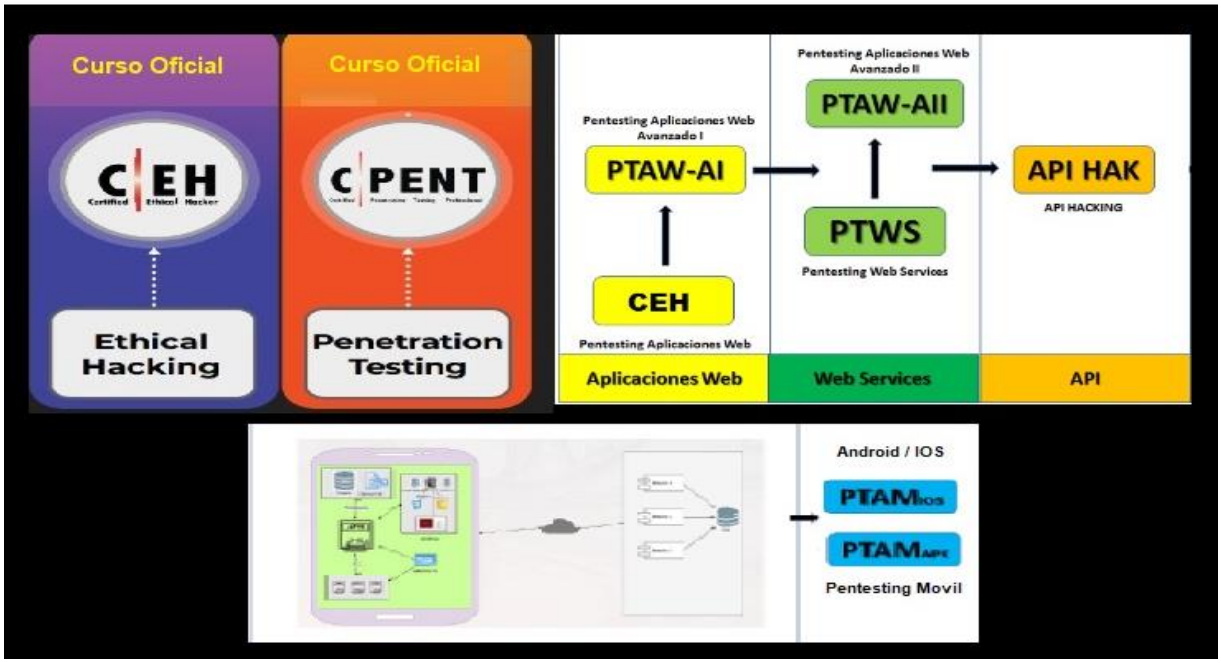
Especialista en Hacking Etico y Pentesting

Programa : Especialista en Hacking Etico y Pentesting
Duración : 224 Horas (8 meses aprox)

I. DESCRIPCIÓN



Es un Programa Integral de Ethical Hacking y Pentesting el cual permitirá a los participantes estar preparado para realizar trabajos de Ethical hacking en ambientes reales utilizando técnicas actuales y metodologías eficientes permitiendo al participante desarrollar destreza de campo y conocimientos avanzados que un especialista en Hacking ético tiene que saber.

A diferencia de otro tipo de formación estrictamente teórico, este se verá inmerso en sesiones interactivas con prácticas en laboratorios después de cada tema. Usted puede explorar sus conocimientos adquiridos en el aula para pentesting, Hacking. El ambiente de laboratorio intenso le da un conocimiento profundo y práctico al experimentar con los sistemas de seguridad actuales y esenciales.

Usted primero comenzará con el curso de CEH (Certified Ethical Hacker) que le permitirá la comprensión de cómo funcionan las defensas del perímetro y luego se trasladan a la exploración y atacar redes, los sistemas y páginas web. También aprenderás cómo los intrusos escalan privilegios y las medidas que se pueden tomar para garantizar un sistema. Usted también ganará conocimiento acerca de

Detección de Intrusos, Creación de Políticas, Ingeniería Social, Ataques DDoS, desbordamientos de búffer, y Creación de Virus.

El Segundo Curso, será CPENT (Certified Penetration Testing Professional) que es un completo programa de formación práctica. Este curso de formación de Pruebas de Penetración utiliza escenarios en tiempo real para formar a los estudiantes en las metodologías de pruebas de penetración. CPENT le ayudará a dominar una metodología de pruebas de penetración documentado que es repetible y que puede ser utilizado en un trabajo de pruebas de penetración, a nivel mundial.

El tercer programa esta conformado por 4 cursos Prácticos de Pentesting de Aplicaciones Web Avanzado centrado en el TOP Ten de OWASP el cual estará basado en el desarrollo de las técnicas utilizadas en el Testing Guide de Owasp para el test de vulnerabilidades de Páginas Web, este será un curso práctico para mejorar las destrezas en las pruebas de vulnerabilidades web.

Para completar las destrezas y herramientas necesarias para el desarrollo de un Pentester, hemos incluido el curso de Pentesting de Aplicaciones Móviles enfocada a poder desarrollar pentesting de aplicaciones móviles en APK e IPA, donde se revisarán temas de Analisis estático y Analisis dinámico de aplicaciones móviles empresariales.

II. METODOLOGÍA

El curso tiene la modalidad virtual. Se empleará material audiovisual con la finalidad de facilitar los procesos de adquisición y evaluación del aprendizaje. Durante las clases se buscará la participación activa de los alumnos mediante el desarrollo de ejercicios de hacking y uso de herramientas.

En caso de desarrollo de casos o laboratorios practicos, cada alumno contara con maquinas virtuales para el desarrollo de las actividades practicas.

III. REQUISITOS

- Conocimiento básicos de Redes LAN y Linux.

IV. MATERIALES

- Manuales Oficiales de CEH v13 y CPENT para los cursos de EC COUNCIL con voucher de Certificación oficial.
- Manuales Digitales para todos los cursos adicionales.

