Consultores Tecnológicos Empresariales

ORACLE Linux

SYLABUS CURSO TALLER ETHICAL HACKING

(30 horas)

1. Introducción al curso

- Presentación
- Objetivos y organización del curso
- Puntos clave para un mejor aprovechamiento del curso
- Definiciones y términos básicos

2. Introducción al Hacking Ético

- Introducción al módulo
- Nociones básicas
- Uso de Mailinator y cómo evadir los controles
- Vectores de ataque
- Dispositivos de seguridad
- Metodologías

3. Despliegue del laboratorio de pruebas

- Introducción del módulo
- Principales distribuciones de Hacking Ético
- Principales distribuciones vulnerables
- Instalación y uso de VirtualBox en Windows
- Instalación del laboratorio I: Kali Linux 2017
- Instalación del laboratorio I: Kali Linux desde OVA
- Despliegue de una máquina virtual desde un VDI (Parrot OS)
- Instalación del laboratorio III: Windows 7
- Instalación del laboratorio IV: Web for pentester
- Definir la configuración de red (Red NAT)
- Creación de máquinas virtuales en dispositivos de almacenamiento externo
- Despliegue y uso de Live-USB

4. Manejo de Kali Linux

- Introducción al módulo
- Introducción al manejo de Kali Linux y conocimiento de principales. Herramientas
- Uso de la terminal I: Manejo básico de la terminal
- Uso de la terminal II: Gestión de procesos, permisos y búsquedas
- Uso de la terminal III: Red e instalación de software
- Uso de la terminal IV: Información del sistema y compresión de datos
- Unix Bash Scripting

5. Anonimato en Internet

- Introducción del módulo
- Nociones básicas
- Instalación y uso de Tor en Windows
- Instalación y uso de Tor en Kali
- Uso de proxies
- Uso de FoxyProxy

- Uso de VPN en Windows y Linux
- Modificación de MAC en Windows y Linux
- Creación de una plataforma de anonimización propia
- Plataforma de anonimización I: Compra de servidores
- Plataforma de anonimización II: Creación de túneles. Herramientas proxychain
- Cambios necesarios en la configuración SSH (para el acceso como root)
- Examen de prueba 1: Evaluación – Aspectos básicos

6. Hacking ético de sistemas

- Introducción
- Nociones básicas
- Whois
- Análisis de direcciones IP
- Evasión de filtrado de Mailinator con Robtex
- Actualización Robtex - Nueva interfaz
- Análisis de sistemas autónomos (AS)
- Análisis de dominios y subdominios
- Browser Hacking (Google y Bing)
- Recopilación de información automática con Maltego
- Recopilación de información automática con Recon-NG
- Búsqueda de cuentas y credenciales de usuario
- Análisis histórico mediante Archive.org
- Información en documentos y metadatos (Foca)
- Enumeración pasiva I: Shodan
- Enumeración pasiva II: ZoomEye y oShadan
- Enumeración pasiva III: Censys
- Enumeración activa I: Escaneos en red local mediante ARP (ARPscan)
- Enumeración activa II: Análisis de tráfico e identificación de sistemas
- Enumeración activa III: Escaneos de red con Nmap
- Enumeración activa IV: Uso avanzado de Nmap
- Enumeración activa V: Uso de Zenmap
- Enumeración activa VI: Escaneo de puertos con herramientas adicionales
- Enumeración activa VII: Enumeración de sistemas mediante DNS
- Enumeración activa VIII: Herramientas para la enumeración mediante DNS
- dentificación manual (Fingerprint, uso de Google, Exploit-db, etc.)
- Identificación automática I: Instalación y uso de Nessus
- Identificación automática II: Uso avanzado de Nessus
- Ejemplo de servicios vulnerables
- SNMP (Community Strings por defecto)
- SMB(Sesiones nulas habilitadas)
- Tipología de exploits y conexiones
- Tipos de conexiones con netcat
- Ejemplo de exploit local: Dirty-Cow en Ubuntu 16.10
- Introducción y estructura
- Información básica de uso I
- Información básica de uso II
- Ejemplo de uso - Exploit Netapi
- Módulo payload. Ejemplos
- Módulo auxiliary. Ejemplos
- Añadir exploits manualmente a Metasploit
- Uso de Armitage (GUI de Metasploit)
- Herramientas avanzadas de Metasploit: Uso de msfvenom
- Introducción y conceptos previos
- Uso de Meterpreter I: Análisis del entorno

