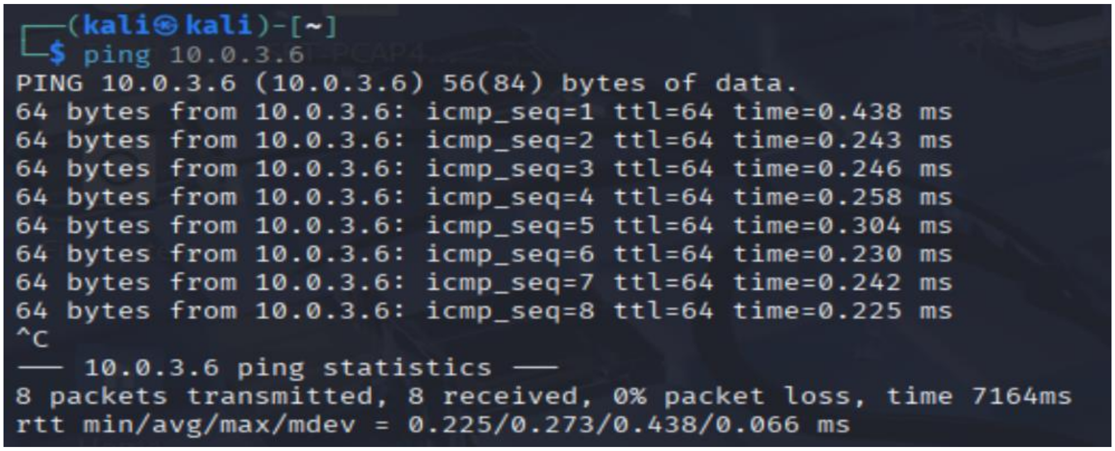
Metasploitable 2 Activity and Quiz

First that all we need to make sure we have connection to our metasploitable2 machine from our kali linux machine. This can be done by the command ping [ip-adddress]

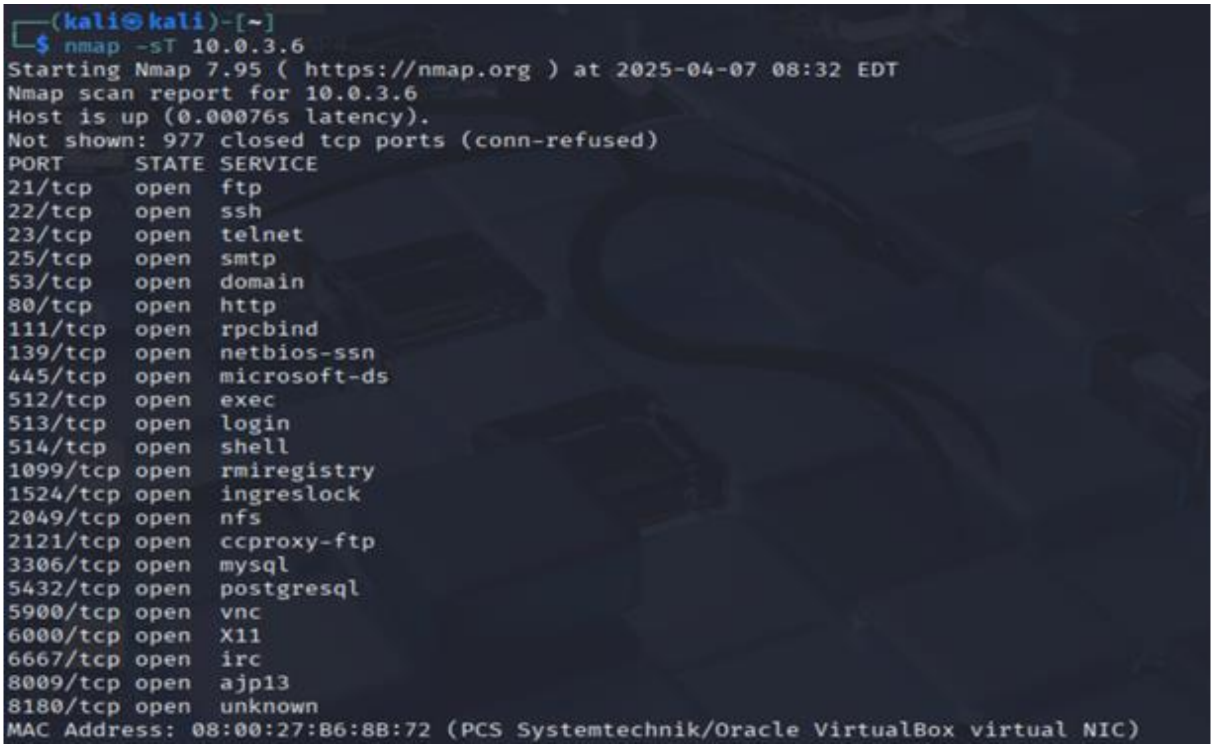


```
┌──(kali㉿kali)-[~]
└─$ ping 10.0.3.6
PING 10.0.3.6 (10.0.3.6) 56(84) bytes of data.
64 bytes from 10.0.3.6: icmp_seq=1 ttl=64 time=0.438 ms
64 bytes from 10.0.3.6: icmp_seq=2 ttl=64 time=0.243 ms
64 bytes from 10.0.3.6: icmp_seq=3 ttl=64 time=0.246 ms
64 bytes from 10.0.3.6: icmp_seq=4 ttl=64 time=0.258 ms
64 bytes from 10.0.3.6: icmp_seq=5 ttl=64 time=0.304 ms
64 bytes from 10.0.3.6: icmp_seq=6 ttl=64 time=0.230 ms
64 bytes from 10.0.3.6: icmp_seq=7 ttl=64 time=0.242 ms
64 bytes from 10.0.3.6: icmp_seq=8 ttl=64 time=0.225 ms
^C
— 10.0.3.6 ping statistics —
8 packets transmitted, 8 received, 0% packet loss, time 7164ms
rtt min/avg/max/mdev = 0.225/0.273/0.438/0.066 ms
```

