EDUCACIÓN IT

Ethical Hacking

Programa de Estudio

Ethical Hacking

Aprende las técnicas más utilizadas para analizar la seguridad de las redes empresariales. Maneja conceptos como Vulnerabilidad y Exploit para asistir a las organizaciones.

Contenido del curso

El curso comienza con la explicación del proceso de Penetration Testing y cada una de sus fases. Luego, vamos a ver las técnicas de reconocimiento, enumeración y escaneo, a fin de detectar las características de la infraestructura que estamos analizando y sus posibles puntos débiles. Esto nos va a permitir identificar vulnerabilidades y posibles puntos de ataque. Más adelante vamos a aprender cómo se pueden explotar las vulnerabilidades utilizando Metasploit, y todas sus funcionalidades que nos van a permitir el control remoto de los sistemas atacados. Trabajaremos siempre sobre vulnerabilidades reales encontradas en software reconocido.

PRÁCTICAS EN CLASE ::
Realizaremos prácticas para identificar los sistemas de una organización, así como para geolocalizar cada uno de los mismos. Haremos escaneos de puertos con Nmap, identificaremos los sistemas operativos y versiones de software, para luego buscar vulnerabilidades asociadas a dichas soluciones. Una vez hecho eso aprenderemos a explotarlas, principalmente utilizando Metasploit, trabajando sobre vulnerabilidades como ?EternalBlue? (MS17-10). También controlaremos los equipos víctima y aprenderemos a obtener información sensible, como credenciales y archivos confidenciales. También aprenderemos a infectar archivos benignos para transformarlos en maliciosos y que nos den acceso remoto a los equipos, así como también aprenderemos a utilizar los equipos ya controlados para atacar a otros equipos de la red.

Requisitos

Conocimientos previos:
Tener conocimientos de seguridad informática o haber realizado el curso de Introducción a la seguridad Informática
Tener conocimientos de criptografía o haber realizado el curso de Criptografía y Blockchain
Tener conocimientos de seguridad en redes o haber realizado el curso de Seguridad en Redes: Network Hacking

Modalidad de cursado

Puedes tomar este curso en modalidad presencial o modalidad online - en vivo

¿Qué aprenderás?

- Fundamentos de la metodología Hacking
- Reconocimiento de vulnerabilidades
- Cómo identificar ubicación y proveedor a través del IP
- Identificación de servidores de eMail y DNS
- Trabajar con Escaneo y Explotación
- Buffer Overflow, Exploit y Shellcode
- Utilización de Metasploit
- Instalación de Keyloggers
- Post Explotación
- Saltar User Account Control
- Obtención de credenciales y eliminación de logs
- Client Side Exploits
- Tipos de ataques más utilizados
- Cracking Local y Remoto

Plan de Estudios

1. Reconocimiento

Whois
NS y MX
Transferencias de Zona
Fuerza bruta de DNS
Virtual Hosts
Geolocalización
Mapeo de IP a ASN
Shodan
Google Hacking
Obtener Direcciones de Email de un Dominio
Análisis de Metadatos
Cabeceras de Correos Electrónicos

2. Escaneo y Explotación

Detección de puertos abiertos
Detección de SO y Versiones de Software
Ejecución de Scripts para detección de vulnerabilidades
Transferencia de archivos con netcat
Conexión con shell de sistema
Shell Bind y Shell Inversa
CVE, CWE y CVSS
Descargar y usar exploits
Modificación de exploits

3. Metasploit

Msfconsole y configuración de la base de datos
Búsqueda de exploits
Selección y configuración de exploits
Selección y configuración de payloads
Explotación
Payloads staged vs non-staged

Manejo de sesiones y upgrade a Meterpreter
Migración de procesos
Gestión de archivos desde Meterpreter
Obtener información del sistema
Instalación de Keyloggers

4. Post Explotación

Saltar User Account Control
Persistencia
Elevación de Privilegios
Exploits Locales
Enumerar aplicaciones Instaladas
Obtener credenciales
Eliminación de Logs
Port Forwarding
Explotación a través de otro equipo
Metasploit resource files
Meterpreter resource files

5. Client Side Exploits

Payloads Ejecutables
Conectarnos con metasploit a una shell de netcat
Infección de ejecutables existentes con msfvenom
Payloads en VBS
Ataque a Internet Explorer
Ataque a Adobe PDF Reader
Payloads multiplataforma con Java
Explotación de EternalBlue
Migración de Meterpreter de 32bits a 64bits
Obtener credenciales desde la memoria
Volcar hashes de contraseñas
Crackear contraseñas con John The Ripper

6. Cracking Local y Remoto

Identificar tipo de hash
Utilizar Wordlists en John The Ripper
Reglas de Crackeo
Generación de diccionarios personalizados
Cracking de VNC
Cracking de POP3
Cracking de FTP
Cracking de SNMP

EDUCACIÓN IT

Centro de Capacitación y Desarrollo Profesional

Lavalle 648 Piso 8, Microcentro, CABA
TEL_PRINCIPAL
info@educacionit.com