



TP2 - Discovery and Analysis of Network Ports and Services

Objectives:

- Learn how to perform different types of network scans using Nmap
- Discover open ports and service versions on a target machine
- Analyze the results and infer information about the scanned machines
- Learn how to manipulate NSE scripts

Introduction

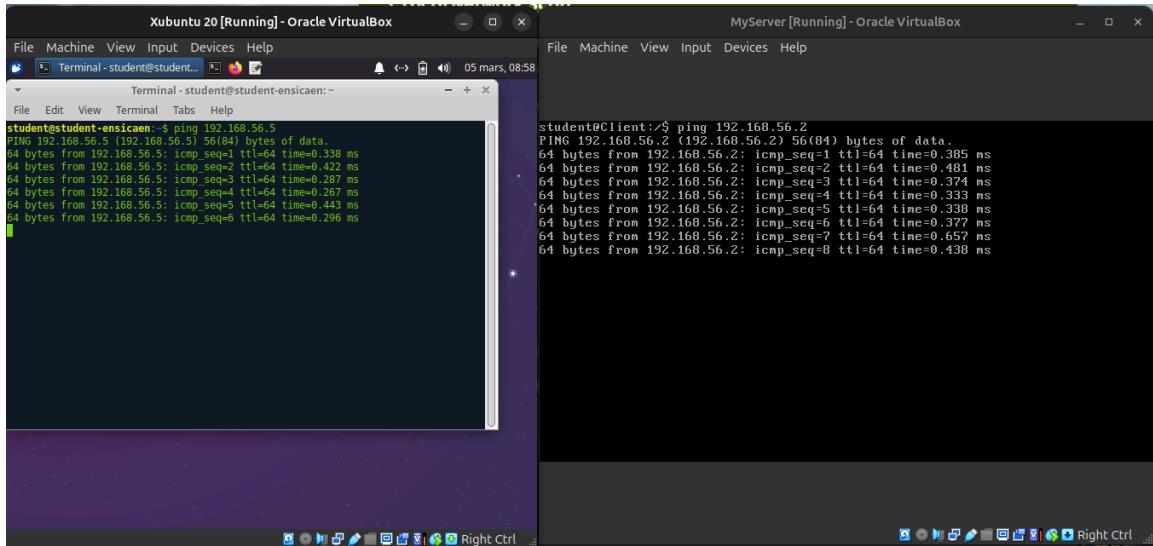
The phase of analyzing and discovering the ports of a target machine is a crucial step in the hacking process. The goal is to determine the type of service running on a machine to assess whether it is vulnerable.

Nmap (Network Mapper) is an open-source software created by Fyodor and distributed by Insecure.org. It allows scanning and detecting open ports, identifying hosted services, and obtaining information about the operating system of a remote computer.

Nmap is equipped with an NSE (Nmap Scripting Engine), which provides more powerful and flexible functionalities during the analysis phase.

I. Local Network Scan

1. Start the two virtual machines: "Student" & "MyServer."
2. Verify connectivity between the two machines.



3. Run Nmap on the "Student" machine and analyze the local network to determine which machines are connected.

```
nmap -sn <Network_IP_Range>
```

```
student@student-ensicaen:~$ nmap -sn 192.168.56.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2025-03-05 09:06 CET
Nmap scan report for 192.168.56.1
Host is up (0.00082s latency).
Nmap scan report for student-ensicaen (192.168.56.2)
Host is up (0.00011s latency).
Nmap scan report for 192.168.56.5
Host is up (0.00076s latency).
Nmap done: 256 IP addresses (3 hosts up) scanned in 2.93 seconds
student@student-ensicaen:~$
```

4. Use Nmap to determine the operating system name of the "MyServer" machine.

```
nmap -O <MyServer_IP>
```

Xubuntu 20 [Running] - Oracle VirtualBox

File Machine View Input Devices Help

Terminal - student@student... Terminal - student@student-ensicaen:~

```
student@student-ensicaen:~$ sudo nmap -O 192.168.56.5
Starting Nmap 7.80 ( https://nmap.org ) at 2025-03-05 09:11 CET
Nmap scan report for 192.168.56.5
Host is up (0.00030s latency).
Not shown: 977 closed ports
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
MAC Address: 08:00:27:4D:08:FC (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/
.
Nmap done: 1 IP address (1 host up) scanned in 1.76 seconds
student@student-ensicaen:~$
```

