas de penetración, incluyendo fases clave como la recolección de información, análisis de vulnerabilidades, explotación y documentación
- Desarrollar competencias prácticas en el uso de herramientas especializadas de *Pentesting* para identificar y evaluar vulnerabilidades en sistemas y redes
- Estudiar y comprender las tácticas, técnicas y procedimientos utilizados por los actores malintencionados, permitiendo la identificación y simulación de amenazas
- Aplicar conocimientos teóricos en escenarios prácticos y simulaciones, enfrentándose a desafíos reales para fortalecer habilidades de *Pentesting*
- Desarrollar habilidades de documentación efectiva, creando informes detallados que reflejan hallazgos, metodologías utilizadas y recomendaciones para la mejora de la seguridad
- Practicar la colaboración efectiva en equipos de seguridad ofensiva, optimizando la coordinación y ejecución de actividades de *Pentesting*

Módulo 2. Gestión de Equipos de Ciberseguridad

- Desarrollar habilidades de liderazgo específicas para equipos de ciberseguridad, incluyendo la capacidad de motivar, inspirar y coordinar esfuerzos para alcanzar objetivos comunes
- Aprender a asignar eficientemente recursos dentro de un equipo de ciberseguridad, considerando las habilidades individuales y maximizando la productividad en proyectos

- Mejorar habilidades de comunicación específicas para entornos técnicos, facilitando la comprensión y coordinación entre los miembros del equipo
- Aprender estrategias para identificar y gestionar conflictos dentro del equipo de ciberseguridad, promoviendo un ambiente de trabajo colaborativo y eficiente
- Aprender a establecer métricas y sistemas de evaluación para medir el desempeño del equipo de ciberseguridad y realizar ajustes según sea necesario
- Promover la integración de prácticas éticas en la gestión de equipos de ciberseguridad, asegurando que todas las actividades sean conducidas de manera ética y legal
- Desarrollar competencias para la preparación y gestión eficiente de incidentes de ciberseguridad, garantizando una respuesta rápida y efectiva ante amenazas

Módulo 3. Gestión de Proyectos de Seguridad

- Desarrollar habilidades para planificar proyectos de seguridad cibernética, definiendo objetivos, alcance, recursos y plazos de ejecución
- Aprender estrategias para la ejecución efectiva de proyectos de seguridad, asegurando la implementación exitosa de las medidas planificadas
- Desarrollar habilidades para la gestión eficiente de presupuestos y asignación de recursos en proyectos de seguridad, maximizando la eficacia y minimizando costos
- Mejorar la comunicación efectiva con los *stakeholders*, presentando informes y actualizaciones de manera clara y comprensible
- Aprender técnicas de seguimiento y control de proyectos, identificando desviaciones y tomando acciones correctivas según sea necesario
- Familiarizar a los alumnos con metodologías ágiles de *Pentesting*
- Desarrollar habilidades en la documentación detallada y la elaboración de informes, proporcionando una visión clara del progreso del proyecto y los resultados obtenidos
- Fomentar la colaboración efectiva entre diferentes equipos y disciplinas dentro de proyectos de seguridad, asegurando una visión integral y coordinada
- Aprender estrategias para evaluar y medir la efectividad de las medidas implementadas, garantizando la mejora continua de la postura de seguridad de la organización

Módulo 4. Ataques a Redes y Sistemas Windows

- Desarrollar habilidades para identificar y evaluar vulnerabilidades específicas en sistemas operativos Windows
- Aprender tácticas avanzadas utilizadas por atacantes para infiltrarse y persistir en redes basadas en entornos Windows
- Adquirir competencias en estrategias y herramientas para mitigar amenazas específicas dirigidas a sistemas operativos Windows
- Familiarizar al egresado con técnicas de análisis forense aplicadas a sistemas Windows, facilitando la identificación y respuesta a incidentes
- Aplicar conocimientos teóricos en entornos simulados, participando en ejercicios prácticos para entender y contrarrestar ataques específicos a sistemas Windows
- Aprender estrategias específicas para asegurar entornos empresariales que utilizan sistemas operativos Windows, considerando las complejidades de infraestructuras empresariales
- Desarrollar competencias para evaluar y mejorar las configuraciones de seguridad en sistemas Windows, asegurando la implementación de medidas eficaces

- Promover prácticas éticas y legales en la ejecución de ataques y pruebas en sistemas Windows, considerando los principios éticos de la ciberseguridad
- Mantener al día al alumno con las últimas tendencias y amenazas en ataques a sistemas Windows, garantizando la relevancia y efectividad constante de las habilidades adquiridas

Módulo 5. *Hacking* Web Avanzado

- Desarrollar habilidades para identificar y evaluar vulnerabilidades en aplicaciones web, incluyendo inyecciones SQL, *Cross-Site Scripting* (XSS) y otros vectores de ataque comunes
- Aprender a realizar pruebas de seguridad en aplicaciones web modernas
- Adquirir competencias en técnicas avanzadas de hacking web, explorando estrategias de evasión de medidas de seguridad y explotación de vulnerabilidades sofisticadas
- Familiarizar al egresado con la evaluación de la seguridad en APIs y servicios web, identificando posibles puntos de vulnerabilidad y fortaleciendo la seguridad en interfaces de programación
- Desarrollar habilidades para implementar medidas de mitigación efectivas en aplicaciones web, reduciendo la exposición a ataques y fortaleciendo la seguridad
- Participar en simulaciones prácticas para evaluar la seguridad en entornos web complejos, aplicando conocimientos en situaciones del mundo real
- Desarrollar competencias en la formulación de estrategias de defensa efectivas para proteger aplicaciones web contra amenazas cibernéticas
- Aprender a lineal las prácticas de *hacking web* avanzado con las normativas y estándares de seguridad relevantes, asegurando la adhesión a marcos legales y éticos
- Fomentar la colaboración efectiva entre equipos de desarrollo y seguridad

Módulo 6. Arquitectura y Seguridad en Redes

- Adquirir conocimientos avanzados sobre la arquitectura de redes, incluyendo topologías, protocolos y componentes clave
- Desarrollar habilidades para identificar y evaluar vulnerabilidades específicas en infraestructuras de red, considerando amenazas potenciales
- Aprender a implementar medidas de seguridad efectivas en redes, incluyendo *firewalls*, sistemas de detección de intrusiones (IDS) y segmentación de red
- Familiarizar al estudiante con tecnologías emergentes en redes, como redes definidas por software (SDN), y comprender su impacto en la seguridad
- Desarrollar habilidades para asegurar las comunicaciones en redes, incluyendo la protección contra amenazas como *sniffing* y ataques de intermediarios
- Aprender a evaluar y mejorar las configuraciones de seguridad en entornos de redes empresariales, garantizando la protección adecuada
- Desarrollar habilidades para implementar medidas de mitigación efectivas contra amenazas en redes empresariales, desde ataques internos hasta amenazas externas
- Fomentar la colaboración efectiva con equipos de seguridad, integrando estrategias y esfuerzos para proteger la infraestructura de red
- Promover prácticas éticas y legales en la implementación de medidas de seguridad en redes, asegurando la adhesión a principios éticos en todas las actividades