CERTIFICACION:

Se incluye 2 voucher para los examen de certificación oficial de EC Council para los cursos de los módulos desarrollados.

- **Certified Ethical Hacker (CEH), Exam 312-50**
- **Certified Penetration Testing Professional (CPENT)**

Adicionalmente se emitirá un certificado de asistencia al curso para los cursos que no incluyen voucher de certificación oficial

V. PLAN DE TEMAS

El programa incluye los siguientes módulos

Módulo 1 : Certified Ethical Hacker - CEH V13 (40Hr)
Módulo 2 : Certified Penetration Testing Professional (40Hr)
Módulo 3 : Pentesting de Aplicaciones Web Avanzado - Online (96Hr)
Módulo 4 : Pentesting de Aplicaciones Móviles - Online (48Hr)

Se incluye 2 voucher para los examen de certificación oficial de EC Council para los cursos de los módulos desarrollados.

- **Certified Ethical Hacker (CEH), Exam 312-50**
- **Certified Penetration Testing Professional (CPENT)**

Módulo 1 : EC Council Certified Ethical Hacking v13 (40 Hrs)

DESCRIPCIÓN

CURSO OFICIAL : **EC Council Certified Ethical Hacking v13**

Duración : 40 Horas

Observaciones:

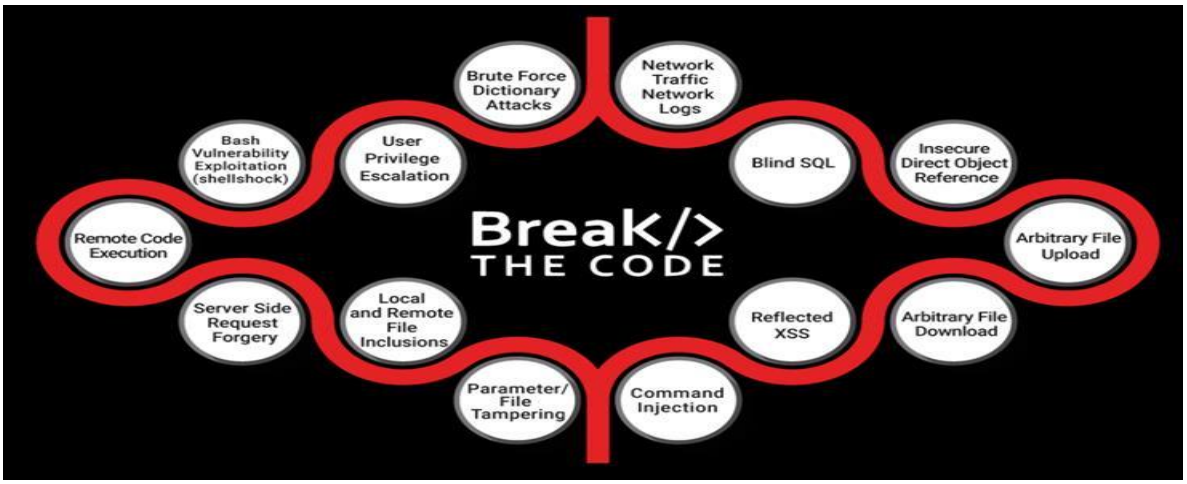
- El curso incluye manuales oficiales del curso
- Herramientas para CEH
- Acceso al Portal de EC Council
- Certificado de Asistencia al Curso
- Los laboratorios son insitu con máquinas reales.
- El curso incluye un voucher de examen para la Certificación CEH 312-50

DESCRIPCION DEL CURSO:

Certified Ethical Hacker CEH v13 le enseñará las últimas herramientas, técnicas con IA y metodologías de Hacking de nivel comercial utilizadas por Hacker y profesionales de seguridad de la información para Hackear legalmente una organización.

Aspectos destacados de algunas de las cosas que distinguen a CEH v13 del resto:

¡24 increíbles desafíos de hacking en 4 niveles de complejidad que cubren 18 vectores de ataque, incluido el OWASP Top 10 como parte de nuestra plataforma de gamificación ahora se incluyen como parte de CEH v13!



¿Quién es un hacker ético certificado?

Un hacker ético certificado es un especialista que normalmente trabaja en un red team, centrado en atacar sistemas informáticos y obtener acceso a redes, aplicaciones, bases de datos y otros datos críticos en sistemas seguros. Un CEH comprende las estrategias de ataque, el uso de vectores de ataque creativos e imita las habilidades y la creatividad de los hackers malintencionados. A diferencia de los hackers y actores malintencionados, los Certified Ethical Hackers operan con el permiso de los propietarios del sistema y toman todas las precauciones para garantizar que los resultados sigan siendo confidenciales. Los investigadores de Bug Bounty son hackers éticos expertos que utilizan sus habilidades de ataque para descubrir vulnerabilidades en los sistemas.

Detalle del Curso

La certificación de Certified Ethical Hacker (CEH) es la certificación y el logro de Hacking etico más confiable recomendado por empleadores a nivel mundial. Es la certificación de seguridad de la información más deseada y representa una de las credenciales cibernéticas de más rápido crecimiento requeridas por la infraestructura crítica y los proveedores de servicios esenciales. Desde la introducción de CEH en 2003, se reconoce como un estándar dentro de la comunidad de seguridad de la información. CEH v13 continúa presentando las últimas técnicas de hacking y las herramientas de hacking y exploits más avanzados que utilizan los piratas informáticos y los profesionales de seguridad de la información en la actualidad.

Las cinco fases del hackeo ético y la misión principal original de CEH siguen siendo válidas y relevantes hoy en día: “Para vencer a un hacker, debes pensar como un hacker.

