**XNET SOLUTIONS**
**Centro de Entrenamiento Autorizado de EC Council**

**Programa : Especialista en Hacking Etico y Pentesting**
**Duración : 120 Horas (4 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 ECSA (EC-Council Certified Security Analyst) 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. ECSA 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 curso será un curso Practico de Pentesting y Auditoria de Aplicaciones Web 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 destreza en las pruebas de vulnerabilidades web.

Para completar las destrezas y herramientas necesarias para el desarrollo de un Pentester, hemos incluido el curso de "Python Scripting Expert for Pentester" el cual lo ayudará a

dominar las secuencias de comandos de Python y su aplicación en Auditoria de Pentesting. Este curso es ideal para Pentester que desean aprender a automatizar tareas o ir más allá del simple uso de herramientas ya preparadas. Cubriremos temas de seguridad del sistema, seguridad de la red, aplicaciones y servicios web de ataque, técnicas de explotación, análisis de malware y binarios y automatización de tareas.

## II. METODOLOGÍA

El curso tiene la modalidad presencial. 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 1 PC para el desarrollo de las actividades practicas.

## III. REQUISITOS

- Conocimiento básicos de Redes LAN y Linux.

## IV. MATERIALES

- Manuales Oficiales de CEH v10 y ECSA v10 para los cursos de EC COUNCIL con voucher de Certificación oficial.
- Manuales Impresos 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**
- **EC Council Security Analist (ECSA), Exam 412-79**

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 V10 (40Hr)**
**Módulo 2 : EC Council Security Analyst – ECSA V10 (40Hr)**
**Módulo 3 : Pentesting y Auditoria de Aplicaciones Web (20Hr)**
**Módulo 4 : Python Scripting Expert for Pentester (20Hr)**

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**
- **EC Council Security Analist (ECSA), Exam 412-79**

## Módulo 1 : EC Council Certified Ethical Hacking v10 (40 Hrs)

## DESCRIPCIÓN

CURSO : **EC Council Certified Ethical Hacking v10**
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:

CEHv10 es un curso Integral de Ethical Hacking y Programa de Auditoría de Sistemas de Información de Seguridad centrado en las amenazas más recientes de seguridad, vector de ataque avanzado, y demostración práctica en tiempo real de la última Técnicas de hacking, metodologías, herramientas, trucos , y medidas de seguridad.

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 el aula para pentesting, Hacking y asegurar sus propios sistemas. El ambiente de laboratorio intenso le da un conocimiento profundo y práctico al experimentar con los sistemas de seguridad actuales y esenciales.

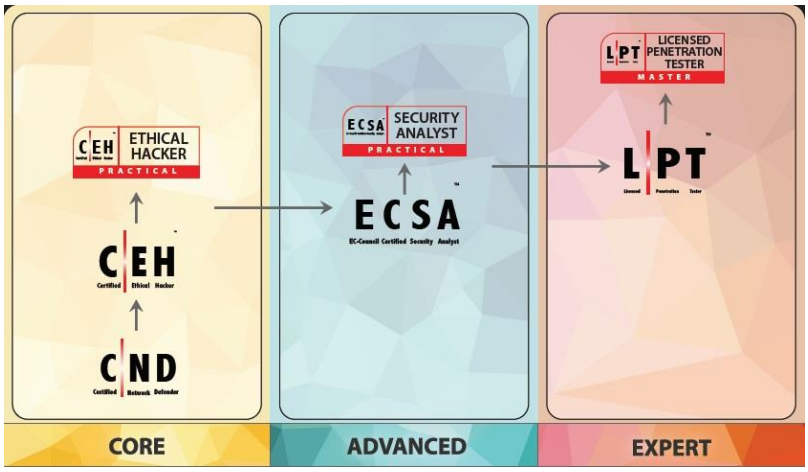
Usted primero comenzará con la comprensión de cómo funcionan las defensas del perímetro y luego se trasladan a la exploración y atacar redes, por supuesto, no se realizara ningún daño a redes reales. También aprenderás cómo los intrusos escalan privilegios y las medidas que se pueden tomar para garantizar 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.

