UNIVERSIDAD NACIONAL DE INGENIERÍA
FACULTAD DE INGENIERÍA INDUSTRIAL Y SISTEMAS
SISTEMAS UNI
Tecnologías de la Información

ETHICAL HACKING – INTERMEDIO

Duración: 24 hrs.

Código:

Curso:

Descripción del curso

El curso enseña a través de teoría y práctica las tres últimas fases del proceso de Ethical Hacking.
-Ganando Acceso.
-Manteniendo Acceso.
-Borrando Huellas.

Dirigido a:

- Publico en General.

Objetivos:

El Participante al finalizar el curso será capaz de:

Aprender técnicas básicas y avanzadas de EXPLOTACIÓN sobre Sistemas Operativos Microsoft Windows y Linux.

REQUISITOS MÍNIMOS

Conocimiento básico del sistema Operativo Microsoft Windows.
Conocimiento básico del sistema Operativo Linux.

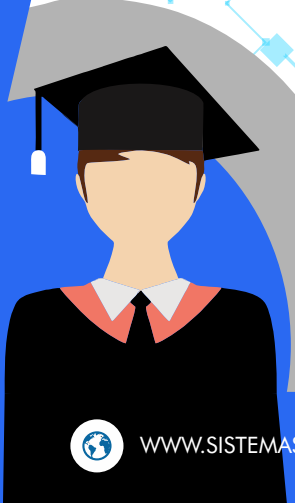
CONTENIDO

Sesión 1

- Fase 03: Ganando Acceso.
- 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

- 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.



CONTENIDO

Sesión 3

- 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.
  - Uso de METASPLOIT.
    - -.Modificación de registros en el S.O.
    - -.Instalación de ejecutables en el S.O.
  - Uso de NETCAT.
    - -.Bind Shell.
    - -.Reverse Shell.
  - Backdoor en Apache Server.
  - Backdoor KNOCKOUT.
  - Instalación de ROOTKIT.
  - Examen Final.

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 PRACTICAS

$$PP=\frac{(PR1 + Pr2 + Pr3 + PR4) - Menor\ (PR)}{3}$$

Nota Final:

$$NF = (PP + EF) / 2$$