CloudLamb

ETHICAL HACKING

Importancia del curso

¿Para quién es el curso de Ethical Hacking?
Para todos aquellos participantes que desee iniciar este mundo de seguridad de la información en la cual aprenderás a analizar sistemas para que estén protegidos contra el robo de información y ataques informáticos.
*No necesitas tener conocimientos previos en el área.

Requisitos para el desarrollo de los laboratorios:

Para las prácticas de laboratorio es importante que el participante disponga de su ordenador en el cual deberá tener instalado un software de virtualización (Virtual Box / VMWare) y virtualizado el sistema operativo Kali Linux en su última versión:

(https://www.offensive-security.com/kali-linux-vm-vmware-virtualbox-image-download/).

Contenido programático

1. Introducción
    - 1.1. ¿Qué es Ethical Hacking?
    - 1.2. Triada de la seguridad
        - 1.2.1. Confidencialidad
        - 1.2.2. Integridad
        - 1.2.3. Disponibilidad
    - 1.3. Conceptos principales
        - 1.3.1. Vulnerabilidad
        - 1.3.2. Amenaza
        - 1.3.3. Riesgo
        - 1.3.4. Exploit
        - 1.3.5. Tipos de ataques
    - 1.4. Tipos de hacker
        - 1.4.1. Sombrero Blanco, Negro, Gris

2. Criptografía
    - 2.1. ¿Qué es la criptografía?
    - 2.2. Conceptos básicos
    - 2.3. Historia
    - 2.4. Tipos de Criptografía
    - 2.5. Algoritmos criptográficos
    - 2.6. Funciones hash
        - 2.6.1. Ataques a contraseñas
    - 2.7. Certificados digitales
    - 2.8. Protocolos criptográficos

3. Vulnerabilidades
    - 3.1. ¿Qué es una vulnerabilidad?
    - 3.2. Clasificación de vulnerabilidades
    - 3.3. Sistema de puntuación de vulnerabilidades
    - 3.4. Diccionarios de vulnerabilidades
        - 3.4.1. CVE
        - 3.4.2. CWE
        - 3.4.3. MSXX-XX
    - 3.5. Web - OWASP Top 10
        - 3.5.1. Injection
        - 3.5.2. Broken Authentication
        - 3.5.3. Sensitive data exposure
        - 3.5.4. XML External Entities (XXE)
        - 3.5.5. Broken Access control
        - 3.5.6. Security misconfigurations
        - 3.5.7. Cross Site Scripting (XSS)
        - 3.5.8. Insecure Deserialization
        - 3.5.9. Using Components with known vulnerabilities
        - 3.5.10. Insufficient logging and monitoring

Contenido programático

4. Penetration Testing
    4.1. ¿Qué es el pentesting?
    4.2. Tipos de pruebas y escenarios
    4.3. Metodología de un Pentesting
        4.3.1. Reconocimiento
            4.3.1.1. Google Hacking
            4.3.1.2. Whols
            4.3.1.3. nslookup
            4.3.1.4. Shodan
        4.3.2. Descubrimiento y enumeración
            4.3.2.1. 3-Way Handshake
        4.3.2.2. nmap
        4.3.2.3. Dirbuster
            4.3.3. Análisis de vulnerabilidades
                4.3.3.1. nikto
                4.3.3.2. Burpsuite
        4.3.3.3. Revisión manual
        4.3.4. Explotación
            4.3.4.1. Metasploit
        4.3.4.2. Escalación de privilegios

5. Ingeniería Social
    5.1. Conceptos principales
    5.2. Técnicas
        5.2.1. Phishing
        5.2.2. Acceso Físico
        5.2.3. Vishing
        5.2.4. SMishing

6. Redacción de Reportes
    6.1. Tipos de reportes
    6.2. Secciones de un reporte
7. Preguntas para Certificaciones
    7.1. Tips

CloudLamb

La digitalización aumentará el alcance de la seguridad cibernética por ello entrenar en estas herramientas es invertir en su Seguridad Informática actual y futura