Al salir de esta intensiva clase de 5 días usted tendrá la comprensión y experiencia en Ethical Hacking. Este curso te prepara para EC-Council Certified Ethical Hacker exam 312-50

## CONTENIDO:

CEHv10 consta de 20 módulos básicos diseñados para facilitar el hacking ético integral y entrenamiento de pruebas de penetración

1. Introduction to Ethical Hacking
2. Footprinting and Reconnaissance
3. Scanning Networks
4. Enumeration
5. Vulnerability Analysis
6. System Hacking
7. Malware Threats
8. Sniffing
9. Social Engineering
10. Denial of Service
11. Session Hijacking
12. Evading IDS, Firewalls and Honeypots
13. Hacking Webservers
14. Hacking Web Applications
15. SQL Injection
16. Hacking Wireless Networks
17. Hacking Mobile Platforms
18. IoT Hacking
19. Cloud Computing
20. Cryptography




## ¿QUE DEBERIAS APRENDER ?

Los estudiantes que llevan el Curso de formación CEH aprenden:

- Los temas clave que se usan en la seguridad de la información en el mundo, el proceso de gestión de incidentes, y pruebas de penetración
- Varios tipos de footprinting, herramientas de footprinting y contramedidas
- Técnicas de escaneo de red y contramedidas de escaneo
- Técnicas de enumeración y contramedidas
- Metodología de hacking, la estenografía, ataques steganalysis y pistas que cubren la estenografía.
- Los diferentes tipos de troyanos, análisis de Troyanos, y contramedidas en Troyanos.
- Trabajar con virus, análisis de virus, gusanos de ordenadores, procedimiento de análisis de malware y contramedidas
- Técnicas de detección de paquetes y la forma de defender
- Técnicas de Ingeniería Social, robo de identidad, y contramedidas de ingeniería social
- Técnicas de ataque DoS / DDoS, botnets, ataques DDoS, herramientas de ataque y contramedidas de DoS / DDoS
- Técnicas de secuestro de sesión y contramedidas
- Diferentes tipos de ataques al servidor web, metodología de ataque y contramedidas
- Diferentes tipos de ataques a aplicaciones web, metodología de hacking de aplicaciones web y contramedidas

- Ataques de inyección SQL y detección de inyección de herramientas
- Encriptación inalámbrica, metodología de hacking inalámbrica, herramientas de hacking inalámbrico y herramientas de seguridad wifi
- Vector de ataque de plataforma móvil, vulnerabilidades android, iOS jailbreaking, vulnerabilidades de Windows phone 8,guidelines en seguridad móvil y herramientas
- Firewall, IDS y técnicas de evasión honeypot, herramientas de evasión y contramedidas
- Varios tipos de desbordamientos de búffer, cómo mutar un exploit de desbordamiento de buffer, herramientas de detección de buffer overflow y contramedidas
- Los diferentes tipos de sistemas de cifrado criptográficos, Infraestructura de llaves públicas (PKI), ataques criptográficos, y herramientas de criptoanálisis
- Varios tipos de pruebas de penetración, auditoría de seguridad, evaluación de la vulnerabilidad, y hoja de ruta de pruebas de penetración.

**Duración:** 40 horas

# Módulo 2 : EC Council Security Analyst – ECSAv10

CURSO : **EC Council Security Analyst - ECSA v10**
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:

El programa EC–Council Certified Security Analyst (ECSA) esta basada en estándares, desarrollada con una metodología de formación integral, intensiva que enseña a los profesionales de seguridad de la información para llevar a cabo pruebas de penetración de la vida real mediante la utilización de la metodología de pruebas de penetración publicada por EC-Council.

El Programa de ECSA es un completo programa de formación práctica en 5 días. 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.

El EC-Council Certified Security Analyst (ECSA) 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.

## LABORATORIOS DE ECSAv10

El curso ECSA es un programa totalmente práctico. Los ejercicios cubren escenario del mundo real. Mediante la práctica de las habilidades que se proporcionan a usted en la clase ECSA, somos capaces de brindar a los candidatos las últimas amenazas a las que las organizaciones pueden ser vulnerables.

Esto se puede lograr con los laboratorios iLabs de EC-Council. Esto permite que los estudiantes tengan acceso de forma dinámica una gran cantidad de máquinas virtuales preconfiguradas con vulnerabilidades, exploits, herramientas y scripts desde cualquier lugar con una conexión a Internet.

