UNIVERSIDAD NACIONAL DE INGENIERÍA
FACULTAD DE INGENIERÍA INDUSTRIAL Y SISTEMAS

SISTEMAS UNI
Tecnologías de la Información

WORKSHOP

ETHICAL HACKING BÁSICO

El curso enseña a través de teoría y práctica las 05 fases de la metodología de Ethical Hacking:
Reconocimiento, Escaneo de Puertos y Vulnerabilidades, Ganando Acceso, Manteniendo Acceso, Borrando Huellas.

• Conocimientos Previos

Conocimiento básico del sistema Operativo Microsoft Windows.

• El participante al final del curso sera capaz de :

Desempeñarse en actividades de Seguridad Informática.

- **Dirigido a:** Estudiantes, Profesionales y Publico en General
- **Duración del curso: 24 Hrs. / 5 sesiones**

Evaluación

Será totalmentepráctica. Se realizarán entre 4 o 5 prácticas de las cuales se eliminará la nota más baja y se obtendrá un promedio (PP). Durante la última sesión se realizará un examen final (EF), el cual se promediará con la nota de prácticas y de esta manera se tendrá la calificación final

PROMEDIO DE PRÁCTICAS:

PP=(PR1 + PR2 + PR3 + PR4 - MENOR (PR)

NOTA FINAL:

NF= PP + EF

Modalidad Online

Requiere una PC con las siguientes caracteristicas:

- Procesador - 1GHZ o más rapido / en un chip (SOC).
- RAM - 1GB para 32 Bits o 2GB para 64.
- Espacio Libre 16GB - SO de 32 bits / 32GB - SO de 64 bits.
- Una tarjeta gráfica - DirectX 9, posterior o controlador WDDM 1.0.
- Pantalla - 800x 600 resolución.
- Conexión a internet estable.

Conéctate a nuestras diferentes Plataformas Digitales:

Telf.: 200 - 9060 Opción 1 / E-mail: sisuni.info@uni.edu.pe

/ /

www.sistemasuni.edu.pe

“Aumenta tus conocimientos, desarrolla nuevas habilidades y construye hoy tu futuro”.

INTRODUCCIÓN AL ETHICAL HACKING

• Historia del Hacking.
• Metodologías utilizadas en Ethical Hacking.
• Casos de estudio en el Perú y el mundo.
• Uso de Sistema Operativo Windows orientado a Hacking.
• Uso de Sistema Operativo Linux orientado a Hacking.
• Conocimiento de redes LAN y WAN ".

FASE I: RECONOCIMIENTO

• Búsqueda de direcciones IP públicas.
• Búsqueda de rangos de direcciones IP con WHOIS.
• Identificación de dominios y subdominios.
• Consulta de registros DNS.
• Identificación de correos electrónicos y servidores.
• Transferencia de zonas DNS.
• OSINT (Open Source Intelligence Techniques).
• Google Hacking.
• Búsqueda en repositorios públicos.
• Búsquedas avanzadas en redes sociales.

FASE II : ESCANEO DE PUERTOS Y SERVICIOS

• Denición del proceso de escaneo de puertos y servicios.
• Análisis del Three Way Handshake.
• Definición y tipos de escaneo.
• Escaneo a los TOP 10, TOP 100 y TOP 1000 de puertos TCP / UDP.
• Identificación de puertos y servicios abiertos: técnicas de escaneo.
• Manejo de tiempo con NMAP Identificación de Sistemas Operativos.
• Definición del proceso de Enumeración.

FASE II: ESCANEO Y ANÁLISIS DE VULNERABILIDADES

• Definición del proceso de escaneo y análisis de vulnerabilidades.
• Definición y categorización de vulnerabilidades.
• Identificación de vulnerabilidades con Nmap Script Engine (Nmap - NSE).
• Identificación de vulnerabilidades con Tenable NESSUS.
• Identificación de vulnerabilidades con Metasploit – Módulo Auxiliar

FASE II: ESCANEO Y ANÁLISIS DE VULNERABILIDADES

• Definición del proceso de Ganar Acceso.
• Definición de conceptos: exploit, payload, stager.
• Explotación de vulnerabilidades en Sistemas Operativos Windows y Linux.