5. Infer the operating system version.

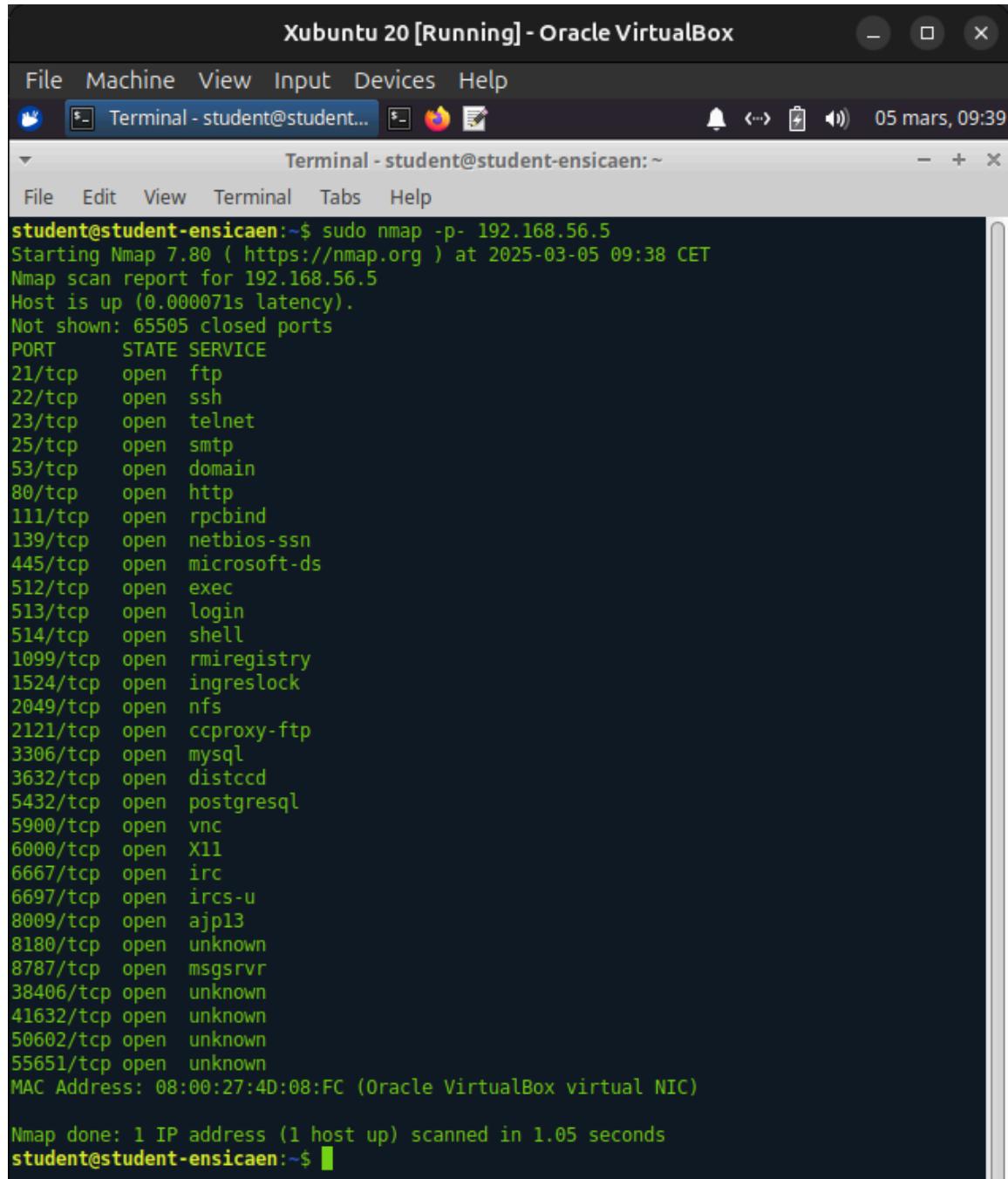
It's a Linux-based Operating System

II. Analysis of MyServer's Ports

1. Use Nmap to determine all open ports on the VM.

```
nmap -p- <MyServer_IP>
```

(`-p-` scans all 65535 ports.)



