

Tarea online HE03.

Título de la tarea: La primera intrusión.

Curso de Especialización y módulo: Ciberseguridad en Entornos de las Tecnologías de la Información - Hacking Ético.

¿Qué contenidos o resultados de aprendizaje trabajaremos?

Resultados de aprendizaje

- ✓ **RA3.** Ataca y defiende en entornos de prueba, redes y sistemas consiguiendo acceso a información y sistemas de terceros.

Contenidos

- 1.- Fase de reconocimiento (Footprinting).
 - 1.1.- Tipos de reconocimiento.
 - 1.2.- Reconocimiento pasivo.
 - 1.3.- Reconocimiento activo.
- 2.- Fase de escaneo (Fingerprinting).
 - 2.1.- Tipos y enfoque de los escaneos.
 - 2.2.- Escaneo de red
 - 2.3.- Escaneo de servicios.
 - 2.4.- Escaneo de vulnerabilidades.
 - 2.5.- Opciones avanzadas de nmap.
 - 2.6.- Herramientas adicionales de búsqueda de vulnerabilidades.
- 3.- Fase de explotación de vulnerabilidades (Exploitation).
 - 3.1.- Vectores de ataque.
 - 3.2.- Concepto de exploit.
 - 3.3.- Concepto de payload.
 - 3.4.- Herramienta Metasploit.
 - 3.5.- Herramienta msfvenom.
- 4.- Interceptación, manipulación y monitorización del tráfico.
 - 4.1.- Interceptación de comunicaciones y monitorización del tráfico.
 - 4.2.- Manipulación e inyección de tráfico.
- 5.- Phishing.
 - 5.1.- Introducción al phishing y sus tipos.
 - 5.2.- Metodología y herramientas.
- 6.- Elevación de privilegios.
 - 6.1.- Introducción a la elevación de privilegios.
 - 6.2.- Elevación de privilegios en Linux.
 - 6.3.- Elevación de privilegios en Windows.

6.4.- Herramientas de elevación de privilegios.

1.- Descripción de la tarea.



Caso práctico

Una vez Luis ha completado el curso en el que ha adquirido los conocimientos necesarios para poder realizar una primera intrusión en un equipo remoto.

Ahora es el turno de poder compartir estos conceptos con sus compañeros de trabajo para que todos puedan tener, al menos, unas nociones básicas de la temática que ha podido aprender Luis en el curso.

Luis piensa que lo mejor para poder afianzar los conceptos es poder trabajar con ellos de manera práctica. Con este fin decide crear un laboratorio de pruebas y resolver en ellas alguna de las actividades.



[Direct Media](#) (Dominio público)

¿Qué te pedimos que hagas?


✓ Apartado 1: Fase de reconocimiento


Utilizando el buscador google y técnicas de google dorking se propone que ayudéis a Luis a realizar las siguientes búsquedas:

- ➡ **Buscar todos los archivos pdf del sitio github.com**
- ➡ **Buscar cualquier url que contenga la cadena “intranet/login.php”**
- ➡ **Buscar un listado de directorios con la carpeta uploads expuesta**
- ➡ **Buscar ficheros con usuarios de Tomcat (tomcat-users.xml)**

✓ Apartado 2: Instalación del Laboratorio

Para los siguientes ejercicios prácticos Luis va a necesitar montar un laboratorio en el que necesitará una máquina de ataque y una máquina víctima sobre la que realizar las pruebas. Tienes que ayudar a Luis a montar un laboratorio con las siguientes características:

- ➡ Utilizar VirtualBox.
- ➡ Configurar en VirtualBox una "RedNAT" con el direccionamiento de red 10.0.2.0/24. ¡¡¡IMPORTANTE!!: No confundir con la opción de NAT ya que en este último no permites que 2 o más máquinas virtuales se encuentren en la misma red.
- ➡ Tener una máquina de ataque tipo Kali Linux. Podéis descargarla de [este enlace](#) .

- ➡ Tener una máquina víctima Metasploitable. Podéis descargarla en el [siguiente enlace](#)  .
¡¡IMPORTANTE!! La máquina Metasploitable2 no es compatible con VirtualBox. Hay que hacer una conversión previa (una búsqueda en Google sobre "instalar metasploitable 2 en virtualbox" os puede ayudar con el proceso)
Has de detallar los pasos necesarios para instalar la Máquina Virtual Kali, la Máquina Virtual Metasploitable2 y la "RedNAT"

✓ Apartado 3: Fase de escaneo

Utilizando el laboratorio de Kali Linux + Metasploitable2 ayudar a Luis a realizar una fase de escaneo con nmap en la que se cubren los 3 tipos de escaneo:

- ➡ Escaneo de red
- ➡ Escaneo de servicios
- ➡ Escaneo de vulnerabilidades (deberéis instalar vulscan para realizar el escaneo)

✓ Apartado 4: Fase de explotación con Metasploit.

