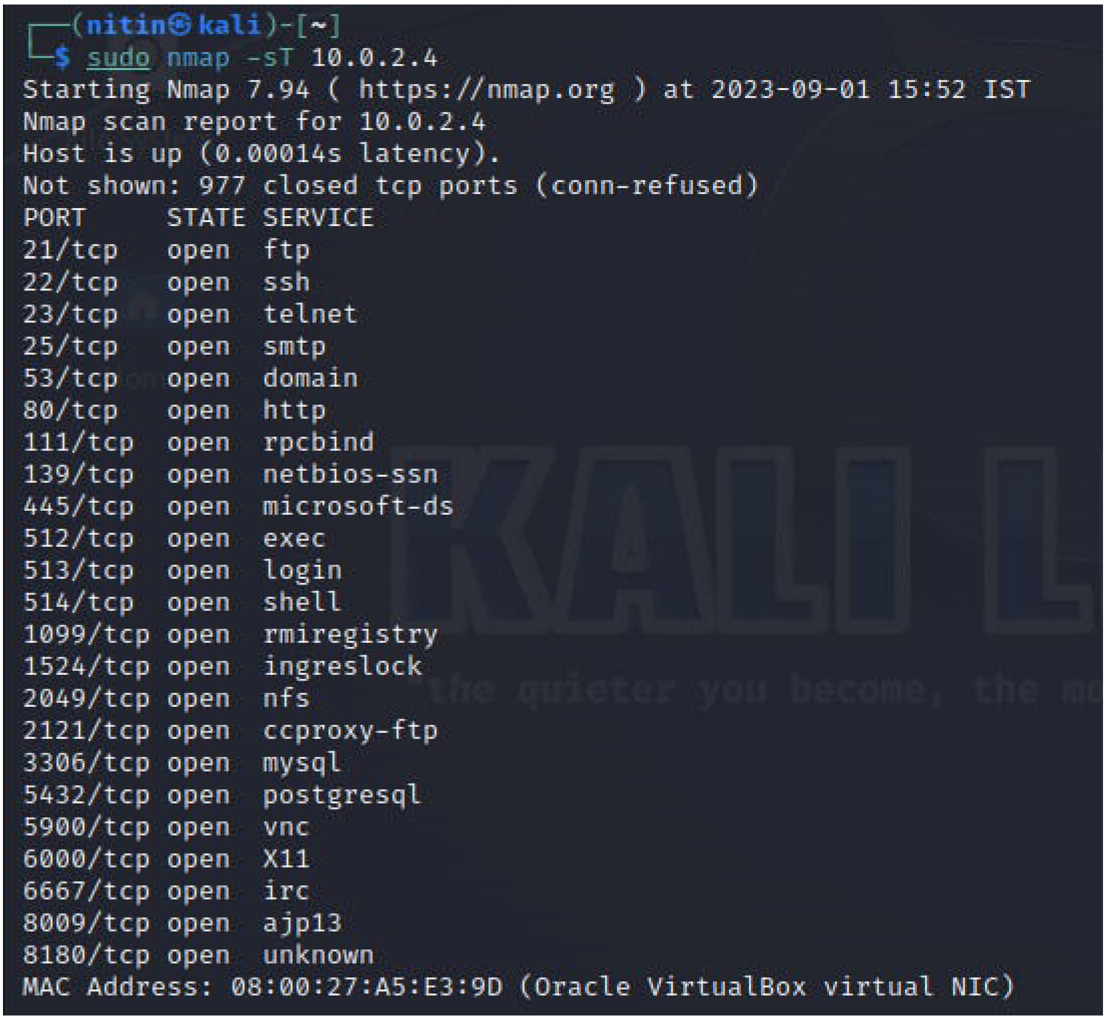
Metasploitable 2 Activity and Quiz

1.Which company created Metasploit and Metasploitable 2?

The company created Metasploit and Metasploitable 2 is ‘Rapid7.’

2.How many TCP ports are OPEN on MS2? (Use the `-sT` flag in Nmap).