The screenshot shows a terminal window titled "Terminal - student@student@student-ensicaen:~". The window is part of the Xubuntu 20 desktop environment running in Oracle VirtualBox. The terminal displays the results of an nmap scan on the host IP 192.168.56.5. The output shows various open ports and their corresponding services:

```
student@student-ensicaen:~$ sudo nmap -p- 192.168.56.5
Starting Nmap 7.80 ( https://nmap.org ) at 2025-03-05 09:38 CET
Nmap scan report for 192.168.56.5
Host is up (0.000071s latency).
Not shown: 65505 closed ports
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
3632/tcp  open  distccd
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
6697/tcp  open  ircs-u
8009/tcp  open  ajp13
8180/tcp  open  unknown
8787/tcp  open  msgsrvr
38406/tcp open  unknown
41632/tcp open  unknown
50602/tcp open  unknown
55651/tcp open  unknown
MAC Address: 08:00:27:4D:08:FC (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.05 seconds
student@student-ensicaen:~$
```

2. Enumerate all services on the VM.

```

student@student-ensicaen:~$ sudo nmap -sR 192.168.56.5
WARNING: -sR is now an alias for -sV and activates version detection as well as RPC scan.
Starting Nmap 7.80 ( https://nmap.org ) at 2025-03-05 09:43 CET
Nmap scan report for 192.168.56.5
Host is up (0.000090s latency).
Not shown: 977 closed ports
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?      Netkit rshd
514/tcp   open  shell        Netkit rshd
1099/tcp  open  java-rmi   GNU Classpath grmiregistry
1524/tcp  open  bindshell   Bash shell (**BACKDOOR**; 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
MAC Address: 08:00:27:4D:08:FC (Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, Client, 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 57.72 seconds

```

III. Analysis of a Local Network Server

1. Ensure that the local server is reachable (@IP: 192.168.246.21).



It must be connected to the ensicaen's wifi

```
raquel@raquel-TUF:~$ ping 192.168.246.21
PING 192.168.246.21 (192.168.246.21) 56(84) bytes of data.
64 bytes from 192.168.246.21: icmp_seq=1 ttl=254 time=2.18 ms
64 bytes from 192.168.246.21: icmp_seq=2 ttl=254 time=4.23 ms
64 bytes from 192.168.246.21: icmp_seq=3 ttl=254 time=2.22 ms
64 bytes from 192.168.246.21: icmp_seq=4 ttl=254 time=2.05 ms
^C
--- 192.168.246.21 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3003ms
rtt min/avg/max/mdev = 2.051/2.670/4.231/0.903 ms
raquel@raquel-TUF:~$ 
```

2. Use Nmap to determine all open ports.

```
raquel@raquel-TUF:~$ nmap -p- 192.168.246.21
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-05 10:58
CET
Nmap scan report for cible.ensicaen.fr (192.168.246.21)
Host is up (0.0047s latency).
Not shown: 65530 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
53/tcp    open  domain
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 4.44 seconds
raquel@raquel-TUF:~$ 
```

3. Enumerate the services.

```
raquel@raquel-TUF:~$ nmap -sV 192.168.246.21
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-05 10:59
CET
Nmap scan report for cible.ensicaen.fr (192.168.246.21)
Host is up (0.0044s latency).
Not shown: 995 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      ProFTPD 1.2.10
22/tcp    open  ssh      OpenSSH 4.2 (protocol 1.99)
23/tcp    open  telnet   Linux telnetd
53/tcp    open  domain   (unknown banner: unknown)
80/tcp    open  http     Apache httpd 1.3.27 ((Unix))
1 service unrecognized despite returning data. If you know the
service/version, please submit the following fingerprint at ht
ps://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port53-TCP:V=7.94SVN%I=7%D=3/5%Time=67C8208F%P=x86_64-pc-lin
ux-gnu%r(DN
SF:SVVersionBindReqTCP,34,"\x002\0\x06\x85\0\0\x01\0\x01\0\0\0\0
\x07version
SF:\x04bind\0\0\x10\0\x03\xc0\x0c\0\x10\0\x03\0\0\0\0\x08\x07
unknown");
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect result
s at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.60 seconds
raquel@raquel-TUF:~$
```