Módulo 7. Análisis y Desarrollo de *Malware*

- Adquirir conocimientos avanzados sobre la naturaleza, funcionalidad y comportamiento del *malware*, comprendiendo sus diversas formas y objetivos
- Desarrollar habilidades en el análisis forense aplicado al *malware*, permitiendo la identificación de indicadores de compromiso (IoC) y patrones de ataque
- Aprender estrategias para la detección y prevención efectiva de malware, incluyendo el despliegue de soluciones de seguridad avanzadas
- Familiarizar al alumno con el desarrollo de *malware* con propósitos educativos y defensivos, permitiendo la comprensión profunda de las tácticas utilizadas por los atacantes
- Promover prácticas éticas y legales en el análisis y desarrollo de *malware*, garantizando la integridad y responsabilidad en todas las actividades
- Aplicar conocimientos teóricos en entornos simulados, participar en ejercicios prácticos para entender y contrarrestar ataques maliciosos
- Desarrollar habilidades para evaluar y seleccionar herramientas de seguridad *anti-malware*, considerando su eficacia y adaptabilidad a entornos específicos
- Aprender a implementar de mitigación efectiva contra amenazas maliciosas, reduciendo el impacto y la propagación del *malware* en sistemas y redes
- Fomentar la colaboración efectiva con equipos de seguridad, integrando estrategias y esfuerzos para proteger contra amenazas de *malware*
- Mantener al día al egresado con las últimas tendencias y técnicas utilizadas en el análisis y desarrollo de *malware*, asegurando la relevancia y eficacia constante de las habilidades adquiridas

Módulo 8. Fundamentos Forenses y DFIR

- Adquirir conocimientos sólidos sobre los principios fundamentales de la investigación forense digital (DFIR) y su aplicación en la resolución de incidentes cibernéticos
- Desarrollar habilidades en la adquisición segura y forense de evidencia digital, garantizando la preservación de la cadena de custodia
- Aprender a realizar análisis forenses de sistemas de archivos
- Familiarizar al estudiante con técnicas avanzadas para el análisis de registros y bitácoras, permitiendo la reconstrucción de eventos en entornos digitales
- Aprender a aplicar metodologías de investigación forense digital en la resolución de casos, desde la identificación hasta la documentación de hallazgos
- Familiarizar al alumno con el análisis de evidencia digital y la aplicación de técnicas forenses en entornos de *Pentesting*
- Desarrollar habilidades en la elaboración de informes forenses detallados y claros, presentando hallazgos y conclusiones de manera comprensible
- Fomentar la colaboración efectiva con equipos de respuesta a incidentes (IR), optimizando la coordinación en la investigación y mitigación de amenazas
- Promover prácticas éticas y legales en la investigación forense digital, asegurando la adhesión a normativas y estándares de conducta en ciberseguridad

Módulo 9. Ejercicios de *Red Team* Avanzados

- Desarrollar competencias en la simulación de amenazas avanzadas, replicando tácticas, técnicas y procedimientos (TTP) utilizados por actores malintencionados atractivos
- Aprender a identificar puntos débiles y vulnerabilidades en la infraestructura mediante ejercicios realistas de *Red Team*, fortaleciendo la postura de seguridad
- Familiarizar al egresado con técnicas avanzadas de evasión de medidas de seguridad, permitiendo evaluar la resistencia de la infraestructura ante ataques deseables
- Desarrollar habilidades de coordinación y colaboración efectiva entre los miembros del equipo de *Red Team*, optimizando la ejecución de tácticas y estrategias para evaluar comprehensivamente la seguridad de la organización
- Aprender a simular escenarios de amenazas actuales, como ataques de *ransomware* o campañas de phishing avanzadas, para evaluar la capacidad de respuesta de la organización
- Familiarizar al estudiante con técnicas de análisis post-ejercicio, evaluando el desempeño del equipo de *Red Team* y extrayendo lecciones aprendidas para la mejora continua
- Desarrollar habilidades para evaluar la resiliencia organizacional ante ataques simulados, identificando áreas de mejora en políticas y procedimientos
- Aprender a elaborar informes detallados que documenten los hallazgos, metodologías utilizadas y recomendaciones derivadas de ejercicios de *Red Team* avanzados
- Promover prácticas éticas y legales en la realización de ejercicios de *Red Team*, asegurando la adhesión a normativas y estándares éticos en ciberseguridad

Módulo 10. Reporte Técnico y Ejecutivo

- Desarrollar habilidades para elaborar informes técnicos detallados, presentando de manera clara y completa los hallazgos, metodologías utilizadas y recomendaciones
- Aprender a comunicar de manera efectiva con audiencias técnicas, utilizando un lenguaje preciso y adecuado para transmitir información técnica compleja
- Desarrollar habilidades para formular recomendaciones accionables y prácticas, orientadas a mitigar vulnerabilidades y mejorar la postura de seguridad
- Aprender a evaluar el impacto potencial de las vulnerabilidades identificadas, considerando aspectos técnicos, operativos y estratégicos
- Familiarizar al alumno con las mejores prácticas para la presentación ejecutiva de informes, adaptando la información técnica para audiencias no técnicas
- Desarrollar competencias para alinear los hallazgos y recomendaciones con los objetivos estratégicos y operativos de la organización
- Aprender a utilizar herramientas de visualización de datos para representar gráficamente la información contenida en los informes, facilitando la comprensión
- Promover la inclusión de información relevante sobre el cumplimiento de normativas y estándares en los informes, garantizando la adhesión a requisitos legales
- Fomentar la colaboración efectiva entre equipos técnicos y ejecutivos, asegurando la comprensión y apoyo para las acciones de mejora propuestas en el informe

03

Competencias

Gracias al presente plan de estudios, los egresados se capacitarán con habilidades especializadas para implementar medidas de defensa activa, fortaleciendo la seguridad de sistemas y redes basadas en las mejores prácticas de ciberseguridad. Además, los alumnos adquirirán competencias avanzadas en pruebas de penetración y simulaciones de *Red Team*, destacando en la identificación y mitigación proactiva de vulnerabilidades. En este sentido, los profesionales dominarán las destrezas técnicas necesarias para enfrentar amenazas del mundo real, preparándose para liderar estrategias efectivas de evaluación y fortificación de la seguridad en entornos cibernéticos dinámicos. Asimismo, el enfoque 100% online flexibiliza el aprendizaje.

Conviértete en un experto en ciberseguridad a través de 1.500 horas de los mejores contenidos multimedia, con el sello de calidad de TECH”

Competencias generales

- Adquirir competencias en la planificación, ejecución y gestión de proyectos de seguridad cibernética, asegurando resultados efectivos y cumplimiento de objetivos
- Adquirir conocimientos avanzados en la arquitectura de redes y sus aspectos de seguridad, evaluando vulnerabilidades y aplicando estrategias para fortalecer la infraestructura
- Desarrollar competencias en la investigación forense digital y la respuesta a incidentes, desde la recopilación de evidencia hasta la mitigación de amenazas y la restauración operativa
- Aplicar tácticas avanzadas en la planificación y ejecución de ejercicios de *Red Team*, simulando escenarios del mundo real para evaluar la resistencia de la infraestructura, detectar debilidades y mejorar la preparación ante amenazas cibernéticas

Actualízate en el proceso de identificación, evaluación y mitigación de riesgos específicos de proyectos de seguridad cibernética. ¡Apuesta por TECH!"

Competencias específicas

- Adquirir habilidades de coaching para el desarrollo profesional de los miembros del equipo, fomentando el crecimiento y la mejora
- Desarrollar habilidades para la toma de decisiones estratégicas en situaciones de ciberseguridad, considerando el impacto a corto y largo plazo en la seguridad organizacional
- Adquirir competencias en la identificación, evaluación y mitigación de riesgos específicos de proyectos de seguridad cibernética
- Desarrollar habilidades para implementar medidas de defensa activa, fortaleciendo la seguridad de sistemas y redes basadas
- Aprender técnicas de análisis de tráfico web para identificar patrones y comportamientos anómalos, facilitando la detección de posibles amenazas
- Adquirir competencias en el análisis forense aplicado a entornos de red, permitiendo la identificación y respuesta efectiva a incidentes cibernéticos
- Aprender estrategias para la detección y prevención efectiva de malware, incluyendo el despliegue de soluciones de seguridad avanzadas
- Desarrollar habilidades en la identificación de indicadores de compromiso (IoC) durante la investigación forense, facilitando la detección y respuesta a incidentes
- Adquirir habilidades para la planificación estratégica de ejercicios de *Red Team*, considerando objetivos, alcance, recursos y escenarios realistas
- Adquirir competencias en la identificación y priorización de vulnerabilidades, destacando aquellas que representan mayores riesgos para la seguridad

04

Dirección del curso

Para la confección del cuerpo docente del Máster Título Propio en Pentesting y Red Team, TECH ha reunido a los mejores especialistas, que cuentan con un extenso y reconocido bagaje profesional en empresas líderes del sector. En este sentido, cada miembro del claustro docente aportará su experiencia práctica y sus conocimientos especializados, garantizando que los alumnos se beneficiarán de la enseñanza de profesionales altamente cualificados. Asimismo, la selección cuidadosa de estos expertos no solo asegurará la calidad académica, sino también la relevancia y aplicabilidad inmediata de los contenidos en el entorno dinámico de la ciberseguridad.

