05/07/2023 (Action)

downloaded metasploitable 2

Login: msfadmin

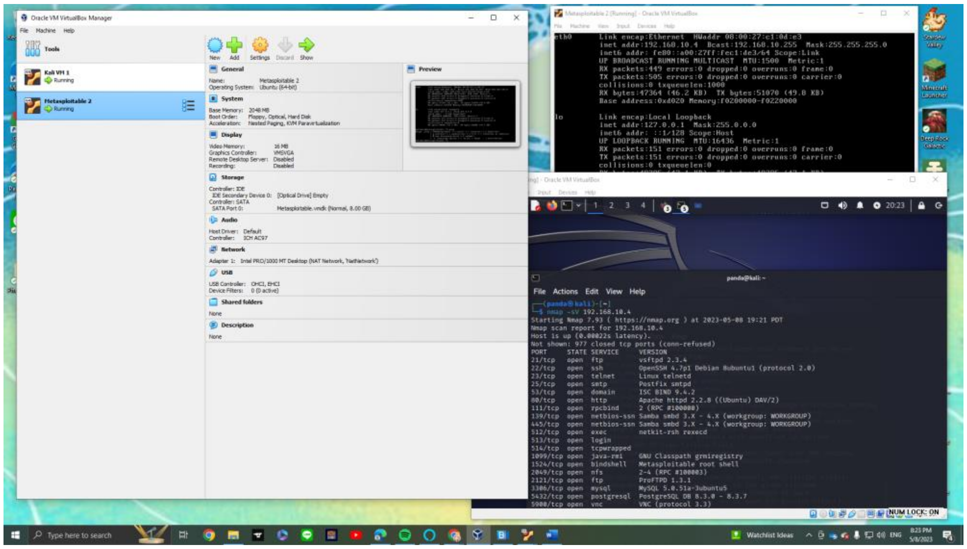
Bulit a bridge between the Kali VM to Metasploitable

05/08/2023 (Meeting)

Looked at what was vulnerable, he mentioned there were a couple of ports that showed that shouldn't be there. Pinged on kali nmap -sV 192.168.10.4 which is the address for the metasploitable.

Talked about zenmap, to do regular updates on github to show my progress.

Also suggested that I could downloaded vm for other operating systems like is04 and android


Oracle VM VirtualBox Manager
File Machine Help
Tools
Kali VM 1
Running
Metasploitable 2
Running
New
Add
Settings
Discard
Show
Preview
Metasploitable 2 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
NUM LOCK: ON
Watchlist Ideas

General
Name: Metasploitable 2
Operating System: Ubuntu (64-bit)

System
Base Memory: 2048 MB
Boot Order: Floppy, Optical, Hard Disk
Acceleration: Nested Paging, KVM Paravirtualization

Display
Video Memory: 16 MB
Graphics Controller: VMSVGA
Remote Desktop Server: Disabled
Recording: Disabled

Storage
Controller: IDE
IDE Secondary Device 0: [Optical Drive] Empty
Controller: SATA
SATA Port 0: Metasploitable.vmdk (Normal, 8.00 GB)

Audio
Host Driver: Default
Controller: ICH AC97

Network
Adapter 1: Intel PRO/1000 MT Desktop (NAT Network, 'NatNetwork')

USB
USB Controller: OHCI, EHCI
Device Filters: 0 (0 active)

Shared folders
None

Description
None

```
eth0      Link encap:Ethernet  HWaddr 08:00:27:c1:0d:e3
          inet addr:192.168.10.4  Bcast:192.168.10.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fec1:de3/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:449 errors:0 dropped:0 overruns:0 frame:0
          TX packets:505 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:47364 (46.2 KB)  TX bytes:51070 (49.8 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:151 errors:0 dropped:0 overruns:0 frame:0
          TX packets:151 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
```

```
┌──(panda㉿kali)-[~]
└─$ nmap -sV 192.168.10.4
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-08 19:21 PDT
Nmap scan report for 192.168.10.4
Host is up (0.00022s latency).
Not shown: 977 closed tcp ports (conn-refused)
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)
```

20:23

8:23 PM
5/8/2023

5/14 Action

Find vulnerable ports:

Port 21 (FTP): let users send and receive files from servers. FTP is known for being outdated and insecure. As such, attackers frequently exploit it through: Brute-forcing passwords, Anonymous authentication (it's possible to log into the FTP port with "anonymous" as the username and password), Cross-site scripting, Directory traversal attacks. can expose sensitive information and network credentials to an attacker when transmitting data across the network or the Internet

Port 22 (SSH): It’s a TCP port for ensuring secure access to servers. Hackers can exploit port 22 by using leaked SSH keys or brute-forcing credentials.

Port 23 (Telnet): is a TCP protocol that connects users to remote computers. For the most part, Telnet has been superseded by SSH, but it’s still used by some websites. Since it’s outdated and insecure, it’s vulnerable to many attacks, including credential brute-forcing, spoofing and credential sniffing. should use a secure protocol such as SFTP or FTPS.

Port 25 (SMTP): is a Simple Mail Transfer Protocol (SMTP) port for receiving and sending emails. Without proper configuration and protection, this TCP port is vulnerable to spoofing and spamming. SMTP port 25 continues to be used primarily for SMTP relaying. SMTP relaying is the transmission of email from email server to email server.

In most cases, modern SMTP email clients (Microsoft Outlook, Mail, Thunderbird, etc.) shouldn't use this port. It is traditionally blocked by residential ISPs and Cloud Hosting Providers, to curb the amount of spam that is relayed from compromised computers or servers. Unless you're specifically managing a mail server, you should have no traffic traversing this port on your computer or server.

Port 53 (DNS): is for Domain Name System (DNS). It’s a UDP and TCP port for queries and transfers, respectively. This port is particularly vulnerable to DDoS attacks. If you need to access the server remotely, you should use a secure protocol such as SFTP or FTPS.

Port 80: HTTP

Port 80 is used for Hypertext Transfer Protocol (HTTP). HTTP is an insecure protocol used to access web pages. It is recommended to close port 80 on your web server to prevent unauthorized access to your server. If you need to access the server remotely, you should use a secure protocol such as SFTP or FTPS.