IV. Website Analysis

We want to analyze the following website: <http://scanme.nmap.org>

1. Determine the open ports.

```
raquel@raquel-TUF:~$ nmap scanme.nmap.org
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-05 11:06
CET
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.17s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f
03c:91ff:fe18:bb2f
Not shown: 977 filtered tcp ports (no-response)
PORT      STATE SERVICE
20/tcp    closed  ftp-data
21/tcp    closed  ftp
22/tcp    open   ssh
23/tcp    closed  telnet
43/tcp    closed  whois
110/tcp   closed  pop3
113/tcp   closed  ident
143/tcp   closed  imap
389/tcp   closed  ldap
443/tcp   closed  https
587/tcp   closed  submission
636/tcp   closed  ldapssl
873/tcp   closed  rsync
993/tcp   closed  imaps
995/tcp   closed  pop3s
1935/tcp  closed  rtmp
2401/tcp  closed  cvspserver
3000/tcp  closed  ppp
3690/tcp  closed  svn
8080/tcp  closed  http-proxy
8081/tcp  closed  blackice-icecap
8180/tcp  closed  unknown
8443/tcp  closed  https-alt

Nmap done: 1 IP address (1 host up) scanned in 35.04 seconds
raquel@raquel-TUF:~$ 
```

2. Enumerate the active services.

```
raquel@raquel-TUF:~$ nmap -sV scanme.nmap.org
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-05 11:08
CET
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.15s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f
03c:91ff:fe18:bb2f
Not shown: 976 filtered tcp ports (no-response)
PORT      STATE SERVICE          VERSION
20/tcp    closed  ftp-data
21/tcp    closed  ftp
22/tcp    open   ssh           OpenSSH 6.6.1p1 Ubuntu 2ubuntu2
.13 (Ubuntu Linux; protocol 2.0)
23/tcp    closed  telnet
43/tcp    closed  whois
80/tcp    open   http          Apache httpd 2.4.7 ((Ubuntu))
110/tcp   closed  pop3
113/tcp   closed  ident
143/tcp   closed  imap
389/tcp   closed  ldap
443/tcp   closed  https
587/tcp   closed  submission
636/tcp   closed  ldapssl
873/tcp   closed  rsync
993/tcp   closed  imaps
995/tcp   closed  pop3s
1935/tcp  closed  rtmp
2401/tcp  closed  cvspserver
3000/tcp  closed  ppp
3690/tcp  closed  svn
8080/tcp  closed  http-proxy
8081/tcp  closed  blackice-icecap
8180/tcp  closed  unknown
8443/tcp  closed  https-alt
Service Info: OS: 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 17.84 seconds
raquel@raquel-TUF:~$ 
```

3. Identify the operating system version.

He couldn't identify the exact one

```
Device type: general purpose|firewall|storage-misc|WAP
Running (JUST GUESSING): Linux 2.6.X|3.X|4.X|2.4.X (86%), WatchGuard Fireware 11.X (86%),
Synology DiskStation Manager 5.X (85%)
OS CPE: cpe:/o:linux:linux_kernel:2.6.32 cpe:/o:linux:linux_kernel:3.10 cpe:/o:linux:linux
_kernel:4.4 cpe:/o:watchguard:fireware:11.8 cpe:/o:linux:linux_kernel cpe:/a:synology:disk
station_manager:5.1 cpe:/o:linux:linux_kernel:2.4
Aggressive OS guesses: Linux 2.6.32 (86%), Linux 2.6.32 or 3.10 (86%), Linux 2.6.39 (86%),
Linux 3.10 - 3.12 (86%), Linux 4.4 (86%), WatchGuard Fireware 11.8 (86%), Synology DiskSt
ation Manager 5.1 (85%), Linux 2.6.35 (85%), Linux 4.9 (85%), Linux 3.4 (85%)
No exact OS matches for host (test conditions non-ideal).
```

V. Nmap Scripting Engine

1. Display all available NSE scripts for Nmap in `/usr/share/nmap/scripts/` .

2. Search for and apply a suitable NSE script for the discovered services. You are required to analyze three services using NSE scripts on the "Client" machine.

- Example: To use an NSE script: `nmap --script script_name -p port_number @IP`

```

student@student-ensicaen:~$ nmap -sV 192.168.56.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2025-03-09 22:36 CET
Nmap scan report for 192.168.56.1
Host is up (0.00012s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE VERSION
80/tcp    open  http   Apache httpd 2.4.58
Service Info: Host: 127.0.1.1

Nmap scan report for student-ensicaen (192.168.56.2)
Host is up (0.00012s latency).
All 1000 scanned ports on student-ensicaen (192.168.56.2) are closed

Nmap scan report for 192.168.56.5
Host is up (0.00013s latency).
Not shown: 977 closed ports
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 Bash shell (**BACKDOOR**; 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, Client, 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: 256 IP addresses (3 hosts up) scanned in 60.33 seconds

