Artículo de Fawn

Preparado por: 0ne-nine9

Introducción

A veces, cuando se nos pide que enumeremos los servicios de hosts específicos en la red del cliente, se nos pedirá que enumeremos los servicios de hosts específicos en la red del cliente.

Me he encontrado con servicios de transferencia de archivos que pueden tener muchas posibilidades de estar mal configurados. El propósito de este

El ejercicio consiste en familiarizarse con el Protocolo de transferencia de archivos (FTP), un protocolo nativo de todos los sistemas operativos host.

sistemas y se han utilizado durante mucho tiempo para tareas sencillas de transferencia de archivos, ya sean automatizadas o manuales. FTP puede ser

fácilmente mal configurable si no se entiende correctamente. Hay casos en los que un empleado de la empresa cliente

Estamos evaluando si es posible que queramos eludir las comprobaciones de archivos o las reglas del firewall para transferir un archivo desde ellos mismos a

sus pares. Teniendo en cuenta los muchos mecanismos diferentes para controlar y monitorear el flujo de datos dentro de una

En las redes empresariales actuales, este escenario se convierte en un caso sustancial y viable que podríamos encontrar en la práctica.

Al mismo tiempo, se puede utilizar FTP para transferir archivos de registro de un dispositivo de red a otro o a un servidor de registro.

servidor de recopilación. Supongamos que el ingeniero de red a cargo de la configuración olvida proteger

El servidor FTP receptor no le da la importancia adecuada o no le da la importancia suficiente a la información contenida en él.

los registros y decide dejar el servicio FTP sin protección intencionalmente. En ese caso, un atacante podría obtener

Aprovechar los registros y extraer todo tipo de información de ellos, que luego se puede utilizar para mapear el

red, enumerar nombres de usuario, detectar servicios activos y más.

Veamos qué es FTP, según la definición de Wikipedia:

Desde las primeras líneas del extracto anterior, podemos ver una mención a la arquitectura del modelo cliente-servidor.

se refiere a los roles que tienen los hosts en la red durante el acto de transferir datos entre ellos. Los usuarios pueden

Descargar y cargar archivos desde el cliente (su propio host) al servidor (un dispositivo de almacenamiento de datos centralizado)

o viceversa. Conceptualmente hablando, el cliente siempre es el host que descarga y carga archivos al servidor.

servidor, y el servidor siempre es el host que almacena de forma segura los datos que se transfieren.

El Protocolo de transferencia de archivos (FTP) es un protocolo de comunicación estándar utilizado para transferir

archivos de computadora desde un servidor a un cliente en una red de computadoras. FTP se basa en un cliente.

Arquitectura del modelo de servidor que utiliza conexiones de datos y control independientes entre el cliente

y el servidor. Los usuarios de FTP pueden autenticarse con un protocolo de inicio de sesión de texto sin formato,

Generalmente en forma de nombre de usuario y contraseña. Sin embargo, pueden conectarse de forma anónima si

El servidor está configurado para permitirlo. Para una transmisión segura que proteja el nombre de usuario.

y contraseña y encripta el contenido, FTP a menudo está protegido con SSL/TLS (FTPS) o

reemplazado por el Protocolo de transferencia de archivos SSH (SFTP).

Los clientes también pueden explorar los archivos disponibles en el servidor cuando utilizan el protocolo FTP. Desde la terminal de un usuario

En perspectiva, esta acción parecerá como si estuvieran explorando los directorios de su propio sistema operativo en busca de archivos que desean.

necesidad. Los servicios FTP también vienen con una GUI (interfaz gráfica de usuario), similar a los programas del sistema operativo Windows, lo que permite

Navegación más sencilla para principiantes. Un ejemplo de un servicio FTP orientado a GUI conocido es FileZilla. Sin embargo,

Primero entendamos qué significa que un puerto ejecute un servicio abiertamente.

Un puerto que ejecuta un servicio activo es un espacio reservado para que la dirección IP del destino reciba solicitudes y

Enviar resultados desde. Si solo tuviéramos direcciones IP o nombres de host, los hosts solo podrían realizar una tarea a la vez.