Port 137-139 (NetBIOS/IP TCP, UDP) and Port 445 (SMB/IP TCP) : Server Message Block (SMB) uses port 445 directly and ports 137 and 139 indirectly. Cybercriminals can exploit these ports through: Using the EternalBlue exploit, which takes advantage of SMBv1 vulnerabilities in older versions of Microsoft computers (hackers used EternalBlue on the SMB port to spread WannaCry ransomware in 2017), Capturing NTLM hashes, Brute-forcing SMB login credentials

Port 514 : vulnerability is caused due to TCP connection information not being properly validated when connecting to a protocol translation resource and can be exploited to cause a reload via specially crafted packets sent to TCP ports 514 or 544.

Port 5900: VNC

Port 5900 is used for Virtual Network Computing (VNC). VNC is an insecure protocol used to remotely access and manage a server. It is recommended to close port 5900 on your web server to prevent unauthorized access to your server. If you need to access the server remotely, you should use a secure protocol such as SFTP or FTPS.

Port 6667: IRC

Port 6667 is used for Internet Relay Chat (IRC). IRC is an insecure protocol used to communicate with other users. It is recommended to close port 6667 on your web server to prevent unauthorized access to your server. If you need to communicate with other users, you should use a secure protocol such as SSL or TLS.

Resources:

https://blog.netwrix.com/2022/08/04/open-port-vulnerabilities-list/

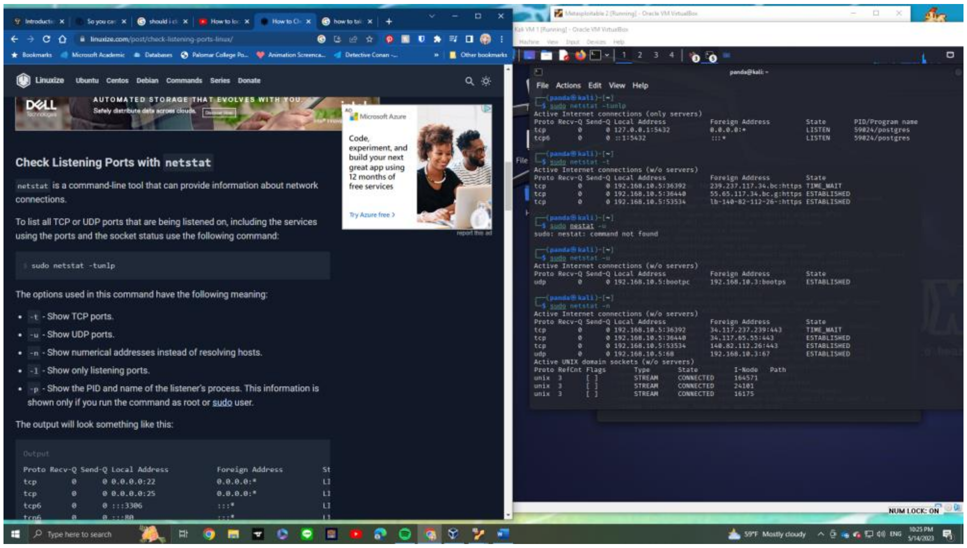
https://www.pcidssguide.com/firewall-rule-configuration-best-practices/

https://www.mailgun.com/blog/email/which-smtp-port-understanding-ports-25-465-587/#subchapter-1

https://www.alibabacloud.com/tech-news/web-server/giqt1yorqp-what-ports-should-i-close-on-my-web-server#:~:text=Port%2023%3A%20Telnet,such%20as%20SFTP%20or%20FTPS.

Check Listening Ports with `netstat`

```
sudo netstat -tunlp
```



Check Listening Ports with `netstat`

`netstat` is a command-line tool that can provide information about network connections.

To list all TCP or UDP ports that are being listened on, including the services using the ports and the socket status use the following command:

```
sudo netstat -tunlp
```

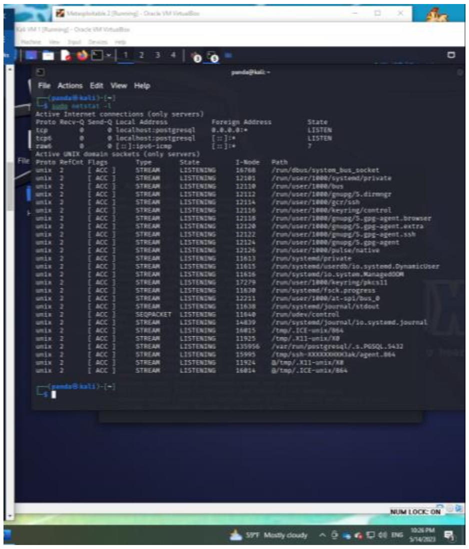
The options used in this command have the following meaning:

- `-t` - Show TCP ports.
- `-u` - Show UDP ports.
- `-n` - Show numerical addresses instead of resolving hosts.
- `-l` - Show only listening ports.
- `-p` - Show the PID and name of the listener's process. This information is shown only if you run the command as root or sudo user.