Gigantes de la industria de la ciberseguridad te catapultarán al éxito en tan solo 12 meses con este exclusivo programa universitario de TECH"

Dirección

D. Gómez Pintado, Carlos

- Gerente de Ciberseguridad y Red Team Cipherbit en Grupo Oesía
- Gerente Advisor & Investor en Wesson App
- Graduado en Ingeniería del Software y Tecnologías de la Sociedad de la Información, por la Universidad Politécnica de Madrid
- Colabora con instituciones educativas para la confección de Ciclos Formativos de Grado Superior en ciberseguridad

Profesores

D. Siles Rubia, Marcelino

- Cibersecurity Engineer
- Ingeniería de la Ciberseguridad en la Universidad Rey Juan Carlos
- Conocimientos: Programación Competitiva, *Hacking Web, Active Directory y Malware Development*
- Ganador del Concurso AdaByron

D. Redondo Castro, Pablo

- Pentester en Grupo Oesía
- Ingeniero de Ciberseguridad por Universidad Rey Juan Carlos
- Amplia experiencia como *Cibersecurity Evaluator Traineev*
- Acumula experiencia docente, impartiendo formaciones relacionadas con torneos de Capture The Flag

D. González Parrilla, Yuba

- Coordinador de Línea Seguridad Ofensiva y Red Team
- Especialista en Dirección de Proyectos *Predictive* en Project Management Institute
- Especialista en *SmartDefense*
- Experto en *Web Application Penetration Tester* en eLearnSecurity
- *Junior Penetration Tester* en eLearnSecurity
- Graduado en Ingeniería computacional en Universidad Politécnica de Madrid

D. González Sanz, Marcos

- Consultor de Ciberseguridad en Cipherbit
- eLearnSecurity Certified eXploit Developer
- Offensive Security Certified Professional
- Offensive Security Wireless Professional
- Virtual Hacking Labs Plus
- Graduado en Ingeniería del Software por la Universidad Politécnica de Madrid

D. Villaverde, David

- Consultor de Ciberseguridad en Cipherbit
- Experto en Plataformas de Retos de Hacking y HackTheBox
- Especialista en Pentesting
- Experto en Malware
- Ingeniero de software especializado en ciberseguridad por el Centro Universitario de Tecnología y Arte Digital Las Rozas

D. Castillo, Carlos

- Cybersecurity Consultant y Red Teamer en Cipherbit
- Offensive Security Wireless Professional
- eLearnSecurity Web Application Penetration Tester
- eLearnSecurity Certified Professional Penetration Tester v2
- eLearnSecurity Junior Penetration Tester
- Consultor de Ciberseguridad
- Ingeniero de Software por la Universidad Politécnica de Madrid

D. Gallego Sánchez, Alejandro

- Pentester en Grupo Oesía
- Consultor de Ciberseguridad en Integración Tecnológica Empresarial, S.L
- Técnico Audiovisual en Ingeniería Audiovisual S.A
- Graduado en Ingeniería de la Ciberseguridad por la Universidad Rey Juan Carlos

D. Mora Navas, Sergio

- Consultor en Ciberseguridad en Grupo Oesía
- Ingeniero en Ciberseguridad por la Universidad Rey Juan Carlos
- Ingeniero Informático por la Universidad de Burgos

05

Estructura y contenido

El presente programa universitario ofrece una inmersión completa en las disciplinas cruciales de pruebas de penetración y simulaciones de *Red Team*. A lo largo del temario, los egresados desarrollarán habilidades avanzadas para identificar y explotar vulnerabilidades en sistemas y redes, utilizando técnicas y herramientas modernas. Esta titulación, diseñada con enfoque práctico, capacitará a los profesionales de ciberseguridad para enfrentar desafíos del mundo real. En este sentido, los alumnos se beneficiarán de una combinación única de teoría y práctica, guiados por expertos de la industria, para fortalecer su comprensión y aplicar eficazmente estrategias de evaluación de seguridad en entornos cibernéticos.

Profundizarás en los distintos roles y responsabilidades del equipo de ciberseguridad. ¡Matricúlate ahora!"

Módulo 1. La Seguridad Ofensiva

1.1. Definición y contexto
- 1.1.1. Conceptos fundamentales de seguridad ofensiva
- 1.1.2. Importancia de la ciberseguridad en la actualidad
- 1.1.3. Desafíos y oportunidades en la seguridad ofensiva

1.2. Bases de la ciberseguridad
- 1.2.1. Primeros desafíos y evolución de las amenazas
- 1.2.2. Hitos tecnológicos y su impacto en la ciberseguridad
- 1.2.3. Ciberseguridad en la era moderna

1.3. Bases de la seguridad ofensiva
- 1.3.1. Conceptos clave y terminología
- 1.3.2. *Think Outside the Box*
- 1.3.3. Diferencias entre hacking ofensivo y defensivo

1.4. Metodologías de seguridad ofensiva
- 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. Roles y responsabilidades en seguridad ofensiva
- 1.5.1. Principales perfiles
- 1.5.2. *Bug Bounty Hunters*
- 1.5.3. *Researching:* El arte de investigar

1.6. Arsenal del auditor ofensivo
- 1.6.1. Sistemas operativos para *hacking*
- 1.6.2. Introducción a los C2
- 1.6.3. *Metasploit*: Fundamentos y Uso
- 1.6.4. Recursos útiles

1.7. OSINT: Inteligencia en Fuentes Abiertas
- 1.7.1. Fundamentos del OSINT
- 1.7.2. Técnicas y herramientas OSINT
- 1.7.3. Aplicaciones de OSINT en seguridad ofensiva

1.8. *Scripting*: Introducción a la automatización
- 1.8.1. Fundamentos de scripting
- 1.8.2. *Scripting* en Bash
- 1.8.3. *Scripting* en Python

1.9. Categorización 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 y *hacking*
- 1.10.1. Principios de la ética *hacker*
- 1.10.2. La línea entre *hacking* ético y *hacking* malicioso
- 1.10.3. Implicaciones legales y consecuencias
- 1.10.4. Casos de estudio: Situaciones éticas en ciberseguridad

Módulo 2. Gestión de Equipos de Ciberseguridad

2.1. La gestión de equipos
- 2.1.1. Quién es quién
- 2.1.2. El director
- 2.1.3. Conclusiones

2.2. Roles y responsabilidades
- 2.2.1. Identificación de roles
- 2.2.2. Delegación efectiva
- 2.2.3. Gestión de expectativas

2.3. Formación y desarrollo de equipos
- 2.3.1. Etapas de formación de equipos
- 2.3.2. Dinámicas de grupo
- 2.3.3. Evaluación y retroalimentación

2.4. Gestión del talento
- 2.4.1. Identificación del talento
- 2.4.2. Desarrollo de capacidades
- 2.4.3. Retención de talentos

2.5. Liderazgo y motivación del equipo
- 2.5.1. Estilos de liderazgo
- 2.5.2. Teorías de la motivación
- 2.5.3. Reconocimiento de los logros

