ESPE - Innovativa
EMPRESA PÚBLICA

Presentación del curso Presencial

Seguridad Informática y Hacking Ético

Módulo I

Tabla de contenido

Presentación del curso

El curso presencial de Seguridad Informática y Hacking Ético I, ofrece herramientas necesarias que nos permite comprender las técnicas y ataques que usan los hacker en la actualidad para realizar un eficiente y eficaz control de seguridad. El curso está orientado específicamente para todas las personas que requieren usar una metodología de hackeo ético, realizar pruebas de penetración e implementación de soluciones de seguridad informática.

Para su mayor comprensión, el curso está distribuido en ocho unidades:

En la primera unidad se verifica los pasos iniciales en el mundo hacker, definiciones utilizadas en seguridad, tipos, metodología, etapas de un Ethical Hacking.

En la segunda unidad, se procede a la identificación y el reconocimiento con técnicas de Footprinting, técnicas de Google Hacking y herramientas online para Mirroring websites.

En la tercera unidad se realiza el escaneo de redes, técnicas de ping sweep, scanning de vulnerabilidades y el uso del NMAP como herramienta del scanning.

En la cuarta unidad permite comprender el proceso de enumeración de hosts, redes y servicios, se utilizan herramientas básicas de enumeración como son nbtscan, enum4linux, etc.

En la quinta unidad se utiliza el Metasploit Framework para el proceso de ataque, se utilizan herramientas para hacking de passwords y comandos básicos de Meterpreter.

Mediante la sexta unidad, se analiza que es un troyano, backdoor, se identifica los tipos de troyanos, se crean troyanos y backdoor para sistemas operativos de Windows y Linux.

En la séptima unidad permite comprender las técnicas de intrusión a redes inalámbricas.

En la octava unidad se realiza la identificación del funcionamiento de aplicaciones web, esta unidad corresponde a introducción al hackeo web, enfocándose en la inyección de código SQL, mayores detalles de hacking web se revisarán en el segundo módulo del curso.

Objetivos de aprendizaje

Objetivo general:

- Conocer las metodologías de hacking más usadas, aplicando conocimientos de ataques internos, externos black box, grey box, usando hackers sombrero blanco, sombrero negro que permita obtener toda la información sensible de una organización con la finalidad de presentar informes y recomendaciones sobre los problemas en la empresa.

Objetivos específicos:

- Analizar la ubicación de un equipo por medio de su dirección IP
- Verificar los servidores de DNS, correos electrónicos de una organización empresarial
- Realizar el escaneo de puertos TCP y UDP usando la herramienta NMAP
- Identificar versiones de software, sistemas operativos, etc.
- Identificar vulnerabilidades de sistemas operativos más usados Windows, Linux, Android
- Utilizar Kali Linux, exploración por Metasploit y Meterpreter.
- Identificar los ataques más usados hacia los Sistemas Operativos.

Contenidos del curso

Unidad 1: Introducción Pasos Iniciales en el mundo Hacker

1.1. Definiciones utilizadas en la Seguridad Informática
1.2. Tipos de Hacking
1.3. Terminología del hacker
1.4. Etapas de un Ethical Hacking
1.5. Metodologías de un Ethical Hacking
1.6. Introducción a la virtualización con VMWare Workstation
1.6.1. NAT
1.6.2. Bridge
1.6.3. Host-only
1.7. Primer entorno de pruebas virtual para hacking
1.8. Comandos y tareas Linux para hacking
1.9. Primeros pasos con Kali Linux
1.9.1. Entorno
1.9.2. Directorios
1.9.3. Archivos de Configuración
1.10. Servicios básicos disponibles en Kali
1.10.1. HTTP
1.10.2. SSH
1.10.3. MSF
1.10.4. POSTGRES

Unidad 2: Footprinting y Reconocimiento

2.1. Identificar y comprender el termino Footprinting
2.2. Identificar la información que busca un hacker
2.3. Técnicas de Google Hacking
2.4. Enumeración de DNS
2.5. Enumeración con WHOIS
2.6. Herramientas online para Mirroring websites
2.7. Email tracking
2.8. The harvester