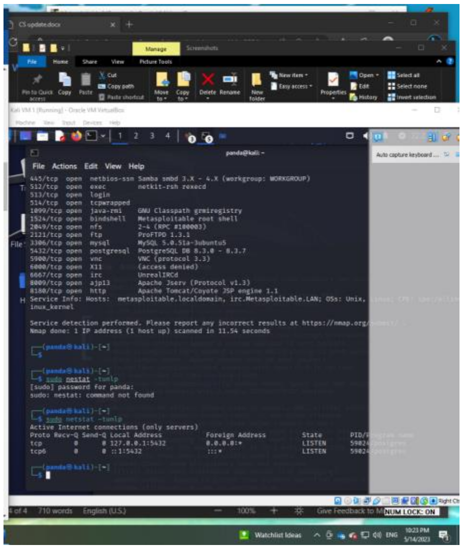
The output will look something like this:

```
Output
Proto Recv-Q Send-Q Local Address           Foreign Address         St
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LI
tcp        0      0 0.0.0.0:25              0.0.0.0:*               LI
tcp6       0      0 :::3306                 :::*                    LI
tcp6       0      0 :::80                   :::*                    LI
```

```
┌──(panda㉿kali)-[~]
└─$ sudo netstat -tunlp
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.1:5432          0.0.0.0:*               LISTEN      59024/postgres
tcp6       0      0 ::1:5432                :::*                    LISTEN      59024/postgres

┌──(panda㉿kali)-[~]
└─$ sudo netstat -t
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 192.168.10.5:36392      239.237.117.34.bc:https TIME_WAIT
tcp        0      0 192.168.10.5:36440      55.65.117.34.bc.g:https ESTABLISHED
tcp        0      0 192.168.10.5:53534      lb-140-82-112-26-:https ESTABLISHED

┌──(panda㉿kali)-[~]
└─$ sudo nestat -u
sudo: nestat: command not found

┌──(panda㉿kali)-[~]
└─$ sudo netstat -u
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
udp        0      0 192.168.10.5:bootpc     192.168.10.3:bootps     ESTABLISHED

┌──(panda㉿kali)-[~]
└─$ sudo netstat -n
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 192.168.10.5:36392      34.117.237.239:443      TIME_WAIT
tcp        0      0 192.168.10.5:36440      34.117.65.55:443        ESTABLISHED
tcp        0      0 192.168.10.5:53534      140.82.112.26:443       ESTABLISHED
udp        0      0 192.168.10.5:68         192.168.10.3:67         ESTABLISHED
Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags       Type       State         I-Node   Path
unix  3      [ ]         STREAM     CONNECTED     164571
unix  3      [ ]         STREAM     CONNECTED     24101
unix  3      [ ]         STREAM     CONNECTED     16175
```



```
┌──(panda㉿kali)-[~]
└─$ sudo netstat -l
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 localhost:postgresql    0.0.0.0:*               LISTEN
tcp6       0      0 localhost:postgresql    [::]:*                  LISTEN
raw6       0      0 [::]:ipv6-icmp          [::]:*                  7
Active UNIX domain sockets (only servers)
Proto RefCnt Flags       Type       State         I-Node   Path
unix  2      [ ACC ]     STREAM     LISTENING     16768    /run/dbus/system_bus_socket
unix  2      [ ACC ]     STREAM     LISTENING     12101    /run/user/1000/systemd/private
unix  2      [ ACC ]     STREAM     LISTENING     12110    /run/user/1000/bus
unix  2      [ ACC ]     STREAM     LISTENING     12112    /run/user/1000/gnupg/S.dirmngr
unix  2      [ ACC ]     STREAM     LISTENING     12114    /run/user/1000/gcr/ssh
unix  2      [ ACC ]     STREAM     LISTENING     12116    /run/user/1000/keyring/control
unix  2      [ ACC ]     STREAM     LISTENING     12118    /run/user/1000/gnupg/S.gpg-agent.browser
unix  2      [ ACC ]     STREAM     LISTENING     12120    /run/user/1000/gnupg/S.gpg-agent.extra
unix  2      [ ACC ]     STREAM     LISTENING     12122    /run/user/1000/gnupg/S.gpg-agent.ssh
unix  2      [ ACC ]     STREAM     LISTENING     12124    /run/user/1000/gnupg/S.gpg-agent
unix  2      [ ACC ]     STREAM     LISTENING     12126    /run/user/1000/pulse/native
unix  2      [ ACC ]     STREAM     LISTENING     11613    /run/systemd/private
unix  2      [ ACC ]     STREAM     LISTENING     11615    /run/systemd/userdb/io.systemd.DynamicUser
unix  2      [ ACC ]     STREAM     LISTENING     11616    /run/systemd/io.system.ManagedOOM
unix  2      [ ACC ]     STREAM     LISTENING     17279    /run/user/1000/keyring/pkcs11
unix  2      [ ACC ]     STREAM     LISTENING     11630    /run/systemd/fsck.progress
unix  2      [ ACC ]     STREAM     LISTENING     12211    /run/user/1000/at-spi/bus_0
unix  2      [ ACC ]     STREAM     LISTENING     11638    /run/systemd/journal/stdout
unix  2      [ ACC ]     SEQPACKET  LISTENING     11640    /run/udev/control
unix  2      [ ACC ]     STREAM     LISTENING     14839    /run/systemd/journal/io.systemd.journal
unix  2      [ ACC ]     STREAM     LISTENING     16015    /tmp/.ICE-unix/864
unix  2      [ ACC ]     STREAM     LISTENING     11925    /tmp/.X11-unix/X0
unix  2      [ ACC ]     STREAM     LISTENING     135956   /var/run/postgresql/.s.PGSQL.5432
unix  2      [ ACC ]     STREAM     LISTENING     15995    /tmp/ssh-XXXXXXXXXX1ak/agent.864
unix  2      [ ACC ]     STREAM     LISTENING     11924    @/tmp/.X11-unix/X0
unix  2      [ ACC ]     STREAM     LISTENING     16014    @/tmp/.ICE-unix/864

┌──(panda㉿kali)-[~]
└─$
```



```
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
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix,
inux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/
Nmap done: 1 IP address (1 host up) scanned in 11.54 seconds

┌──(panda㉿kali)-[~]
└─$

┌──(panda㉿kali)-[~]
└─$ sudo nestat -tunlp
[sudo] password for panda:
sudo: nestat: command not found

┌──(panda㉿kali)-[~]
└─$ sudo netstat -tunlp
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/
tcp        0      0 127.0.0.1:5432          0.0.0.0:*               LISTEN      5902
tcp6       0      0 ::1:5432                :::*                    LISTEN      5902

┌──(panda㉿kali)-[~]
└─$
```

5/15 Meeting

Discussed about the vulnerable ports I found in my vm. For my next step is to close those ports and document them. The steps I took and why they need to be closed

Next meeting will be held 5/23 Tue.

