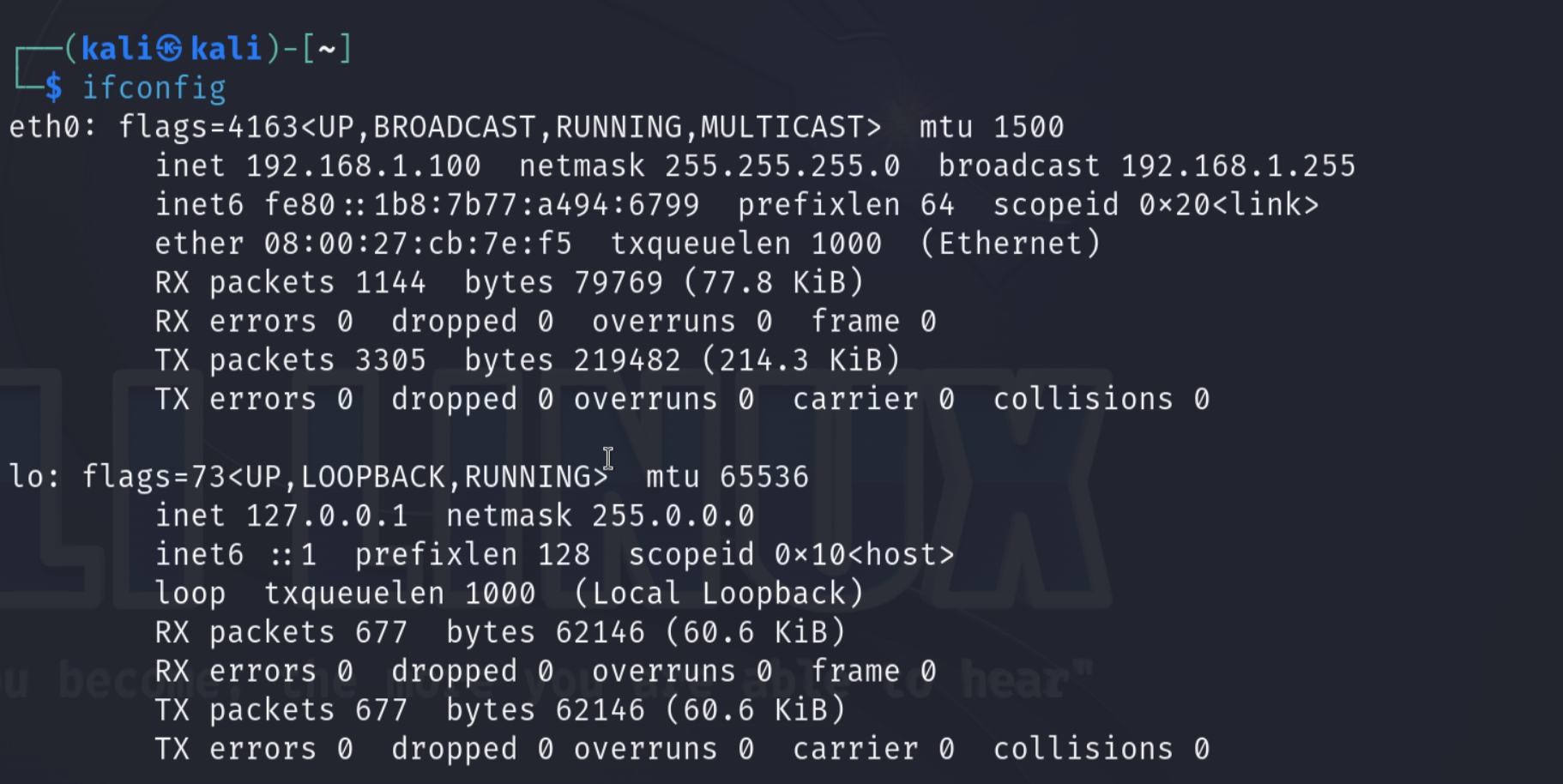
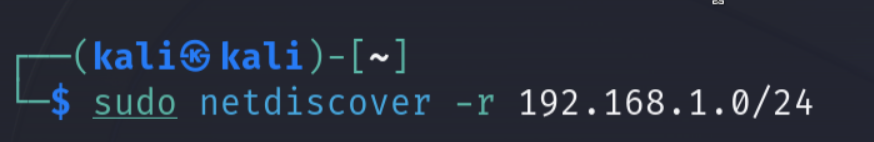
