“Curso de Ethical Hacking y Red Team”

XNET SOLUTIONS

Xnet Academy

Material Actualizado 2026

1. Curso de Ethical Hacking

CURSO : CURSO DE ETHICAL HACKING Y RED TEAM

Duración : 72 Horas

Modalidad : On-Demand

DESCRIPCION DEL CURSO:

El curso de Ethical Hacker y Red Team está diseñado para formar profesionales en el campo de la ciberseguridad, enseñándoles a identificar y validar vulnerabilidades en sistemas informáticos de manera ética y legal. A lo largo del curso, los participantes adquirirán habilidades prácticas en la realización de pruebas de penetración (pentesting), simulando ataques cibernéticos para evaluar la seguridad de redes lan, Servidores corporativos, Equipos de Perímetro, aplicaciones web, Sistemas IoT y mucho más.

Se profundiza en el uso de herramientas y técnicas avanzadas para detectar fallos en infraestructuras tecnológicas, enumeración de protocolos, ataques de ingeniería social, explotación de vulnerabilidades, uso de técnicas avanzadas de ataques basado en IA. Además, el curso aborda estrategias para proteger información sensible, implementando medidas preventivas y correctivas para garantizar la integridad y confidencialidad de los sistemas. Al finalizar, los participantes estarán preparados para actuar como profesionales de la ciberseguridad, ofreciendo soluciones para mitigar riesgos y fortalecer la seguridad en las organizaciones.

Competencias:

- Comprende un ataque a servidores y estaciones de trabajo a través de Internet
- Realiza una prueba de penetración
- Utiliza las herramientas idóneas para realizar un proceso de Ethical Hacking
- Conoce la metodología OSSTMM desarrollada por ISECOM para tests de seguridad
- Entiende el funcionamiento de los ataques más comunes desde Internet
- Comprende cómo protegerse de los ataques implementando medida de seguridad
- Reconoce las ventajas de la tecnología y los peligros al no tener una cultura de seguridad

Requisitos:

- Conocimiento intermedio de redes
- Conocimiento básico de Linux

Para los laboratorios:

- Se necesita tener una Computadora con 16GB RAM
- VMware Workstation o Player

Dirigido a:

- Profesionales y Técnicos en Tecnologías de la Información
- Profesionales y Técnicos en Seguridad de la Información
- Consultores, Jefes de Proyectos e Integradores de Sistemas
- Administración de Redes y Sistemas Operativos Plan curricular

Metodología:

El curso contará con sesiones teórico-prácticas. Se empleará material audiovisual con la finalidad de facilitar los procesos de adquisición y evaluación del aprendizaje. Durante las clases se buscará la participación activa de los alumnos mediante el desarrollo de ejercicios y discusión en clase. Se trabaja con equipos reales y máquinas virtuales.

- Se utilizará la plataforma de zoom para el desarrollo de las clases en vivo
- Durante las clases teóricas, el instructor desarrollara algunos casos prácticos para enfatizar los puntos en aprendizaje.
- Durante las clases el instructor desarrollara alguno de los laboratorios en vivo
- Los alumnos deberán desarrollar todos los laboratorios de cada modulo fuera de horario de clase y presentar una breve captura del desarrollo del laboratorio

Campus Educativo:

- Xnet Solutions cuenta con un campus educativo donde todos los alumnos tendrán acceso para poder ver los videos de las clases en vivo, posterior a las sesiones en vivo.
- A través del campus educativo, podrán descargar el material educativo de las clases, guías de laboratorio y máquinas virtuales

Certificado del Curso:

Al finalizar el curso, cada alumno recibirá un certificado de asistencia al curso emitido por Xnet Academy.

Beneficios de llevar el curso con Xnet Solutions:

- 72 Horas de Clases en vivo, en español
- Instructor con más de 15 años de experiencia en Hacking Ético
- Material educativo de cada Módulo en español
- Guía de Laboratorios detallado
- Máquinas Virtuales para desarrollo de laboratorio
- Herramientas de Hacking Ético usadas en el Curso
- Videos Guiados de Laboratorios y Clases en vivo
- Certificado del Curso de Ethical Hacking y Red Team
- Revisión de casos utilizado en ambientes corporativos
- Evaluación de los alumnos para un mejor aprendizaje

- Guía constante de un experto en Penetration Testing Profesional
- Examen del Curso y Retos para afianzar conocimientos