Temas nuevos de CEH v13

CEH proporciona una comprensión profunda de las fases de piratería ética, varios vectores de ataque y contramedidas preventivas. Le enseñará cómo piensan y actúan los hackers de manera maliciosa para que esté mejor posicionado para configurar su infraestructura de seguridad y defender ataques futuros. Comprender las debilidades y vulnerabilidades del sistema ayuda a las organizaciones a fortalecer sus controles de seguridad del sistema para minimizar el riesgo de un incidente. CEH se creó para incorporar un entorno práctico y un proceso sistemático en todos los dominios y metodologías de piratería ética, lo que le brinda la oportunidad de trabajar para demostrar el conocimientos y habilidades necesarios para realizar el trabajo de un hacker ético. Estará expuesto a una postura completamente diferente hacia las responsabilidades y medidas necesarias para estar seguro. En su versión 13, CEH continúa evolucionando con los últimos sistemas operativos, herramientas, tácticas, exploits y tecnologías.

Aquí hay algunas actualizaciones críticas de CEH v13:

- **Incorporación del sistema operativo Parrot Security**

En comparación con Kali Linux, Parrot Security OS ofrece un mejor rendimiento en computadoras portátiles y máquinas de menor potencia al tiempo que ofrece una apariencia intuitiva con un repositorio más grande de herramientas generales.

- **Reasignado al marco NIST / NICE**

CEH v13 se asigna rigurosamente a áreas de especialidad importantes bajo la categoría de rol de trabajo Proteger y defender (PR) del marco NIST / NICE que se superpone con otros roles de trabajo, incluidos Analizar (AN) y Provisión segura (SP).

- **Módulos mejorados de seguridad en la nube, IoT y OT**

CEH v13 cubre los módulos actualizados de Cloud e IoT para incorporar las tecnologías de contenedores de CSP (por ejemplo, Docker, Kubernetes), amenazas de Cloud Computing y una serie de herramientas de piratería de IoT (por ejemplo, Shikra, Bus Pirate, Facedancer21 y más). Esto es fundamental a medida que el mundo avanza hacia una adopción de la nube más amplia y profunda.

- **Amenazas basadas en la nube**

  Dado que se estima que la industria de la nube alcanzará los $ 354 mil millones para 2022, las empresas luchan por limitar la frecuencia de los incidentes de robo de datos debido a entornos de nube mal configurados. Solo de enero a abril de 2020 se registró un aumento del 630% en los ataques basados en la nube. Aprenda a evitar, identificar y responder a los ataques basados en la nube con CEH v13

- **Amenazas de IoT**

  Los informes de mercado anticipan que se espera que los dispositivos conectados a IoT en todo el mundo alcancen los 43 mil millones en 2023. Para respaldar esta rápida expansión, los jugadores prominentes de Internet, incluidos Amazon Web Services, Google, IBM, Microsoft, están cambiando rápidamente a servicios de nube privada. , creando complejidades en los ecosistemas de IoT. Aprenda a lidiar con los ataques basados en IoT con el curso CEH v13 que cubre las últimas herramientas de piratería de IoT, como Shikra, Bus Pirate, Facedancer21 y muchas otras.

- **Ataques de tecnología operativa (OT)**

  El año pasado, las empresas experimentaron un aumento del 2,000% en incidentes basados en OT. Puede adquirir experiencia en OT, TI e IIoT (IoT industrial) para asegurar las implementaciones de OT / IoT empresariales críticas. Para aprender las habilidades avanzadas de OT, CEH cubre conceptos de OT, como ICS, SCADA y PLC, varios desafíos de OT, metodología de piratería OT, herramientas, protocolos de comunicación de una red OT como Modbus, Profinet, HART-IP, SOAP , CANopen, DeviceNet, Zigbee, Profibus, etc., y obteniendo acceso remoto mediante el protocolo DNP3.

- **Análisis de malware moderno**

CEH v13 ahora incluye las últimas tácticas de análisis de malware para ransomware, malware bancario y financiero, botnets de IoT, análisis de malware OT, malware de Android y más.

- **Cubriendo las últimas amenazas: malware sin archivos**

A medida que la comunidad de seguridad observó un aumento en los ataques sin archivos, comenzó a generar preocupaciones sobre los ataques de malware sin archivos. Dado que el malware sin archivos es una forma relativamente nueva de ataque de malware, a las organizaciones les resulta difícil de detectar con soluciones

de seguridad para terminales. Con CEH v13, ahora puede aprender varias técnicas de malware sin archivos con estrategias defensivas asociadas, ya que el curso se enfoca en la taxonomía de las amenazas de malware sin archivos, técnicas de ofuscación de malware sin archivos para evitar el antivirus, lanzar malware sin archivos a través de la inyección basada en scripts, lanzar malware sin archivos. a través del phishing y más.

- **Nuevos diseños de laboratorio y sistemas operativos**

Esta última versión de CEH v13 incluye nuevos sistemas operativos, incluidos Windows Server 2022, Windows Server 2019 y Windows 11 configurados con controlador de dominio, firewalls y aplicaciones web vulnerables para practicar y mejorar las habilidades de piratería.

- **Mayor tiempo de laboratorio y enfoque práctico**

Más del 50% del curso CEH v13 está dedicado a habilidades prácticas en rangos en vivo a través de los laboratorios del EC-Council. EC-Council es líder en este aspecto de la industria.

- **La biblioteca de herramientas más completa de la industria**

El curso CEH v13 incluye una biblioteca de las últimas herramientas requeridas por los profesionales de la seguridad y los probadores de escritura en todo el mundo.

Esquema del curso

Module 01	Introduction to Ethical Hacking
Module 02	Footprinting and Reconnaissance
Module 03	Scanning Networks
Module 04	Enumeration
Module 05	Vulnerability Analysis
Module 06	System Hacking
Module 07	Malware Threats
Module 08	Sniffing
Module 09	Social Engineering
Module 10	Denial-of-Service
Module 11	Session Hijacking
Module 12	Evading IDS, Firewalls, and Honeypots
Module 13	Hacking Web Servers
Module 14	Hacking Web Applications
Module 15	SQL Injection
Module 16	Hacking Wireless Networks
Module 17	Hacking Mobile Platforms
Module 18	IoT and OT Hacking
Module 19	Cloud Computing
Module 20	Cryptography

BREAK-THE-CODE Challenge!