5/17 Action

Learn how to close ports

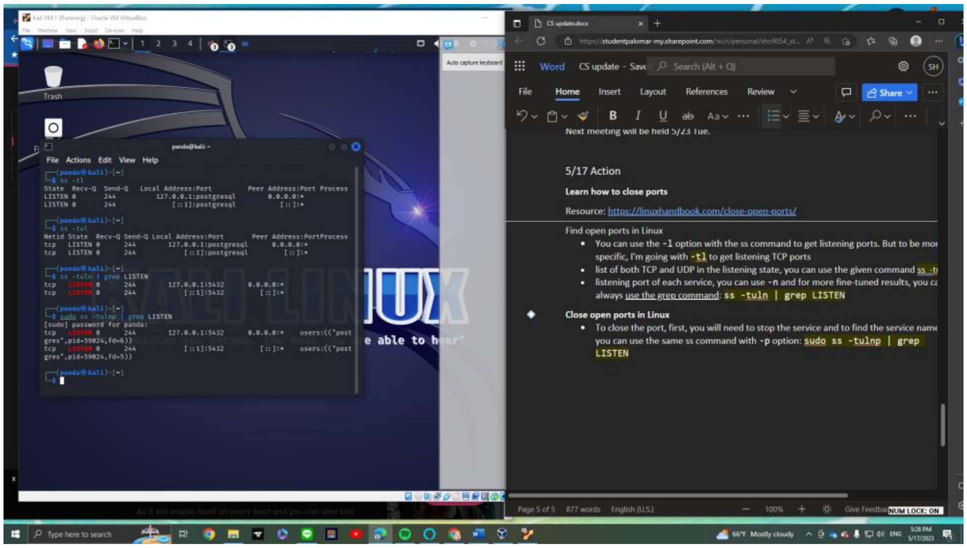
Resource: https://linuxhandbook.com/close-open-ports/

Find open ports in Linux

- You can use the `-l` option with the ss command to get listening ports. But to be more specific, I'm going with `-tl` to get listening TCP ports
- list of both TCP and UDP in the listening state, you can use the given command ss -tul
- listening port of each service, you can use `-n` and for more fine-tuned results, you can always use the grep command: `ss -tuln | grep LISTEN`

Close open ports in Linux

- To close the port, first, you will need to stop the service and to find the service name, you can use the same ss command with `-p` option: `sudo ss -tulnp | grep LISTEN`



```
┌──(panda㉿kali)-[~]
└─$ ss -tl
State  Recv-Q  Send-Q   Local Address:Port        Peer Address:Port Process
LISTEN 0       244          127.0.0.1:postgresql       0.0.0.0:*
LISTEN 0       244              [::1]:postgresql          [::]:*

┌──(panda㉿kali)-[~]
└─$ ss -tul
Netid State  Recv-Q Send-Q Local Address:Port        Peer Address:PortProcess
tcp   LISTEN 0      244        127.0.0.1:postgresql      0.0.0.0:*
tcp   LISTEN 0      244            [::1]:postgresql         [::]:*

┌──(panda㉿kali)-[~]
└─$ ss -tuln | grep LISTEN
tcp   LISTEN 0      244        127.0.0.1:5432      0.0.0.0:*
tcp   LISTEN 0      244            [::1]:5432         [::]:*

┌──(panda㉿kali)-[~]
└─$ sudo ss -tulnp | grep LISTEN
[sudo] password for panda:
tcp   LISTEN 0      244        127.0.0.1:5432      0.0.0.0:*    users:(("post
gres",pid=59024,fd=6))
tcp   LISTEN 0      244            [::1]:5432         [::]:*    users:(("post
gres",pid=59024,fd=5))

┌──(panda㉿kali)-[~]
└─$ 
```

Next meeting will be held 5/23 Tue.

5/17 Action

Learn how to close ports

Resource: https://linuxhandbook.com/close-open-ports/

Find open ports in Linux

- You can use the `-l` option with the ss command to get listening ports. But to be mor specific, I'm going with `-tl` to get listening TCP ports
- list of both TCP and UDP in the listening state, you can use the given command ss -t
- listening port of each service, you can use `-n` and for more fine-tuned results, you ca always use the grep command: `ss -tuln | grep LISTEN`

Close open ports in Linux

- To close the port, first, you will need to stop the service and to find the service name you can use the same ss command with `-p` option: `sudo ss -tulnp | grep LISTEN`

Note: the website shows how to close a certain port and changing firewall rules, so I am thinking I need to look up more specific closures for the ports I want to close.

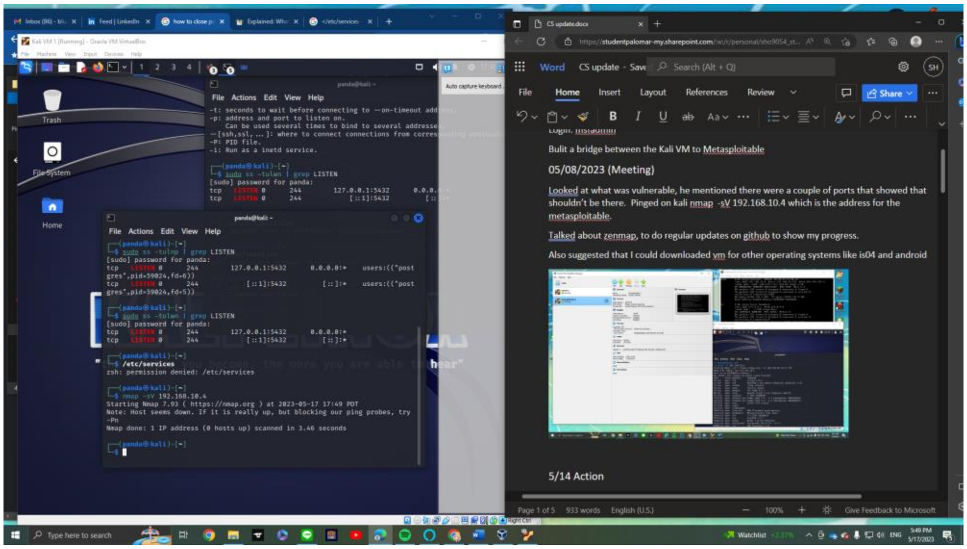
Following YouTube tutorial How to locate and close an open port in Linux https://www.youtube.com/watch?v=JNQnQAm4XjQ&ab_channel=HowToMakeTechWorkfromTechRepublic

1. Opened sshl
2. Type in sudo ss -tulwn | grep LISTEN
3. Type in sudo ufw deny _____ port

Notes:

- Doesn't show the ports I am looking for that I want to close. In the video the person said to type in less slash etsy slash services to see a listing of every port available to Linux.