PLAN DE TEMAS

El programa incluye los siguientes módulos

Módulo 1 : Fundamentos de Ethical Hacking

Introducción al Ethical Hacking

- Panorama Mundial de Amenazas
- Ciberataques del 2024 – 2025
- Penetration Testing
- Red Team
- Purple Team
- Fases del Hacking Ético
- Metodología de Hacking Ético
- Tipos de Evaluaciones
- Linux para Pentester
- Instalación de Maquinas Virtuales

Footprinting y Reconocimiento

- Técnicas de FootPrinting
- Google Hacking / GHDB
- Netcraft , Shodan , Censys
- Sublist3r , dnsmap, theHarvester
- Sherlock, dmitry
- Duplicación de Sitios Web, Httrack
- Exfiltración de Datos : HaveiBeenPwned
- Dehashed, darkweb
- Extracción de Metadata : ExifTool
- Whois , Registros DNS, mxtoolbox
- Dig, DNSRecon,
- Maltego, Recon-ng, Foca,
- Osintframework, Argus, Kraken

Escaneo de Redes

- Introducción
- Modelo TCP/IP
- Three Way Handshake
- Técnicas de Escaneo de Puertos
- Escaneo con NMAP : Discovery
- Escaneo con NMAP : Host, Servicios
- TCP Connect, Syn Scan, Null Scan

- XMAS Scan, FIN Scan, UDP Scan
- Bypass Firewall, IPS , Scripts
- Masscan, Netcat para Pentester

Enumeración de Servicios

- Introducción
- Técnicas de Enumeración
- Enumeración de Netbios : Nbtstat, net view
- Enumeración de SMB : nmap, smbclient, enum4linux
- Fuerza Bruta SMB2: crackmapexec, hydra
- Enumeración de cuentas de usuario : PSTools, Psexec, PsList, PsFile,..
- Enumeración de SNMP V1, V2 , V3 : smnp-check , onesixtyone, snmpwalk
- Creando de Script y técnicas de hacking para SNMPv3
- Enumeración de LDAP : nmap, ldapsearch
- Enumeración de NTP, NFS , SMTP : nmap, metasploit
- Enumeración de DNSSEC, Transferencia Zona, DNS Cache Snooping, Zone Walking
- Enumeración de Telnet, FTP, TFTP, BGP, Linux

Analisis de Vulnerabilidades

- Introducción
- Conceptos Básicos
- Sistemas de Puntuación de Vulnerabilidades y Base de Datos
- CVSS , CVE , CWE
- Ciclo de Vida de Gestión de Vulnerabilidades
- Tipos de Evaluación de Vulnerabilidades
- Tipos de Analizadores
- Analizador a Nivel de Plataforma
- Analizador a Nivel de Aplicación
- Herramientas de Evaluación de Vulnerabilidades
- Componentes de un Informe de Evaluación de Vulnerabilidades
- Qualys Guard , Acunetix
- Nessus Professional, GFI LanGuard
- OpenVAS, Nikto , Nuclei
- CIS Benchmark

Módulo 2 : Ethical Hacking Avanzado

Explotación Vulnerabilidades Metasploit

- Introducción
- Arquitectura de Metasploit
- Módulos de Metasploit
- Interfaces de Metasploit
- Procesos para el test de penetración
- Proceso de Ataque
- Configurando Databases
- Escaneo de Puertos con NMAP
- Payload
- Exploits
- Exploit Remotos y Exploit Locales
- Msfvenom
- Postexplotación
- Meterpreter
- Escalamiento de Privilegios

Creación de Exploit para Windows

- Introducción a Assembly

- Registros Internos
- STACK
- CALL & RET
- STACK FRAME
- Variables Locales
- Otras instrucciones
- Buffer Overflow
- Immunity Debugger
- Empezando a Atacar
- Controlando el EIP
- ¿Qué son los Badchar?
- Shellcode
- Ejecutando un Exploit
- Stack Cookie
- Address Space Layout Randomization (ASLR)
- Data Execution Prevention (DEP)
- Return Into Lib
- Trucos Anti-Dep

Hackeando Sistemas

- Mecanismo de Autenticación de Microsoft
- Almacenamiento de credenciales en Windows
- Kerberos y Autenticación de Red
- Password Cracking
- Creando diccionarios de credenciales avanzado
- Mecanismo de creación de diccionarios complejos
- Ataques online: Password Spraying
- Ataques sin conexión : Rainbown table attack
- Pwdump7, L0phtCrack, ophcrack, RainbowCrack
- Ataques de LLMNR / NBT-NS : Responder
- Escalamiento de Privilegios
- Pivoting y Relaying
- Borrando Logs
- Deshabilitando auditoria : auditpol