- BTC lleva la ramificación al siguiente nivel, repleto de 24 desafíos de hacking increíbles (¡con esteroides!), En 4 niveles de complejidad que cubren 18 vectores de ataque, ¡incluido el Top 10 de OWASP!

- Cubre vulnerabilidades que van desde una secuencia de comandos básica entre sitios hasta una dinámica avanzada de varios niveles, lo que finalmente brinda acceso a todo el servidor.

- Algunas de las vulnerabilidades cubiertas son XSS, SQLi, IDoR y ejecución remota de código.

- Se requiere que los estudiantes posean diversas habilidades y procedimientos para capturar la bandera de cada vulnerabilidad en diferentes niveles.

- Viene con una interfaz de usuario interactiva, a la que los alumnos se conectan a través de una VPN para acceder a las aplicaciones.

- Contiene un sistema de puntuación dinámico que rastrea los niveles de ascenso de un alumno, y los competidores lo ven en el panel del portal.

¿Qué deberías aprender?

- Los problemas clave incluyen plagar el mundo de la seguridad de la información, piratería ética, controles de seguridad de la información, leyes y estándares.
- Realice huellas y reconocimiento utilizando las últimas técnicas y herramientas de huellas como fase crítica previa al ataque requerida en la piratería ética.
- Técnicas de exploración en red y contramedidas de exploración.
- Técnicas de enumeración y contramedidas de enumeración.
- Análisis de vulnerabilidades para identificar lagunas de seguridad en la red, la infraestructura de comunicaciones y los sistemas finales de la organización objetivo.
- Metodología de pirateo del sistema, esteganografía, ataques de esteganálisis y cobertura de pistas para descubrir vulnerabilidades del sistema y la red.
- Diferentes tipos de malware (troyanos, virus, gusanos, etc.), auditoría del sistema para detectar ataques de malware, análisis de malware y contramedidas.
- Técnicas de rastreo de paquetes para descubrir vulnerabilidades de la red y contramedidas para defender el rastreo.
- Técnicas de ingeniería social y cómo identificar ataques de robo para auditar vulnerabilidades a nivel humano y sugerir contramedidas de ingeniería social.
- Técnicas y herramientas de ataque DoS / DDoS para auditar un objetivo y contramedidas DoS / DDoS.
- Técnicas de secuestro de sesiones para descubrir la gestión de sesiones a nivel de red, autenticación / autorización, debilidades criptográficas y contramedidas.
- Ataques al servidor web y una metodología de ataque integral para auditar vulnerabilidades en la infraestructura del servidor web y contramedidas.
- Ataques a aplicaciones web y metodología integral de pirateo de aplicaciones web para auditar vulnerabilidades en aplicaciones web y contramedidas.
- Técnicas de ataque de inyección de SQL, herramientas de detección de inyección para detectar intentos de inyección de SQL y contramedidas.

- Encriptación inalámbrica, metodología de piratería inalámbrica, herramientas de piratería inalámbricas y herramientas de seguridad Wi-Fi.

- Vector de ataque de plataforma móvil, explotación de vulnerabilidades de Android y pautas y herramientas de seguridad móvil.

- Técnicas de evasión de firewall, IDS y honeypot, herramientas y técnicas de evasión para auditar el perímetro de una red en busca de debilidades y contramedidas.

- Conceptos de computación en la nube (tecnología de contenedores, computación sin servidor), diversas amenazas / ataques y técnicas y herramientas de seguridad.

- Hoja de ruta de pruebas de penetración, auditoría de seguridad, evaluación de vulnerabilidades y pruebas de penetración.

- Amenazas a las plataformas de IoT y OT y aprenda a defender los dispositivos de IoT y OT de forma segura.

- Cifrados de criptografía, infraestructura de clave pública (PKI), ataques de criptografía y herramientas de criptoanálisis.

Público Objetivo

- Information Security Analyst /Administrator
- Information Assurance (IA) Security Officer
- Information Security Manager / Specialist
- Information Systems Security Engineer /Manager
- Information Security Professionals /Officers
- Information Security / IT Auditors
- Risk / Threat/Vulnerability Analyst
- System Administrators
- Network Administrators and Engineers

Detalle del Examen

Exam Title:

Certified Ethical Hacker (ANSI)

Exam Code:

312-50 (ECC EXAM), 312-50 (VUE)

Number of Questions:

125

Duration:

4 hours

Availability:

ECCEXAM / VUE

Test Format:

Multiple Choice

Passing Score:

Please refer to

https://cert.eccouncil.org/faq.html

Módulo 2 : Certified Penetration Testing Professional

CURSO OFICIAL : **Certified Penetration Testing Professional – CPENT**

Duración : 40 Horas

Observaciones:

- El curso incluye manuales oficiales del curso
- El usuario tiene acceso al Portal de EC Council para material electrónico
- Los laboratorios son especialmente creados desde EC Council a través de iLab – Portal de Laboratorio Especializado de EC Council.
- El curso incluye un voucher de examen para la Certificación ECSA.