```

```
student@student-ensicaen:~$ ls /usr/share/nmap/scripts/ | grep vuln
afp-path-vuln.nse
ftp-vuln-cve2010-4221.nse
http-huawei-hg5xx-vuln.nse
http-iis-webdav-vuln.nse
http-vmware-path-vuln.nse
http-vuln-cve2006-3392.nse
http-vuln-cve2009-3960.nse
http-vuln-cve2010-0738.nse
http-vuln-cve2010-2861.nse
http-vuln-cve2011-3192.nse
http-vuln-cve2011-3368.nse
http-vuln-cve2012-1823.nse
http-vuln-cve2013-0156.nse
http-vuln-cve2013-6786.nse
http-vuln-cve2013-7091.nse
http-vuln-cve2014-2126.nse
http-vuln-cve2014-2127.nse
http-vuln-cve2014-2128.nse
http-vuln-cve2014-2129.nse
http-vuln-cve2014-3704.nse
http-vuln-cve2014-8877.nse
http-vuln-cve2015-1427.nse
http-vuln-cve2015-1635.nse
http-vuln-cve2017-1001000.nse
http-vuln-cve2017-5638.nse
http-vuln-cve2017-5689.nse
http-vuln-cve2017-8917.nse
http-vuln-misfortune-cookie.nse
http-vuln-wnr1000-creds.nse
mysql-vuln-cve2012-2122.nse
rdp-vuln-ms12-020.nse
rmi-vuln-classloader.nse
rsa-vuln-roca.nse
samba-vuln-cve-2012-1182.nse
smb2-vuln-uptime.nse
smb-vuln-conficker.nse
smb-vuln-cve2009-3103.nse
smb-vuln-cve-2017-7494.nse
smb-vuln-ms06-025.nse
smb-vuln-ms07-029.nse
smb-vuln-ms08-067.nse
smb-vuln-ms10-054.nse
smb-vuln-ms10-061.nse
smb-vuln-ms17-010.nse
smb-vuln-regsvc-dos.nse
smb-vuln-webexec.nse
smtp-vuln-cve2010-4344.nse
smtp-vuln-cve2011-1720.nse
smtp-vuln-cve2011-1764.nse
vulnerers.nse
```

```
student@student-ensicaen:~$ ls /usr/share/nmap/scripts/ | grep mysql
mysql-audit.nse
mysql-brute.nse
mysql-databases.nse
mysql-dump-hashes.nse
mysql-empty-password.nse
mysql-enum.nse
mysql-info.nse
mysql-query.nse
mysql-users.nse
mysql-variables.nse
mysql-vuln-cve2012-2122.nse
student@student-ensicaen:~$ ls /usr/share/nmap/scripts/ | grep ftp
ftp-anon.nse
ftp-bounce.nse
ftp-brute.nse
ftp-libopie.nse
ftp-proftpd-backdoor.nse
ftp-syst.nse
ftp-vsftpd-backdoor.nse
ftp-vuln-cve2010-4221.nse
tftp-enum.nse
student@student-ensicaen:~$ ls /usr/share/nmap/scripts/ | grep http
http-adobe-coldfusion-apsal301.nse
http-affiliate-id.nse
http-apache-negotiation.nse
http-apache-server-status.nse
http-aspnet-debug.nse
http-auth-finder.nse
http-auth.nse
http-avaya-ipoffice-users.nse
http-awstatstotals-exec.nse
http-axis2-dir-traversal.nse
http-backup-finder.nse
http-barracuda-dir-traversal.nse
http-bigip-cookie.nse
http-brute.nse
http-cakephp-version.nse
http-chrono.nse
http-cisco-anyconnect.nse
http-coldfusion-subzero.nse
http-comments-displayer.nse
http-config-backup.nse
http-cookie-flags.nse
http-cors.nse
http-cross-domain-policy.nse
http-csrftoken.nse
http-date.nse
http-default-accounts.nse
http-devframework.nse
http-dlink-backdoor.nse
http-dombased-xss.nse
http-domino-enum-passwords.nse
http-drupal-enum.nse
http-drupal-enum-users.nse
*** .nse
```

```
student@student-ensicaen:~$ nmap --script=http-title -p 80 192.168.56.5
Starting Nmap 7.80 ( https://nmap.org ) at 2025-03-09 23:51 CET
Nmap scan report for 192.168.56.5
Host is up (0.00024s latency).

PORT      STATE SERVICE
80/tcp    open  http
|_http-title: Metasploitable2 - Linux

Nmap done: 1 IP address (1 host up) scanned in 0.19 seconds
student@student-ensicaen:~$
```