La simplicidad de nuestro portal web permite al estudiante poner en marcha toda una serie de equipos y acceder a ellos de forma remota con un simple clic. Es la solución de laboratorio más rentable, fácil de usar disponible.

Con iLabs, ejercicios de laboratorio se puede acceder 24x7 permitiendo al estudiante practicar habilidades de una manera segura, redes totalmente funcionales todo el tiempo es muy conveniente.

Nuestros laboratorios guiados paso a paso incluyen ejercicios con tareas detalladas, herramientas de soporte y los materiales adicionales, así como nuestro estado-of-the-art "Open Environment", permitiendo a los estudiantes a poner en marcha una completa red en vivo para cualquier prueba de hacking.

Disponibilidad de máquinas son completamente virtualizados permitiendo controlar y reprogramar las máquinas de forma rápida y sencilla sin instructor requerido o interacción de un administrador.

## BENEFICIOS DE SER ECSA

Programa de Seguridad de Datos (Advanced Penetration Testing )

- El EC-Council Certified Security Analyst es para profesionales con experiencia en la industria y está respaldado por un plan de estudios diseñado por los mejores en el campo.
- Los estudiantes obtienen una mayor aceptación de la industria como profesionales de la seguridad.
- Los analistas de seguridad certificados aprenden a analizar los resultados de las herramientas de seguridad y técnicas de pruebas de seguridad.
- ECSA enseña a los estudiantes el camino hacia el logro de la certificación LPT.

## SYLABUS DEL CURSO:

**Módulos Principales:**

1. Introduction to Penetration Testing and Methodologies
2. Penetration Testing Scoping and Engagement Methodology
3. Open-Source Intelligence (OSINT) Methodology
4. Social Engineering Penetration Testing Methodology
5. Network Penetration Testing Methodology – External
6. Network Penetration Testing Methodology – Internal
7. Network Penetration Testing Methodology – Perimeter Devices
8. Web Application Penetration Testing Methodology
9. Database Penetration Testing Methodology
10. Wireless Penetration Testing Methodology
11. Cloud Penetration Testing Methodology
12. Report Writing and Post Testing Actions

## Módulos de Auto Estudio:


1. Password Cracking Penetration Testing
2. Router and Switches Penetration Testing
3. Denial-of-Service Penetration Testing
4. Stolen Laptop, PDAs and Cell Phones Penetration Testing
5. Source Code Penetration Testing
6. Physical Security Penetration Testing
7. Surveillance Camera Penetration Testing
8. VoIP Penetration Testing
9. VPN Penetration Testing
10. Virtual Machine Penetration Testing
11. War Dialing
12. Virus and Trojan Detection

13. Log Management Penetration Testing
14. File Integrity Checking
15. Telecommunication and Broadband Communication Penetration Testing
16. Email Security Penetration Testing
17. Security Patches Penetration Testing
18. Data Leakage Penetration Testing
19. SAP Penetration Testing
20. Standards and Compliance
21. Information System Security Principles
22. Information System Incident Handling and Response
23. Information System Auditing and Certification

**Duración:** 40 horas

# Módulo 3 : Pentesting y Auditoria de Aplicaciones Web

CURSO : **Pentesting y Auditoria de Aplicaciones Web**
Duración : 20 Horas


## DESCRIPCION DEL CURSO:

Este curso está diseñado para capacitar a profesionales y técnicos en TI en las técnicas y herramientas disponibles, usadas por los hackers para realizar un ataque desde Internet, redes internas a aplicaciones web y entornos basados en servidores web y de aplicaciones.

## Objetivo:

Proporcionar al participante los conocimientos teóricos-prácticos que permita desarrollar las competencias necesarias realizar un proceso controlado de Pentesting que permite conocer las vulnerabilidades y de esta manera tomar las medidas preventivas en contra de agresiones maliciosas, valiéndose para ello de los tests de intrusión, que evalúan la seguridad técnica de los sistemas de información, redes de datos, aplicaciones web y servidores expuestos.

