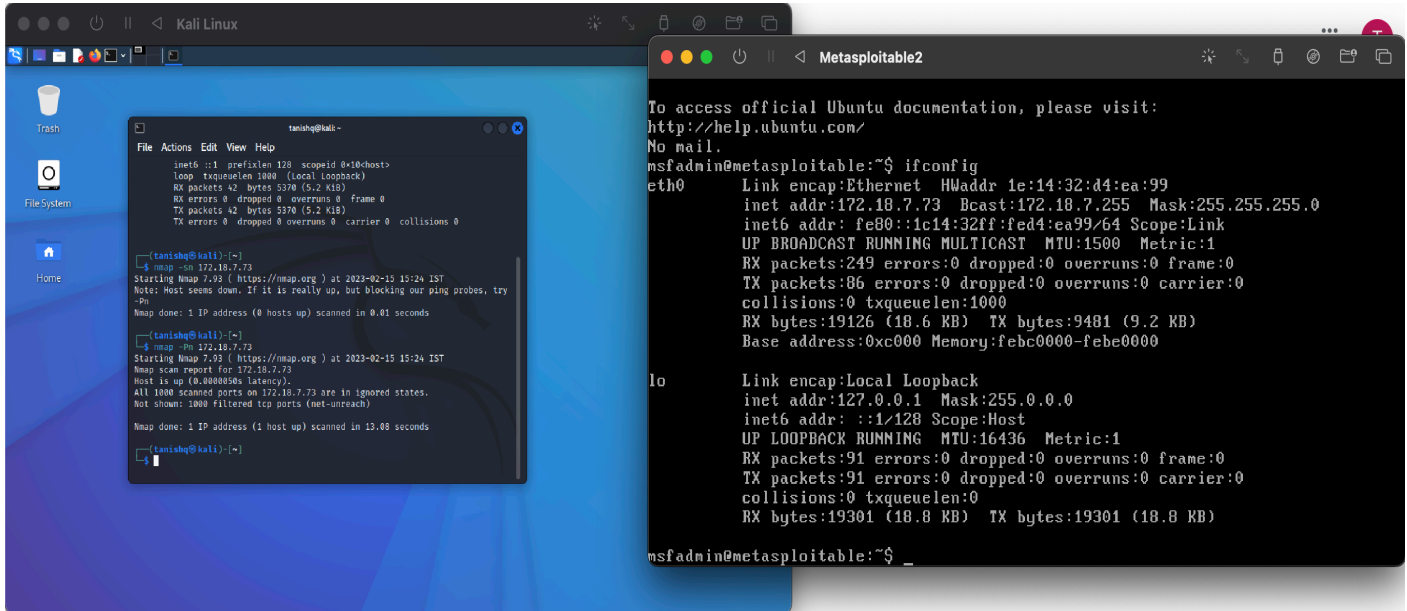


Assignment-3

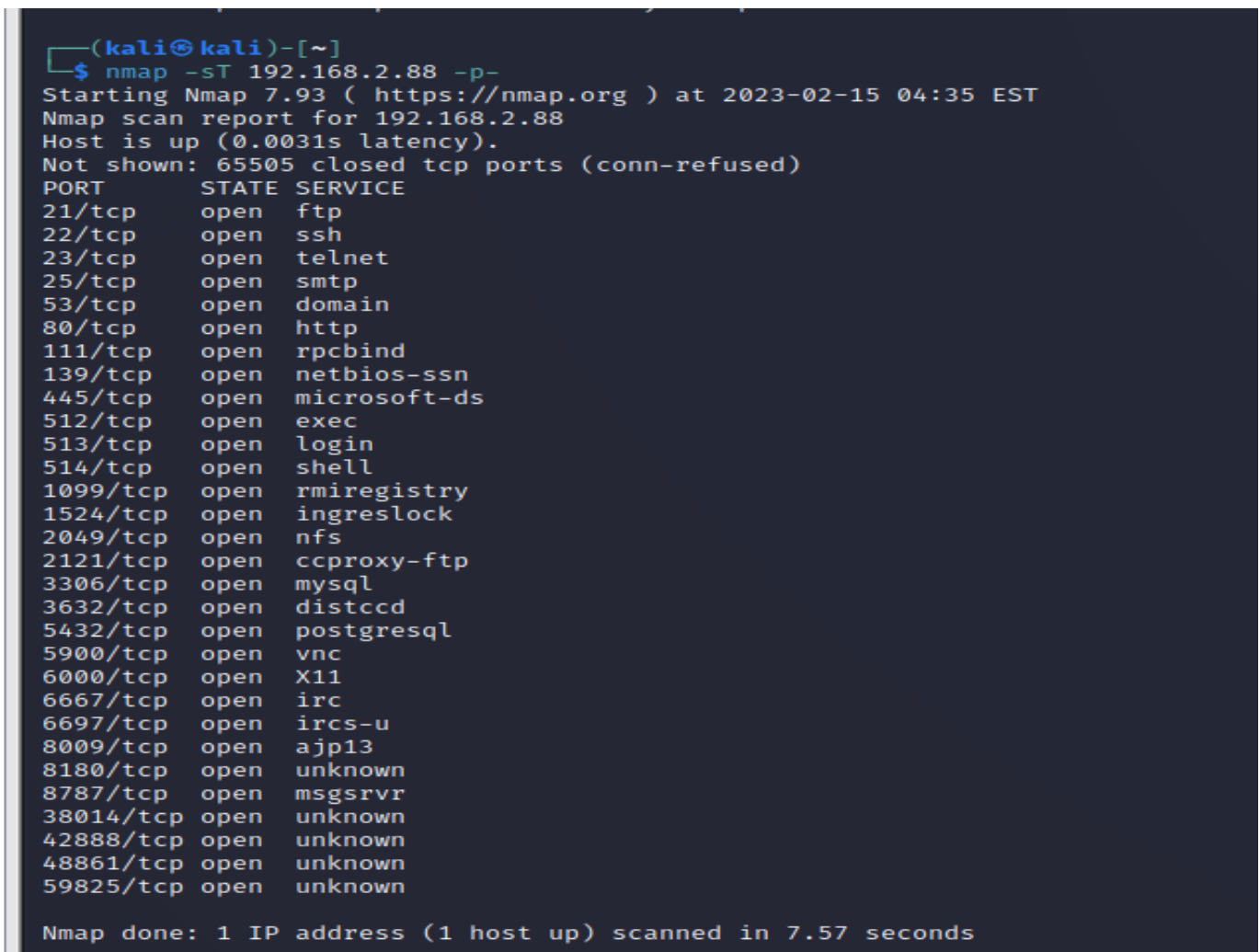
1. What kind of information is shown when you run ping scan for Metasploitable2?

1. \$ Nmap -sn 172.18.7.73



2. Which ports are open on the Metasploitable2 VM? Did you find any additional ports?

2. \$ nmap -sT 172.18.7.73 -p-



3. What additional information about the open ports on Metasploitable2 were you able to obtain by using the -sV and -A flags?

```
$ nmap -sT 192.168.2.88 -p- -sV -A
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-15 04:56 EST
Nmap scan report for 192.168.2.88
Host is up (0.0037s latency).
Not shown: 65505 closed tcp ports (conn-refused)
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 192.168.2.87
|_  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 600fcfe1c05f6a74d69024fac4d56ccd (DSA)
|_ 2048 5656240f211ddea72bae61b1243de8f3 (RSA)
23/tcp    open  telnet   Linux telnetd
25/tcp    open  smtp     Postfix smtpd
|_ssl-date: 2023-02-15T09:58:58+00:00; +11s from scanner time.
|_ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/
stateOrProvinceName=There is no such thing outside US/countryName=XX
|_Not valid before: 2010-03-17T14:07:45
|_Not valid after: 2010-04-16T14:07:45
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS,
ENHANCEDSTATUSCODES, 8BITMIME, DSN
|_sslv2:
|_SSLv2 supported
|_ciphers:
|_  SSL2_RC4_128_WITH_MD5
|_  SSL2_RC4_128_EXPORT40_WITH_MD5
|_  SSL2_DES_64_CBC_WITH_MD5
|_  SSL2_DES_192_EDE3_CBC_WITH_MD5
|_  SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|_  SSL2_RC2_128_CBC_WITH_MD5
53/tcp    open  domain   ISC BIND 9.4.2
