	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:

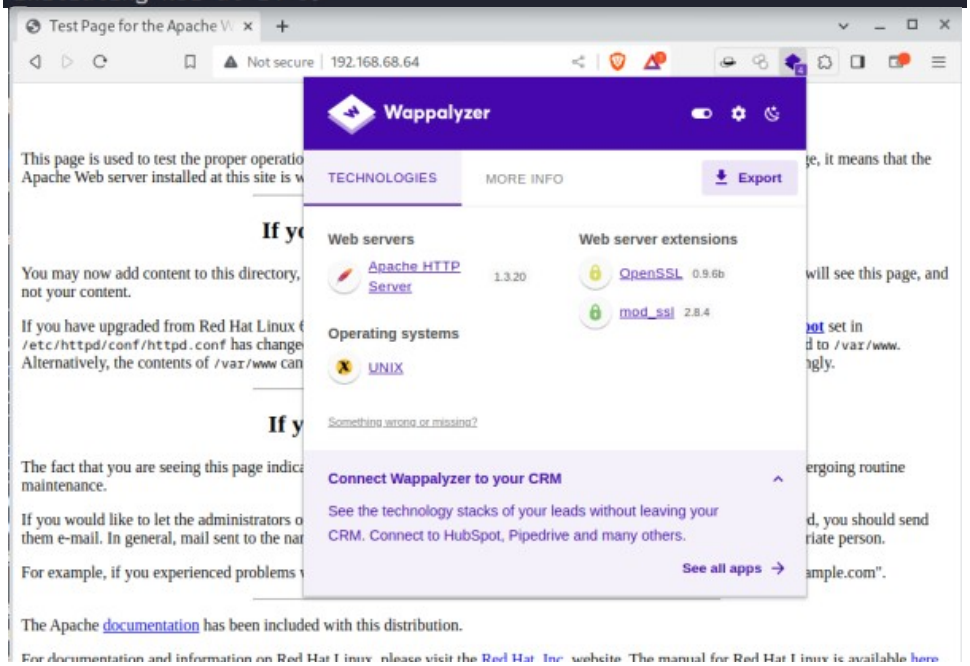
Nestor Guzman

Fecha de creación:
xx.xx.2025

Índice

1. Reconocimiento

```
└─$ 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
```

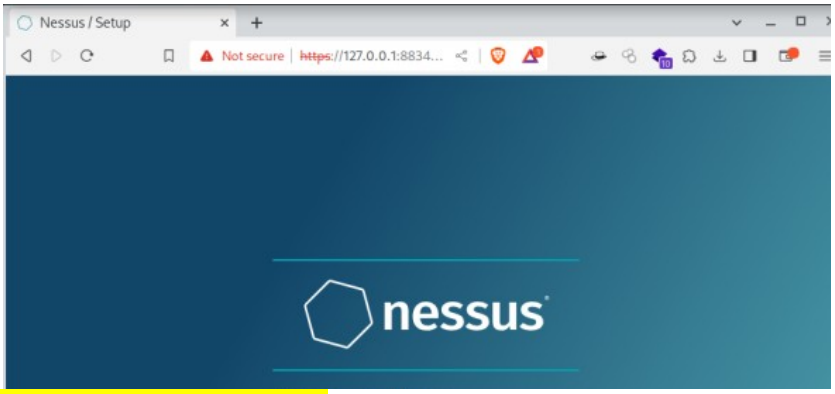


IP, Puertos Sistema operativo

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
```



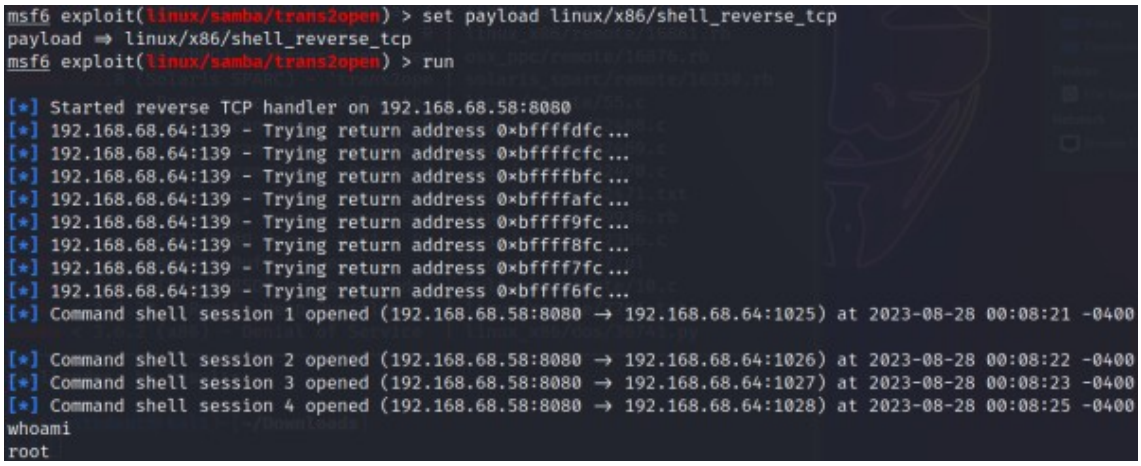
Ejemplo Reporte resumen de Nessus, auxiliares de metaexploit