2.6. Comunicación y coordinación
- 2.6.1. Herramientas de comunicación
- 2.6.2. Barreras en la comunicación
- 2.6.3. Estrategias de coordinación

2.7. Planificaciones estratégicas del desarrollo profesional del personal
- 2.7.1. Identificación de necesidades de formación
- 2.7.2. Planes de desarrollo individual
- 2.7.3. Seguimiento y evaluación

2.8. Resolución de conflictos
- 2.8.1. Identificación de conflictos
- 2.8.2. Métodos de medición
- 2.8.3. Prevención de conflictos

2.9. Gestión de la calidad y la mejora continua
- 2.9.1. Principios de calidad
- 2.9.2. Técnicas para la mejora continua
- 2.9.3. *Feedback* y retroalimentación

2.10. Herramientas y tecnologías
- 2.10.1. Plataformas de colaboración
- 2.10.2. Gestión de proyectos
- 2.10.3. Conclusiones

Módulo 3. Gestión de Proyectos de Seguridad

3.1. La gestión de proyectos de seguridad
- 3.1.1. Definición y propósito de la gestión de proyectos en ciberseguridad
- 3.1.2. Principales desafíos
- 3.1.3. Consideraciones

3.2. Ciclo de vida de un proyecto de seguridad
- 3.2.1. Etapas iniciales y definición de objetivos
- 3.2.2. Implementación y ejecución
- 3.2.3. Evaluación y revisión

3.3. Planificación y estimación de recursos
- 3.3.1. Conceptos básicos de gestión económica
- 3.3.2. Determinación de recursos humanos y técnicos
- 3.3.3. Presupuestación y costos asociados

3.4. Ejecución y control del proyecto
- 3.4.1. Monitorización y seguimiento
- 3.4.2. Adaptación y cambios en el proyecto
- 3.4.3. Evaluación intermedia y revisiones

3.5. Comunicación y reporte del proyecto
- 3.5.1. Estrategias de comunicación efectiva
- 3.5.2. Elaboración de informes y presentaciones
- 3.5.3. Comunicación con el cliente y la dirección

3.6. Herramientas y tecnologías
- 3.6.1. Herramientas de planificación y organización
- 3.6.2. Herramientas de colaboración y comunicación
- 3.6.3. Herramientas de documentación y almacenamiento

3.7. Documentación y protocolos
- 3.7.1. Estructuración y creación de documentación
- 3.7.2. Protocolos de actuación
- 3.7.3. Guías

3.8. Normativas y cumplimiento en proyectos de ciberseguridad
- 3.8.1. Leyes y regulaciones internacionales
- 3.8.2. Cumplimiento
- 3.8.3. Auditorías

3.9. Gestión de riesgos en proyectos de seguridad
- 3.9.1. Identificación y análisis de riesgos
- 3.9.2. Estrategias de mitigación
- 3.9.3. Monitorización y revisión de riesgos

3.10. Cierre del proyecto
- 3.10.1. Revisión y evaluación
- 3.10.2. Documentación final
- 3.10.3. Feedback

Módulo 4. Ataques a Redes y Sistemas Windows

4.1. Windows y Directorio Activo
- 4.1.1. Historia y evolución de Windows
- 4.1.2. Conceptos básicos de Directorio Activo
- 4.1.3. Funciones y servicios del Directorio Activo
- 4.1.4. Arquitectura general del Directorio Activo

4.2. Redes en entornos de Directorio Activo
- 4.2.1. Protocolos de red en Windows
- 4.2.2. DNS y su funcionamiento en el Directorio Activo
- 4.2.3. Herramientas de diagnóstico de red
- 4.2.4. Implementación de redes en Directorio Activo

4.3. Autenticación y autorización en Directorio Activo
- 4.3.1. Proceso y flujo de autenticación
- 4.3.2. Tipos de credenciales
- 4.3.3. Almacenamiento y gestión de credenciales
- 4.3.4. Seguridad en la autenticación

4.4. Permisos y políticas en Directorio Activo
- 4.4.1. GPOs
- 4.4.2. Aplicación y gestión de GPOs
- 4.4.3. Administración de permisos en Directorio Activo
- 4.4.4. Vulnerabilidades y mitigaciones en permisos

4.5. Fundamentos de Kerberos
- 4.5.1. ¿Qué es Kerberos?
- 4.5.2. Componentes y funcionamiento
- 4.5.3. Tickets en Kerberos
- 4.5.4. Kerberos en el contexto de Directorio Activo

4.6. Técnicas avanzadas en Kerberos
- 4.6.1. Ataques comunes en Kerberos
- 4.6.2. Mitigaciones y protecciones
- 4.6.3. Monitorización del tráfico Kerberos
- 4.6.4. Ataques avanzados en Kerberos

4.7. *Active Directory Certificate Services* (ADCS)
- 4.7.1. Conceptos básicos de PKI
- 4.7.2. Roles y componentes de ADCS
- 4.7.3. Configuración y despliegue de ADCS
- 4.7.4. Seguridad en ADCS

4.8. Ataques y defensas en *Active Directory Certificate Services* (ADCS)
- 4.8.1. Vulnerabilidades comunes en ADCS
- 4.8.2. Ataques y técnicas de explotación
- 4.8.3. Defensas y mitigaciones
- 4.8.4. Monitorización y auditoría de ADCS

4.9. Auditoría del Directorio Activo
- 4.9.1. Importancia de la auditoría en el Directorio Activo
- 4.9.2. Herramientas de auditoría
- 4.9.3. Detección de anomalías y comportamientos sospechosos
- 4.9.4. Respuesta a incidentes y recuperación

4.10. Azure AD
- 4.10.1. Conceptos básicos de Azure AD
- 4.10.2. Sincronización con el Directorio Activo local
- 4.10.3. Gestión de identidades en Azure AD
- 4.10.4. Integración con aplicaciones y servicios

Módulo 5. *Hacking* Web Avanzado

5.1. Funcionamiento de una web
- 5.1.1. La URL y sus partes
- 5.1.2. Los métodos HTTP
- 5.1.3. Las cabeceras
- 5.1.4. Cómo ver peticiones web con Burp Suite

5.2. Sesiones
- 5.2.1. Las *cookies*
- 5.2.2. *Tokens* JWT
- 5.2.3. Ataques de robo de sesión
- 5.2.4. Ataques a JWT

5.3. *Cross Site Scripting* (XSS)
- 5.3.1. Qué es un XSS
- 5.3.2. Tipos de XSS
- 5.3.3. Explotando un XSS
- 5.3.4. Introducción a los *XSLeaks*

5.4. Inyecciones a bases de datos
- 5.4.1. Qué es una *SQL Injection*
- 5.4.2. Exfiltrando información con *SQLi*
- 5.4.3. *SQLi Blind, Time-Based y Error-Based*
- 5.4.4. Inyecciones NoSQLi

5.5. *Path Traversal* y *Local File Inclusion*
- 5.5.1. Qué son y sus diferencias
- 5.5.2. Filtros comunes y cómo saltarlos
- 5.5.3. *Log Poisoning*
- 5.5.4. LFIs en PHP

5.6. *Broken Authentication*
- 5.6.1. *User Enumeration*
- 5.6.2. *Password Bruteforce*
- 5.6.3. *2FA Bypass*
- 5.6.4. *Cookies* con información sensible y modificable

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 en subidas de ficheros
- 5.8.3. XML *External Entity* (XXE) *Injection*
- 5.8.4. *Path traversal* en subidas de fichero

5.9. *Broken Acess Control*
- 5.9.1. Acceso a paneles sin restricción
- 5.9.2. *Insecure Direct Object References* (IDOR)
- 5.9.3. Bypass de filtros
- 5.9.4. Métodos de autorización insuficientes

5.10. Vulnerabilidades de DOM y ataques más avanzados
- 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. Arquitectura y Seguridad en Redes