|_dns-nsid:
|_bind.version: 9.4.2
80/tcp    open  http     Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-title: Metasploitable2 - Linux
111/tcp   open  rpcbind  2 (RPC #100000)
|_rpcinfo:
|_program version port/proto service
|_100000 2          111/tcp  rpcbind
|_100000 2          111/udp  rpcbind
|_100003 2,3,4      2049/tcp nfs
```

```

| 100003 2,3,4 2049/udp nfs
| 100005 1,2,3 41731/udp mountd
| 100005 1,2,3 59825/tcp mountd
| 100021 1,3,4 34904/udp nlockmgr
| 100021 1,3,4 42888/tcp nlockmgr
| 100024 1 38014/tcp status
|_ 100024 1 40304/udp status
139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp open exec netkit-rsh rexecd
513/tcp open login OpenBSD or Solaris rlogind
514/tcp open tcpwrapped
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
| mysql-info:
| Protocol: 10
| Version: 5.0.51a-3ubuntu5
| Thread ID: 11
| Capabilities flags: 43564
| Some Capabilities: SupportsTransactions, Speaks41ProtocolNew, SwitchToSSLAfterHandshake,
ConnectWithDatabase, SupportsCompression, LongColumnFlag, Support41Auth
| Status: Autocommit
|_ Salt: A,VM`|m.=&DeO=#6%Wh$
3632/tcp open distccd distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
5432/tcp open postgresql PostgreSQL DB 8.3.0 - 8.3.7
|_ ssl-date: 2023-02-15T09:58:58+00:00; +11s from scanner time.
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/
stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_ Not valid after: 2010-04-16T14:07:45
5900/tcp open vnc VNC (protocol 3.3)
| vnc-info:
| Protocol version: 3.3
| Security types:
|_ VNC Authentication (2)

6000/tcp open X11 (access denied)