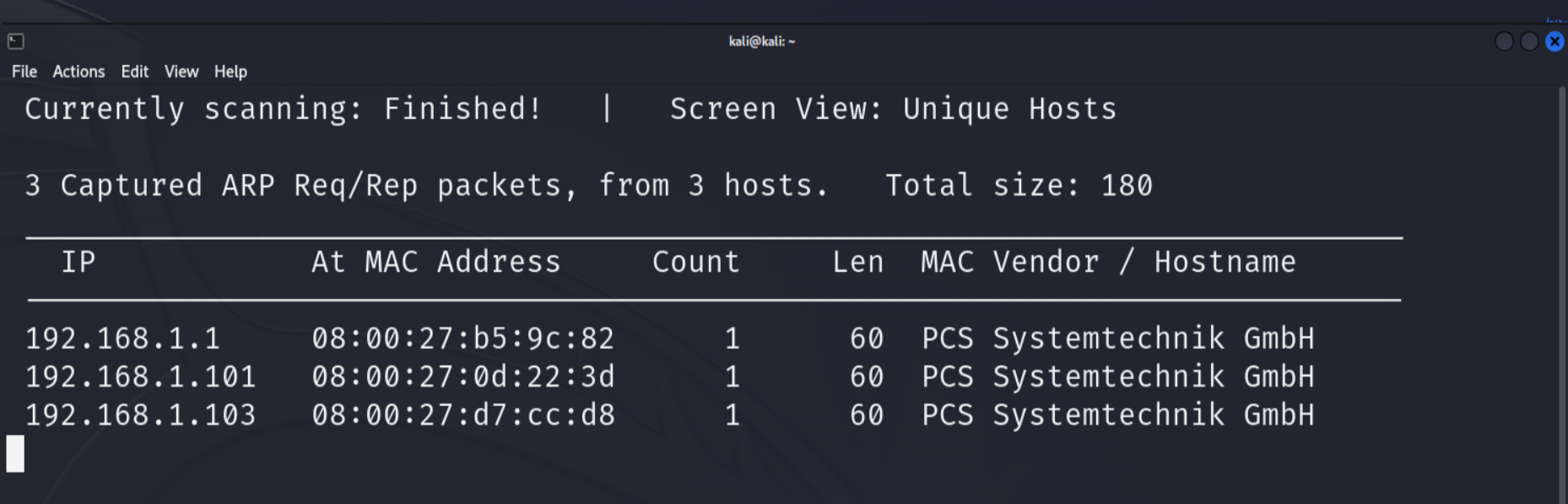
# Discovering Live Systems