Unidad 3: Scanning de Redes

3.1. Identificar las técnicas de scanning
3.1.1. Scanning de puertos
3.1.2. Scanning de red
3.1.3. Scanning de vulnerabilidades
3.2. Comprender los objetivos del scanning
3.3. Técnicas Ping sweep
3.4. Uso del NMAP como herramienta de scanning
3.5. Banner grabbing mediante fingerprinting de Sistema Operativo y otras herramientas

Unidad 4: Enumeración

4.1. Comprender el proceso de enumeración de host, redes y servicios
4.2. Enumeración SNMP
4.3.1. Nmap
4.3.2. Unicorn scan
4.3.3. Enum4linux
4.3.4. Nbtscan
4.3.5. Onesixtyone
4.3.6. Snmpwalk
4.3.7. Snmpchecker

Unidad 5: Ataques

5.1. Uso de Metasploit Framework para el proceso de ataque
5.1.1. Auxiliary
5.1.2. Exploit
5.1.3. Post
5.2. Conseguir contraseñas utilizando
5.2.1. PWDUMP
5.2.2. WCE
5.3. Ataques de password
5.3.1. Diccionario
5.3.2. Fuerza Bruta
5.3.3. Rainbow Tables
5.4. Uso de herramientas para cracking de passwords
5.4.1. John the ripper
5.4.2. Hashcat
5.4.3. Ophcrack
5.4.4. Hydra
5.4.4. Medussa
5.5. Introducción a PAYLOADS
5.5.1. Reverse payload
5.5.2. Bind payload
5.6. METERPRETER y sus comandos básicos

Unidad 6: Troyanos y Backdoors

6.1. ¿Qué es un troyano?
6.2. ¿Qué es un backdoor?
6.3. Identificar los tipos de troyanos
6.4. Creación de troyanos
6.5. Keyloggers
6.6. Creación de bakdoors para sistemas Windows y Linux

Unidad 7: Ingeniería Social

7.1. Comprender el funcionamiento de redes inalámbricas
7.2. Comprender los distintos tipos de redes inalámbricas
7.3. Identificar las formas de autenticación Wi-Fi
7.4. Métodos de encriptación Wireless
7.4.1. WEP
7.4.2. WPA/WPA2
7.5. Amenazas Wireless
7.6. Metodología de Wireless Hacking
7.7. Herramientas Wireless Hacking
7.8. Defensa ante ataques wireless

Unidad 8: Hacking de aplicaciones WEB

8.1. Identificar cómo funcionan las aplicaciones web
8.2. Componentes de una aplicación web
8.3. ¿Qué es OWASP?
8.3.1 OWASP Top 10
8.4. ¿Cómo funciona la inyección de código SQL?
8.5. Prácticas de Inyección de Código.

Competencias previas

- Conocimientos de sistemas operativos Windows y Linux Basico
- Conocimientos básicos Redes IP/TCP
- Administración básica de Base de datos

Recursos

- Acceso a las máquinas virtuales con VMWare Workstation
- Acceso a la conexión de internet en las máquinas virtuales de Windows y Kali
- Acceso a la red local y externa.

Aspectos metodológicos

En el curso presencial tiene una duración total de 40 horas, proporcionado un enfoque principal a la Ética Profesional en la Seguridad Informática e identificando los tipos de Hacker que existen.

Los contenidos del curso están divididos en un 20% de la teoría, permitiendo identificar los conceptos de hacker, sus fases, las clases de vulnerabilidades y los tipos de ataques a los que nos encuentran expuestos.

El 80% restante del curso está enfocado a la práctica de cada una de las Fases del Hacking, dividiéndolas en el Reconocimiento del Objetivo, el Escaneo del Objetivo Específico, el Obtener acceso al Objetivo, el Mantener el Acceso al Objetivo y Finalmente el Cubrir Huellas.

Criterios de aprobación

- Evaluaciones prácticas, una al intermedio del curso y otra al final del curso aplicando todos los conceptos y las prácticas realizadas en el desarrollo del curso.
- Participación activa durante el desarrollo del curso
- Cumplimiento de las trabajos y deberes propuestos
- Obtención de un rendimiento mínimo de 14/20 puntos
- Asistencia mínima de 80/100