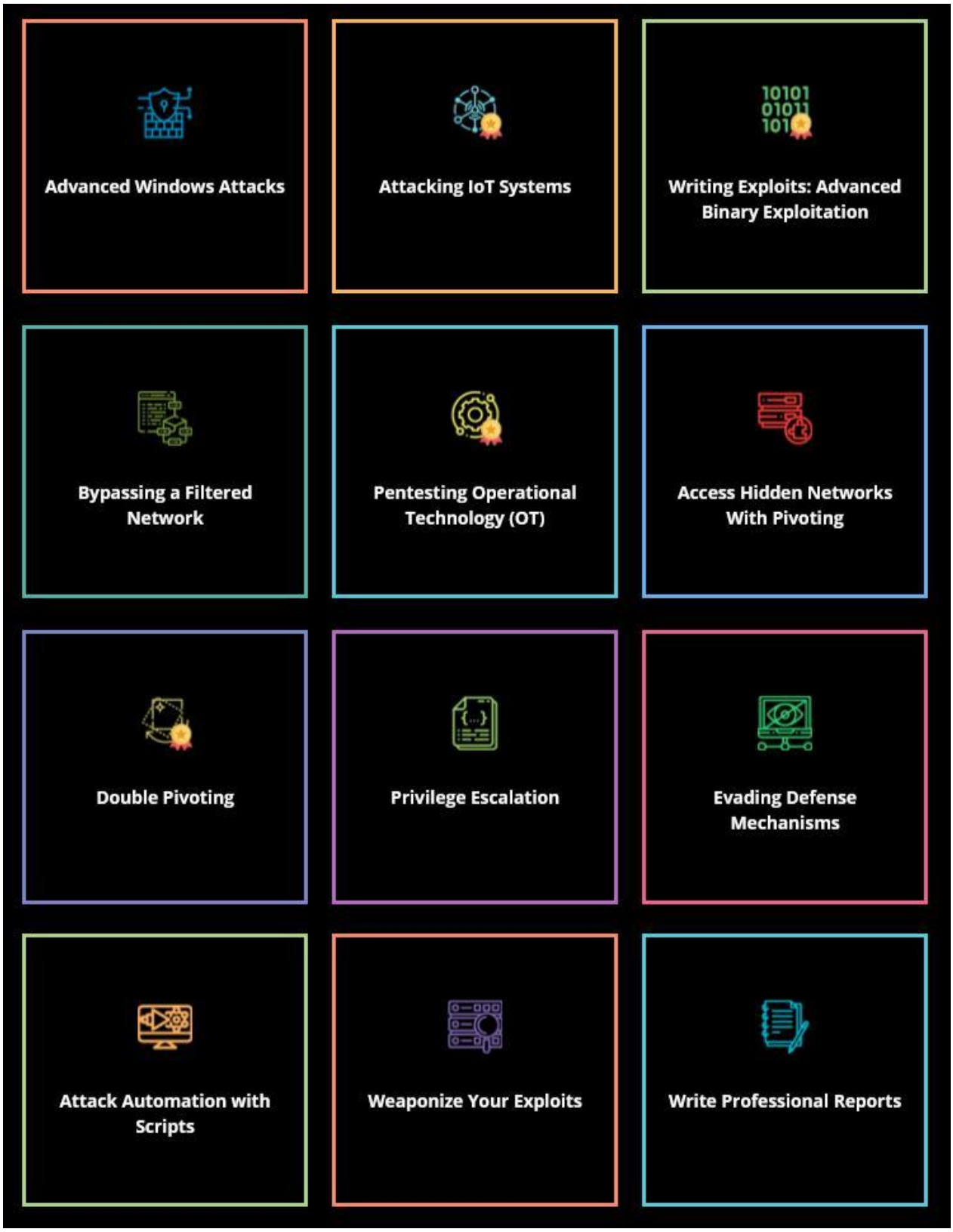
DESCRIPCION DEL CURSO:

Es un programa riguroso de pruebas de penetración que, a diferencia de los cursos de pruebas de penetración contemporáneos, le enseña cómo realizar una prueba de penetración eficaz a través de redes filtradas, herramientas propias, explotación avanzada de binarios, doble pivote para acceder a redes ocultas y diversas tecnologías. En resumen, ¡no existe un programa de este tipo en el mundo!

Por eso, por primera vez en la industria, la evaluación para el Certified Penetration Tester (CPENT) se trata de múltiples disciplinas y no solo de uno o dos tipos de especialidades.

- El curso se presenta a través de un entorno de red empresarial que debe ser atacado, explotado, evadido y defendido.
- CPENT de EC-Council brinda a la industria la capacidad de evaluar las habilidades de un Pen Tester en un amplio espectro de "zonas de red".
- Lo que hace diferente al CPENT es el requisito de que se le proporcione una variedad de diferentes ámbitos de trabajo para que el candidato pueda "pensar con rapidez".
- El resultado de esto es que hay diferentes zonas que representan diferentes tipos de pruebas.
- Cualquiera que intente la prueba deberá realizar su evaluación en estas diferentes zonas

¿Qué hace que el Certified Penetration Testing Professional (CPENT) sea único?



Para entrenar para la certificación de CPENT, EC-Council ha introducido el programa CPENT.

Las siguientes son 12 razones que hacen que el Programa CPENT sea único en su tipo. Este curso excepcional puede convertirlo en uno de los probadores de penetración más avanzados del mundo. El curso tiene un propósito: ayudarlo a superar algunos de los obstáculos más avanzados que enfrentan los practicantes del mundo real cuando realizan pruebas de penetración. Aquí hay algunos ejemplos de los desafíos que enfrentará cuando se exponga a la gama CPENT:

1. Ataques avanzados de Windows

Esta zona contiene un bosque completo al que primero debe obtener acceso y luego usar PowerShell y cualquier otro medio para ejecutar **Silver and Gold Ticket y Kerberoasting.** Las máquinas se configurarán con defensas en su lugar, lo que significa que debe usar técnicas de derivación de PowerShell y otros métodos avanzados para sumar puntos dentro de la zona.

2. Atacar los sistemas de IoT

CPENT es la primera certificación que requiere que ubique dispositivos IoT y luego obtenga acceso a la red. Una vez en la red, debe identificar el firmware del dispositivo IoT, extraerlo y luego realizar ingeniería inversa.

3. Explotaciones de escritura: explotación binaria avanzada

Encontrar código defectuoso es una habilidad que necesitan los Pentester competentes. En esta zona, necesitará encontrar binarios defectuosos y aplicar ingeniería inversa para escribir exploits y tomar el control de la ejecución del programa. La tarea es complicada ya que primero debe penetrar el perímetro para obtener acceso y luego descubrir los binarios. Una vez hecho esto, deberá aplicar ingeniería inversa al código. A diferencia de otras certificaciones, CPENT incluye desafíos de código de 32 y 64 bits y parte del código se compilará con protecciones básicas de stacks no ejecutables. Debe poder escribir un programa para explotar estos binarios y luego descubrir un método para escalar los privilegios. Esto requerirá habilidades avanzadas en explotación binaria para incluir los últimos conceptos de depuración y técnicas de egg hunting. Primero debe crear un código de entrada para tomar el control de la ejecución del programa.