```

4. What operating system does nmap report Metasploitable2 to be?

```

4. $ sudo nmap -o 172.18.7.73
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-15 15:49 IST
Nmap scan report for 172.18.7.73
Host is up (0.0024s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind

```

139/tcp open netbios-ssn
445/tcp open microsoft-ds
512/tcp open exec
513/tcp open login
514/tcp open shell
1099/tcp open rmiregistry
1524/tcp open ingreslock
2049/tcp open nfs
2121/tcp open ccproxy-ftp
3306/tcp open mysql
5432/tcp open postgresql
5900/tcp open vnc
6000/tcp open X11
6667/tcp open irc
8009/tcp open ajp13
8180/tcp open unknown

No exact OS matches for host (If you know what OS is running on it, see <https://nmap.org/submit/>).

TCP/IP fingerprint:

OS:SCAN(V=7.93%E=4%D=2/15%OT=21%CT=1%CU=36294%PV=Y%DS=2%DC=I%G=Y%
TM=63ECB1D
OS:4%P=aarch64-unknown-linux-
gnu)SEQ(SP=C4%GCD=2%ISR=C9%TI=Z%CI=Z%II=I%TS=7
OS:)SEQ(SP=C7%GCD=1%ISR=CE%TI=Z%II=I%TS=7)OPS(O1=M5B4ST11NW6%O2=M5B
4ST11NW6
OS:
%O3=M5B4NNT11NW6%O4=M5B4ST11NW6%O5=M5B4ST11NW6%O6=M5B4ST11)WIN(W
1=16A0%W
OS:2=16A0%W3=16A0%W4=16A0%W5=16A0%W6=16A0)ECN(R=Y%DF=N%T=40%W=16
D0%O=M5B4NN
OS:SNW6%CC=N%Q=)T1(R=Y%DF=N%T=40%S=O%A=S+
%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y
OS:
%DF=N%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T4(R=N)T5(R=Y%DF=N%T=40%
W=0%S=Z%A=
OS:S+
%F=AR%O=%RD=0%Q=)T6(R=Y%DF=N%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)
T6(R=N)T7
OS:
(R=N)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=DDA3
%RUD=G)
OS:IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 2 hops

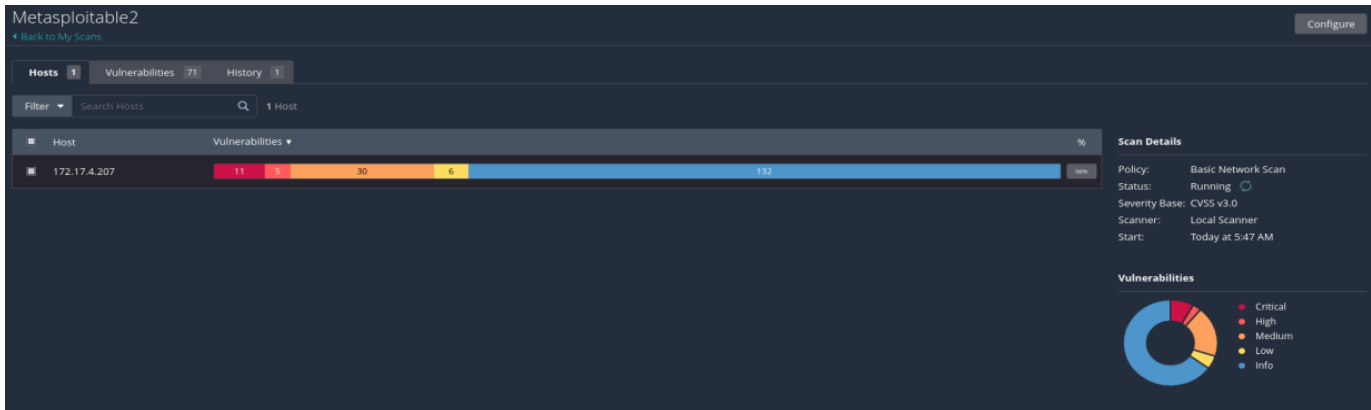
OS detection performed. Please report any incorrect results at <https://nmap.org/submit/> .