Tras haber completado la fase de Escaneo, cuando se realizó el escaneo de vulnerabilidades con vulscan, se pudo comprobar que el servidor FTP en el puerto TCP/21 presenta una vulnerabilidad pública. Ayuda a Luis a realizar la explotación de una vulnerabilidad del servidor *vsftpd2.3.4* . Utiliza Metasploit para realizar esta tarea y conseguir una shell en el equipo remoto.

NOTA IMPORTANTE

Para los apartados en los que se solicita realizar una captura de pantalla hay que tener en cuenta que las capturas realizadas deben tener como fondo de pantalla la plataforma con tu usuario mostrando claramente la foto de tu perfil. Aquellos apartados/subapartados que no cumplan esta condición no serán corregidos.

2.- Información de interés.

Recursos necesarios y recomendaciones

Recursos necesarios

- ✓ Ordenador personal con, al menos, 4 Gigabytes de memoria RAM.
- ✓ Conexión a Internet para consultar ejemplos de la Unidad 3.
- ✓ Sistemas Operativos preferidos Kali Linux, Parrot Linux.
- ✓ Sistema Operativo de la víctima Metasploitable2.
- ✓ Navegador web.
- ✓ Software para comprimir los archivos de la tarea.

Recomendaciones

- ✓ Antes de abordar la tarea:
- ➡ lee con detenimiento la unidad, consulta los enlaces para saber más, examina el material proporcionado por el profesor y aclara las dudas que te surjan con él.
- ➡ Realiza el examen online de la unidad, y consulta nuevamente las dudas que te surjan. Solo cuando lo tengas todo claro, debes abordar la realización de la tarea.
- ✓ No olvides elaborar el documento explicativo.



Indicaciones de entrega

Una vez realizada la tarea, el envío se realizará a través de la plataforma. El archivo se nombrará siguiendo las siguientes pautas:

Apellido1_Apellido2_Nombre_HE03_Tarea

Asegúrate que el nombre no contenga la letra ñ, tildes ni caracteres especiales extraños. Así por ejemplo la alumna **Begoña Sánchez Mañas para la tercera unidad del MP de HE**, debería nombrar esta tarea como...

sanchez_manas_begona_HE03_Tarea

3.- Evaluación de la tarea.

Criterios de evaluación RA3

- ✓ a) Se ha recopilado información sobre la red y sistemas objetivo mediante técnicas pasivas.
- ✓ b) Se ha creado un inventario de equipos, cuentas de usuario y potenciales vulnerabilidades de la red y sistemas objetivo mediante técnicas activas.
- ✓ c) Se ha interceptado tráfico de red de terceros para buscar información sensible.
- ✓ d) Se ha realizado un ataque de intermediario, leyendo, insertando y modificando, a voluntad, el tráfico intercambiado por dos extremos remotos.
- ✓ e) Se han comprometido sistemas remotos explotando sus vulnerabilidades.

¿Cómo valoramos y puntuamos tu tarea?

Rúbrica de la tarea	
Apartado 1: Configura correctamente mediante los operadores necesarios la búsqueda en Google que devuelve el resultado de "Buscar todos los archivos pdf del sitio github.com"	0,5 puntos
Apartado 1: Configura correctamente mediante los operadores necesarios la búsqueda en Google que devuelve el resultado de "Buscar cualquier url que contenga la cadena "intranet/login.php""	0,5 puntos
Apartado 1: Configura correctamente mediante los operadores necesarios la búsqueda en Google que devuelve el resultado de "Buscar un listado de directorios con la carpeta uploads expuesta"	0,5 puntos
Apartado 1: Configura correctamente mediante los operadores necesarios la búsqueda en Google que devuelve el resultado de "Buscar ficheros con usuarios de Tomcat (tomcat-users.xml)"	0,5 puntos
Apartado 2: Realiza y detalla correctamente el proceso de instalación de la Máquina Virtual Kali Linux.	0,75 puntos
Apartado 2: Realiza y detalla correctamente la configuración de la "RedNAT"	0,5 puntos
Apartado 2: Realiza y detalla correctamente el proceso de instalación de la Máquina Virtual Metasploitable2	0,75 puntos
Apartado 3: Realiza de manera correcta el escaneo de red.	1 punto

Apartado 3: Realiza de manera correcta el escaneo de servicios.	1 punto
Apartado 3: Realiza de manera correcta el escaneo de vulnerabilidades.	1 punto
Apartado 4: Selecciona el módulo de exploit correcto para explotar la vulnerabilidad.	1 punto
Apartado 4: Configura de manera correcta las opciones del exploit.	1 punto
Apartado 4: Consigue una shell en el sistema remoto.	1 punto
Redacción clara y correcta, sin errores ortográficos	Se resta 0,1 puntos por cada error ortográfico o expresiones incorrectas.

NOTA IMPORTANTE

Aquellos apartados/subapartados en los que las capturas de pantalla no sean claras o no tengan como fondo de pantalla la plataforma con tu usuario mostrando claramente la foto de tu perfil, no serán corregidos.