UNIVERSIDAD NACIONAL DE INGENIERÍA
FACULTAD DE INGENIERÍA INDUSTRIAL Y SISTEMAS

SISTEMAS UNI
Tecnologías de la Información

WORKSHOP

ETHICAL HACKING AVANZADO

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”.

EXPLOTACIÓN DE VULNERABILIDADES EN SISTEMAS OPERATIVOS WINDOWS Y LINUX.

- Configuración y uso de METASPLOIT.
- Módulo Auxiliar, módulo payload, módulo exploit.
- Módulo de POST EXPLOTACIÓN.
- DUMP de memoria RAM.
- Instalación de Keylogger.
- Evaluación de privilegios (bypass UAC).

EXPLOTACIÓN DE VULNERABILIDADES EN SERVICIOS DE RED.

- Ataques sobre servicios Microsoft SQL Server.
- Ataques sobre servicios MySQL.
- Ataques sobre servicios WEB: JBOSS y TOMCAT.
- Ataques basados en diccionarios.
- Ataques de fuerza bruta.
- Herramientas: HYDRA, Metasploit Módulo Auxiliar.

LISTA DE TEMAS

- Cracking de contraseñas LM y NTLM.
  - Fuerza Bruta.
  - Diccionario de Contraseña.
  - Tablas Pre-Computadas.
  - Herramientas: OPHCRACK, LC5, JOHN THE RIPPER.
- Cracking de contraseñas SHA, MD5.
  - Fuerza Bruta.
  - Diccionario de Contraseña.
  - Tablas Pre-Computadas.
  - Herramientas: OPHCRACK, LC5, JOHN THE RIPPER.
- Ataques del lado del cliente (client side attack).
  - Concepto del ataque.
  - Ataque sobre navegadores web.
  - Ataque sobre archivos PDF.

LISTA DE TEMAS

- Ataques del lado del cliente (client side attack).
  - Ataque sobre archivos EXCEL.
  - Ataque con archivos EXE.
  - Herramienta: Empire.
- Técnicas de PIVOTING.
  - Migración de procesos.
  - Configuración de rutas.
  - Escaneo de puertos.
  - Explotación de vulnerabilidad.

MANTENIENDO ACCESO

- Definición del proceso de mantener acceso.
- Definición de conceptos: rootkis, backdoors y accesos no autorizados.
- Instalación y configuración de backdoors.