## Competencias:

- Comprende un ataque a servidores web y aplicaciones a través de Internet
- Realiza una prueba de penetración
- Utiliza las herramientas idóneas para realizar un proceso de Auditoria
- Entender el funcionamiento de los ataques más comunes desde Internet como SQL Injection, Cross Site Scripting, Path Traversal, Session Hijacking, entre otros
- Comprende cómo protegerse de los ataque implementando medida de seguridad
- Reconoce las ventajas de la tecnología y los peligros al no tener una cultura de seguridad

## Requisitos:

- Conocimiento básicos de redes
- Conocimiento básico de programación web

## Dirigido a:

- Profesionales y Técnicos en Tecnologías de la Información
- Desarrolladores de Aplicaciones Web
- Administradores de TI, Programadores
- Ingenieros de Testing de Aplicaciones Web

## DETALLES DEL CURSO

**Tema 1: Introducción a las Aplicaciones Web**

- Funcionamiento de las Aplicaciones Web
- Seguridad de las Aplicaciones Web
- Owasp Top 10
- Owasp Testing Guide

**Tema 2: Denegación de Servicio y Session Hijacking**

- Técnicas de ataque DoS
- Herramientas de Ataque DoS
- Ataques basado en Session Hijacking
- Técnicas de Session Hijacking
- Tipos de Session Hijacking

**Tema 3 : Pentesting de Servidores Web**

- Arquitectura de Servidores Web
- Metodología para ataques a servidores web
- Recopilación de Información
- Analizando Metadata
- Footprinting de Servidores Web
- Mirroring de Sitios Web
- Hacking de Contraseñas en Aplicaciones Web
    - ❖ Hydra
    - ❖ DirBuster / WebSlayer

**Tema 4: Análisis de Vulnerabilidades de Servidores Web**

- Analizadores a Nivel Plataforma
- Analizadores a Nivel Aplicación
- Análisis de Vulnerabilidades a Nivel Plataforma
- Análisis de Vulnerabilidades a Nivel Aplicación
    - ❖ Nessus
    - ❖ Acunetix Web Vulnerability Scanner
    - ❖ Webshag
    - ❖ Skipfish
    - ❖ Nikto
    - ❖ Owasp-Zap

**Tema 5: Pentesting de Aplicaciones Web**

- Cómo funcionan las aplicaciones Web
- Como empezar a hackear una Aplicación Web
- Frameworks de Aprendizaje
- Métodos, Header, Body
- Entradas Inválidas
- Ataques de Directory Traversal
- URL encoding
- Cross Site Scripting
- SQL Injection
- Ejecución de Comandos
- Manejos de Shell

**Tema 6: Explotación de Vulnerabilidades**

- Trabajando con Exploits
- Metasploit Framework
- La Navaja Suiza del Hacker
- Proceso de Explotación de Vulnerabilidades

**Duración:** 20 horas.

## Módulo 4 : Python Scripting Expert for Pentester

Duración : 20 Horas


# DESCRIPCIÓN

Python Scripting Expert for Pentester tiene como objetivo enseñarle cómo aplicar el poderoso lenguaje Python a la investigación de seguridad, pruebas de penetración y automatización de ataques utilizando un enfoque práctico con una curva de aprendizaje gradual.

Python Scripting Expert for Pentester lo ayudará a dominar las secuencias de comandos de Python y su aplicación a los problemas de seguridad informática y de red. Este curso es ideal para Pentester, entusiastas de la seguridad y administradores de redes que desean aprender a automatizar tareas o ir más allá del simple uso de herramientas ya preparadas. Cubriremos temas de seguridad del sistema, seguridad de la red, aplicaciones y servicios web de ataque, técnicas de explotación, análisis de malware y binarios y automatización de tareas.

### METODOLOGÍA

El curso contará con sesiones teórico-prácticas. 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.