Nmap done: 1 IP address (1 host up) scanned in 12.59 seconds

5. What web applications are available on Metasploitable2?

5. TWiki, phpMyAdmin, Multillidae, DVWA, WebDAV

6. Which vulnerabilities are critical? Of these, which appear to be most serious? Double-click a vulnerability in the report and read the description
- 6.



Metasploitable2

← Back to My Scans

Hosts 1 Vulnerabilities 71 History 1

Filter Search Vulnerabilities 71 Vulnerabilities

Sev	Score	Name	Family	Count
CRITICAL	10.0 *	rexec Service Detection	Service detection	1
CRITICAL	10.0	Unix Operating System Unsupported Version Detection	General	1
CRITICAL	10.0 *	VNC Server 'password' Password	Gain a shell remotely	1
CRITICAL	9.8	Apache Tomcat AJP Connector Request Injection (Ghostcat)	Web Servers	1
CRITICAL	9.8	Bind Shell Backdoor Detection	Backdoors	1
CRITICAL	...	SSL (Multiple Issues)	Gain a shell remotely	3
MIXED	...	SSL (Multiple Issues)	Service detection	3
MIXED	...	Phpmyadmin (Multiple Issues)	CGI abuses	2
HIGH	7.5	NFS Shares World Readable	RPC	1
HIGH	7.5	Samba Badlock Vulnerability	General	1
MIXED	...	SSL (Multiple Issues)	General	26
MIXED	...	ISC Bind (Multiple Issues)	DNS	5
MEDIUM	6.5	TLS Version 1.0 Protocol Detection	Service detection	2
MEDIUM	6.5	Unencrypted Telnet Server	Misc.	1
MEDIUM	5.9	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)	Misc.	1
MEDIUM	5.3	Browsable Web Directories	CGI abuses	1
MEDIUM	5.3	Web Server info.php / phpinfo.php Detection	CGI abuses	1
MEDIUM	5.0 *	Backup Files Disclosure	CGI abuses	1
MEDIUM	4.3 *	CGI Generic HTML Injections (quick test)	CGI abuses : XSS	1
MEDIUM	4.3 *	Web Application Potentially Vulnerable to Clickjacking	Web Servers	1
MIXED	...	SSH (Multiple Issues)	Misc.	6

Scan Details

Policy: Basic Network Scan
Status: Running
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 5:47 AM

Vulnerabilities

Donut chart showing vulnerability distribution: Critical (red), High (orange), Medium (yellow), Low (green), Info (blue).

Hosts 1 Vulnerabilities 71 History 1

CRITICAL Bind Shell Backdoor Detection

Description

A shell is listening on the remote port without any authentication being required. An attacker may use it by connecting to the remote port and sending commands directly.

Solution

Verify if the remote host has been compromised, and reinstall the system if necessary.

Output

```
Nessus was able to execute the command "id" using the following request :

This produced the following truncated output (limited to 10 lines) :
..... snip .....
root@metasploitable:/# uid=0(root) gid=0(root) groups=0(root)
root@metasploitable:/#
..... snip .....
```

To see debug logs, please visit individual host

Port	Hosts
1524 / tcp / wild_shell	172.17.4.207

Plugin Details

Severity: Critical
ID: 51988
Version: 1.10
Type: remote
Family: Backdoors
Published: February 15, 2011
Modified: April 11, 2022

Risk Information

Risk Factor: Critical
CVSS v3.0 Base Score 9.8
CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/AU:N/S:U/C:H/H/A/H
CVSS v2.0 Base Score: 10.0
CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C