ESPE - Innovativa
EMPRESA PÚBLICA

Presentación del Curso

Seguridad Informática y Hacking Ético I

Tabla de contenido

SEGURIDAD INFORMÁTICA Y HACKING ÉTICO I

Descripción general

El presente curso se desarrollará en la modalidad presencial, el cual permitirá aprender como los hackers pueden escalar privilegios y que medidas pueden tomar para asegurar un sistema, es así que el hacking ético constituye una herramienta moderna de prevención y protección de datos, para evitar fugas de información.

En esta capacitación se estudiará los pasos iniciales en el mundo de Hacker, saber utilizar las herramientas de forma adecuada, al igual que las tecnologías que sirven como barrera para proteger y garantizar la confidencialidad de toda la información de la empresa.

Este curso se encuentra organizado en ocho unidades:

En la primera unidad se analiza los pasos iniciales en el mundo de hacker, etapas de un Ethical Hacking, comandos básicos que son utilizados en las pruebas de virtualización con VMWare Workstation.

En la segunda unidad se identifica que información busca el Hacker, como se aplica las técnicas de google hacking, reconocimiento de herramientas online para Mirroring websites y el funcionamiento the harvester que anticipa los ataques de ingeniería social.

En la tercera unidad se analiza técnicas de scanning en hosts, puertos y redes, creando un perfil del objetivo.

En la cuarta unidad se analiza el proceso de enumeración de objetivos que son escaneos simples a la máquina o en simples peticiones o consultas.

En la quinta unidad se identifica ataques informáticos más comunes.

En la sexta unidad se analiza los permisos que el atacante obtiene que dependen de los privilegios del usuario al que está atacando y de las características del troyano.

En la séptima unidad se analiza las técnicas más usadas por los hackers para explotar vulnerabilidades y penetrar las defensas de las wifi.

En la octava unidad se identifica las vulnerabilidades más comunes en los aplicativos web sin importar el sistema operativo que se maneja.

Con esta capacitación logrará mejorar el desempeño profesional y competente de las personas que trabajan en los diferentes departamentos de la empresa, considerando medidas de prevención, detección y corrección, orientadas a proteger la confidencialidad, la integridad y la disponibilidad de los recursos informáticos.

Público objetivo

El curso está dirigido a jóvenes bachilleres, jóvenes universitarios, egresados, técnicos, profesionales, administradores de red y público en general que deseen conocer sobre la seguridad informática y los tipos de amenazas a las que nos podemos enfrentar, para poder defendernos de ellas.

Objetivos de aprendizaje

Objetivo general

- Analizar nuevas técnicas que utilizan para infectar los sistemas con el fin de identificar las herramientas que se puede utilizar para aportar con soluciones a los posibles problemas o incluso adelantarnos a los acontecimientos, evitando de ésta manera que el sistema de la empresa pueda ser hackeado.

Objetivos específicos

- Estar en la capacidad de identificar vulnerabilidades de sistemas operativos más usados como: Windows, Linux y Android.
- Aplicar correctamente las herramientas al igual que las tecnologías que sirven como barrera para evitar cualquier problema de seguridad en los sistemas de las empresas.
- Definir estrategias necesarias para que el sistema de la empresa no se vea amenazado.

Duración

El curso tiene una duración de 40 horas.

Contenidos

BLOQUE 1: Identificar vulnerabilidades de sistemas operativos más usados Windows, Linux, Android

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

BLOQUE 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

BLOQUE 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.

BLOQUE 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

BLOQUE 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

BLOQUE 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 backdoors para sistemas Windows y Linux

BLOQUE 7: Hacking Wireless

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

BLOQUE 8: Hacking Wireless

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: Los participantes deben tener conocimiento básicos de Linux, Windows y de Redes IP/TCP.

Habilidades o destrezas: Los participantes deben manejar herramientas ofimáticas, principalmente el internet.

Valores: Los participantes deben tener criterios éticos para aplicar estrategias necesarias para la protección de los sistemas que se encuentren amenazados.

Recursos

Los recursos que se requieren para la ejecución del curso presencial son los siguientes:

- Acceso a un equipo de computación con conexión a internet.
- Acceso al paquete Microsoft Office en sus componentes Word, Excel y power point.
- Disponer de un software para lectura de archivos PDF.
- Casos prácticos
- Block, esfero

Aspectos metodológicos

El curso presencial se desarrolla totalmente en las aulas de clase, la metodología a seguirse en este curso será sobre la base de charlas magistrales, de aprendizaje participativo que promueva el análisis de los casos relacionados con la experiencia de los participantes, en cuyo caso el profesor tendrá un rol de Facilitador.

Se examinará los análisis técnicos correspondientes que forman parte de las auditorias sobre los problemas que aparecen dentro del sistema informático con el que estamos trabajando.

Se desarrollarán casos prácticos que permitan a los estudiantes poner en práctica el conocimiento teórico impartido.

El contenido del curso se pondrá a disposición de todos los participantes, para el desarrollo del proceso de capacitación.

Criterios de aprobación

- Cumplimiento de las actividades propuestas en el plazo establecido
- Participación activa en las clases
- Asistencia del 80%
- Obtención de un rendimiento mínimo de 7/10 puntos en el curso

Certificado

El participante que cumpla con los criterios de aprobación, recibirá un certificado con el aval de la Universidad de las Fuerzas Armadas – ESPE, ESPE INNOVATIVA EP y SETEC.

Perfil del Facilitador

Formación académica

Pregrado:
Tecnólogo en sistemas de la información
Ingeniero en Sistemas
Ingeniero en informática y ciencias de la computación
Áreas afines

Posgrado (De preferencia)
Magíster en tecnologías de la información.

Otros
Capacitación en seguridad informática

Experiencia relacionada

Experiencia profesional en el sector público-privado y docencia en el área de seguridad informática.