Not sure what to type in still because it did not show, so I tried /etc/servies and it showed permission denied.



```
-t: seconds to wait before connecting to --on-timeout add
-p: address and port to listen on.
    Can be used several times to bind to several addresse
--[ssh,ssl, ... ]: where to connect connections from corres
-P: PID file.
-i: Run as a inetd service.

┌──(panda㉿kali)-[~]
└─$ sudo ss -tulwn | grep LISTEN
[sudo] password for panda:
tcp   LISTEN 0      244        127.0.0.1:5432      0.0.0.
tcp   LISTEN 0      244            [::1]:5432         [::
```

```
┌──(panda㉿kali)-[~]
└─$ sudo ss -tulnp | grep LISTEN
[sudo] password for panda:
tcp   LISTEN 0      244        127.0.0.1:5432      0.0.0.0:*    users:(("post
gres",pid=59024,fd=6))
tcp   LISTEN 0      244            [::1]:5432         [::]:*    users:(("post
gres",pid=59024,fd=5))

┌──(panda㉿kali)-[~]
└─$ sudo ss -tulwn | grep LISTEN
[sudo] password for panda:
tcp   LISTEN 0      244        127.0.0.1:5432      0.0.0.0:*
tcp   LISTEN 0      244            [::1]:5432         [::]:*

┌──(panda㉿kali)-[~]
└─$ /etc/services
zsh: permission denied: /etc/services

┌──(panda㉿kali)-[~]
└─$ nmap -sV 192.168.10.4
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-17 17:49 PDT
Note: Host seems down. If it is really up, but blocking our ping probes, try
-Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.46 seconds

┌──(panda㉿kali)-[~]
└─$
```

Bulit a bridge between the Kali VM to Metasploitable

05/08/2023 (Meeting)

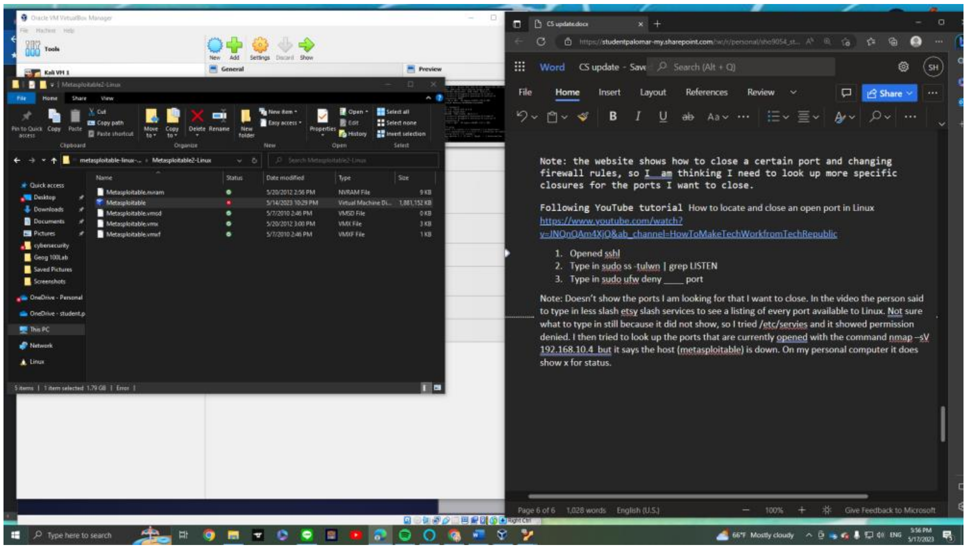
Looked at what was vulnerable, he mentioned there were a couple of ports that showed that shouldn't be there. Pinged on kali nmap -sV 192.168.10.4 which is the address for the metasploitable.

Talked about zenmap, to do regular updates on github to show my progress.

Also suggested that I could downloaded vm for other operating systems like is04 and android

5/14 Action

- I then tried to look up the ports that are currently opened with the command nmap –sV 192.168.10.4 but it says the host (metasploitable) is down. On my personal computer it does show x for status.



metasploitable-linux-... > Metasploitable2-Linux

Name	Status	Date modified	Type	Size
Metasploitable.nvram	●	5/20/2012 2:56 PM	NVRAM File	9 KB
Metasploitable	☒	5/14/2023 10:29 PM	Virtual Machine Di...	1,881,152 KB
Metasploitable.vmsd	●	5/7/2010 2:46 PM	VMSD File	0 KB
Metasploitable.vmx	●	5/20/2012 3:00 PM	VMX File	3 KB
Metasploitable.vmxf	●	5/7/2010 2:46 PM	VMXF File	1 KB

5 items | 1 item selected 1.79 GB | Error |

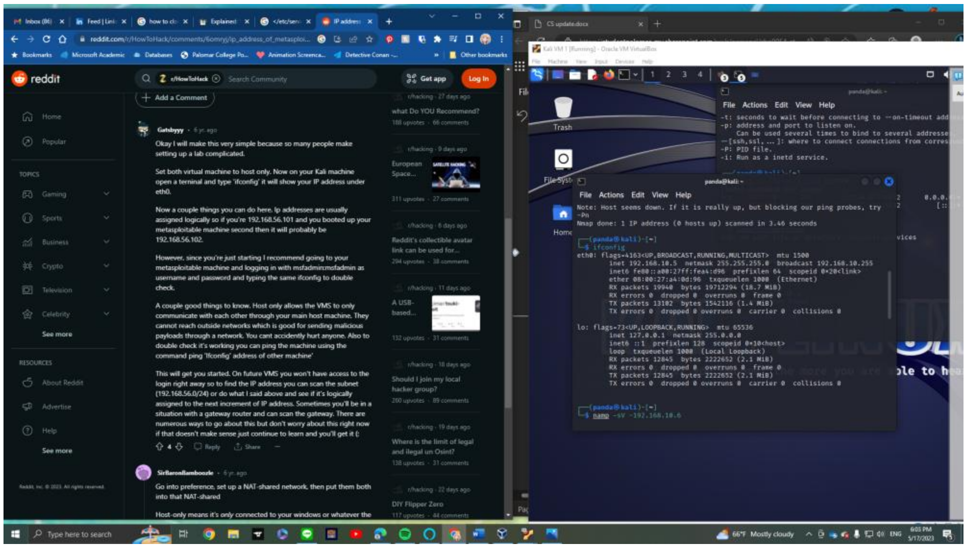
Note: the website shows how to close a certain port and changing firewall rules, so I am thinking I need to look up more specific closures for the ports I want to close.

