ESPE - Innovativa
EMPRESA PÚBLICA

Presentación del curso Presencial

Seguridad Informática y Hacking Ético

Módulo II

Tabla de contenido

Presentación del curso

El curso presencial de Seguridad Informática y Hacking Ético II, ofrece herramientas necesarias que nos permite comprender las técnicas y ataques que usan los hacker en la actualidad para realizar un eficiente 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 revisan las técnicas y metodologías para realizar auditorías de intrusión a aplicaciones web, se estudia la metodología OWASP y se realizan prácticas enfocadas en inyección de código, XSS, etc.

En la segunda unidad, se procede con aseguramiento de sitios web, después de conocer las técnicas de intrusión de la unidad anterior, el estudiante podrá proteger aplicaciones web de los ataques más utilizados por atacantes en la actualidad.

En la tercera unidad, se revisará las técnicas de tunneling y de esta forma ampliar el ataque a dispositivos internos.

En la cuarta unidad, el estudiante ingresará al mundo de la investigación forense, se realizarán prácticas esenciales de búsqueda de información después de un incidente así como análisis forense de muestras de tráfico en formato pcap.

En la quinta unidad, revisaremos técnicas de ingeniería reversa para vulnerar aplicaciones de escritorio de Windows.

Finalmente, en la sexta unidad, el estudiante podrá realizar validaciones de desbordamiento de memoria (Buffer Overflow) de aplicaciones y de esta forma generar sus propios códigos de explotación (exploit).

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:

- Identificar las principales vulnerabilidades de aplicaciones web y proponer soluciones a las mismas.
- Validar evidencia digital utilizando técnicas forenses obtenidas después de un hackeo a un equipo de cómputo.
- Conocer e interpretar las distintas técnicas utilizadas para realizar ingeniería inversa de aplicaciones.
- Identificar fallos de seguridad a nivel de aplicación y aprovechar problemas relacionados a Buffer Overflow.
- Desarrollar un código de explotación (exploit) y obtener accesos a aplicaciones al aprovechar Buffer Overflow.

Contenidos de cursos

Unidad 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

Unidad 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.

Unidad 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

Unidad 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.

Unidad 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

Unidad 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 del primer módulo de Hacking Ético.
- Conocimientos de sistemas operativos Windows y Linux Básico
- Conocimientos básicos Redes IP/TCP
- Conocimiento básico de programación.

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 se encuentran expuestos.

El 80% restante del curso está enfocado a la práctica de cada una de las etapas, hasta que el alumno pueda desarrollar su propio exploit después de identificar vulnerabilidades en aplicaciones conocidas.

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