1. Which company created Metasploit and Metasploitable 2? Answer Rapid 7

2. How many TCP ports are OPEN on MS2? (Use the -sT flag in Nmap). Answer is 23

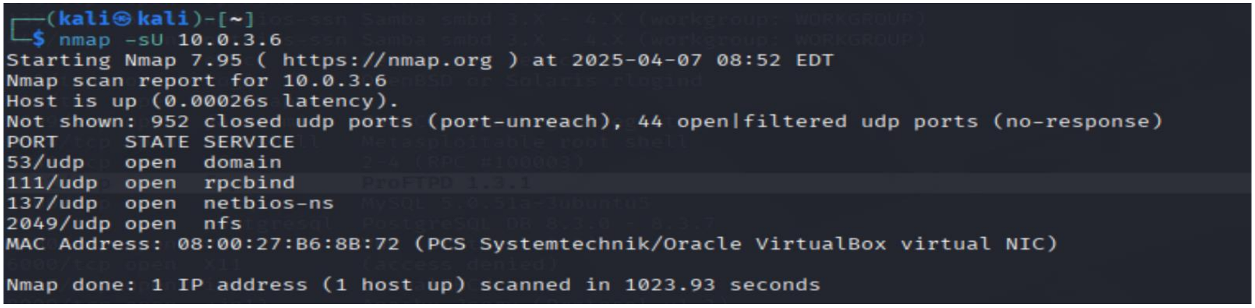
   To get this we need to use this command nmap –sT [target ip-address]



```
┌──(kali㉿kali)-[~]
└─$ nmap -sT 10.0.3.6
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-07 08:32 EDT
Nmap scan report for 10.0.3.6
Host is up (0.00076s 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:B6:8B:72 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
```

3. How many UDP ports are OPEN on MS2? (Use the -sU flag in Nmap – this may take a while). Answer 4

   To get this we need to use this command nmap –sU [target ip-address]