- Elevación de privilegios y extracción de credenciales
- Borrado de evidencias y eliminación de sistemas de seguridad
- Espionaje al usuario
- Sniffing de las comunicaciones
- Implantación de Backdoors
- Pivoting entre sistemas
- Uso de Psexec
- Extracción de credenciales mediante Mimikatz
- De una shell a Meterpreter
- Veil-Evasion
- Shelter Framework
- Introducción y conceptos
- Ataques de fuerza bruta online contra servicios habilitados
- Uso de PWdump7
- Uso de Ophcrack
- Uso de Mimikatz
- Uso de Procdump y Mimikatz
- Extracción de credenciales en Linux
- Acceso a recursos mediante el uso de Live CD
- Evasión del proceso de autenticación en Windows
- Evasión del proceso de autenticación en Linux

7. Hacking ético de aplicaciones web

- Introducción
- Nociones básicas
- Herramientas principales
- Herramientas principales – Mantra
- Herramientas principales – BurpSuite
- Herramientas principales - ZAP Proxy
- Herramientas principales - Charles Proxy
- Uso avanzado de BurpSuite - Intruder
- Uso avanzado de BurpSuite – Repeater
- Uso avanzado de BurpSuite - Comparer y Decoder
- Exploración de la aplicación
- Detección de contenido oculto - Dirbuster
- Detección de contenido oculto - Dirbuster y BurpSuite
- Detección de métodos HTTP
- Identificación de funcionalidades y tecnologías
- Pruebas en los controles del cliente – Envío de datos
- Pruebas en los controles del cliente - Detección de controles
- Pruebas en el mecanismo de autenticación - Análisis del proceso
- Pruebas en el mecanismo de autenticación Enumeración de usuarios
- Pruebas en el manejo de sesiones – Introdución
- Pruebas en el manejo de sesiones – CSRF
- Pruebas en el control de autorización - Introducción
- Pruebas en el control de autorización - Elevación de privilegios
- Definición de XSS
- XSS Reflejado
- XSS Persistente
- Evasión de filtros para la explotación de ataques XSS
- Robo de cookies mediante XSS
- Definición de SQL Injection
- Evasión de login mediante SQL Injection
- Explotación de SQL Injection

- Evasión de filtros para la explotación de ataques SQL Injection
- Uso de la herramienta SQLmap

8. Hacking ético de redes

- Introducción
- Nociones básicas
- Obtención y análisis de trafico con Wireshark
- Análisis pasivo de la red
- Interceptación de tráfico con Bettercap
- Interceptación de tráfico con CAIN
- Interceptación de tráfico mediante servidor DHCP falso

9. Hacking ético de redes Wi-Fi

- Introducción
- Nociones básicas
- Conexión de la tarjeta de red
- Pasos básicos y AirCrack-NG
- Despliegue de una red Wi-Fi WEP
- Cracking de una red Wi-Fi WEP
- Despliegue y cracking de una red WPA /WPA2
- Automatización de acciones

10. Ingeniería Social

- Introducción
- Nociones básicas
- Pretextos y escenarios
- Envío de Phishing
- Instalación de GoPhish
- Uso de GoPhish

11. Pautas para la ejecución de ejercicios Red Team

- Introducción
- Nociones básicas
- Infraestructura
- Obtención de información
- Enumeración de aplicaciones en pre-producción
- Enumeración de rangos y servicios ocultos
- Enumeración de redes no protegidas

- **Examen de prueba 2: Evaluación final**

✓ Ejercicios prácticos de todo los aprendido