6.1. Las redes informáticas
- 6.1.1. Conceptos básicos: Protocolos LAN, WAN, CP, CC
- 6.1.2. Modelo OSI y TCP/IP
- 6.1.3. *Switching:* Conceptos básicos
- 6.1.4. *Routing:* Conceptos básicos

6.2. *Switching*
- 6.2.1. Introducción a VLAN's
- 6.2.2. STP
- 6.2.3. *EtherChannel*
- 6.2.4. Ataques a capa 2

6.3. VLAN´s
- 6.3.1. Importancia de las VLAN's
- 6.3.2. Vulnerabilidades en VLAN's
- 6.3.3. Ataques comunes en VLAN's
- 6.3.4. Mitigaciones

6.4. *Routing*
- 6.4.1. Direccionamiento IP- IPv4 e IPv6
- 6.4.2. Enrutamiento: Conceptos Clave
- 6.4.3. Enrutamiento Estático
- 6.4.4. Enrutamiento Dinámico: Introducción

6.5. Protocolos IGP
- 6.5.1. RIP
- 6.5.2. OSPF
- 6.5.3. RIP vs OSPF
- 6.5.4. Análisis de necesidades de la topología

6.6. Protección perimetral
- 6.6.1. DMZs
- 6.6.2. *Firewalls*
- 6.6.3. Arquitecturas comunes
- 6.6.4. *Zero Trust Network Access*

6.7. IDS e IPS
- 6.7.1. Características
- 6.7.2. Implementación
- 6.7.3. SIEM y SIEM CLOUDS
- 6.7.4. Detección basada en *HoneyPots*

6.8. TLS y VPN´s
- 6.8.1. SSL/TLS
- 6.8.2. TLS: Ataques comunes
- 6.8.3. VPNs con TLS
- 6.8.4. VPNs con IPSEC

6.9. Seguridad en redes inalámbricas
- 6.9.1. Introducción a las redes inalámbricas
- 6.9.2. Protocolos
- 6.9.3. Elementos claves
- 6.9.4. Ataques comunes

6.10. Redes empresariales y cómo afrontarlas
- 6.10.1. Segmentación lógica
- 6.10.2. Segmentación física
- 6.10.3. Control de acceso
- 6.10.4. Otras medidas a tomar en cuenta

Módulo 7. Análisis y Desarrollo de *Malware*

7.1. Análisis y desarrollo de *malware*
- 7.1.1. Historia y evolución del *malware*
- 7.1.2. Clasificación y tipos de *malware*
- 7.1.3. Análisis de *malware*
- 7.1.4. Desarrollo de *malware*

7.2. Preparando el entorno
- 7.2.1. Configuración de Máquinas Virtuales y *Snapshots*
- 7.2.2. Herramientas para análisis de *malware*
- 7.2.3. Herramientas para desarrollo de *malware*

7.3. Fundamentos de Windows
- 7.3.1. Formato de fichero PE (*Portable Executable*)
- 7.3.2. Procesos y *Threads*
- 7.3.3. Sistema de archivos y registro
- 7.3.4. *Windows Defender*

7.4. Técnicas de malware básicas
- 7.4.1. Generación de *shellcode*
- 7.4.2. Ejecución de *shellcode* en disco
- 7.4.3. Disco vs memoria
- 7.4.4. Ejecución de shellcode en memoria

7.5. Técnicas de malware intermedias
- 7.5.1. Persistencia en Windows
- 7.5.2. Carpeta de inicio
- 7.5.3. Claves del registro
- 7.5.4. Salvapantallas

7.6. Técnicas de *malware* avanzadas
- 7.6.1. Cifrado de *shellcode* (XOR)
- 7.6.2. Cifrado de *shellcode* (RSA)
- 7.6.3. Ofuscación de *strings*
- 7.6.4. Inyección de procesos

7.7. Análisis estático de *malware*
- 7.7.1. Analizando *packers* con DIE (Detect It Easy)
- 7.7.2. Analizando secciones con PE-Bear
- 7.7.3. Decompilación con Ghidra

7.8. Análisis dinámico de *malware*
- 7.8.1. Observando el comportamiento con Process Hacker
- 7.8.2. Analizando llamadas con API Monitor
- 7.8.3. Analizando cambios de registro con Regshot
- 7.8.4. Observando peticiones en red con TCPView

7.9. Análisis en .NET
- 7.9.1. Introducción a .NET
- 7.9.2. Decompilando con dnSpy
- 7.9.3. Depurando con dnSpy

7.10. Analizando un *malware* real
- 7.10.1. Preparando el entorno
- 7.10.2. Análisis estático del *malware*
- 7.10.3. Análisis dinámico del *malware*
- 7.10.4. Creación de reglas YARA

Módulo 8. Fundamentos Forenses y DFIR

8.1. Forense digital
- 8.1.1. Historia y evolución de la informática forense
- 8.1.2. Importancia de la informática forense en la ciberseguridad
- 8.1.3. Historia y evolución de la informática forense

8.2. Fundamentos de la informática forense
- 8.2.1. Cadena de custodia y su aplicación
- 8.2.2. Tipos de evidencia digital
- 8.2.3. Procesos de adquisición de evidencia

8.3. Sistemas de archivos y estructura de datos
- 8.3.1. Principales sistemas de archivos
- 8.3.2. Métodos de ocultamiento de datos
- 8.3.3. Análisis de metadatos y atributos de archivos

8.4. Análisis de Sistemas Operativos
- 8.4.1. Análisis forense de sistemas Windows
- 8.4.2. Análisis forense de sistemas Linux
- 8.4.3. Análisis forense de sistemas macOS

8.5. Recuperación de datos y análisis de disco
- 8.5.1. Recuperación de datos de medios dañados
- 8.5.2. Herramientas de análisis de disco
- 8.5.3. Interpretación de tablas de asignación de archivos

8.6. Análisis de redes y tráfico
- 8.6.1. Captura y análisis de paquetes de red
- 8.6.2. Análisis de registros de *firewall*
- 8.6.3. Detección de intrusiones en red

8.7. Malware y análisis de código malicioso
- 8.7.1. Clasificación de *malware* y sus características
- 8.7.2. Análisis estático y dinámico de *malware*
- 8.7.3. Técnicas de desensamblado y depuración

8.8. Análisis de registros y eventos
- 8.8.1. Tipos de registros en sistemas y aplicaciones
- 8.8.2. Interpretación de eventos relevantes
- 8.8.3. Herramientas de análisis de registros

8.9. Responder a incidentes de seguridad
- 8.9.1. Proceso de respuesta a incidentes
- 8.9.2. Creación de un plan de respuesta a incidentes
- 8.9.3. Coordinación con equipos de seguridad

8.10. Presentación de evidencia y jurídico
- 8.10.1 . Reglas de evidencia digital en el ámbito legal
- 8.10.2. Preparación de informes forenses
- 8.10.3. Comparecencia en juicio como testigo experto

Módulo 9. Ejercicios de *Red Team* Avanzados

9.1. Técnicas avanzadas de reconocimiento
- 9.1.1. Enumeración avanzada de subdominios
- 9.1.2. *Google Dorking* avanzado
- 9.1.3. Redes Sociales y theHarvester

9.2. Campañas de *phishing* avanzadas
- 9.2.1. Qué es *Reverse-Proxy Phishing*
- 9.2.2. *2FA Bypass* con Evilginx
- 9.2.3. Exfiltración de datos

9.3. Técnicas avanzadas de persistencia
- 9.3.1. *Golden Tickets*
- 9.3.2. *Silver Tickets*
- 9.3.3. Técnica *DCShadow*

9.4. Técnicas avanzadas de evasión
- 9.4.1. Bypass de AMSI
- 9.4.2. Modificación de herramientas existentes
- 9.4.3. Ofuscación de *Powershell*

9.5. Técnicas avanzadas de movimiento 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 avanzadas de post-explotación
- 9.6.1. *Dump* de LSASS
- 9.6.2. *Dump* de SAM
- 9.6.3. Ataque *DCSync*