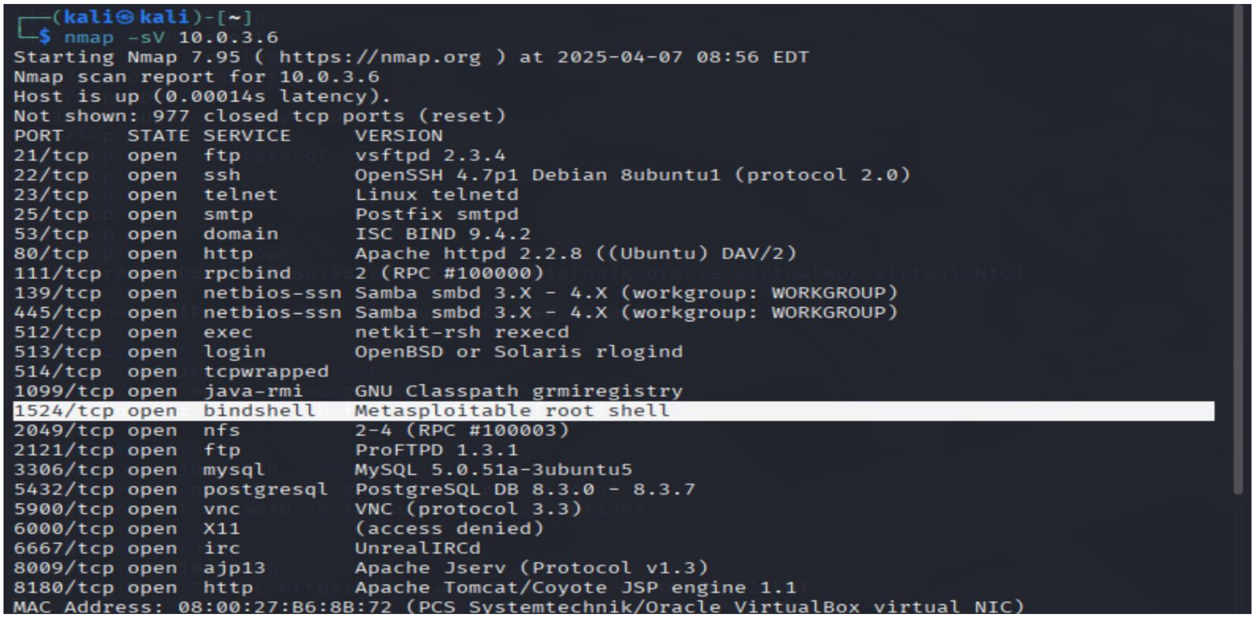


```
┌──(kali㉿kali)-[~]
└─$ nmap -sU 10.0.3.6
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-07 08:52 EDT
Nmap scan report for 10.0.3.6
Host is up (0.00026s latency).
Not shown: 952 closed udp ports (port-unreach), 44 open|filtered udp ports (no-response)
PORT     STATE SERVICE
53/udp   open  domain
111/udp  open  rpcbind
137/udp  open  netbios-ns
2049/udp open  nfs
MAC Address: 08:00:27:B6:8B:72 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1023.93 seconds
```

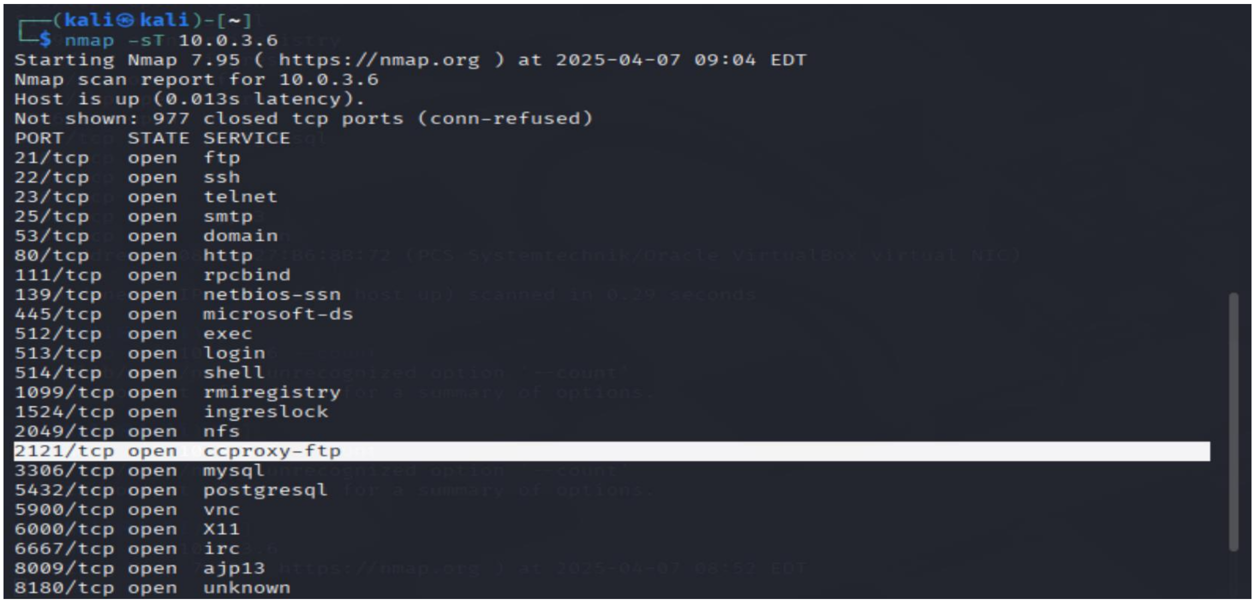
4. What port is running a Metasploitable Root Shell? (Use the -sV flag in Nmap) Answer 1524