4. Bypasear una red filtrada

La certificación CPENT proporciona los desafíos de la zona web que existen dentro de una arquitectura de segmentación, por lo que debe identificar el filtrado de la arquitectura y luego aprovechar este conocimiento para obtener acceso a las aplicaciones web. El siguiente desafío es comprometer y luego extraer los datos necesarios de las aplicaciones web para lograr puntos.

5. Pentesting Operational Technology (OT)

La gama CPENT contiene una zona dedicada a las redes ICS SCADA que deberá penetrar desde el lado de la red de TI y obtener acceso a la red OT. Una vez allí, deberá identificar el controlador lógico programable (PLC) y luego modificar los datos para impactar la red OT. Debe poder interceptar el protocolo de comunicación Mod Bus y la comunicación entre el PLC y otros nodos.

6. Acceda a redes ocultas con pivoting

Según nuestras pruebas beta, los Pentester tienen dificultades para identificar las reglas vigentes cuando se encuentran con una red en capas. Por lo tanto, en esta zona, deberá identificar las reglas de filtrado y luego penetrar en la red directa. A partir de ahí, tendrá que intentar pivotar en redes ocultas utilizando métodos de pivoting único, pero mediante un filtro. La mayoría de las certificaciones no tienen un verdadero pivoting entre redes dispares y pocas (si las hay) tienen el requisito de entrar y salir de un dispositivo de filtrado.

7. Doble pivoting

Una vez que haya desafiado y dominado los desafíos del pivoting, el siguiente desafío es el doble pivoting. Esto no es algo para lo que pueda utilizar una herramienta; en la mayoría de los casos, el pivoting debe configurarse manualmente. CPENT es la primera certificación en el mundo que requiere que acceda a redes ocultas utilizando doble pivoting.

8. Escalamiento de privilegios

En este desafío, se deben implementar los últimos métodos de código de ingeniería inversa de escalamiento de privilegios para tomar el control de la ejecución, luego se requiere elevar privilegios en el shell reverso para obtener root / admin.

9. Evadir los mecanismos de defensa

El programa requiere de exploits para ser probadas por diferentes defensas que tu estas probablemente viendo en la red. Tu deberás conseguir explotar estas defensas utilizándolas como armas.

10. Automatización de ataques con scripts

Prepárese para técnicas avanzadas de pruebas de penetración y secuencias de comandos con siete apéndices de autoaprendizaje: pruebas de penetración con Ruby, Python, PowerShell, Perl, BASH, Fuzzing y Metasploit.

11. Arma tu arsenal: Construya sus exploits

Personalice sus propias herramientas y construya su arsenal con su experiencia en codificación para hackear los desafíos que se le presentan como lo haría en la vida real.

12. Escribe informes profesionales

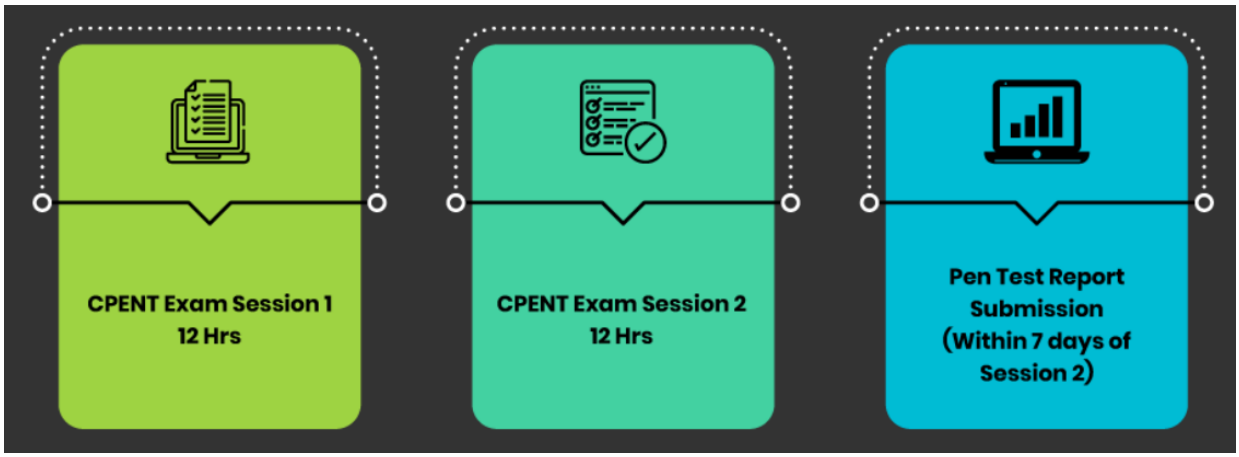
Experimente cómo un Pentester puede mitigar los riesgos y validar el informe presentado al cliente para realmente tener un impacto. ¡Las buenas pruebas de penetración no significan mucho para los clientes sin un informe claramente escrito!

Examen en vivo de CPENT

¡demuestre que tiene lo que se necesita!

CPENT es un examen práctico supervisado de forma remota y totalmente en línea que desafía a los candidatos a través de un extenuante examen práctico de 24 horas basado en el rendimiento. El examen se divide en 2 exámenes prácticos de 12 horas cada uno que pondrán a prueba su perseverancia y concentración al obligarlo a superarse en cada nuevo desafío. Los candidatos tienen la opción de elegir entre 2 exámenes de 12 horas o uno de 24 horas.

Los candidatos que obtengan una puntuación superior al **70%** obtendrán la certificación **CPENT**. Los candidatos que obtienen más del **90%** obtienen la prestigiosa credencial **LPT (Master)**.