9.7. Técnicas avanzadas de *pivoting*
- 9.7.1. Qué es el *pivoting*
- 9.7.2. Túneles con SSH
- 9.7.3. Pivoting con Chisel

9.8. Intrusiones físicas
- 9.8.1. Vigilancia y reconocimiento
- 9.8.2. *Tailgating* y *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. Lectura de tarjetas RFID
- 9.10.2. Manipulación de tarjetas RFID
- 9.10.3. Creación de tarjetas clonadas

Módulo 10. Reporte Técnico y Ejecutivo

10.1. Proceso de reporte
- 10.1.1. Estructura de un reporte
- 10.1.2. Proceso de reporte
- 10.1.3. Conceptos clave
- 10.1.4. Ejecutivo vs Técnico

10.2. Guías
- 10.2.1. Introducción
- 10.2.2. Tipos de Guías
- 10.2.3. Guías nacionales
- 10.2.4. Casos de uso

10.3. Metodologías
- 10.3.1. Evaluación
- 10.3.2. *Pentesting*
- 10.3.3. Repaso de metodologías comunes
- 10.3.4. Introducción a metodologías nacionales

10.4. Enfoque técnico de la fase de reporte
- 10.4.1. Entendiendo los límites del *pentester*
- 10.4.2. Uso y claves del lenguaje
- 10.4.3. Presentación de la información
- 10.4.4. Errores comunes

10.5. Enfoque ejecutivo de la fase de reporte
- 10.5.1. Ajustando el informe al contexto
- 10.5.2. Uso y claves del lenguaje
- 10.5.3. Estandarización
- 10.5.4. Errores comunes

10.6. OSSTMM
- 10.6.1. Entendiendo la metodología
- 10.6.2. Reconocimiento
- 10.6.3. Documentación
- 10.6.4. Elaboración del informe

10.7. LINCE
- 10.7.1. Entendiendo la metodología
- 10.7.2. Reconocimiento
- 10.7.3. Documentación
- 10.7.4. Elaboración del informe

10.8. Reportando vulnerabilidades
- 10.8.1. Conceptos clave
- 10.8.2. Cuantificación del alcance
- 10.8.3. Vulnerabilidades y evidencias
- 10.8.4. Errores comunes

10.9. Enfocando el informe al cliente
- 10.9.1. Importancia de las pruebas de trabajo
- 10.9.2. Soluciones y mitigaciones
- 10.9.3. Datos sensibles y relevantes
- 10.9.4. Ejemplos prácticos y casos

10.10. Reportando *retakes*
- 10.10.1. Conceptos claves
- 10.10.2. Entendiendo la información heredada
- 10.10.3. Comprobación de errores
- 10.10.4. Añadiendo información

06

Metodología

Este programa de capacitación ofrece una forma diferente de aprender. Nuestra metodología se desarrolla a través de un modo de aprendizaje de forma cíclica: ***el Relearning***.

Este sistema de enseñanza es utilizado, por ejemplo, en las facultades de medicina más prestigiosas del mundo y se ha considerado uno de los más eficaces por publicaciones de gran relevancia como el ***New England Journal of Medicine.***

Descubre el Relearning, un sistema que abandona el aprendizaje lineal convencional para llevarte a través de sistemas cíclicos de enseñanza: una forma de aprender que ha demostrado su enorme eficacia, especialmente en las materias que requieren memorización"

Estudio de Caso para contextualizar todo el contenido

Nuestro programa ofrece un método revolucionario de desarrollo de habilidades y conocimientos. Nuestro objetivo es afianzar competencias en un contexto cambiante, competitivo y de alta exigencia.

Con TECH podrás experimentar una forma de aprender que está moviendo los cimientos de las universidades tradicionales de todo el mundo"

Accederás a un sistema de aprendizaje basado en la reiteración, con una enseñanza natural y progresiva a lo largo de todo el temario.

El alumno aprenderá, mediante actividades colaborativas y casos reales, la resolución de situaciones complejas en entornos empresariales reales.

Un método de aprendizaje innovador y diferente

El presente programa de TECH es una enseñanza intensiva, creada desde 0, que propone los retos y decisiones más exigentes en este campo, ya sea en el ámbito nacional o internacional. Gracias a esta metodología se impulsa el crecimiento personal y profesional, dando un paso decisivo para conseguir el éxito. El método del caso, técnica que sienta las bases de este contenido, garantiza que se sigue la realidad económica, social y profesional más vigente.

> *Nuestro programa te prepara para afrontar nuevos retos en entornos inciertos y lograr el éxito en tu carrera"*

El método del caso ha sido el sistema de aprendizaje más utilizado por las mejores escuelas de Informática del mundo desde que éstas existen. Desarrollado en 1912 para que los estudiantes de Derecho no solo aprendiesen las leyes a base de contenidos teóricos, el método del caso consistió en presentarles situaciones complejas reales para que tomasen decisiones y emitiesen juicios de valor fundamentados sobre cómo resolverlas. En 1924 se estableció como método estándar de enseñanza en Harvard.

Ante una determinada situación, ¿qué debería hacer un profesional? Esta es la pregunta a la que te enfrentamos en el método del caso, un método de aprendizaje orientado a la acción. A lo largo del curso, los estudiantes se enfrentarán a múltiples casos reales. Deberán integrar todos sus conocimientos, investigar, argumentar y defender sus ideas y decisiones.

Relearning Methodology

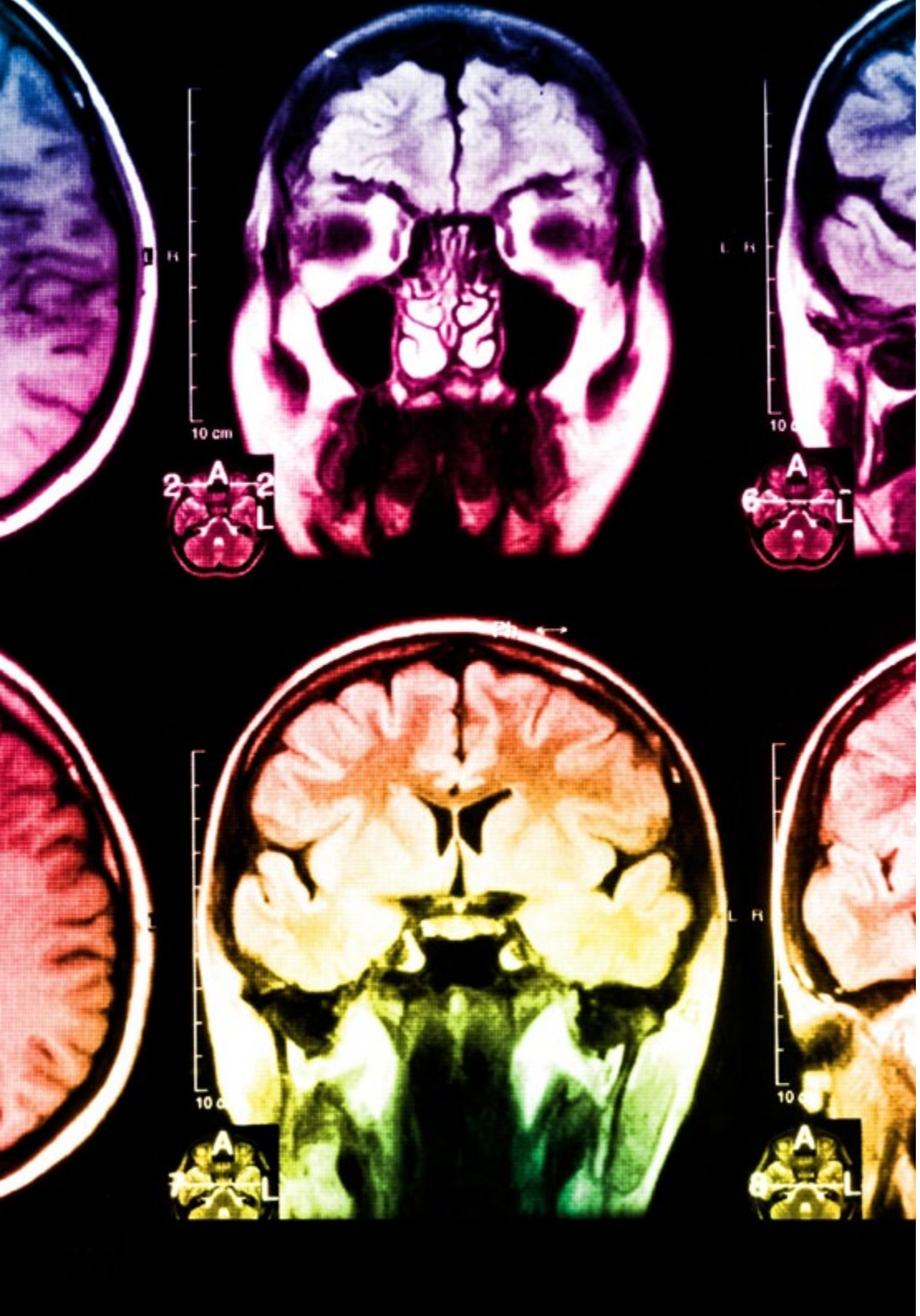
TECH aúna de forma eficaz la metodología del Estudio de Caso con un sistema de aprendizaje 100% online basado en la reiteración, que combina elementos didácticos diferentes en cada lección.