   To get this we use the command –nmap –sV [target ip-address]



```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 10.0.3.6
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-07 08:56 EDT
Nmap scan report for 10.0.3.6
Host is up (0.00014s 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:B6:8B:72 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
```

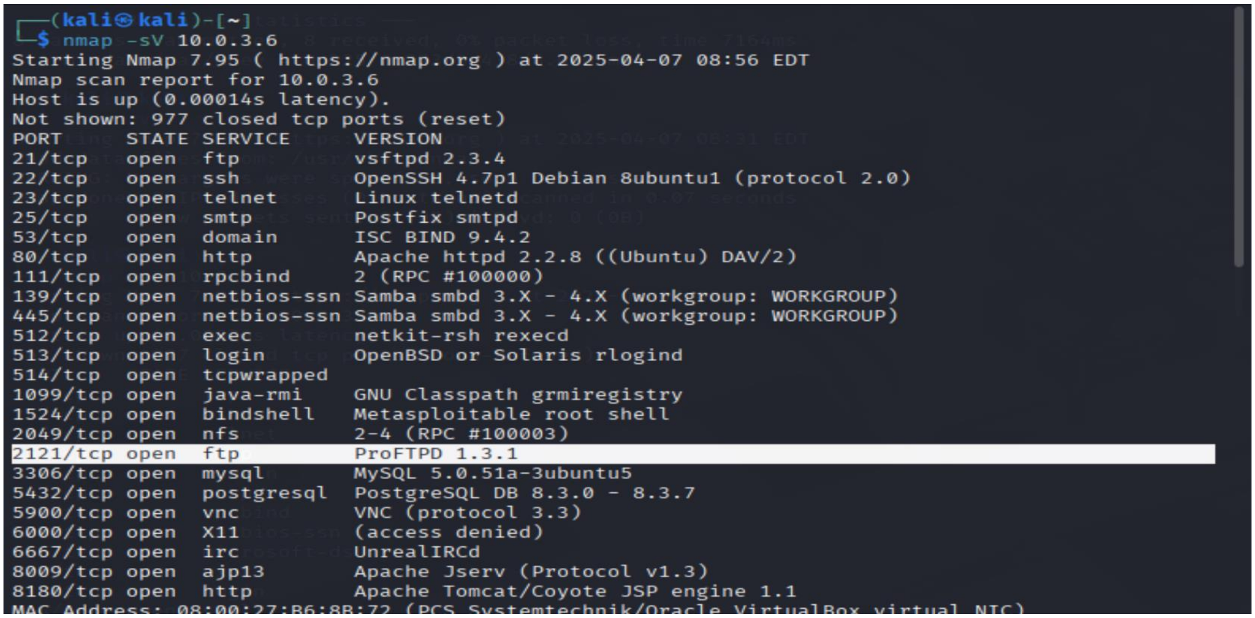
5. What non-standard port is FTP running on? (NOT p21) (Use the -sT flag in Nmap)
   answer 2121
   Use the nmap –sT [target ip-address]



```
┌──(kali㉿kali)-[~]
└─$ nmap -sT 10.0.3.6
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-07 09:04 EDT
Nmap scan report for 10.0.3.6
Host is up (0.013s 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
```

6. What version of FTP is running on the non-standard port? (Use the -sV flag in Nmap)
   1.3.1

   To get this we use the command –nmap –sV [target ip-address]



```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 10.0.3.6
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-07 08:56 EDT
Nmap scan report for 10.0.3.6
Host is up (0.00014s 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:B6:8B:72 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
```