### DURACION

El curso tendra una duración de 20 Horas

**CONTENIDO**

- Module 1: **Python Scripting – Language Essentials**
- Module 2: **System Programming and Security**
- Module 3: **Network Security Programming – Sniffers and Packet Injectors**
- Module 4: **Attacking Web Applications**
- Module 5: **Exploitation Techniques**

**Module 1: Python Scripting – Language Essentials**

- Introduction to Interpreted Languages and Python
- Data Types and variables
- Operators and Expressions
- Program Structure and Control
- Functions and Functional Programming
- Classes, Objects and other OOPS concepts
- Modules, Packages and Distribution
- Python in Linux and Unixes
- Python in Windows
- Python in Mobiles: iPhone and Androids
- Python in Embedded Devices: Routers
- Program Portability

**Module 2: System Programming and Security**

- I/O in Python
- File and Directory Access
- Multithreading and Concurrency
- Inter Process Communication (IPC)
- Permissions and Controls
- Case Studies

**Module 3: Network Security Programming – Sniffers and Packet Injectors**

- Raw Socket basics
- Socket Libraries and Functionality
- Programming Servers and Clients
- Programming Wired and Wireless Sniffers
- Programming arbitrary packet injectors
- PCAP file parsing and analysis
- Case Studies

**Module 4: Web Application Security**

- Web Servers and Client scripting
- Web Application Fuzzers
- Scraping Web Applications – HTML and XML file analysis
- Web Browser Emulation
- Attacking Web Services
- Application Proxies and Data Mangling
- Automation of attacks such as SQL Injection, XSS etc.
- Case Studies

**Module 5: Exploitation Techniques**

- Exploit Development techniques
- Immunity Debuggers and Libs
- Writing plugins in Python
- Binary data analysis
- Exploit analysis Automation
- Case Studies
- Lab Exercises

**Duración:** 20 horas.

# INFORMES

El Programa de Certificación en Pentesting y Hacking Etico está compuesto por cursos oficiales de EC Council los cuales incluyen la certificación oficial y algunos cursos de apoyo para fortalecer los conocimientos y aumentar las capacidades en el tema.

Estos cursos se dictan generalmente en horarios fuera de oficina o se pueden dictar a solicitud de los participantes.

Para Informes y detalle de horarios y precios, ud puede :

Informes : www.xnet.com.pe
Lugar : Av del Parque Sur 185 – Oficina 501 , San Isidro
Contacto : Jean del Carpio Foronda
Email : ventas@xnet.com.pe
Teléfono : 945045737

# DOCENTE

El programa cuenta con la participación de reconocidos profesionales con amplia experiencia académica y profesional, entre los que podemos destacar:

## Jean del Carpio Foronda.

Ingeniero Electrónico con 15 años de Experiencia en Seguridad Informática y Networking de la Universidad Nacional de Ingeniería con Maestría en Dirección de Operaciones y Postgrado en Data Networking en la Universidad Peruana de Ciencias Aplicadas.

Conocimiento avanzados de TCP/IP, Redes LAN, Redes WAN ATM, Redes VSAT, Soluciones Satelitales, Redes SDH, MPLS, Voz Sobre IP, Telefonía IP, Call Manager, Switching, Seguridad Cisco ASA, IPS, Seguridad de la Información, Implementación de Sistemas de Gestión de la Seguridad de la Información SGSI, ISO27001, Ethical Hacker, Computo Forense, entre otros.

Catedrático de la Maestría de Seguridad Informática y Maestría de Telecomunicaciones de la UTP (Universidad Tecnológica del Perú), instructor de la UPC en el Programa de Especialista en Seguridad, ISO 27001, Hardening aplicaciones Windows, Linux, Auditoria de sistemas de Información.

A participado en Análisis de Ethical Hacking para el Ministerio del Interior, Banco Financiero, INPE, Ministerio de Defensa, Bancos y entidades comerciales.

Cuenta con las certificaciones:
- Certified Ethical Hacking ( **CEH )**
**-** EC Council Security Analyst – **(ECSA )**
- Computer Hacking Forensic Investigator **(CHFI )**
- Certified Penetration Testing Engineer **- CPTE**
- CERTIFIED ISO/IEC 27001 Lead Implementer (**ISO 27001 LI**)
- EC Council Certified Chief Information Security Officer - **CCISO**
**-** EC Council Ethical Hacking Instructor **(CEI)**
- Certificacion Qualys Guard **(Qualys Guard CERTIFIED SPECIALIST)**
- Certificación **CCNA**, **CCNP**, **CCAI** (Cisco Certified Academy Instructor)
- Fortinet Certified Network Security Administrator **FCNSA**.
- Fortinet Certified NSE 1, NSE 2, NSE 3
- CheckPoint Certified SandBlast Administrator - **CCSA**