**Step 1:** Scan using ifconfig.

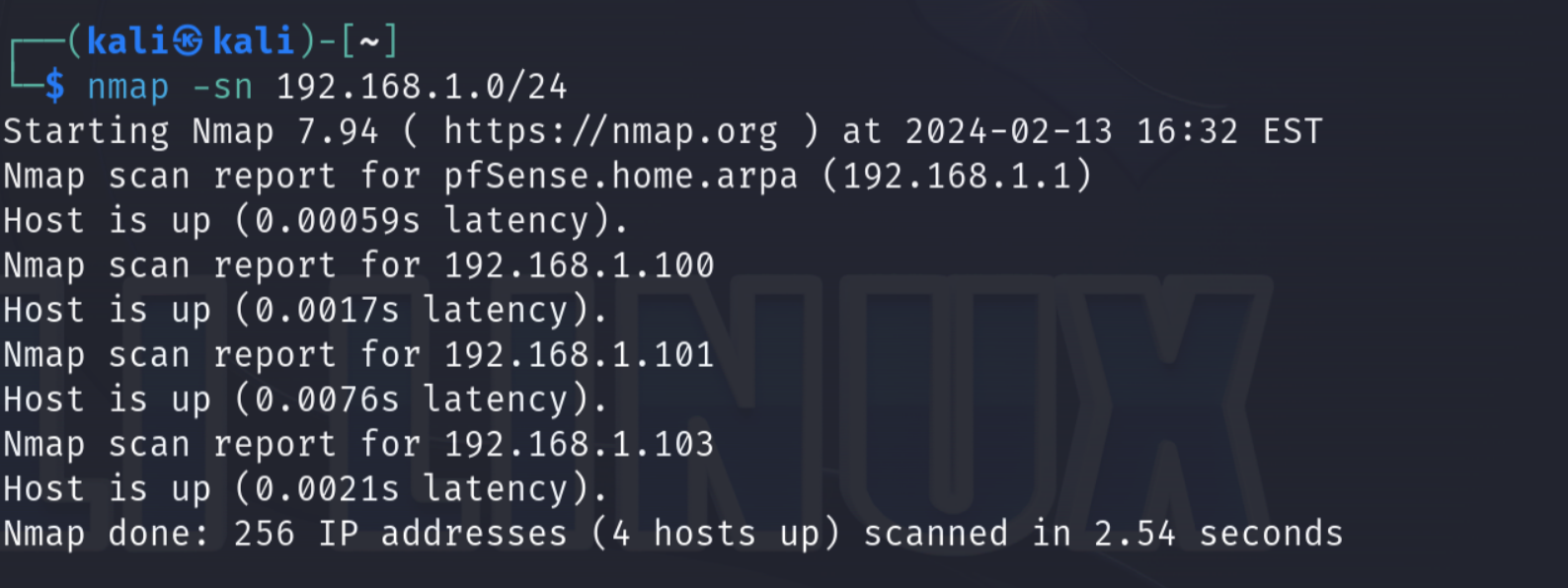


**Step 2:** Scan with netdiscover.

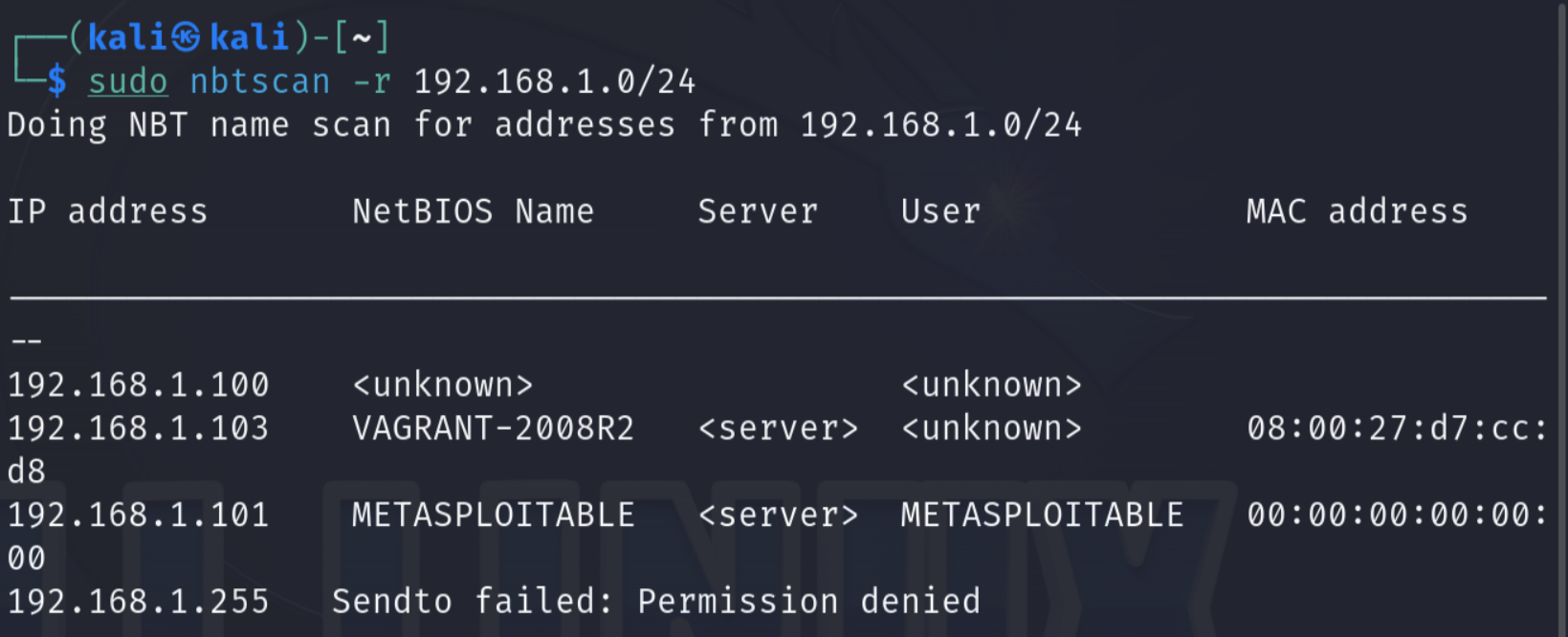




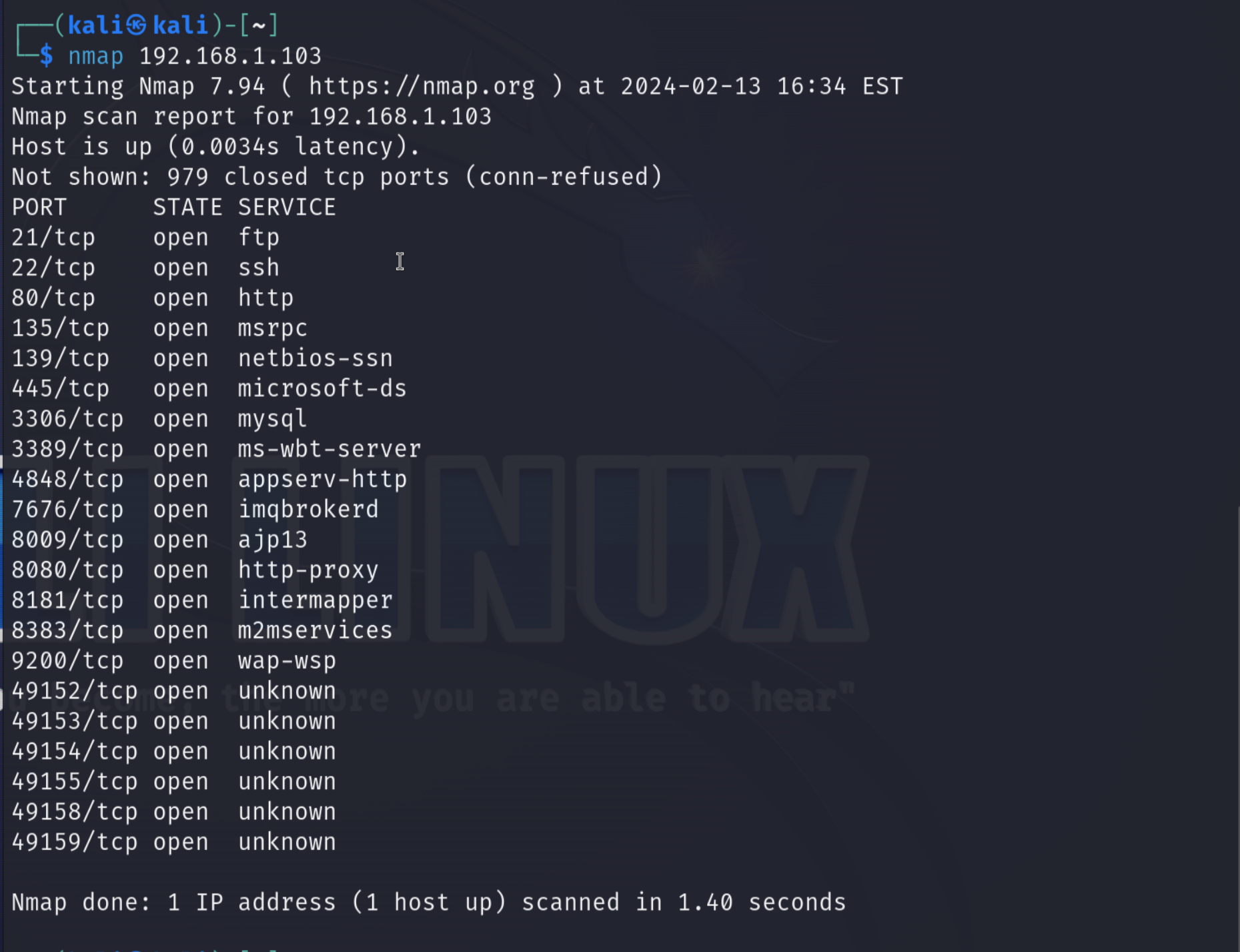
**Step 3:** Scan with Nmap



Step 4: Scan using ntbscan.



**Step 5:** Run Nmap against the Metasploitable machine.

****

# Section 2. Profiling a Target System

**Step 1:** Power on all VMs.

**Step 2:** Use Nmap to find operating systems, versions, and SMB script scanning for Metasploitable 3.

┌──(kali㉿kali)-[~]

└─$ nmap -A 192.168.1.103

Not shown: 979 closed tcp ports (conn-refused)

PORT STATE SERVICE VERSION

21/tcp open ftp Microsoft ftpd

| ftp-syst:

|\_ SYST: Windows\_NT

22/tcp open ssh OpenSSH 7.1 (protocol 2.0)

| ssh-hostkey:

| 2048 fd:08:98:ca:3c:e8:c1:3c:ea:dd:09:1a:2e:89:a5:1f (RSA)

