CYBERIUM ARENA

Descripción

La formación en Pruebas de Penetración equipa a los aprendices con habilidades cruciales para identificar y explotar vulnerabilidades del sistema. Cubriendo la recopilación de datos, infiltración del sistema, técnicas post-violación y enfatizando en la Seguridad de Aplicaciones Web, este programa prepara a los participantes para proteger efectivamente los activos digitales contra amenazas cibernéticas.

ZX301 - PRUEBAS DE PENETRACIÓN

Módulo 1: Recolección de Información

Este módulo empodera a los aprendices con habilidades fundamentales de pruebas de penetración. Comienza con la Recopilación de Información, permitiendo entender los sistemas objetivos. Le sigue el Escaneo, enseñando la detección de puertos abiertos y servicios. Por último, la Enumeración proporciona información detallada del sistema, crítica para elaborar estrategias efectivas de ciberataque.

Recolección de Información
Whois y Dmitry
Google y GHDB
Shodan CLI
Reconocimiento DNS
Bases de Datos en Línea
Escaneo
Escaneo con Nmap
Scripting NSE
Enumeración
Servicios
Msfconsole
Herramientas de Enumeración
Métodos de Detección de Vulnerabilidades
Nessus

Módulo 2: Explotación

Este módulo se centra en los aspectos prácticos de las pruebas de penetración, con un enfoque agudo en la Explotación. Comienza enseñando las metodologías para aprovechar las vulnerabilidades para el acceso no autorizado al sistema. Además, explora los payloads, que son piezas de código ejecutadas después de una explotación exitosa, proporcionando conocimientos cruciales sobre la mecánica de ciberataque.

Explotación
Herramientas de Fuerza Bruta
Base de Datos de Exploits
Msfconsole
Explotación Manual
Payloads
Payloads de Msfvenom
Automatización de Payloads
Meterpreter

Módulo 3: Post Explotación

Las tácticas de post explotación, utilizadas después de obtener acceso no autorizado, se exploran, dando información sobre el mantenimiento del acceso, extracción de datos y cómo cubrir las huellas. Además, examina la ingeniería social, una táctica de manipulación humana para obtener información o acceso, subrayando el elemento humano en la ciberseguridad.

Explotaciones Locales vs. Remotas
Escalación de Privilegios
Persistencia
Desactivación de Seguridad
Ingeniería Social
Servicios en Línea
BeEF
Marcos de Phishing
Técnicas Avanzadas

Módulo 4: Seguridad de Aplicaciones Web

Este módulo arroja luz sobre el aspecto crucial de proteger las aplicaciones web. Navega a través de varios aspectos de la seguridad de aplicaciones web, destacando vulnerabilidades comunes y proporcionando estrategias efectivas para contrarrestarlas. Un enfoque clave es en asegurar las transacciones de datos, procesos de autenticación de usuarios y garantizar la integridad general de la aplicación.

Fundamentos de HTML
Acerca de OWASP
XSS
LFI/RFI
Fuerza Bruta
Inyección SQL
Payloads Web
Shell Reverso
Burp Suite
Proxy
Repetidor
Intruso
Codificador

ZX Ofensiva | NIVEL: 3 | DURACIÓN: 10-12 semanas (autoaprendizaje) / 40h (con instructor)