SISTEMAS UNI
Tecnologías de la Información

# UNIVERSIDAD NACIONAL DE INGENIERÍA
## FACULTAD DE INGENIERÍA INDUSTRIAL Y DE SISTEMAS

# ETHICAL HACKING BÁSICO

WORKSHOP

**Duración 24 horas.**

**5 Sesiones.**

**Dirigido a:**

- Estudiantes
- Profesionales
- Público en general.

## OBJETIVOS:

El Participante al finalizar el curso será capaz de:

- Desempeñarse en actividades de Seguridad Informática.

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

## REQUERIMIENTOS:

- Conocimiento básico del sistema Operativo Microsoft Windows.

WWW.SISTEMASUNI.EDU.PE
SISUNI.INFO@UNI.EDU.PE
CENTRAL: 200-9060
DIRECTO: 481 - 1070 ANEXO 5231

SISTEMAS UNI
Tecnologías de la Información

# UNIVERSIDAD NACIONAL DE INGENIERÍA

## FACULTAD DE INGENIERÍA INDUSTRIAL Y DE SISTEMAS

# CONTENIDO:

## Sesión 1

### 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 ".

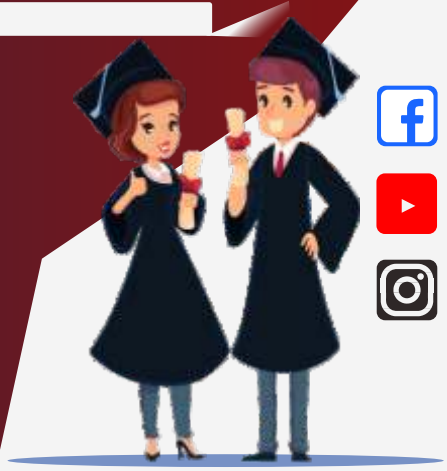
### FASE I: RECONOCIMIENTO

- 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.

## Sesión 2

### FASE II : ESCANEO DE PUERTOS Y SERVICIOS

- De nición 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:



WWW.SISTEMASUNI.EDU.PE
SISUNI.INFO@UNI.EDU.PE
CENTRAL: 200-9060
DIRECTO: 481 - 1070 ANEXO 5231

SISTEMAS UNI
Tecnologías de la Información

# UNIVERSIDAD NACIONAL DE INGENIERÍA

## FACULTAD DE INGENIERÍA INDUSTRIAL Y DE SISTEMAS

# CONTENIDO:

## Sesión 3

### 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

## Sesión 4

### 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.

**EVALUACIÓN:** La evaluación de cursos será totalmente práctica. Se realizarán entre 4 y 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 | Nota Final: |
|---|---|
| $PP=\frac{(PR1 + Pr2 + Pr3 + PR4) - Menor\ (PR)}{3}$ | $NF = (PP + EF) / 2$ |

WWW.SISTEMASUNI.EDU.PE
SISUNI.INFO@UNI.EDU.PE
CENTRAL: 200-9060
DIRECTO: 481 - 1070 ANEXO 5231