|\_ 521 7e:57:81:8e:f6:3c:1d:cf:eb:7d:ba:d1:12:31:b5:a8 (ECDSA)

80/tcp open http Microsoft IIS httpd 7.5

|\_http-server-header: Microsoft-IIS/7.5

| http-methods:

|\_ Potentially risky methods: TRACE

|\_http-title: Site doesn't have a title (text/html).

135/tcp open msrpc Microsoft Windows RPC

139/tcp open netbios-ssn Microsoft Windows netbios-ssn

445/tcp open sonal-freemail@thawte.com Windows Server 2008 R2 Standard 7601 Service Pack 1 microsoft-ds

3306/tcp open mysql MySQL 5.5.20-log

| mysql-info:

| Protocol: 10

| Version: 5.5.20-log

| Thread ID: 4

| Capabilities flags: 63487

| Some Capabilities: ConnectWithDatabase, ODBCClient, Support41Auth, SupportsTransactions, SupportsLoadDataLocal, InteractiveClient, Speaks41ProtocolOld, LongColumnFlag, IgnoreSpaceBeforeParenthesis, Speaks41ProtocolNew, SupportsCompression, FoundRows, IgnoreSigpipes, LongPassword, DontAllowDatabaseTableColumn, SupportsMultipleResults, SupportsAuthPlugins, SupportsMultipleStatments

| Status: Autocommit

| Salt: {54E<<W%M6f!l}PXG=<S

|\_ Auth Plugin Name: mysql\_native\_password

3389/tcp open ssl/ms-wbt-server?

| rdp-ntlm-info:

| Target\_Name: VAGRANT-2008R2

| NetBIOS\_Domain\_Name: VAGRANT-2008R2

| NetBIOS\_Computer\_Name: VAGRANT-2008R2

| DNS\_Domain\_Name: vagrant-2008R2

| DNS\_Computer\_Name: vagrant-2008R2

| Product\_Version: 6.1.7601

|\_ System\_Time: 2024-02-13T21:57:35+00:00

| ssl-cert: Subject: commonName=vagrant-2008R2

| Not valid before: 2024-01-07T15:49:21

|\_Not valid after: 2024-07-08T15:49:21

|\_ssl-date: 2024-02-13T21:57:54+00:00; 0s from scanner time.