Following YouTube tutorial How to locate and close an open port in Linux https://www.youtube.com/watch?v=JNQnQAm4XjQ&ab_channel=HowToMakeTechWorkfromTechRepublic

1. Opened sshl
2. Type in sudo ss -tulwn | grep LISTEN
3. Type in sudo ufw deny ____ port

Note: Doesn't show the ports I am looking for that I want to close. In the video the person said to type in less slash etsy slash services to see a listing of every port available to Linux. Not sure what to type in still because it did not show, so I tried /etc/servies and it showed permission denied. I then tried to look up the ports that are currently opened with the command nmap –sV 192.168.10.4 but it says the host (metasploitable) is down. On my personal computer it does show x for status.

- Looked up how to find the ip address for metasploitable to make sure. In kali I typed in ifconfig



Gatsbyyy · 6 yr. ago

Okay I will make this very simple because so many people make setting up a lab complicated.

Set both virtual machine to host only. Now on your Kali machine open a terminal and type 'ifconfig' it will show your IP address under eth0.

Now a couple things you can do here. Ip addresses are usually assigned logically so if you're 192.168.56.101 and you booted up your metasploitable machine second then it will probably be 192.168.56.102.

However, since you're just starting I recommend going to your metasploitable machine and logging in with msfadmin:msfadmin as username and password and typing the same ifconfig to double check.

A couple good things to know. Host only allows the VMS to only communicate with each other through your main host machine. They cannot reach outside networks which is good for sending malicious payloads through a network. You cant accidently hurt anyone. Also to double check it's working you can ping the machine using the command ping 'ifconfig' address of other machine'

This will get you started. On future VMS you won't have access to the login right away so to find the IP address you can scan the subnet (192.168.56.0/24) or do what I said above and see if it's logically assigned to the next increment of IP address. Sometimes you'll be in a situation with a gateway router and can scan the gateway. There are numerous ways to go about this but don't worry about this right now if that doesn't make sense just continue to learn and you'll get it (;

SirBaronBamboozle · 6 yr. ago

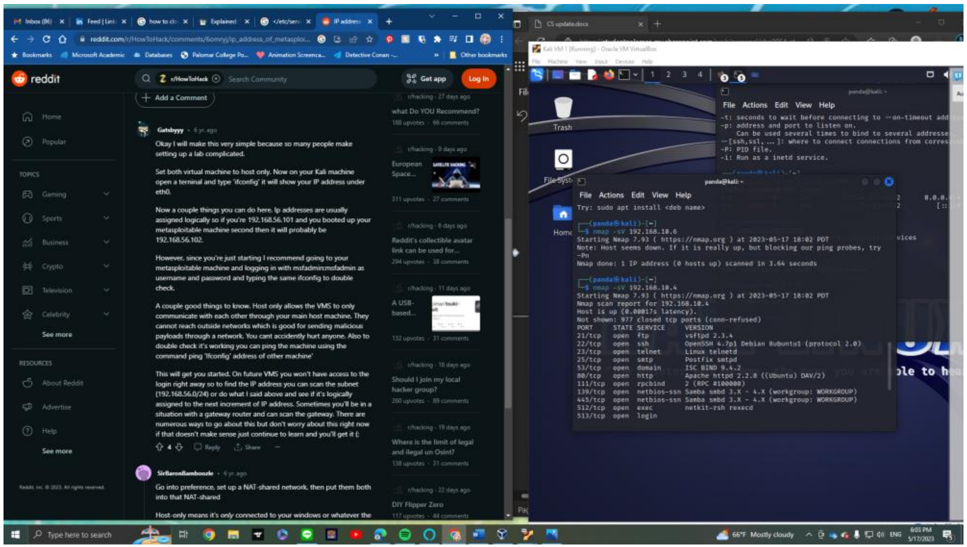
Go into preference, set up a NAT-shared network, then put them both into that NAT-shared

Host-only means it's only connected to your windows or whatever the

```
-t: seconds to wait before connecting to --on-timeout add
-p: address and port to listen on.
    Can be used several times to bind to several addresse
--[ssh,ssl, ... ]: where to connect connections from corres
-P: PID file.
-i: Run as a inetd service.
```

```
Note: Host seems down. If it is really up, but blocking our ping probes, try
-Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.46 seconds

┌──(panda㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.10.5  netmask 255.255.255.0  broadcast 192.168.10.255
        inet6 fe80::a00:27ff:fea4:d96  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:a4:0d:96  txqueuelen 1000  (Ethernet)
        RX packets 19940  bytes 19712294 (18.7 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 13102  bytes 1542116 (1.4 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 12845  bytes 2222652 (2.1 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 12845  bytes 2222652 (2.1 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(panda㉿kali)-[~]
└─$ namp -sV -192.168.10.6
```

- Then tried going up and down a number and found it.



Gatsbyyy · 6 yr. ago

Okay I will make this very simple because so many people make setting up a lab complicated.

Set both virtual machine to host only. Now on your Kali machine open a terminal and type 'ifconfig' it will show your IP address under eth0.

Now a couple things you can do here. Ip addresses are usually assigned logically so if you're 192.168.56.101 and you booted up your metasploitable machine second then it will probably be 192.168.56.102.

However, since you're just starting I recommend going to your metasploitable machine and logging in with msfadmin:msfadmin as username and password and typing the same ifconfig to double check.