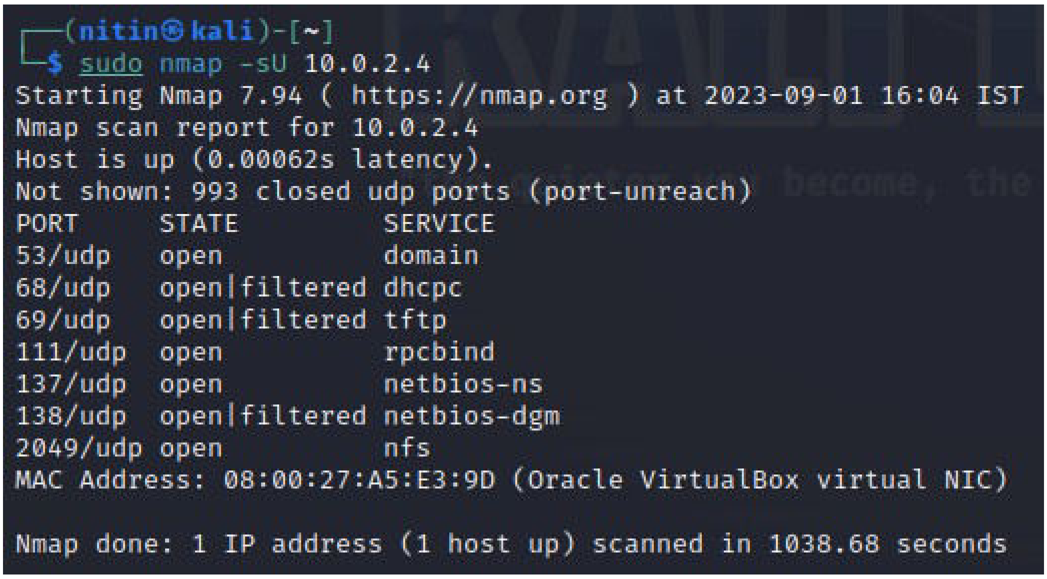
Use the command ‘sudo nmap -sT 10.0.2.4’. The -sT flag is used to specify a TCP (Transmission Control Protocol) scan. There will be 23 TCP ports displayed on the screen.



```
┌──(nitin㉿kali)-[~]
└─$ sudo nmap -sT 10.0.2.4
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-01 15:52 IST
Nmap scan report for 10.0.2.4
Host is up (0.00014s latency).
Not shown: 977 closed tcp ports (conn-refused)
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:A5:E3:9D (Oracle VirtualBox virtual NIC)
```

3.How many UDP ports are OPEN on MS2? (Use the `-sU` flag in Nmap – this may take a while).

Use the command 'sudo nmap -sU 10.0.2.4'. The -sU flag is used to specify a UDP (User Datagram Protocol) scan. There will be a total of 7 UDP ports displayed on the screen but only 4 are open.