Xubuntu 20 [Running] - Oracle VirtualBox

File Machine View Input Devices Help

Terminal - student@student... 09 mars, 23:43

Terminal - student@student-ensicaen:~

File Edit View Terminal Tabs Help

```
Nmap done: 1 IP address (1 host up) scanned in 10.12 seconds
student@student-ensicaen:~$ nmap --script=mysql-info -p 3306 192.168.56.5
Starting Nmap 7.80 ( https://nmap.org ) at 2025-03-09 23:42 CET
Nmap scan report for 192.168.56.5
Host is up (0.00032s latency).

PORT      STATE SERVICE
3306/tcp  open  mysql
| mysql-info:
|   Protocol: 10
|   Version: 5.0.51a-3ubuntu5
|   Thread ID: 21
|   Capabilities flags: 43564
|   Some Capabilities: Support41Auth, ConnectWithDatabase, SupportsTransactions
, Speaks41ProtocolNew, LongColumnFlag, SupportsCompression, SwitchToSSLAfterHandshake
|   Status: Autocommit
|_  Salt: Nc)@DvHAOI^!&8*gL#ik

Nmap done: 1 IP address (1 host up) scanned in 10.12 seconds
student@student-ensicaen:~$
```

Xubuntu 20 [Running] - Oracle VirtualBox

File Machine View Input Devices Help

Terminal - student@student... Terminal - student@student... 09 mars, 23:49

Terminal - student@student-ensicaen:~

File Edit View Terminal Tabs Help

```
student@student-ensicaen:~$ nmap --script=vuln -p 21 192.168.56.5
Starting Nmap 7.80 ( https://nmap.org ) at 2025-03-09 23:49 CET
Nmap scan report for 192.168.56.5
Host is up (0.00028s latency).

PORT      STATE SERVICE
21/tcp    open  ftp
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
| ftp-vsftpd-backdoor:
|   VULNERABLE:
|     vsFTPD version 2.3.4 backdoor
|       State: VULNERABLE (Exploitable)
|       IDs: CVE:2011-2523 BID:48539
|         vsFTPD version 2.3.4 backdoor, this was reported on 2011-07-04.
|       Disclosure date: 2011-07-03
|     Exploit results:
|       Shell command: id
|       Results: uid=0(root) gid=0(root)
|     References:
|       https://www.securityfocus.com/bid/48539
|       http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|     https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
|     _sslv2-drown:

Nmap done: 1 IP address (1 host up) scanned in 1.21 seconds
student@student-ensicaen:~$
```

VI. Research on Service Vulnerabilities

1. Use a public vulnerability research site, as seen in the course, to find vulnerabilities in three services identified during the scan.

An official website of the United States government [Here's how you know](#)



NIST

Information Technology Laboratory

NATIONAL VULNERABILITY DATABASE



NATIONAL VULNERABILITY
DATABASE
NVD

VULNERABILITIES

CVE-2011-2523 Detail

MODIFIED

This CVE record has been updated after NVD enrichment efforts were completed. Enrichment data supplied by the NVD may require amendment due to these changes.

Description

vsftpd 2.3.4 downloaded between 20110630 and 20110703 contains a backdoor which opens a shell on port 6200/tcp.

Metrics

[CVSS Version 4.0](#)

[CVSS Version 3.x](#)

[CVSS Version 2.0](#)

NVD enrichment efforts reference publicly available information to associate vector strings. CVSS information contributed by other sources is also displayed.

CVSS 3.x Severity and Vector Strings:



NIST: NVD

Base Score: **9.8 CRITICAL**

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

QUICK INFO

[CVE Dictionary Entry:](#)

[CVE-2011-2523](#)

NVD Published Date:

11/27/2019

NVD Last Modified:

11/20/2024

Source:

Red Hat, Inc.

References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites. Please address comments about this page to nvd@nist.gov.

1. Identify the specific vulnerability and its associated CVE ID.
2. Determine the CVSS (Common Vulnerability Scoring System) score and the impact of exploiting the vulnerability.

Metrics

[CVSS Version 4.0](#)

[CVSS Version 3.x](#)

[CVSS Version 2.0](#)

NVD enrichment efforts reference publicly available information to associate vector strings. CVSS information contributed by other sources is also displayed.

CVSS 3.x Severity and Vector Strings:



NIST: NVD

Base Score: **9.8 CRITICAL**

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H