SISTEMAS UNI
Tecnologías de la Información

UNIVERSIDAD NACIONAL DE INGENIERÍA
FACULTAD DE INGENIERÍA INDUSTRIAL Y DE SISTEMAS

ETHICAL HACKING AVANZADO

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

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.

Sesión 2

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

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

CONTENIDO:

Sesión 3

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.

Sesión 4

FASE 04: MANTENIENDO ACCESO

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

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:
$PP=\frac{(PR1 + Pr2 + Pr3 + PR4) - Menor\ (PR)}{3}$	$NF = (PP + EF) / 2$