Esto significa que si desea navegar por la web y reproducir música desde una aplicación en su computadora

Al mismo tiempo, no podría, porque la dirección IP se usaría para manejar el primero o el segundo.

Este último, pero no ambos al mismo tiempo. Al tener puertos, puede tener una dirección IP que maneje múltiples

servicios, ya que añade otra capa de distinción.

En el caso que se muestra a continuación, podemos ver que el FTP está activo en el puerto 21. Sin embargo, agreguemos algunos servicios adicionales como

SSH (Secure Shell Protocol) y HTTPD (Web Server) para explorar un ejemplo más típico. Con esto

tipo de configuración, un administrador de red ha configurado una configuración de servidor web básico rudimentario,

permitiéndoles lograr lo siguiente, todo al mismo tiempo si es necesario:

Recibir y enviar archivos que se pueden utilizar para configurar el servidor web o servir registros a una fuente externa

Poder iniciar sesión para administración remota desde un host distante, en caso de que se requiera alguna configuración

Se necesitan cambios

Ofrecer contenido web al que se pueda acceder de forma remota a través del navegador web de otro host

En el gráfico a continuación, puede ver dónde se ubica el FTP en la estructura lógica del host, junto con otros

servicios que potencialmente podrían estar ejecutándose al mismo tiempo.

El artículo de Wiki muestra que no se considera estándar utilizar FTP sin la capa de cifrado.

proporcionada por protocolos como SSL/TLS (FTPS) o SSH-tunneling (SFTP). FTP por sí mismo tiene la capacidad de

Requiere credenciales antes de permitir el acceso a los archivos almacenados. Sin embargo, la deficiencia aquí es que el tráfico

que contienen dichos archivos pueden ser interceptados con lo que se conoce como un ataque Man-in-the-Middle (MitM).

El contenido de los archivos se puede leer en texto simple (es decir, en formato no cifrado y legible para humanos).

Sin embargo, si los administradores de red eligen envolver la conexión con el protocolo SSL/TLS o el túnel

la conexión FTP a través de SSH (como se muestra a continuación) para agregar una capa de cifrado que solo la fuente y

Los hosts de destino pueden descifrar, lo que frustraría con éxito la mayoría de los ataques de intermediarios. Observe cómo el puerto

21 ha desaparecido, ya que el protocolo FTP se ha movido bajo el protocolo SSH en el puerto 22, quedando así

Tunelizado a través de él y asegurado contra cualquier interceptación.

Sin embargo, la situación que nos ocupa en este caso es mucho más sencilla. Solo vamos a interactuar con

El objetivo ejecuta un servicio FTP simple y mal configurado. Procedamos a analizar cómo funciona un servicio de este tipo.

Ejecutándose en un host interno se vería así.

Enumeración

En primer lugar, verifiquemos si nuestra conexión VPN está establecida. El uso del protocolo ping puede ayudar con esto, ya que es

un método de bajo consumo para llegar al objetivo y obtener una respuesta, lo que confirma nuestra conexión.

establecido y el objetivo es alcanzable. Bajo consumo de recursos significa que se envían muy pocos datos al objetivo por

predeterminado, lo que nos permite verificar rápidamente el estado de la conexión sin tener que esperar a que se realice un escaneo completo.

Completar de antemano. El protocolo ping se puede invocar desde la terminal utilizando ping {target_IP}

comando, donde {target_IP} es la dirección IP de su instancia de la máquina Fawn, como se muestra en la

Página web de Hack The Box.

Tenga en cuenta que esto podría no funcionar siempre en un entorno corporativo a gran escala, ya que los firewalls generalmente tienen reglas.

para evitar hacer ping entre hosts, incluso en la misma subred (LAN), para evitar amenazas internas y descubrir

Otros hosts y servicios.

Podemos cancelar el comando ping presionando CTRL+C en nuestro teclado, de lo contrario se ejecutará infinitamente.

Siguiendo la salida del comando, podemos ver que se están recibiendo respuestas del objetivo.

host. Esto significa que se puede acceder al host a través del túnel VPN que hemos creado. Ahora podemos empezar a escanear

los servicios abiertos en el host.

Al escanear utilizando nuestro comando utilizado anteriormente, podemos ver el servicio FTP abierto y ejecutándose en el puerto 21.