A couple good things to know. Host only allows the VMS to only communicate with each other through your main host machine. They cannot reach outside networks which is good for sending malicious payloads through a network. You cant accidently hurt anyone. Also to double check it's working you can ping the machine using the command ping 'Ifconfig' address of other machine'

This will get you started. On future VMS you won't have access to the login right away so to find the IP address you can scan the subnet (192.168.56.0/24) or do what I said above and see if it's logically assigned to the next increment of IP address. Sometimes you'll be in a situation with a gateway router and can scan the gateway. There are numerous ways to go about this but don't worry about this right now if that doesn't make sense just continue to learn and you'll get it (:

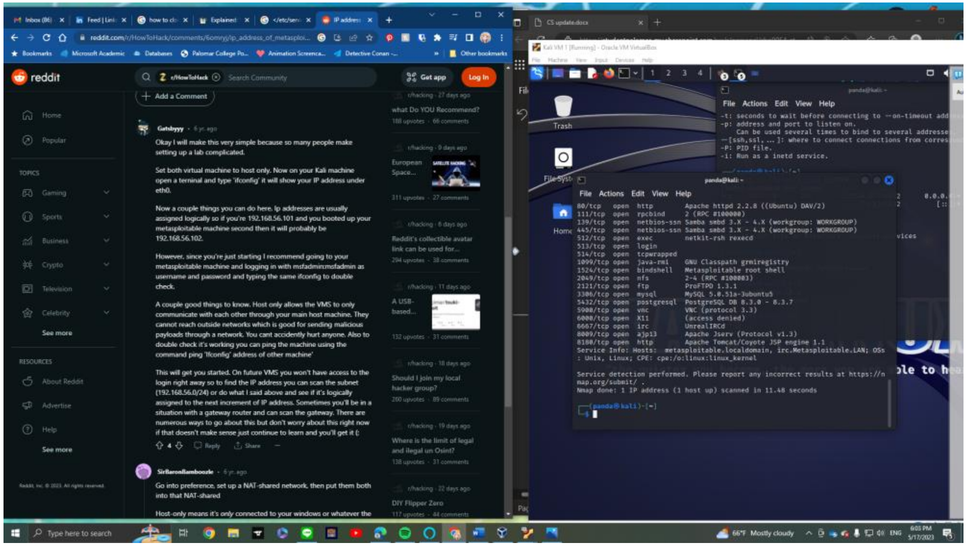
SirBaronBamboozle · 6 yr. ago

Go into preference, set up a NAT-shared network, then put them both into that NAT-shared

Host-only means it's only connected to your windows or whatever the

```
-t: seconds to wait before connecting to --on-timeout add
-p: address and port to listen on.
    Can be used several times to bind to several addresse
--[ssh,ssl, ... ]: where to connect connections from corres
-P: PID file.
-i: Run as a inetd service.
```

```
Try: sudo apt install <deb name>

┌──(panda㉿kali)-[~]
└─$ nmap -sV 192.168.10.6
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-17 18:02 PDT
Note: Host seems down. If it is really up, but blocking our ping probes, try
-Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.64 seconds

┌──(panda㉿kali)-[~]
└─$ nmap -sV 192.168.10.4
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-17 18:02 PDT
Nmap scan report for 192.168.10.4
Host is up (0.00017s latency).
Not shown: 977 closed tcp ports (conn-refused)
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
```



Gatsbyyy · 6 yr. ago

Okay I will make this very simple because so many people make setting up a lab complicated.

Set both virtual machine to host only. Now on your Kali machine open a terminal and type 'ifconfig' it will show your IP address under eth0.

Now a couple things you can do here. Ip addresses are usually assigned logically so if you're 192.168.56.101 and you booted up your metasploitable machine second then it will probably be 192.168.56.102.

However, since you're just starting I recommend going to your metasploitable machine and logging in with msfadmin:msfadmin as username and password and typing the same ifconfig to double check.

A couple good things to know. Host only allows the VMS to only communicate with each other through your main host machine. They cannot reach outside networks which is good for sending malicious payloads through a network. You cant accidently hurt anyone. Also to double check it's working you can ping the machine using the command ping 'Ifconfig' address of other machine'

This will get you started. On future VMS you won't have access to the login right away so to find the IP address you can scan the subnet (192.168.56.0/24) or do what I said above and see if it's logically assigned to the next increment of IP address. Sometimes you'll be in a situation with a gateway router and can scan the gateway. There are numerous ways to go about this but don't worry about this right now if that doesn't make sense just continue to learn and you'll get it (:

SirBaronBamboozle · 6 yr. ago

Go into preference, set up a NAT-shared network, then put them both into that NAT-shared

Host-only means it's only connected to your windows or whatever the

```
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
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://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.48 seconds

┌──(panda㉿kali)-[~]
└─$ 
```

Source: https://www.baeldung.com/linux/close-port-command-line

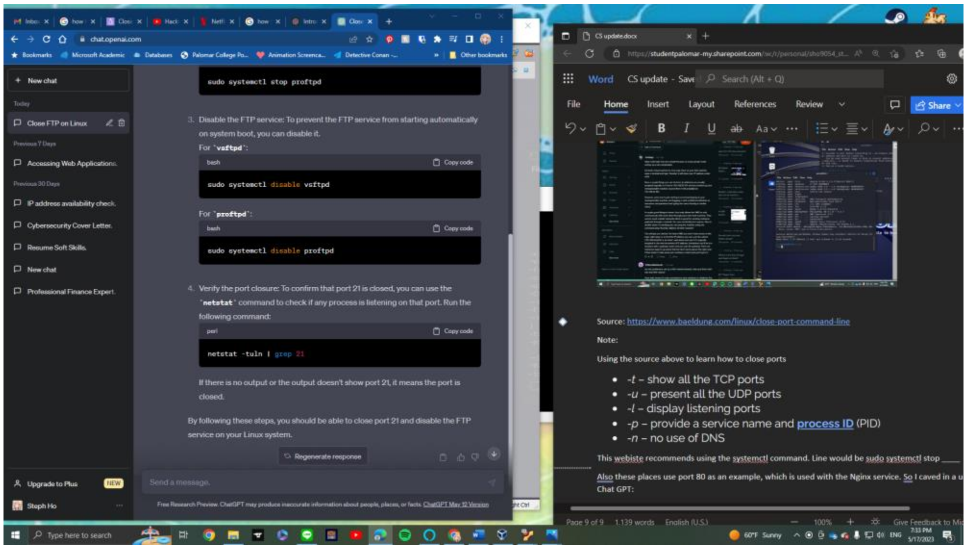
Note:

Using the source above to learn how to close ports

- *-t* – show all the TCP ports
- *-u* – present all the UDP ports
- *-l* – display listening ports
- *-p* – provide a service name and **process ID** (PID)
- *-n* – no use of DNS

This webiste recommends using the systemctl command. Line would be sudo systemctl stop _____

Also these places use port 80 as an example, which is used with the Nginx service. So I caved in a used Chat GPT:



```
sudo systemctl stop proftpd
```

3. Disable the FTP service: To prevent the FTP service from starting automatically on system boot, you can disable it.
   For `vsftpd`:

```bash
sudo systemctl disable vsftpd
```

   For `proftpd`:

```bash
sudo systemctl disable proftpd
```

4. Verify the port closure: To confirm that port 21 is closed, you can use the `netstat` command to check if any process is listening on that port. Run the following command:

```perl
netstat -tuln | grep 21
```

   If there is no output or the output doesn't show port 21, it means the port is closed.

