Task 1 : Basic Network Scanning with Nmap

Introduction

Nmap is a free, open source network scanning tool used for network exploration and security auditing. This task involves performing a basic network scan, identify open ports, services with its versions and default script scan. The goal is to understand active services and their significance in network security.

Objectives

-Install and run Nmap
-Scan local system
-dentify open ports and services
-Document findings

Tools used

-Nmap
-Metaspolit
-Terminal

Methodology

1. Installation of Nmap :

```
sudo apt install nmap
```

(As I have used Virtual Kali linux nmap is a preinstalled tool)

2. Perform Basic Scan :

```
nmap 192.168.0.107
```

(Here, mentioned IP address is the address of Metaspolit which is connected on the same network as kali linux)

3. Version + Service scan :

```
nmap -sV 192.168.0.107
```

(Here, -sV refers to Service Version Detection used to identify vulnerable versions)

4. Default Script Scan :

```
nmap -sC 192.168.0.107
```

(Here, -sC refers to run default Nmap Scripting Engine - Default script)

5. To save outputs of -sV and -sC :

```
nmap -sV -sC 192.168.0.107 -oN nmap_scan_results.txt
```

(Outputs will be saved in nmap_scan_results.txt)

Findings

These findings are from scanning Metasploitable, which contains intentionally vulnerable services.

1. FTP (Port 21) - Anonymous Login ENABLED :

" 21/tcp open ftp vsftpd 2.3.4
ftp-anon: Anonymous FTP login allowed"

-Anonymous login means anyone can access the FTP server without authentication.
-FTP also sends credentials and data in plaintext which is vulnerable to sniffing.
Severity: High

2. SSH (Port 22) - Outdated Version :

“OpenSSH 4.7p1 Debian 8ubuntu1”

-Outdated SSH version with publicly known vulnerabilities.

-May be vulnerable to brute-force and misconfiguration exploits.

Severity: Medium

3. Telnet (Port 23) - Insecure Protocol :

“23/tcp open telnet Linux telnetd”

-Telnet sends credentials in plain text.

-Completely insecure for remote login.

Severity: High

4. SMTP (Port 25) — Open & Enumeratable :

“25/tcp open smtp Postfix smtpd”

-SMTP allows username enumeration with VRFY/EXPN.

-Attackers can gather valid email addresses for social engineering.

Severity: Medium

5. DNS (Port 53) — ISC BIND 9.4.2 :

-Known for multiple past vulnerabilities (DoS, cache poisoning)

-Running old version.

Severity: Medium

6. HTTP (Port 80) — Apache 2.2.8 (Very Old) :

“Apache httpd 2.2.8 (Ubuntu)
_http-title: Metasploitable2 - Linux”

-Apache 2.2.x is end-of-life, has multiple critical vulnerabilities.

-May allow directory traversal, RCE, etc.

Severity: Critical

7. NetBIOS / SMB (Ports 139, 445) :

“Samba smbd 3.0.20”

-Samba 3.0.20 is vulnerable to RCE (Remote Code Execution).

-Known exploit: CVE-2007-2447 (Samba usermap script).

Severity: Critical

8. MySQL Database (Port 3306) :

“MySQL 5.0.51a”

-Outdated version with known RCE and authentication flaws.

Severity: High

9. PostgreSQL (Port 5432) :

“PostgreSQL 8.3.0 - 8.3.7”

-Old version with vulnerabilities in authentication and buffer handling.

Severity: Medium

10. VNC (Port 5900) — No Authentication :

“VNC Authentication (2)”

-VNC sessions can be hijacked.