Características del examen:

- ¡Elige tu desafío! ¡Dos sesiones de 12 horas o un solo examen de 24 horas!
- Los especialistas del EC-Council supervisan todo el examen: la validez no está en duda.
- Obtén al menos un 70% y conviértete en un CPENT
- ¡Obtenga al menos un 90% y obtenga la reconocida designación LPT (Master)!

CONTENIDO DEL CURSO

Module 01: Introduction to Penetration Testing

Module 02: Penetration Testing Scoping and Engagement

Module 03: Open Source Intelligence (OSINT)

Module 04: Social Engineering Penetration Testing

Module 05: Network Penetration Testing – External

Module 06: Network Penetration Testing– Internal

Module 07: Network Penetration Testing – Perimeter Devices

Module 08: Web Application Penetration Testing

Module 09: Wireless Penetration Testing

Module 10: IoT Penetration Testing

Module 11: OT/SCADA Penetration Testing

Module 12: Cloud Penetration Testing

Module 13: Binary Analysis and Exploitation

Module 14: Report Writing and Post Testing Actions

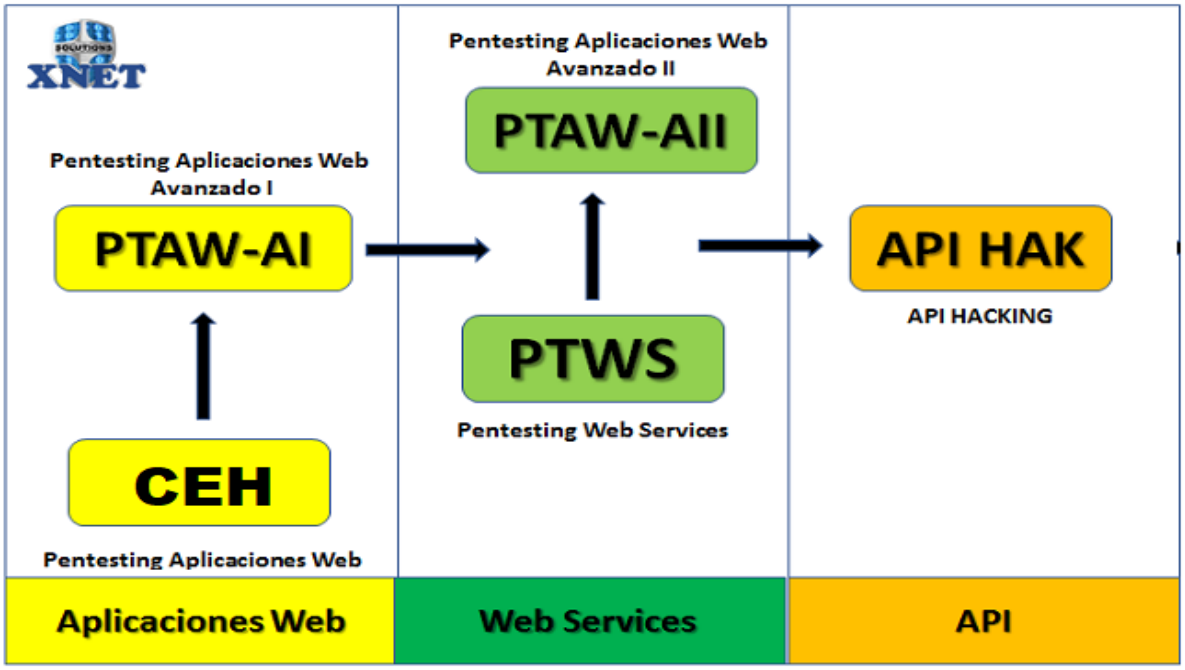
Appendix A: Penetration Testing Essential Concepts	Appendix G: Perl Environment and Scripting
Appendix B: Fuzzing	Appendix H: Ruby Environment and Scripting
Appendix C: Mastering Metasploit Framework	Appendix I: Active Directory Pen Testing
Appendix D: PowerShell Scripting	Appendix J: Database Penetration Testing
Appendix E: Bash Environment and Scripting	Appendix K: Mobile Device Penetration Testing
Appendix F: Python Environment and Scripting	

Módulo 3 : Pentesting de Aplicaciones Web Avanzado

Programa : Pentesting de Aplicaciones Web Avanzado - Online

Duración : 96 Horas (Incluye 4 cursos)

PENTESTING APLICACIONES WEB AVANZADO



El Programa de Pentesting de Aplicaciones Web Avanzado se ha desarrollado con el objetivo de entregar a los participantes la habilidad practica de realizar Análisis de Vulnerabilidades de Aplicaciones Web basado en la metodología de OWASP.

Está dirigido a profesionales de TI que cuenten con el conocimiento o hayan llevado el curso de CEH y quieran adquirir destreza en el desarrollo de Análisis de vulnerabilidades de Aplicaciones Web.

Durante este programa se desarrollarán 120 vulnerabilidades del Top Ten de Owasp, asi como metodología para desarrollar Análisis de Vulnerabilidades de Web Services y API Hacking