Sin embargo, ¿qué sucede si queremos saber la versión real del servicio que se ejecuta en este puerto?

¿Escanearlo con diferentes interruptores nos presenta la información necesaria?

En nuestro caso, el modificador -sV significa detección de versiones. El uso de este modificador hará que nuestro análisis sea más fácil.

Tomará más tiempo pero nos ofrecerá más información sobre la versión del servicio que se ejecuta en el detectado previamente.

puerto. Esto significa que, de un vistazo, podríamos saber si el objetivo es vulnerable debido a la ejecución de archivos obsoletos.

software o si necesitamos cavar más profundo para encontrar nuestro vector de ataque.

No buscaremos explotar el servicio en sí. Daremos pequeños pasos hacia nuestros objetivos y el

El siguiente paso será simplemente interactuar con el servicio tal como está para aprender más sobre cómo debemos abordarlo.

objetivos. Sin embargo, tener la versión del servicio siempre nos ayuda a tener más información sobre lo que se está ejecutando en el

puerto escaneado.

Asidero para el pie

Es hora de que interactuemos con el objetivo.

Para acceder al servicio FTP, utilizaremos el comando ftp en nuestro propio host. Es una buena práctica tener

Una comprobación rápida de que su FTP está actualizado y correctamente instalado. Al ejecutar el siguiente comando se mostrará

El mismo resultado que se muestra en la imagen si el servicio FTP está instalado. De lo contrario, continuará con la instalación.

El modificador -y al final del comando se utiliza para aceptar la instalación sin interrumpir el proceso.

Para preguntarle si desea continuar.

Una vez finalizada la instalación, puedes ejecutar el comando ftp -? para ver de qué es capaz el servicio.

Del extracto anterior, podemos ver que podemos conectarnos al host de destino usando el siguiente comando.

iniciará una solicitud de autenticación en el servicio FTP que se ejecuta en el destino, que devolverá un mensaje

Volviendo a nuestro anfitrión:

El mensaje nos pedirá el nombre de usuario con el que queremos iniciar sesión. Aquí es donde ocurre la magia.

Una configuración incorrecta típica para ejecutar servicios FTP permite que una cuenta anónima acceda al servicio como

cualquier otro usuario autenticado. El nombre de usuario anónimo se puede ingresar cuando aparece el mensaje, seguido

mediante cualquier contraseña, ya que el servicio ignorará la contraseña de esta cuenta específica.

Al pulsar Enter después de rellenar la contraseña, podremos comprobar que hemos iniciado sesión correctamente. Nuestro terminal

cambios para mostrarnos que ahora podemos emitir comandos ftp.

Al escribir el comando de ayuda, podremos ver qué comandos están disponibles. Podrás ver esto

patrón con cada script y servicio al que tenga acceso. Escriba -h, --help o help

Los comandos siempre emitirán una lista de todos los comandos disponibles para usted como usuario, con descripciones

Ocasionalmente se incluye. Si desea aprender más sobre un comando específico, puede utilizar un

Comando diferente: man {commandName} . Sin embargo, por ahora, volvamos a nuestro objetivo.

Algunos de los comandos que aparecen aquí nos resultan familiares. Ya sabemos cómo utilizar ls y cd.

Emita el primer comando y vea el contenido de la carpeta.

Como puede observar en la salida, el funcionamiento de los servicios FTP también emite el estado de los comandos.

Está enviando un mensaje al host remoto. El significado de las actualizaciones de estado es el siguiente:

Ahora, podemos proceder a descargar el flag.txt a nuestro host (Máquina Virtual). Para ello, podemos:

Usamos el comando get, seguido del nombre del archivo que queremos descargar. En nuestro caso quedaría así:

este:

Esto activará la descarga del archivo al mismo directorio en el que estaba cuando emitió el FTP.

Comando {machineIP}. Si salimos del servicio FTP, veremos el mismo archivo en nuestro host.

¡Ahora podemos tomar la bandera y enviarla a la plataforma para poder ser dueños de la caja!

¡Buen trabajo!

200: Comando PORT exitoso. Considere usar PASV.

150 : Aquí viene el listado del directorio.

226 : Envío de directorio OK.