-Outdated protocol version 3.3

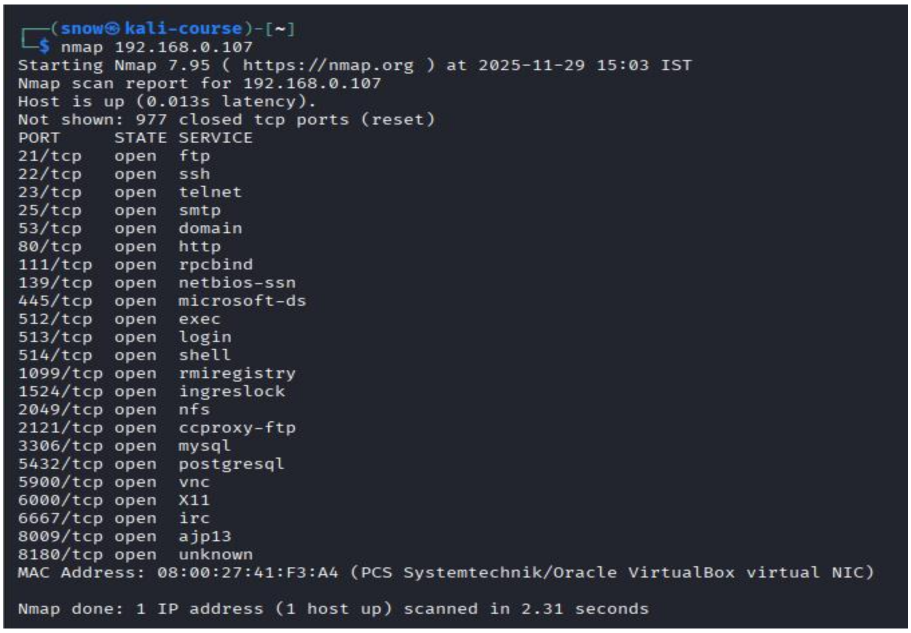
Severity: High

11. IRC Service (Port 6667) :
-Usually unnecessary and opens server to botnet communication.
Severity: Medium

12. Apache Tomcat (Ports 8009,8180) :
“Apache Jserv
Apache Tomcat/Coyote JSP engine 1.1”
-Old vulnerable Tomcat engines allow authentication bypass and RCE.
Severity: High

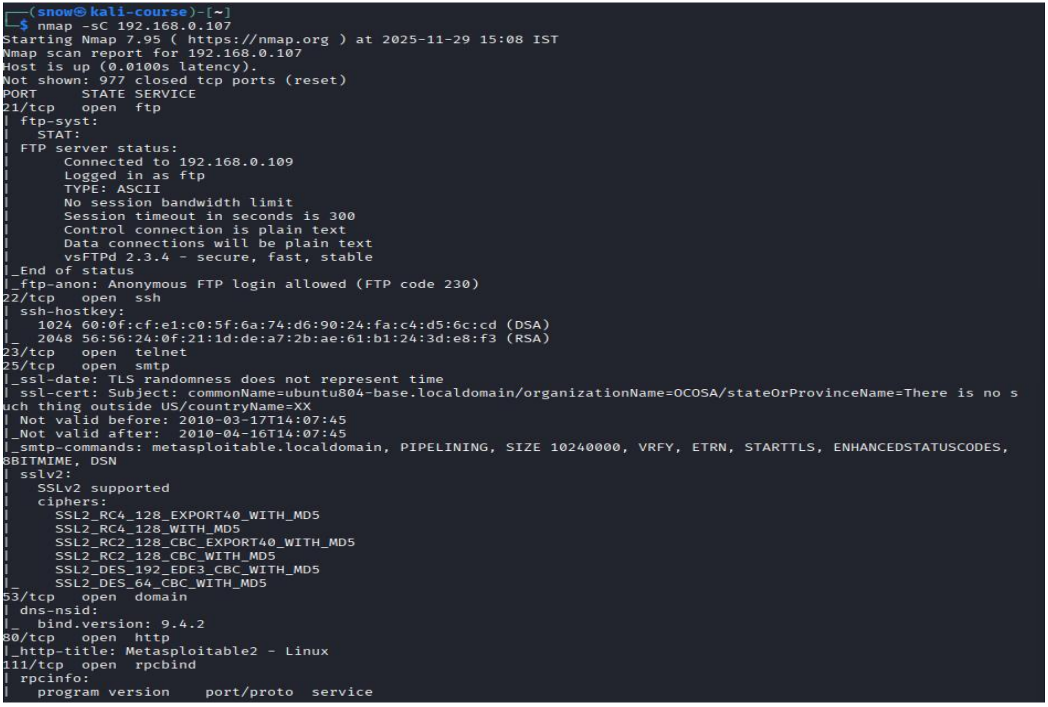
Screenshots

Basic scan:



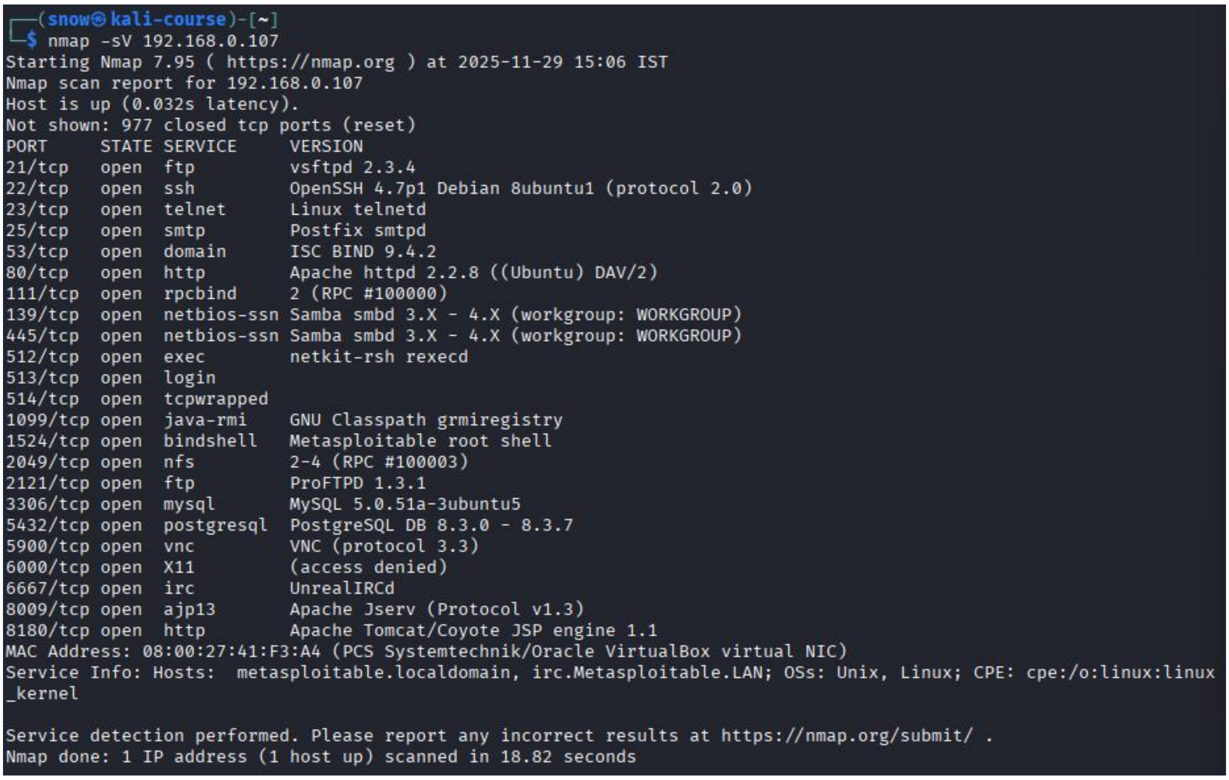
```
┌──(snow㉿kali-course)-[~]
└─$ nmap 192.168.0.107
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-29 15:03 IST
Nmap scan report for 192.168.0.107
Host is up (0.013s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
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
MAC Address: 08:00:27:41:F3:A4 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 2.31 seconds
```

Default script scan:



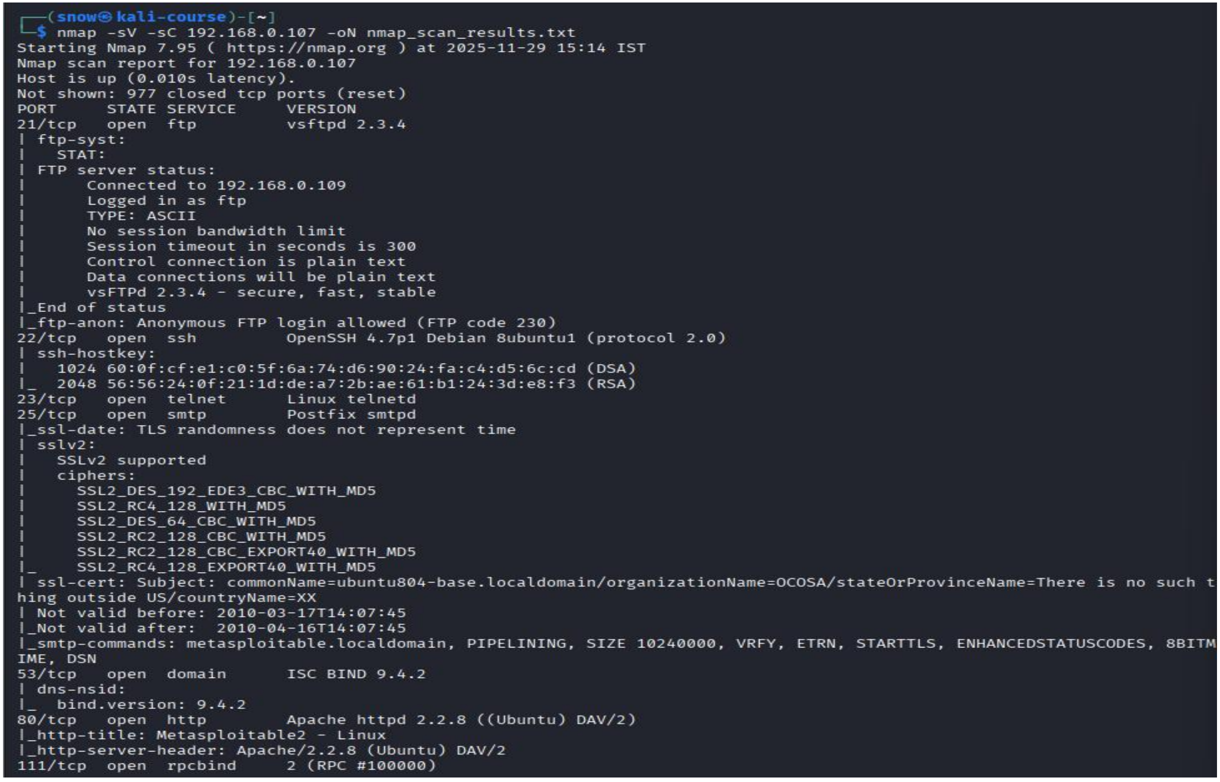
```
┌──(snow㉿kali-course)-[~]
└─$ nmap -sC 192.168.0.107
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-29 15:08 IST
Nmap scan report for 192.168.0.107
Host is up (0.0100s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.0.109
|      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
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp   open  ssh
| 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
25/tcp   open  smtp
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no s
uch 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_EXPORT40_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|_    SSL2_DES_64_CBC_WITH_MD5
53/tcp   open  domain
| dns-nsid:
|_  bind.version: 9.4.2
80/tcp   open  http
|_http-title: Metasploitable2 - Linux
111/tcp  open  rpcbind
| rpcinfo:
|   program version    port/proto  service
```

Service + version scan:



```
┌──(snow㉿kali-course)-[~]
└─$ nmap -sV 192.168.0.107
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-29 15:06 IST
Nmap scan report for 192.168.0.107
Host is up (0.032s latency).
Not shown: 977 closed tcp ports (reset)
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  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
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: 08:00:27:41:F3:A4 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
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 18.82 seconds
```

To Save Output:



```
┌──(snow㉿kali-course)-[~]
└─$ nmap -sV -sC 192.168.0.107 -oN nmap_scan_results.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-29 15:14 IST
Nmap scan report for 192.168.0.107
Host is up (0.010s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.0.109
|      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
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
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: TLS randomness does not represent time
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|_    SSL2_RC4_128_EXPORT40_WITH_MD5
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such t
hing 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, 8BITM
IME, DSN
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-title: Metasploitable2 - Linux
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
111/tcp  open  rpcbind     2 (RPC #100000)
```

Conclusion:

The Nmap scan revealed multiple active services. Understanding these open ports is essential for assessing security posture and hardning the system.