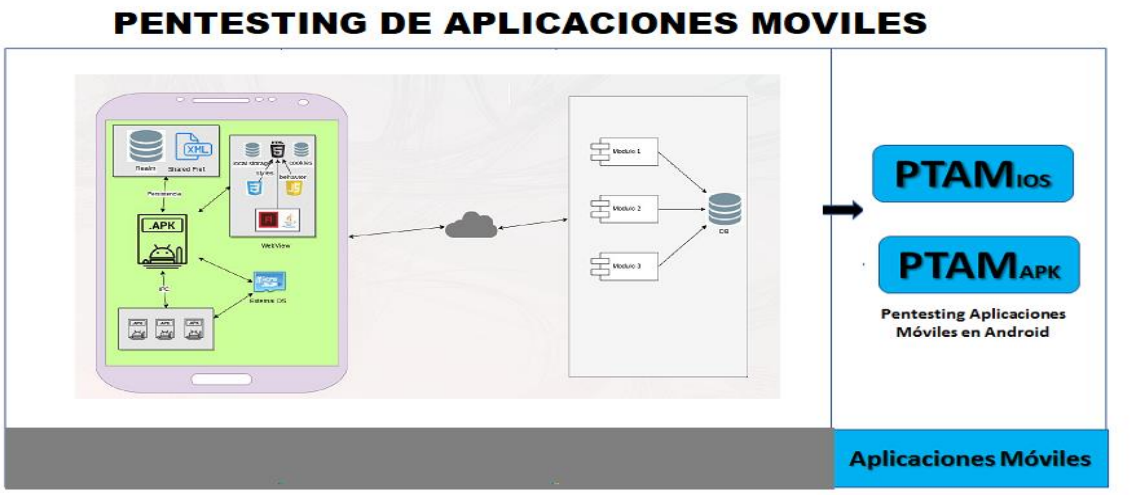
Detalle del Programa:

- Modulo 1 : Pentesting de Aplicaciones Web Avanzado I (24 Hrs)
- Modulo 2 : Pentesting Web Services (24 Hrs)
- Modulo 3 : Pentesting de Aplicaciones Web Avanzado II (24 Hrs)
- Modulo 4 : API Hacking (24 Hrs)

Módulo 4 : Pentesting de Aplicaciones Móviles

Programa : Pentesting de Aplicaciones Moviles

Duración : 48 Horas



El Programa de Pentesting de Aplicaciones Moviles ha sido desarrollado con el objetivo de entregar a los participantes el conocimiento de técnicas y metodología para el Análisis de Aplicaciones Moviles desarrollado en APK con en IPA.

Esta dirigido a profesionales de TI que quieran adquirir los conocimientos para poder realizar el Análisis de Aplicaciones Moviles, Análisis estático de Aplicaciones (APK/IPA) , Análisis dinámico , captura de tráfico seguro, reversing de código fuente

Durante el curso los participantes trabajaran con Aplicaciones Moviles reales

Detalle del Programa :

- Modulo 1 : Pentesting de Aplicaciones Moviles en Android (24 Hrs)

- Modulo 2 : Pentesting de Aplicaciones Moviles en IOS (24 Hrs)

Mod 1: Pentesting de Aplicaciones Moviles en Android (24 Hrs)

- En este curso se le mostrará cómo realizar actividades profesionales de pruebas de penetración contra aplicaciones móviles Android, mediante ingeniería inversa, análisis estático y análisis dinámico.
- Primero, aprenderá todo sobre la superficie de ataque de las aplicaciones de Android y las técnicas para explotar cada vulnerabilidad cubierta (incluida la ingeniería inversa).
- Se presentan primero los fundamentos del sistema operativo Android (VM de Android, modelo de seguridad de Android, etc.), el proceso de compilación (estructura de APK, aplicaciones de compilación / firma, etc.) y cómo configurar su propio entorno de prueba.
- Como atacar las aplicaciones de Android. Los APK de ingeniería inversa para la recopilación de información, el enraizamiento de dispositivos y toda la superficie de ataque de las aplicaciones de Android se tratan en detalle para que estén al tanto de lo que explota cada ataque.
- Análisis de tráfico de aplicaciones móviles (incluidas Bypass Certified Pinning).
- Durante el módulo de análisis estático, explotará la inyección de SQL y las vulnerabilidades de Path Traversal, así como las actividades vulnerables, los receptores vulnerables, los servicios vulnerables y las preferencias compartidas inseguras, entre otros.
- Análisis dinámico, aprovechará ADB para lograr la depuración en vivo y la interacción de la base de datos con fines de explotación.

CONTENIDO DEL CURSO

- Arquitectura Android
- Android Security Module
- Configuración de Ambientes de Testing
- Android Studio
- Proceso de Construcción Android
- Reversing de Aplicaciones APK
- Rooting de dispositivos android
- Fundamentos de Aplicaciones Android
- Técnicas de Inspección
- Inspección de Trafico de Red
- TapJacking
- Análisis de código Estático
- Análisis de Código Dinámico

Duración: 24 horas.

Mod 2 Pentesting de Aplicaciones Moviles en IOS (24 Hrs)

- En este curso, aprenderá todo sobre la superficie de ataque de las aplicaciones iOS y las técnicas para explotar cada vulnerabilidad (incluida la ingeniería inversa).
- Los fundamentos de iOS (arquitectura de seguridad, enclave seguro, touchID, firma de código), proceso de construcción (identidad de aprovisionamiento, programa de desarrollador de Apple, ofuscación, etc.) y cómo configurar su propio entorno de prueba.
- Se tratara en detalle ingeniería inversa para las aplicaciones de iOS, para la recopilación de información, el jailbreak de dispositivos y toda la superficie de ataque de las aplicaciones de iOS.
- Se cubrira el análisis de tráfico de aplicaciones móviles (incluidas Certificate pinning bypasses).
- Durante el módulo de análisis estático, aprenderá todo sobre el keychain, plist, controladores de URI personalizados y SDK de terceros.
- Durante el módulo de análisis dinámico, aprenderá a analizar en tiempo de ejecución de Objective-C, Cycript, atacar aplicaciones personalizadas y eludir la autenticación de una aplicación a través de runtime instrumentation, entre otros.

CONTENIDO DEL CURSO

- Arquitectura iOS
- Jailbreaking de Dispositivos iOS
- Configuracion de Ambientes de Testing
- Instalacion de Herramientas y Uso Basico
- Proceso de Contruccion iOS
- Reversing de Aplicaciones iOS
- Fundamentos de Aplicaciones iOS
- Fundamentos de Pruebas de iOS
- Tecnicas de Inspeccion
- Inspeccion de Trafico de Red
- Administracion de Dispositivos
- Analisis Dinamico

Duración: 24 horas.