Curso:

Ethical Hacking – Básico

Duración: 24 hrs.

Código: ETHAC

Descripción del curso

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

Objetivos:

El Participante al finalizar el curso será capaz de:

Brindar los conocimientos y metodología de Ethical Hacking a los participantes para que estos puedan desempeñarse en actividades de Seguridad Informática.

Dirigido a:

- Estudiante.
- Profesional.
- Publico en General.

REQUISITOS MÍNIMOS

Conocimiento básico del sistema Operativo Microsoft Windows.

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 ".

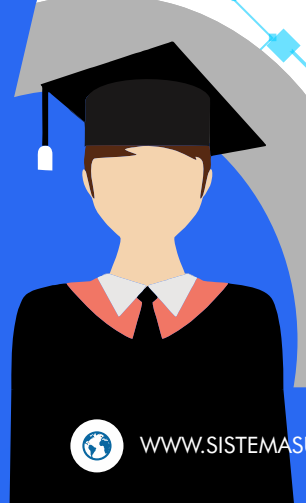
FASE I: RECONOCIMIENTO

- 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

- Definición del proceso de escaneo de puertos y servicios.
- Análisis del Three Way Handshake.
- Definición y tipos de escaneo.
  - SYN, TCP, FIN, XMAS, NULL, UDP.
- 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:
  - Enumeración de usuarios.
  - Enumeración de nombres de computadores.
  - Enumeración de Recursos de Red compartidos.
  - Enumeración de servicios de red: SNMP, LDAP, SMB.
  - Enumeración de configuraciones.



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).
  - Vulnerabilidades en puertos y servicios de red.
- Identificación de vulnerabilidades con Tenable NESSUS.
  - Vulnerabilidades en puertos y servicios de red.
  - Vulnerabilidades en sistemas operativos sin autenticación.
  - Vulnerabilidades en sistemas operativos con autenticación.
- Identificación de vulnerabilidades con Metasploit – Módulo Auxiliar.
  - Reconocimiento del Framework Metasploit.
  - Principales comandos y opciones del Framework Metasploit.
  - Identificación de vulnerabilidades con módulo Auxiliar.

Sesión 4

FASE III: GANANDO ACCESO

- Definición del proceso de Ganar Acceso.
- Definición de conceptos: exploit, payload, stager.
- Explotación de vulnerabilidades en Sistemas Operativos Windows y Linux.
  - Configuración y uso de METASPLOIT.
  - Módulo Auxiliar.
  - Módulo Payload.
  - Módulo Exploit.

  Cracking de contraseñas LM y NTLM.
  - Fuerza Bruta.
  - Diccionario de Contraseña.
  - Tablas Pre-Computadas.
- Examen FINAL de Ethical Hacking Básico.

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:

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