4848/tcp open ssl/http Oracle GlassFish 4.0 (Servlet 3.1; JSP 2.3; Java 1.8)

| ssl-cert: Subject: commonName=localhost/organizationName=Oracle Corporation/stateOrProvinceName=California/countryName=US

| Not valid before: 2013-05-15T05:33:38

|\_Not valid after: 2023-05-13T05:33:38

|\_http-server-header: GlassFish Server Open Source Edition 4.0

|\_ssl-date: 2024-02-13T21:57:54+00:00; 0s from scanner time.

|\_http-title: Did not follow redirect to https://192.168.1.103:4848/

7676/tcp open java-message-service Java Message Service 301

8009/tcp open ajp13 Apache Jserv (Protocol v1.3)

|\_ajp-methods: Failed to get a valid response for the OPTION request

8080/tcp open http Sun GlassFish Open Source Edition 4.0

|\_http-title: Site doesn't have a title (text/html).

|\_http-server-header: GlassFish Server Open Source Edition 4.0

| http-methods:

|\_ Potentially risky methods: PUT DELETE TRACE

8181/tcp open ssl/intermapper?

| ssl-cert: Subject: commonName=localhost/organizationName=Oracle Corporation/stateOrProvinceName=California/countryName=US

| Not valid before: 2013-05-15T05:33:38

|\_Not valid after: 2023-05-13T05:33:38

|\_ssl-date: 2024-02-13T21:57:54+00:00; 0s from scanner time.

8383/tcp open http Apache httpd

|\_http-server-header: Apache

|\_http-title: 400 Bad Request

9200/tcp open wap-wsp?

| fingerprint-strings:

| FourOhFourRequest:

| HTTP/1.0 400 Bad Request

| Content-Type: text/plain; charset=UTF-8

| Content-Length: 80

| handler found for uri [/nice%20ports%2C/Tri%6Eity.txt%2ebak] and method [GET]

| GetRequest:

| HTTP/1.0 200 OK

| Content-Type: application/json; charset=UTF-8

| Content-Length: 307

| "status" : 200,

| "name" : "Gravity",

| "version" : {

| "number" : "1.1.1",

| "build\_hash" : "f1585f096d3f3985e73456debdc1a0745f512bbc",

| "build\_timestamp" : "2014-04-16T14:27:12Z",

| "build\_snapshot" : false,

| "lucene\_version" : "4.7"

| "tagline" : "You Know, for Search"

| HTTPOptions:

| HTTP/1.0 200 OK

| Content-Type: text/plain; charset=UTF-8

| Content-Length: 0

| RTSPRequest, SIPOptions:

| HTTP/1.1 200 OK

| Content-Type: text/plain; charset=UTF-8

|\_ Content-Length: 0

49152/tcp open msrpc Microsoft Windows RPC

49153/tcp open msrpc Microsoft Windows RPC

49154/tcp open msrpc Microsoft Windows RPC

49155/tcp open msrpc Microsoft Windows RPC

49158/tcp open java-rmi Java RMI

49159/tcp open tcpwrapped

Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Host script results:

|\_nbstat: NetBIOS name: VAGRANT-2008R2, NetBIOS user: <unknown>, NetBIOS MAC: 08:00:27:d7:cc:d8 (Oracle VirtualBox virtual NIC)

| smb-os-discovery:

| OS: Windows Server 2008 R2 Standard 7601 Service Pack 1 (Windows Server 2008 R2 Standard 6.1)

