TÉCNICO EN ETHICAL HACKING

- Curso universitario de especialización en «TÉCNICO EN ETHICAL HACKING».

- **CONDICIONES DE ACCESO DE LOS ALUMNOS:**
  Las establecidas por la legislación vigente para el acceso al sistema universitario. Adicionalmente podrán ser admitidos los alumnos que acrediten enseñanzas medias a través de una prueba de acceso, y alumnos que acrediten experiencia profesional en el área.

PRESENTACIÓN DEL CURSO

Está formado por:

- Curso de Seguridad Informática Ofensiva
- Curso de Seguridad y Hacking Web
- Curso de Seguridad y Creación de Exploits

Duración del ciclo: 450 horas.

Todas las personas que realicen este curso se podrán dar de alta en la Asociación Nacional de Tasadores, Peritos y Mediadores (ANTPM).

PROGRAMA

CURSO DE SEGURIDAD INFORMÁTICA OFENSIVA

MÓDULO 0 – INTRODUCCIÓN

- ¿Qué es un hacker?
- Perfiles de hackers
- APT (Amenazas Persistentes Avanzadas)
- Cibercriminales
- Tipos de auditorías
- Distribuciones de pentesting

MÓDULO 1 – RECOPILACIÓN DE INFORMACIÓN

- Conceptos
- Herramientas básicas

- Metadatos
- Google Dorks
- Maltego
- The harvester
- Dmitry
- Information Gathering gracias a servicios

MÓDULO 2 – ANÁLISIS DE PUERTOS Y VULNERABILIDADES

- Conceptos
- Descubrimiento de máquinas: ARP
- Recopilación de información gracias a servicios
- Análisis de puertos y vulnerabilidades: Conceptos
- Nmap, Nessus, Nikto, OWASP-ZAP
- Metasploit
- Websploit
- Searchsploit
- WPScan/JoomScan

MÓDULO 3 – CREACIÓN Y USO DE DICCIONARIOS

- Conceptos
- Diccionarios disponibles en la red
- Cruch, CeWL, CuPP
- Hydra
- Medusa
- HashCat

MÓDULO 4 – HERRAMIENTAS DE EXPLOTACIÓN

- Conceptos
- Metodología manual
- Metasploit Framwork Exploit remotos
- Exploits remotos
- Exploits locales
- Metasploit Framework Post-Explotación
- Denegación de servicios

MÓDULO 5 – EVASIÓN DE DETECCIÓN

- Introducción
- TOR, No-IP
- Malware modding

MÓDULO 6 – REDES WIRELESS

- Conceptos
- Suite Airplay
- Esnifando paquetes
- Ataques de desautenticación
- Tratando el handshake
- Evil Twin

MÓDULO 7 – ENVENERAR Y/O SUPLANTAR SERVICIOS

- Conceptos
- Envenenamiento ARP
- Bettercap, Responder
- Analizando el tráfico
- Wireshark, Xplico, IPv6

MÓDULO 8 – INGENIERÍA SOCIAL

- Conceptos
- Rogue Servers
- Beef XSS
- Falsificación de página web
- Contramedidas

MÓDULO 9 – HACKING APLICACIONES WEB

- Conceptos
- Herramientas
- RCE, SQLi, XSS, File Inclusion
- Trabajando con OWASP ZAP Y OWASP Mantra

MÓDULO 10 – TELEFONÍA MÓVIL

- Conceptos
- Auditorías de dispositivos móviles
- Creación de APK maliciosa
- Malware
- Análisis de APK sospechosa

MÓDULO 11 – POST-EXPLOTACIÓN

- Conceptos
- Escalada de privilegios
- Recolección de información
- Pivoting
- Port Forwarding
- Agujeros de configuración

CURSO DE SEGURIDAD Y HACKING WEB

MÓDULO 0 – INTRODUCCIÓN

- Conceptos básicos
- Tipos de auditoría
- Fases de auditoría
- Metodologías
- OWASP TOP 10