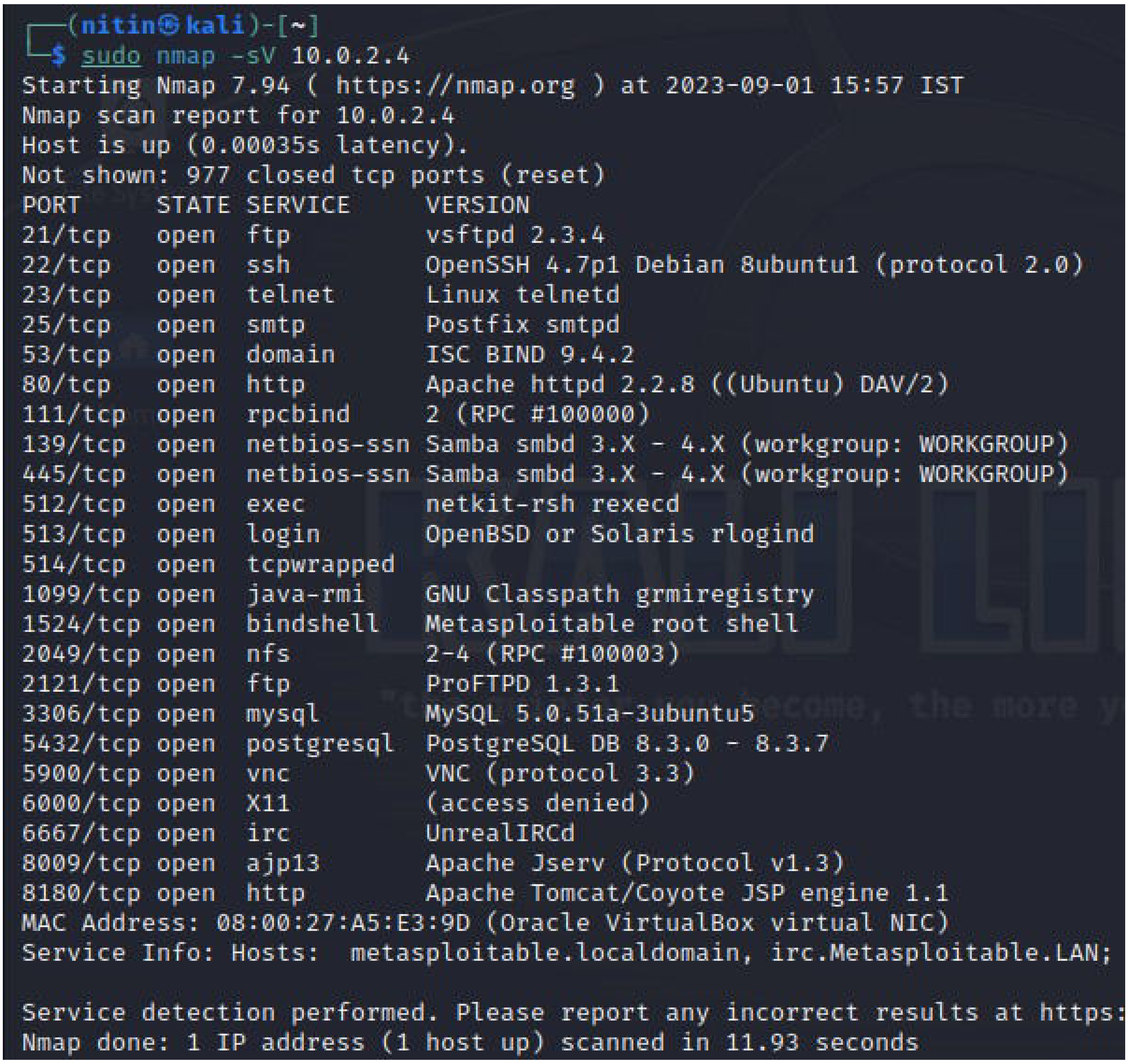


```
┌──(nitin㉿kali)-[~]
└─$ sudo nmap -sU 10.0.2.4
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-01 16:04 IST
Nmap scan report for 10.0.2.4
Host is up (0.00062s latency).
Not shown: 993 closed udp ports (port-unreach)
PORT     STATE         SERVICE
53/udp   open          domain
68/udp   open|filtered dhcpc
69/udp   open|filtered tftp
111/udp  open          rpcbind
137/udp  open          netbios-ns
138/udp  open|filtered netbios-dgm
2049/udp open          nfs
MAC Address: 08:00:27:A5:E3:9D (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1038.68 seconds
```

4.What port is running a Metasploitable Root Shell? (Use the `-sV` flag in Nmap).

Use the command ‘sudo nmap -sV 10.0.2.4’. The -sV flag probe open port to determine service/version information. It will display the port on which the Metasploitable Root Shell is running i.e.1524