Puerto	**Vulnerabilidad**
80	Apache
443	openssl

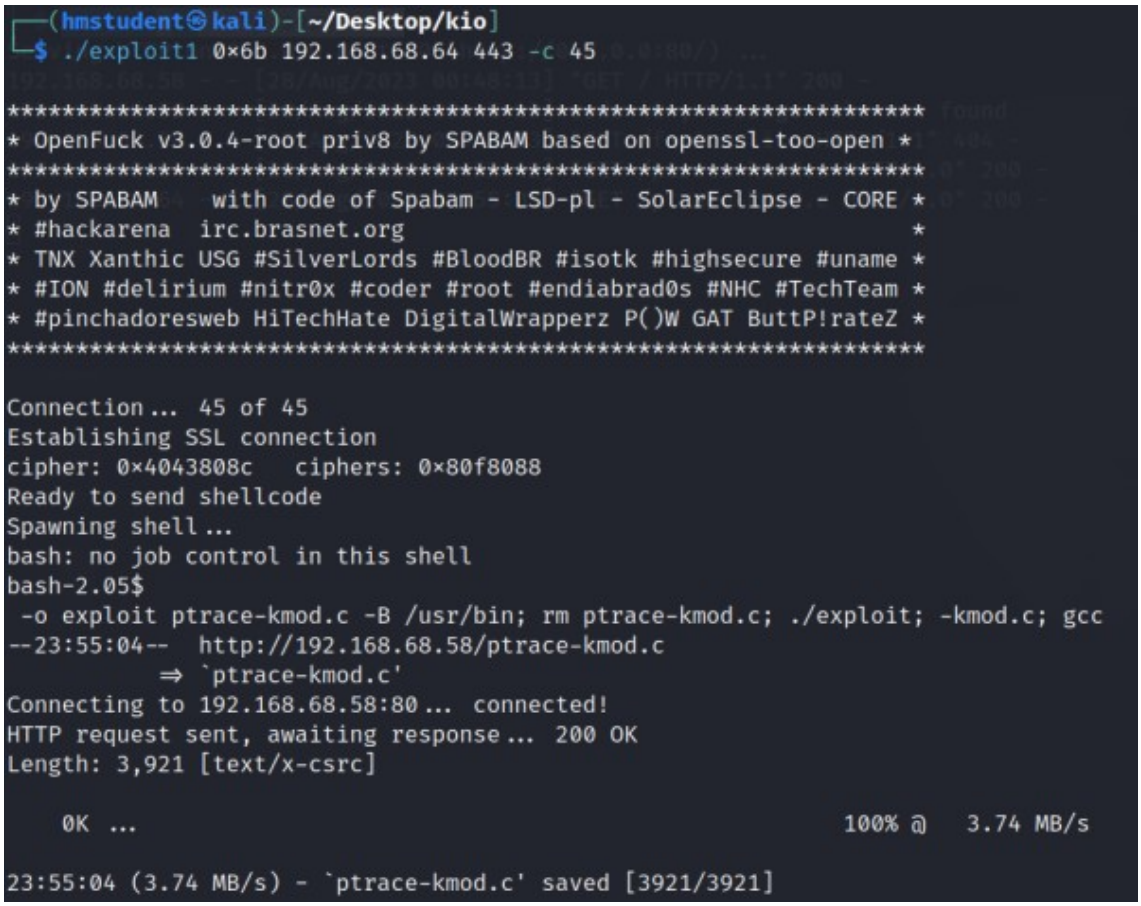
3. Explotación

Proceso manual/ automatizado.

Automatizado



Manual



4. Escalación de privilegios si/no

Método de escalada

5. Banderas

Bandera	12345678912345678897332598 9

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

N.- MQ-HM-KIO

1	
Bandera 2	12345678912345678897332598 9
Bandera 3	12345678912345678897332598 9

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)