Pentesting con Kali Linux

Objetivo

Aplicar los conocimientos de diversas áreas informáticas tales como programación, bases de datos, redes de datos y sistemas operativos con el fin de identificar, analizar y explotar de manera general diversos tipos de vulnerabilidades presentes en la infraestructura de sistemas informáticos sensibles o críticos.

Público objetivo

Este curso está dirigido a estudiantes de computación o áreas afines a la informática que estén interesados en la seguridad informática, administradores de sistemas, oficiales y auditores de seguridad, gerentes y responsables de áreas informáticas que requiera, por sus actividades profesionales contar con los conocimientos de pruebas de penetración.

Conocimientos previos

El participante deberá contar de preferencia con conocimientos básicos en las siguientes áreas:

- Redes de datos.
- Sistemas operativos Windows o Linux.
- Uso de línea de comandos.
- Programación Estructurada u Orientada a objetos.
- Uso de algún lenguaje de programación(C, PHP o Python)
- Administración de servicios

Temario

1. Introducción (2.5 hrs.)
    a. Qué es una evaluación de seguridad (Pentest)
    b. Utilidad de un pentest
    c. Reglamentación y legislación para un pentest
    d. Alcance de un pentest
    e. Tipos de reportes
    f. Estructura del laboratorio
2. Metodología (2.5 hrs.)
    a. Reconocimiento
    b. Escaneo
    c. Enumeración

    d. Explotación
    e. Postexplotación
        i. Escalación de privilegios
        ii. Cubrir rastros
        iii. Puertas traseras
3. Reconocimiento (2.5 hrs.)
    a. Pasivo
        i. Informtation Gathering
        ii. Email Harvesting
        iii. Redes Sociales
        iv. Noticias y medios electrónicos
        v. Análisis de documentos digitales
    b. Activo
        i. Enumeracion DNS
        ii. Banner Grabbing
        iii. Tracing
        iv. Forward Lookup Brute Force
        v. Reverse Lookup Brute Force
        vi. Transferencia de zonas
4. Escaneo (2.5 hrs)
    a. Identificación de redes y hosts
    b. Identificación de puertos y servicios
    c. Escaneo de Vulnerabilidades
5. Enumeración (2.5 hrs)
    a. Obtención de registros y cuentas de usuario
    b. Identificación de clientes y cuentas en Windows
    c. Identificación de cliente Samba
    d. Enumeración de clientes SNMP
6. Explotación (15 horas)
    a. Bases de datos de exploits
    b. Ingeniería Social
    c. Explotación de sistemas
    d. Ataques a Redes
        i. Estructura de protocolos TCP/IP
        ii. Man in the middle
        iii. ARP Spoofing
        iv. DNS Spoofing
        v. SSL Trip
        vi. Hijacking
        vii. Sniffers
    e. Servidores Web
        i. Identificación de vulnerabilidades web

        ii. Proxies
        iii. SQL Injection
        iv. XSS
        v. Session Hijacking
        vi. CSRF
        vii. Remote File Inclusion
    f. Denial of Service
        i. Conexión (SYN Flood)
        ii. Recursos
        iii. Ancho de banda
7. Escalación de privilegios (5 hrs.)
    a. Offline
        i. Diccionario
        ii. Fuerza bruta
        iii. Híbridos
        iv. Obtención de contraseñas de usuarios
    b. Online
        i. Hydra
8. Cubrir rastros (2.5 hrs.)
    a. Borrado seguro
9. Puertas traseras (5 hrs.)
    a. Backdoors
    b. Keyloggers
    c. Troyanos
    d. Netcat
    e. Rootkits
10. Generación de documentación