ESPE Innovativa

DESARROLLA
ESPECIALIZA
TRANSFIERE

Presentación del Curso

Seguridad Informática y Hacking Ético II

Unidad de
Capacitación y Certificación

Tabla de contenido

SEGURIDAD INFORMÁTICA Y HACKING ÉTICO II

Descripción general

El presente curso se desarrollará en la modalidad presencial, el cual permitirá fortalecer conocimientos más importantes de todas las fases que involucran un hacking ético, así como los tipos de amenazas a las que nos podemos enfrentar y posibles mecanismos de defensa.

En esta capacitación se estudiará la web vulnerable y las mejores medidas de seguridad para contrarrestar los ataques informáticos.

Este curso se encuentra organizado en seis unidades:

En la primera unidad se analiza las vulnerabilidades web que se tiene que preveer.

En la segunda unidad se identifica los tipos de aseguramiento de sitios web que se debe conocer para minimizar el robo de la información.

En la tercera unidad se analiza la identidad del atacante en la red de destino, evento que aumenta la posibilidad que el hacker sea atrapado.

En la cuarta unidad se analiza el proceso de infectar o atacar el software de una empresa y esto ocurre cuando existe vulnerabilidades en dicho software e intenta explotar usando combinaciones para lograr que dicho error sea activado.

En la quinta unidad se analiza cómo funcionan los Buffer Overflow y los tipos de fallos que son utilizados por los ciberdelicuentes.

En la sexta unidad se analiza el tema de introducción a la seguridad forense que permite recuperar y validar la información de dispositivos extraíbles.

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

- Promover el desarrollo de conocimientos a los participantes para diseñar técnicas y procedimientos necesarios para proteger la información teniendo en cuenta las últimas amenazas que se aplican en sistemas y en entornos web.

Objetivos específicos

- Estar en la capacidad de identificar las principales vulnerabilidades de aplicaciones web y proponer soluciones a las mismas.
- Estar en la capacidad de Identificar fallos de seguridad a nivel de aplicación y aprovechar problemas relacionados a Buffer Overflow.
- Conocer e interpretar las distintas técnicas utilizadas para realizar ingeniería inversa de aplicaciones.

Duración

El curso tiene una duración de 40 horas.

Contenidos

BLOQUE 1: Vulnerabilidades de sitios web

1.1 Identificar cómo funcionan las aplicaciones web
1.2. Componentes de una aplicación web
1.3. ¿Qué es OWASP?
1.3.1 OWASP Top 10
1.4. Herramientas para Tampering
1.4.2. OWASP ZAP
1.4.3. Burpsuite
1.5. Cross Site Scripting (XSS)
1.5.1. Reflejado
1.5.2. Almacenado
1.6. Local File Inclussion
1.7. Remote File Inclussion
1.8. Command Injections
1.9. SQL Injections
1.9.1. Comprender SQL Injections

BLOQUE 2: Aseguramiento de sitios web

2.1. Web Application Firewall (WAF)
2.2. Distintas formas de implementar un WAF
2.3. Introducción a WAF Open Source
2.4. Instalación de WAF Open Source
2.5. Configuración de WAF
2.6. Pruebas de WAF contra aplicaciones vulnerables.
2.7. Validación de resultados.

BLOQUE 3: Tunneling y Port Redirection

3.1. Port Forwarding/Redirection
3.2. SSH Tunneling
3.3.1. Local Port Forwarding
3.3.2. Remote Port Forwarding
3.3.3. Dynamic Port Forwarding.
3.3 Proxychains.

BLOQUE 4: Ingeniería Inversa

4.1. ¿Qué es la ingeniería inversa de aplicaciones?
4.2. Recordando Assembler.
4.3. Recordando leguaje C.
4.4. Herramientas para ingeniería inversa.
4.5. Ejercicios prácticos.

BLOQUE 5: Buffer Overflow

5.1. Identificando Buffer Overflow
5.2. Tipos de Buffer Overflow
5.1. Win32 Buffer Overflow
5.1.1. Fuzzing
5.1.2. Controlando EIP
5.1.3. Encontrando espacio para la shellcode
5.1.4. Verificando badchars
5.1.5. Re-direccionando el flujo de ejecución
5.1.6. Identificar un Return Address
5.1.7. Generando la shellcode.
5.1.8. Accediendo al sistema

BLOQUE 6: Pasos iniciales en investigación forense.

6.1. ¿Qué es la investigación forense digital?
6.2. Tipos de análisis forense (reactivo, proactivo)
6.3. Cadena de custodia
6.4. Recuperación de datos y análisis de evidencia

6.5. Validación forense de dispositivos extraíbles.
6.6. Validación de capturas de tráfico.

Competencias previas

Conocimientos: Los participantes deben tener conocimientos básicos de Linux, Windows y de Redes IP/TCP, Tener aprobado el curso de seguridad informática y hacking ético I.

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 analizara nuevos métodos para combatir amenazas que aumenta de forma exponencial en las empresas privadas y públicas, evitando tener pérdidas económicas por cualquier tipo de vulnerabilidad a la seguridad de la empresa.

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:
Ingeniero en Sistemas
Ingeniero en informática y ciencias de la computación
Áreas afines

Posgrado
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.