| OS CPE: cpe:/o:microsoft:windows\_server\_2008::sp1

| Computer name: vagrant-2008R2

| NetBIOS computer name: VAGRANT-2008R2\x00

| Workgroup: WORKGROUP\x00

|\_ System time: 2024-02-13T13:57:32-08:00

| smb2-time:

| date: 2024-02-13T21:57:32

|\_ start\_date: 2024-02-13T21:27:20

| smb2-security-mode:

| 2:1:0:

|\_ Message signing enabled but not required

| smb-security-mode:

| account\_used: <blank>

| authentication\_level: user

| challenge\_response: supported

|\_ message\_signing: disabled (dangerous, but default)

|\_clock-skew: mean: 1h08m34s, deviation: 3h01m25s, median: 0s

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 130.61 seconds

┌──(kali㉿kali)-[~]

└─$

**Step 3:** Use Nmap to find operating systems, versions, and SMB script scanning for Metasploitable.

┌──(kali㉿kali)-[~]

└─$ nmap -A 192.168.1.101

Starting Nmap 7.94 ( https://nmap.org ) at 2024-02-13 17:01 EST

Nmap scan report for 192.168.1.101

Host is up (0.00095s latency).

Not shown: 977 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 192.168.1.100

| 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

| sslv2:

| SSLv2 supported

| ciphers:

| SSL2\_RC2\_128\_CBC\_WITH\_MD5

| SSL2\_DES\_64\_CBC\_WITH\_MD5

| SSL2\_RC4\_128\_WITH\_MD5

| SSL2\_RC4\_128\_EXPORT40\_WITH\_MD5

| SSL2\_RC2\_128\_CBC\_EXPORT40\_WITH\_MD5

|\_ SSL2\_DES\_192\_EDE3\_CBC\_WITH\_MD5

|\_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN

|\_ssl-date: 2024-02-13T22:02:12+00:00; -1s 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

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 40316/udp mountd

| 100005 1,2,3 57301/tcp mountd

| 100021 1,3,4 50276/tcp nlockmgr

| 100021 1,3,4 60764/udp nlockmgr

| 100024 1 41106/tcp status

|\_ 100024 1 41428/udp status

139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)

445/tcp open P���U 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: 10

| Capabilities flags: 43564

| Some Capabilities: Speaks41ProtocolNew, LongColumnFlag, SupportsCompression, SupportsTransactions, SwitchToSSLAfterHandshake, Support41Auth, ConnectWithDatabase

| Status: Autocommit

|\_ Salt: ACks"I)1YMWOb!zgs,!^

5432/tcp open postgresql PostgreSQL DB 8.3.0 - 8.3.7

| 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

|\_ssl-date: 2024-02-13T22:02:12+00:00; -1s from scanner time.

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)

6667/tcp open irc UnrealIRCd

| irc-info:

| users: 1

| servers: 1

| lusers: 1

| lservers: 0

| server: irc.Metasploitable.LAN

| version: Unreal3.2.8.1. irc.Metasploitable.LAN

| uptime: 0 days, 0:35:30

| source ident: nmap

| source host: 37D4021C.78DED367.FFFA6D49.IP

|\_ error: Closing Link: jesoaqnjl[192.168.1.100] (Quit: jesoaqnjl)

8009/tcp open ajp13 Apache Jserv (Protocol v1.3)

|\_ajp-methods: Failed to get a valid response for the OPTION request

8180/tcp open http Apache Tomcat/Coyote JSP engine 1.1

|\_http-title: Apache Tomcat/5.5

|\_http-favicon: Apache Tomcat

|\_http-server-header: Apache-Coyote/1.1

Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux\_kernel

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: 2024-02-13T17:02:00-05:00

|\_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)

|\_smb2-time: Protocol negotiation failed (SMB2)

| smb-security-mode:

| account\_used: <blank>

| authentication\_level: user

| challenge\_response: supported

|\_ message\_signing: disabled (dangerous, but default)

|\_clock-skew: mean: 1h14m59s, deviation: 2h30m00s, median: -1s

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 25.34 seconds

┌──(kali㉿kali)-[~]

└─$