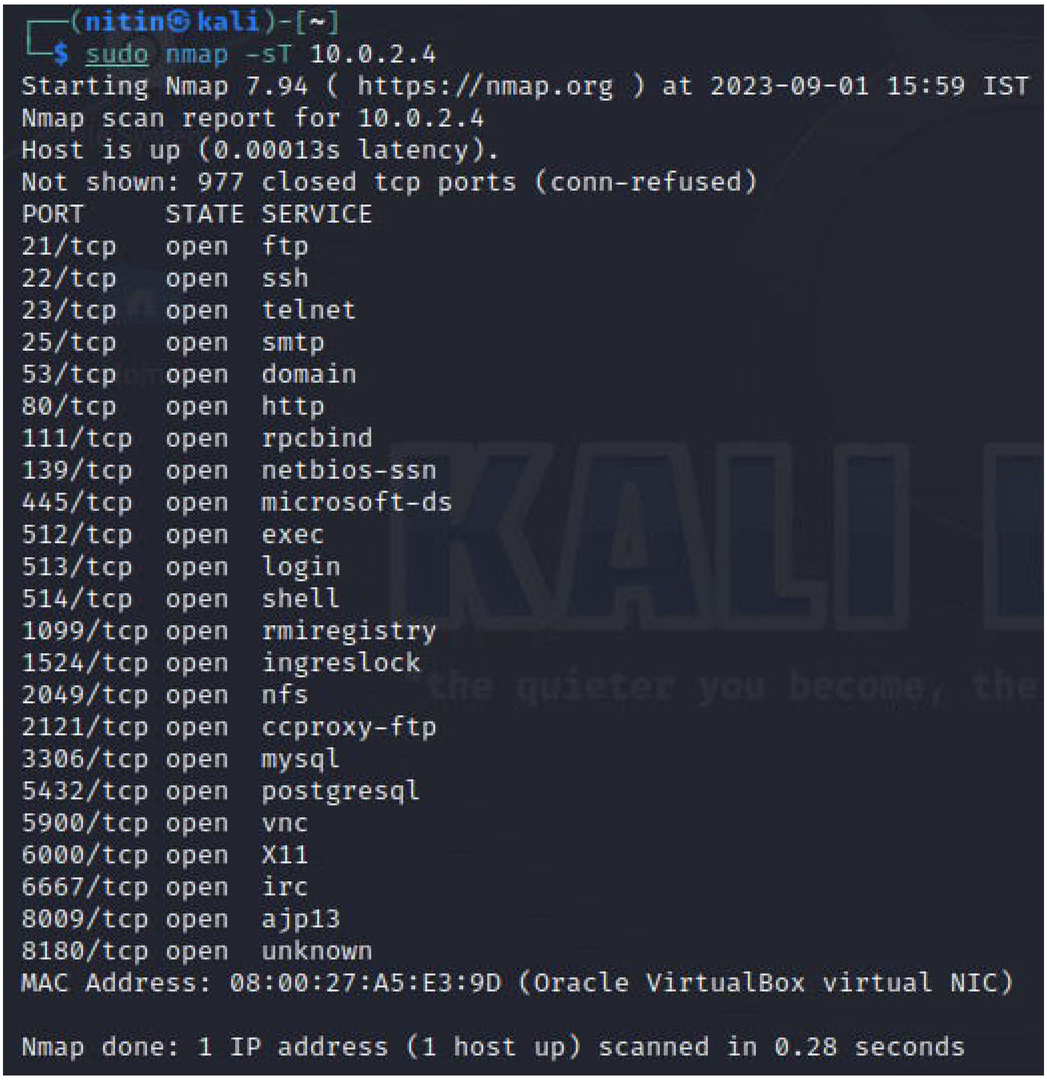


```
┌──(nitin㉿kali)-[~]
└─$ sudo nmap -sV 10.0.2.4
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-01 15:57 IST
Nmap scan report for 10.0.2.4
Host is up (0.00035s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  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       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
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:A5:E3:9D (Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN;

Service detection performed. Please report any incorrect results at https:
Nmap done: 1 IP address (1 host up) scanned in 11.93 seconds
```

5.What non-standard port is FTP running on? (NOT p21) (Use the `-sT` flag in Nmap)

Use the command 'sudo nmap -sT 10.0.2.4'. The -sT flag is used to specify a TCP (Transmission Control Protocol) scan. With help of this commnad, it is observed that there is another FTP running called ccproxy-ftp on port 2121.