Post – Explotación Avanzada - Red Team

- Actividades Post-Explotación
- Técnicas Post-Explotación
- Seatbelt
- Escalamiento privilegios en Linux
- Escalamiento privilegios en Windows
- Bloodhound
- Obteniendo Password, Hashes de acceso
- MSF psexec, hashdumping, Mimikatz
- Crackeando con John the Ripper y Hashcat

Movimiento Lateral y Command and Control

- Corriendo comandos con SC y WMIC
- Impacket
- Pass-the-Hash
- Command and control (C2)
- Empire
- Sliver
- Netcat

Ingenieria Social

- Ingeniería Social
- Tipos de Ingeniería Social
- Impersonation
- Vishing
- TailGating, Piggybacking
- Baiting
- Phishing
- Herramientas para Phishing
- IA en Phishing

Módulo 3 : Ethical Hacking Páginas Web

Hackeando Servidores Web

- Mercado para Servidores Web Actuales
- Arquitectura de Servidores Web Open Source
- Arquitectura de Servidores IIS
- Problemas de Seguridad del Servidor Web
- DNS SERVER HIJACKING
- Ataques de Amplificación de DNS
- Ataques Transversales de Directorio
- Web Defacement
- Mala Configuración del Servidor Web
- Ataque de División de Respuesta HTTP
- Ataque de Envenenamiento de Cache Web
- Descifrando Contraseñas del Servidor Web
- Comprometidos
- Metodología para Ataques de Web
- Como detectar Balanceadores de Carga
- Como detectar Proxies
- Proxies
- Detectando Web App Firewalls (WAF)
- HTTPRINT
- HTTPRECON
- Clonando un Website
- Escaneadores de Vulnerabilidades Web
- Técnicas de Craqueo de Contraseñas
- Crackeo de Contraseñas
- Ataque de Fuerza Bruta
- Cracking Passwords

Hacking de Aplicaciones Web

- Aplicaciones Web
- Componentes de Aplicación Web
- Arquitectura de Aplicaciones Web
- Pilares de Vulnerabilidad Web
- Vectores de Ataque de APP Web
- Amenazas de Aplicaciones Web
- URI HACKING
- METHODS, HEADER Y BODY
- Autenticación, Sesión y Autorización
- El Cliente Web en HTML
- Java Clases y Applets
- Flash and Silverlight Objects
- Query String
- Explotación de Cookie: Envenenamiento de Cookie
- Metodologías para Hackeo de Aplicaciones Web

- Ataque de Administración de Sesión
- Atacando el Mecanismo de la Sesión de Generación de Token
- Ataque del Manipulación del Mecanismo de Token de Sesión: Capturando Token de Sesión
- Ataque de Conectividad de Datos
- Inyección de Cadena de Conexión
- Errores de Configuración en Páginas Web

Módulo 4 : Ethical Hacking Redes Wireless

Autenticación WLAN y Defectos de Cifrado

- Descubrimiento de SSID oculto
- Filtros MAC
- Bypaseando Open Autentication
- Bypaseando Autentication Shared Key
- Encriptación WPA y Cracking WPA2
- Acelerando Ataques en WPA/WPA2
- Desencriptando Paquetes WEP y WPA
- Conectándose a Redes WEP y WPA

Hackeando Redes Inalámbricas 802.1X

- Aspectos de Seguridad
- Topología de una Red WIFI 802.1X
- Implementación de Radius con MD5
- Ataques a Redes Inalámbricas con 802.1X
- Atacando a Redes WPA2 con Radius
- Atacando a Redes Inalámbricas 802.1X

Módulo 5 : Ethical Hacking dispositivos Moviles

Atacando a dispositivos Móviles

- Áreas vulnerables de un dispositivo Movil
- Owasp Top 10 Mobile Risks
- Sanboxing en dispositivos móviles
- Android Rooting
- Jailbreaking iOS
- Identificando vulnerabilidades con drozer
- Explotando dispositivos Android con ADB
- Explotando dispositivos Android con Metasploit

Módulo 6 : Ethical Hacking en Ambientes Cloud

Realizando Hacking Ético en Ambientes Cloud

- Tipos de Servicios Cloud
- Tecnologías : Container, Microservicios, Orquestación
- Vulnerabilidades típicas en Cloud
- Ataques en Cloud
- Cloud Hacking
- Metodología de Hacking en Cloud
- Enumeración de AWS S3 Buckets
- Enumeración AWS EC2 Instances
- Analizando AWS Account IDs y IAM Roles
- Utilizando CloudFox
- Explotando AWS S3 Buckets
- Utilizando varias Herramientas en Cloud