CURSO

WINDOWS SERVER HACKING

Plan de estudio

educación IT

Nuestro propósito

Transformar positivamente la vida de las personas.

Queremos que seas protagonista en la transformación que estamos viviendo. Por eso, nos comprometemos a capacitarte para que estés al día con las necesidades digitales actuales.

Te invitamos a trabajar en conjunto para que descubras tu mejor versión y la potencies. Anímate, toma las riendas de tu futuro.

Code your future!

Contenido del curso

Domina el ataque y defensa en los servidores Windows: detecta vulnerabilidades, escala privilegios y asegura persistencia.

¿Qué aprenderás?

- Políticas de seguridad en Windows.
- Monitoreo y auditoría avanzada.
- Hardening de Windows.
- Reconocimiento, enumeración y análisis.
- Vulnerabilidades en sistemas Windows.
- Explotación de vulnerabilidades críticas.
- Elevación de privilegios.
- Técnicas de persistencia.
- Movimiento lateral y gestión de credenciales.
- Uso de credenciales comprometidas.
- Defensa contra ataques conocidos.
- Técnicas de evasión.

Plan de estudios

1 Introducción y configuración inicial

- Concepto de Windows Hacking.
- Modelos de amenazas en Windows.
- Configuración inicial y update de Windows.
- Uso de msconfig y UAC.
- Configuración de políticas de contraseñas.
- Políticas de bloqueo de cuentas.
- Configuración de auditoría de eventos.
- Análisis del visor de eventos de Windows.
- Diagnóstico de seguridad del sistema.

2 Hardening de Windows: protección y seguridad

- Control de Cuentas Administrativas.
- Políticas de expiración de sesiones.
- Desactivación de cuentas inactivas.
- Configuración de Firewall de Windows.
- Control de puertos y apps permitidas.
- Desactivación de servicios no esenciales.
- Software Restriction Policy.
- Configuración avanzada de AppLocker.
- Windows Defender Application Control (WDAC).
- Implementación de BitLocker para cifrado.
- Protección contra ataques de Ransomware.

3 Monitoreo y auditoría avanzada

- Políticas de auditoría avanzada.
- Auditoría de eventos de inicio de sesión.
- Auditoría de acceso a archivos y carpetas.
- Análisis del visor de eventos de Windows.
- Identificación de eventos críticos.
- Monitoreo en tiempo real con Procmon.
- Análisis del sistema con Sysmon.
- Diagnóstico de Actividad Sospechosa.

4 Explotación de Windows

- Vulnerabilidades comunes en Windows.
- Análisis de vulnerabilidades con wes.py.
- Uso de Atomic Red Team para explotación.
- Explotación de vulnerabilidades críticas.
- EternalBlue (CVE-2017-0144).
- BlueKeep (CVE-2019-0708).
- PrintNightmare (CVE-2021-1675).
- Zerologon (CVE-2020-1472).
- PetitPotam (CVE-2021-36942).
- SMBGhost (CVE-2020-0796).
- Ejecución de Payloads con Metasploit.
- Explotación de Windows Remote Management.
- Mitigación de Vulnerabilidades Exploited.

5 Elevación de privilegios

- Identificación de configuraciones débiles.
- Explotación de configuraciones vulnerables.
- Bypass de User Account Control (UAC).

- Explotación de UACME.
- Explotación de servicios vulnerables (binPath).
- Manipulación de servicios existentes.
- Uso de COMahawk para explotación COM.
- DLL Hijacking: escalamiento de privilegios.

6 Movimiento lateral y gestión de credenciales

- Introducción a la gestión de credenciales.
- Volcado de hashes (SAM y Security).
- Extracción de hashes con reg save.
- Uso de secretsdump.py para volcado remoto.
- Extracción de credenciales de LSASS.
- Credenciales volcadas (hash y texto plano).
- Introducción al movimiento lateral.
- Pass-the-Hash (PTH).
- Pass-the-Ticket (PTT).
- Over-Pass-the-Hash (Pass-the-Key).
- Windows Management Instrumentation (WMI).
- PSExec.
- Windows Remote Management (WinRM).

7 Persistencia (Mantener el acceso)

- Introducción a las técnicas de persistencia.
- Persistencia con tareas programadas.
- Persistencia a través de servicios.
- Modificación de servicios existentes.
- Persistencia en el registro de Windows.
- Persistencia con WMI.

- Persistencia mediante DLL Hijacking.
- Persistencia con PowerShell (Profile.ps1).

Modalidad del Curso

Duración
5 semanas / 20 h

Frecuencia semanal
2 encuentros de 2 h

Modalidad
Online en vivo

Grupos reducidos
Promedio 20 personas

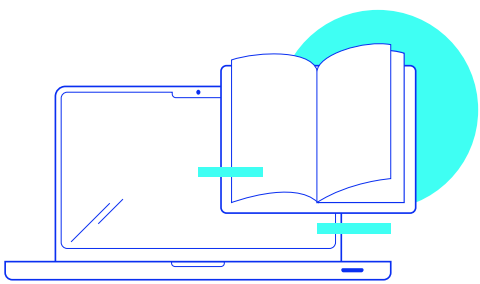
Nivel: **Principiante**

Requisitos

Es recomendable tener una base sobre: **Ethical Hacking**

Dedicación fuera de clase

Además de las horas de clase, recomendamos que inviertas 4 h semanales extras para realizar los desafíos complementarios, estudiar el material de lectura y completar los exámenes del Alumni.



¿Cómo será tu experiencia?

Aprender haciendo

Ejercita y pon en práctica lo estudiado.

Trabajo en equipo

Une esfuerzos y potencia los resultados.

Clases grabadas

Consúltalas las veces que quieras.

Profesores expertos

Aprende de gigantes de la industria.

Asistente académico

Recibe soporte dentro y fuera de clase.

Plataforma Alumni

Encuentra recursos, materiales y clases.

¿Por qué Educación IT?

IT Créditos

Gana puntos al aprobar los exámenes de los cursos. Luego, podrás canjearlos por nuevos cursos sin costo alguno. Los IT Créditos que acumules no vencen ni se devalúan.

Garantía de aprendizaje

Si necesitas reforzar conceptos, recuperar clases o no estás satisfecho, ¡vuelve a tomar el curso sin ningún costo! Puede ser de forma total o parcial.

Comunidad en Discord

Mantente en contacto con la comunidad de EducaciónIT a través de nuestro servidor de Discord. Podrás hablar con tus compañeros, profesores, asistentes académicos y soporte.

Preguntas frecuentes

Si me pierdo una o más clases, ¿puedo recuperarlas?

Todas las clases quedan grabadas de por vida en tu plataforma Alumni. ¡Siempre podrás volver a verlas cada vez que lo necesites!

¿Cómo voy a aprender?

Te enfrentarás a situaciones de trabajo reales, en donde tendrás que aplicar lo aprendido de forma individual y en equipo. Por medio de la prueba y el error, irás superando desafíos y obteniendo nuevas habilidades que luego podrás aplicar en el ámbito laboral.

¿Cómo son las clases online en vivo?

Las clases duran entre 2 y 3 horas de lunes a viernes (sábados 3 o 4 hs) y se desarrollan de forma online en vivo en aulas virtuales, donde vas a poder interactuar con el instructor y tus compañeros.
Manejamos cupos reducidos para que puedas tener un seguimiento más personalizado durante tu aprendizaje.

educación IT

Plan de estudio

Code your future

www.educacionit.com

@educacionit