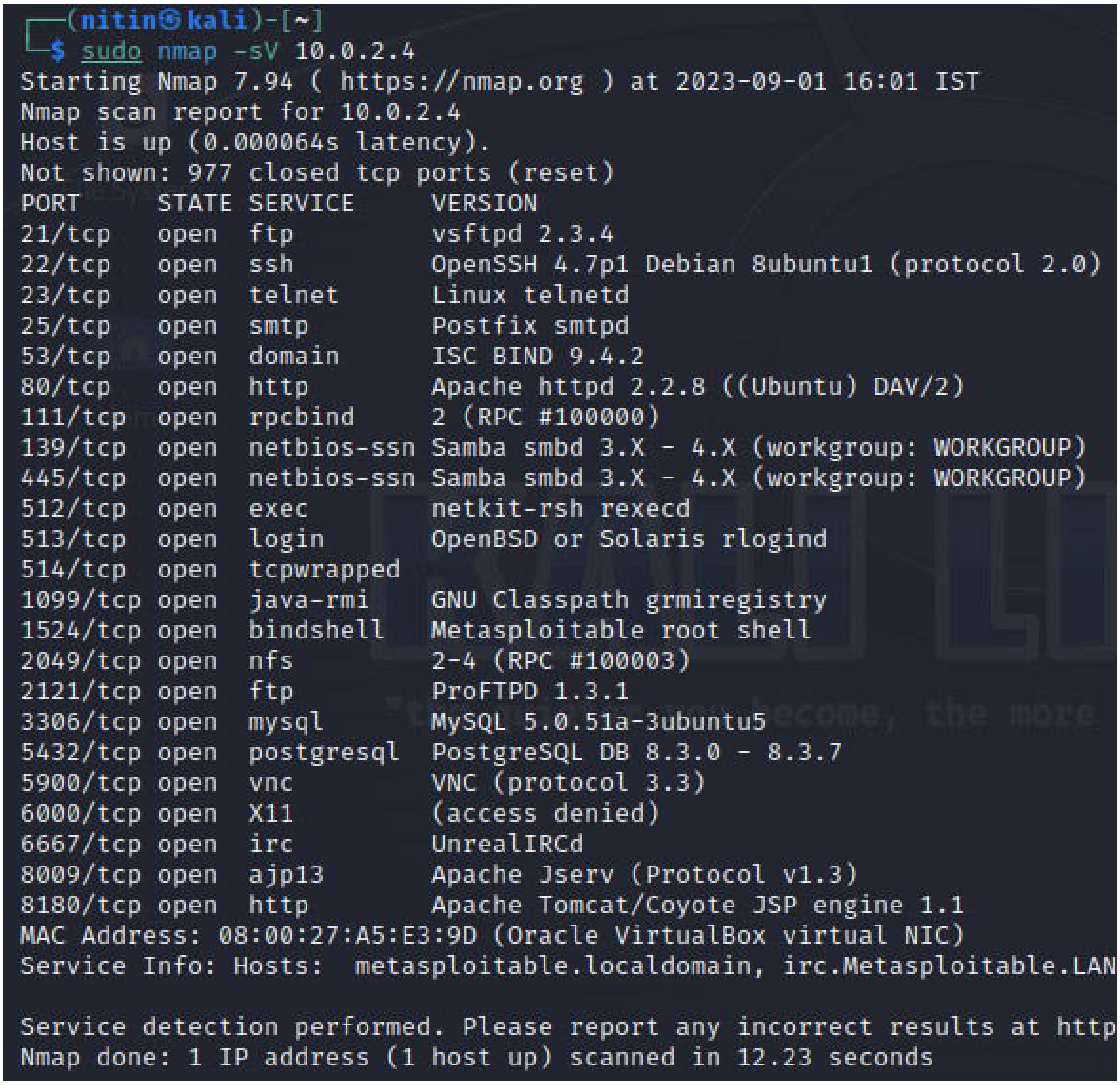


```
┌──(nitin㉿kali)-[~]
└─$ sudo nmap -sT 10.0.2.4
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-01 15:59 IST
Nmap scan report for 10.0.2.4
Host is up (0.00013s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
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:A5:E3:9D (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.28 seconds
```

6.What version of FTP is running on the non-standard port? (Use the -sV flag in Nmap).

Use the command 'sudo nmap -sV 10.0.2.4'. The -sV flag probe open port to determine service/version information. The version of FTP is running on the non-standard port 1.3.1.



```
┌──(nitin㉿kali)-[~]
└─$ sudo nmap -sV 10.0.2.4
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-01 16:01 IST
Nmap scan report for 10.0.2.4
Host is up (0.000064s 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       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
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:A5:E3:9D (Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN

Service detection performed. Please report any incorrect results at http
Nmap done: 1 IP address (1 host up) scanned in 12.23 seconds
```