Potenciamos el Estudio de Caso con el mejor método de enseñanza 100% online: el Relearning.

En 2019 obtuvimos los mejores resultados de aprendizaje de todas las universidades online en español en el mundo.

En TECH aprenderás con una metodología vanguardista concebida para capacitar a los directivos del futuro. Este método, a la vanguardia pedagógica mundial, se denomina Relearning.

Nuestra universidad es la única en habla hispana licenciada para emplear este exitoso método. En 2019, conseguimos mejorar los niveles de satisfacción global de nuestros alumnos (calidad docente, calidad de los materiales, estructura del curso, objetivos…) con respecto a los indicadores de la mejor universidad online en español.



En nuestro programa, el aprendizaje no es un proceso lineal, sino que sucede en espiral (aprender, desaprender, olvidar y reaprender). Por eso, se combinan cada uno de estos elementos de forma concéntrica. Con esta metodología se han capacitado más de 650.000 graduados universitarios con un éxito sin precedentes en ámbitos tan distintos como la bioquímica, la genética, la cirugía, el derecho internacional, las habilidades directivas, las ciencias del deporte, la filosofía, el derecho, la ingeniería, el periodismo, la historia o los mercados e instrumentos financieros. Todo ello en un entorno de alta exigencia, con un alumnado universitario de un perfil socioeconómico alto y una media de edad de 43,5 años.

El Relearning te permitirá aprender con menos esfuerzo y más rendimiento, implicándote más en tu capacitación, desarrollando el espíritu crítico, la defensa de argumentos y el contraste de opiniones: una ecuación directa al éxito.

A partir de la última evidencia científica en el ámbito de la neurociencia, no solo sabemos organizar la información, las ideas, las imágenes y los recuerdos, sino que sabemos que el lugar y el contexto donde hemos aprendido algo es fundamental para que seamos capaces de recordarlo y almacenarlo en el hipocampo, para retenerlo en nuestra memoria a largo plazo.

De esta manera, y en lo que se denomina Neurocognitive context-dependent e-learning, los diferentes elementos de nuestro programa están conectados con el contexto donde el participante desarrolla su práctica profesional.

Este programa ofrece los mejores materiales educativos, preparados a conciencia para los profesionales:

Material de estudio

Todos los contenidos didácticos son creados por los especialistas que van a impartir el curso, específicamente para él, de manera que el desarrollo didáctico sea realmente específico y concreto.

Estos contenidos son aplicados después al formato audiovisual, para crear el método de trabajo online de TECH. Todo ello, con las técnicas más novedosas que ofrecen piezas de gran calidad en todos y cada uno los materiales que se ponen a disposición del alumno.

Clases magistrales

Existe evidencia científica sobre la utilidad de la observación de terceros expertos.

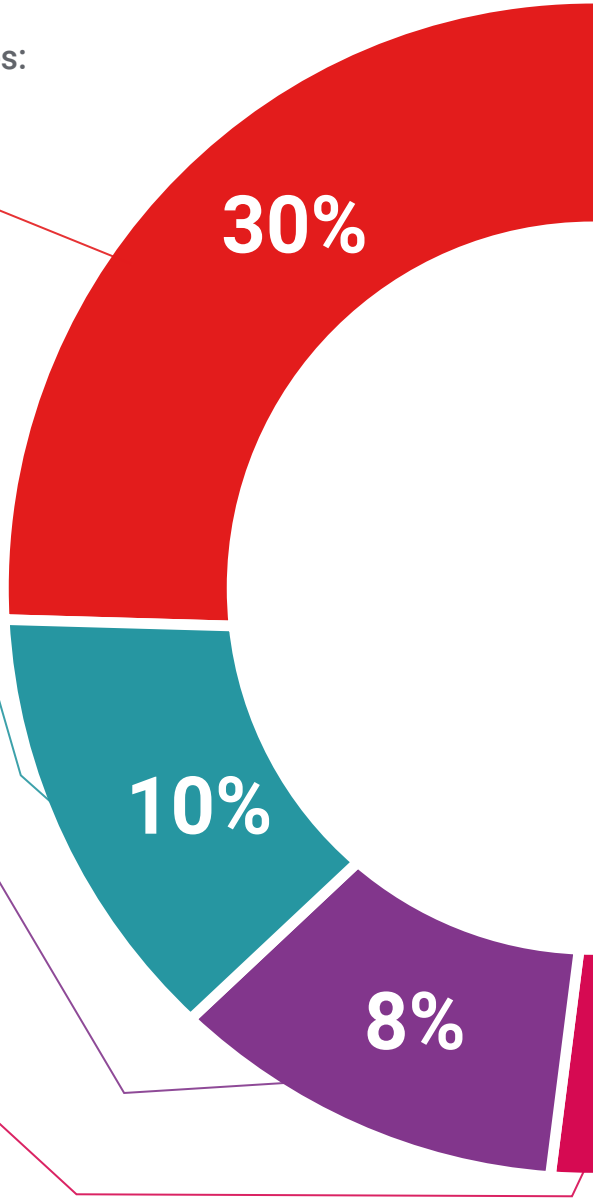
El denominado Learning from an Expert afianza el conocimiento y el recuerdo, y genera seguridad en las futuras decisiones difíciles.