MÓDULO 1 – ENTORNO

- Kali
- DVWA
- Terminator
- Payloads
- Web for Pentester I y II

MÓDULO 2 – BURPSUITE

MÓDULO 3 – RECOLECCIÓN DE INFORMACIÓN

- Footprinting/Fingerprinting
- OSINT
- Redes Sociales
- Whois
- Buscadores
- Google Hacking
- Shodan
- theharvester
- org
- nmap
- fuerza bruta
- Metadatos
- WAF

MÓDULO 4 – DETECCIÓN DE VULNERABILIDADES

- Configuración
- Metodos HTTP
- Cabeceras de Seguridad
- Vulnerabilidades conocidas: cvedetails, NVD NIST, snyk
- Gestión de Errores
- Almacenamiento Navegador
- Entradas de datos
- SQLi , Command injection, XSS, LFI/RFI
- Autenticación
- Sesiones, cookies
- Enumeración de usuarios
- Autorización
- Roles / Varios usuarios
- Comunicaciones
- HTTPS, SSL
- Herramientas
- Otras vulnerabilidades
- CSRF, Clickjacking

MÓDULO 5 – INFORME

- Esquema
- Criticidad de las vulnerabilidades, CVVS (v2 y v3)

- Informe Ejecutivo
- Informe Técnico

CURSO DE SEGURIDAD Y CREACIÓN DE EXPLOITS

MÓDULO 0 – INTRODUCCIÓN

- Qué es el debugging
- Qué es el fuzzing
- Laboratorios
- Fundamentos del curso

MÓDULO 1 – CONCEPTOS DE DEBUGGING Y FUZZING

- Definiciones
- Ensamblado
- EIP
- Instrucciones
- Prólogo de una función
- Epilogo de una función
- Dirección de retorno
- Reversing estático

MÓDULO 2 – INTRODUCCIÓN AL BUFFER OVERFLOW (SMASHING STACK)

- Introducción
- Buffer Overflow
- Fuzzing y debugging
- Encontrando el offset para el exploit
- Creación del exploit

MÓDULO 3 – SOBREESCRITURA DE SEH (BUFFER OVERRUN)

- Introducción
- SEH
- Fuzzing y debugging
- Egghunting

MÓDULO 4 – BYPASS DE DEP

- Introducción
- Teoría adicional de Buffer Overflow
- Llamadas de Windows
- Return Oriented Programming

MÓDULO 5 – BYPASS DE NX Y ASLR

- Introducción
- Teoría adicional de Buffer Overflow
- GDB Linux
- Depurando un binario en Linux

- Evadiendo ASLR y NX

MÓDULO 6 – BUFFER OVERFLOW EN ENTORNO DE 64 BITS

- Introducción
- Registros
- Instrucciones
- Arrays
- Llamando una función
- Escribiendo una función
- Alojamiento dinámico en la stack
- Stack Smashing en 64 bits
- Evasión de NX

TARIFAS DE PRECIOS óHM̂ L± ! ƛyŎfdzƛŘƧú

Modalidad	Inscripción	Mensualidades	Cantidad	TOTAL
CONTADO A	*4.245,00* *1.450,00* ***Euros***	- 6	*-* *500,00* ***Euros***	*4.245,00* *4.450,00* ***Euros***

ADEMÁS INTESA LE OFRECE

En este marco INTESA y la Asociación Nacional de Tasadores, Peritos y Mediadores (ANTPM), han firmado un protocolo que establece los programas de formación y los requisitos de las diferentes especialidades aprovechando la experiencia formativa y profesional de ambas entidades.

Incluido en el precio alta en la Asociación Nacional de Tasadores, Peritos y Mediadores (ANTPM):
El certificado obtenido tendrá el reconocimiento de la Asociación Nacional de Tasadores, Peritos y Mediadores (ANTPM), la cual le remitirá la documentación para darse de alta.

«La expedición del Diploma por parte de la Universidad Europea Miguel de Cervantes está incluida dentro del precio»

Las tasas de gestión y envío por parte de INTESA serán de 70 euros. Los alumnos que lo recojan en las oficinas de INTESA no tendrán que efectuar este pago. Los alumnos y exalumnos de la UEMC tendrán un 10% de descuento.