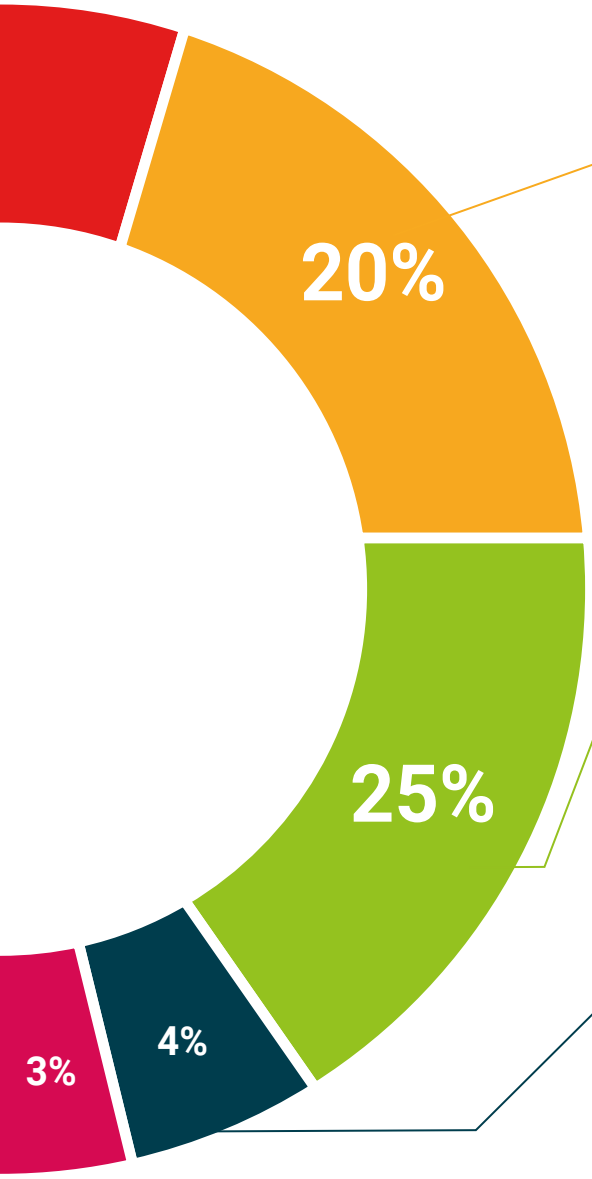
Prácticas de habilidades y competencias

Realizarán actividades de desarrollo de competencias y habilidades específicas en cada área temática. Prácticas y dinámicas para adquirir y desarrollar las destrezas y habilidades que un especialista precisa desarrollar en el marco de la globalización que vivimos.

Lecturas complementarias

Artículos recientes, documentos de consenso y guías internacionales, entre otros. En la biblioteca virtual de TECH el estudiante tendrá acceso a todo lo que necesita para completar su capacitación.





Case studies

Completarán una selección de los mejores casos de estudio elegidos expresamente para esta titulación. Casos presentados, analizados y tutorizados por los mejores especialistas del panorama internacional.

Resúmenes interactivos

El equipo de TECH presenta los contenidos de manera atractiva y dinámica en píldoras multimedia que incluyen audios, vídeos, imágenes, esquemas y mapas conceptuales con el fin de afianzar el conocimiento.

Este exclusivo sistema educativo para la presentación de contenidos multimedia fue premiado por Microsoft como "Caso de éxito en Europa".

Testing & Retesting

Se evalúan y reevalúan periódicamente los conocimientos del alumno a lo largo del programa, mediante actividades y ejercicios evaluativos y autoevaluativos para que, de esta manera, el estudiante compruebe cómo va consiguiendo sus metas.

07

Titulación

El Máster Título Propio en Pentesting y Red Team garantiza, además de la capacitación más rigurosa y actualizada, el acceso a un título de Máster Propio expedido por TECH Universidad Tecnológica.

Supera con éxito este programa y recibe tu titulación universitaria sin desplazamientos ni farragosos trámites”

Este **Máster Título Propio en Pentesting y Red Team** contiene el programa más completo y actualizado del mercado.

Tras la superación de la evaluación, el alumno recibirá por correo postal* con acuse de recibo su correspondiente título de **Máster Propio** emitido por **TECH Universidad Tecnológica.**

El título expedido por **TECH Universidad Tecnológica** expresará la calificación que haya obtenido en el Máster Título Propio, y reunirá los requisitos comúnmente exigidos por las bolsas de trabajo, oposiciones y comités evaluadores de carreras profesionales.

Título: **Máster Título Propio en Pentesting y Red Team**

Modalidad: **online**

Duración: **12 meses**

tech universidad tecnológica

Otorga la presente

CONSTANCIA

a

C. _____, con documento de identificación nº_____

Por haber superado con éxito y acreditado el programa de

MÁSTER TÍTULO PROPIO

en

Pentesting y Red Team

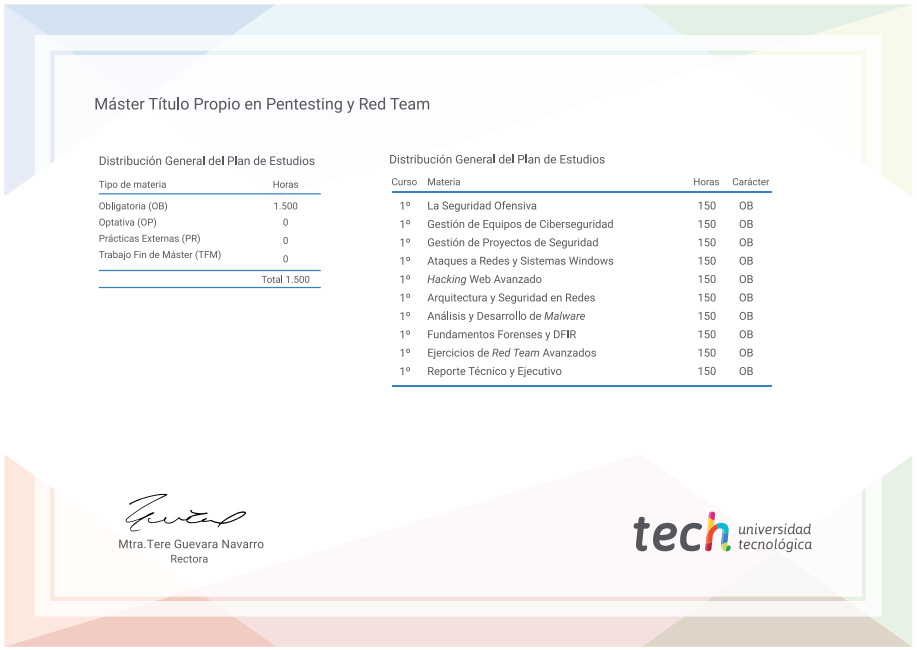
Se trata de un título propio de esta Universidad con una duración de 1.500 horas, con fecha de inicio dd/mm/aaaa y fecha de finalización dd/mm/aaaa.

TECH es una Institución Particular de Educación Superior reconocida por la Secretaría de Educación Pública a partir del 28 de junio de 2018.

A 17 de junio de 2020

Mtra.Tere Guevara Navarro
Rectora

código único TECH: AFWOR23S techtitute.com/titulos



Máster Título Propio en Pentesting y Red Team

Distribución General del Plan de Estudios

Tipo de materia	Horas
Obligatoria (OB)	1.500
Optativa (OP)	0
Prácticas Externas (PR)	0
Trabajo Fin de Máster (TFM)	0
	Total 1.500

Distribución General del Plan de Estudios

Curso	Materia	Horas	Carácter
1º	La Seguridad Ofensiva	150	OB
1º	Gestión de Equipos de Ciberseguridad	150	OB
1º	Gestión de Proyectos de Seguridad	150	OB
1º	Ataques a Redes y Sistemas Windows	150	OB
1º	*Hacking* Web Avanzado	150	OB
1º	Arquitectura y Seguridad en Redes	150	OB
1º	Análisis y Desarrollo de *Malware*	150	OB
1º	Fundamentos Forenses y DFIR	150	OB
1º	Ejercicios de *Red Team* Avanzados	150	OB
1º	Reporte Técnico y Ejecutivo	150	OB

Mtra.Tere Guevara Navarro
Rectora

tech universidad tecnológica

*Apostilla de La Haya. En caso de que el alumno solicite que su título en papel recabe la Apostilla de La Haya, TECH EDUCATION realizará las gestiones oportunas para su obtención, con un coste adicional.

tech universidad tecnológica

Máster Título Propio
Pentesting y Red Team

- Modalidad: **online**
- Duración: **12 meses**
- Titulación: **TECH Universidad Tecnológica**
- Horario: **a tu ritmo**
- Exámenes: **online**

Máster Título Propio
Pentesting y Red Team

tech universidad tecnológica