By following these steps, you should be able to close port 21 and disable the FTP service on your Linux system.

Free Research Preview. ChatGPT may produce inaccurate information about people, places, or facts. ChatGPT May 12 Version

Source: https://www.baeldung.com/linux/close-port-command-line

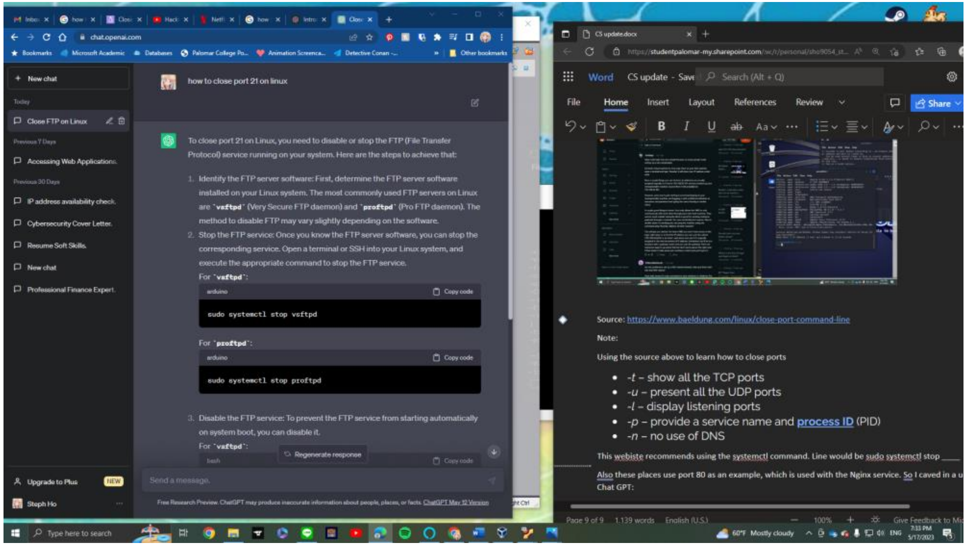
Note:

Using the source above to learn how to close ports

- *-t* – show all the TCP ports
- *-u* – present all the UDP ports
- *-l* – display listening ports
- *-p* – provide a service name and process ID (PID)
- *-n* – no use of DNS

This webiste recommends using the systemctl command. Line would be sudo systemctl stop ____

Also these places use port 80 as an example, which is used with the Nginx service. So I caved in a u
Chat GPT:



how to close port 21 on linux

To close port 21 on Linux, you need to disable or stop the FTP (File Transfer Protocol) service running on your system. Here are the steps to achieve that:

1. Identify the FTP server software: First, determine the FTP server software installed on your Linux system. The most commonly used FTP servers on Linux are `vsftpd` (Very Secure FTP daemon) and `proftpd` (Pro FTP daemon). The method to disable FTP may vary slightly depending on the software.
2. Stop the FTP service: Once you know the FTP server software, you can stop the corresponding service. Open a terminal or SSH into your Linux system, and execute the appropriate command to stop the FTP service.
   For `vsftpd`:

```arduino
sudo systemctl stop vsftpd
```

   For `proftpd`:

```arduino
sudo systemctl stop proftpd
```

3. Disable the FTP service: To prevent the FTP service from starting automatically on system boot, you can disable it.
   For `vsftpd`:

Source: https://www.baeldung.com/linux/close-port-command-line

Note:

Using the source above to learn how to close ports

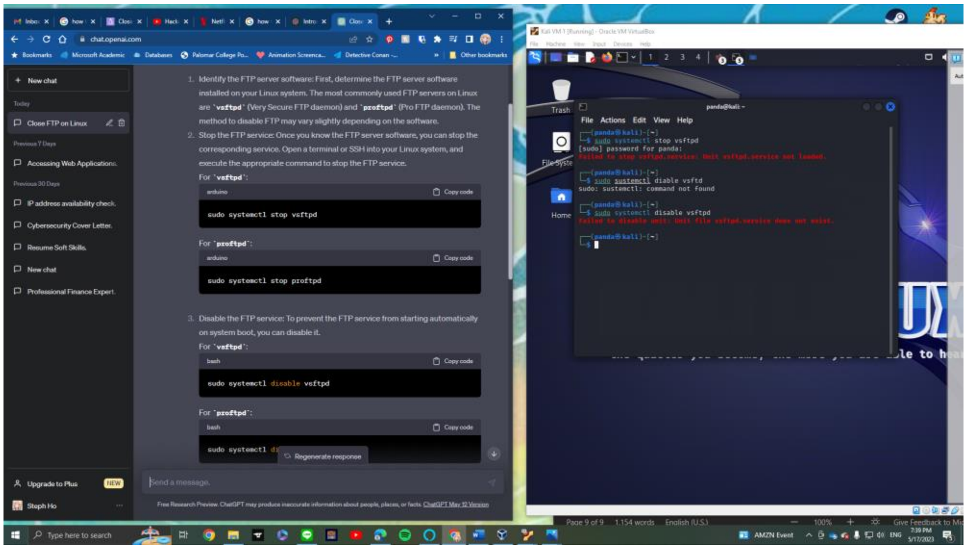
- *-t* – show all the TCP ports
- *-u* – present all the UDP ports
- *-l* – display listening ports
- *-p* – provide a service name and process ID (PID)
- *-n* – no use of DNS

This webiste recommends using the systemctl command. Line would be sudo systemctl stop ____

Also these places use port 80 as an example, which is used with the Nginx service. So I caved in a u
Chat GPT:

1. Identify the FTP server software: vsftpd
2. Used command sudo systemctl stop vsftpd

3. It failed and tried to disable but then says it doesn’t exist

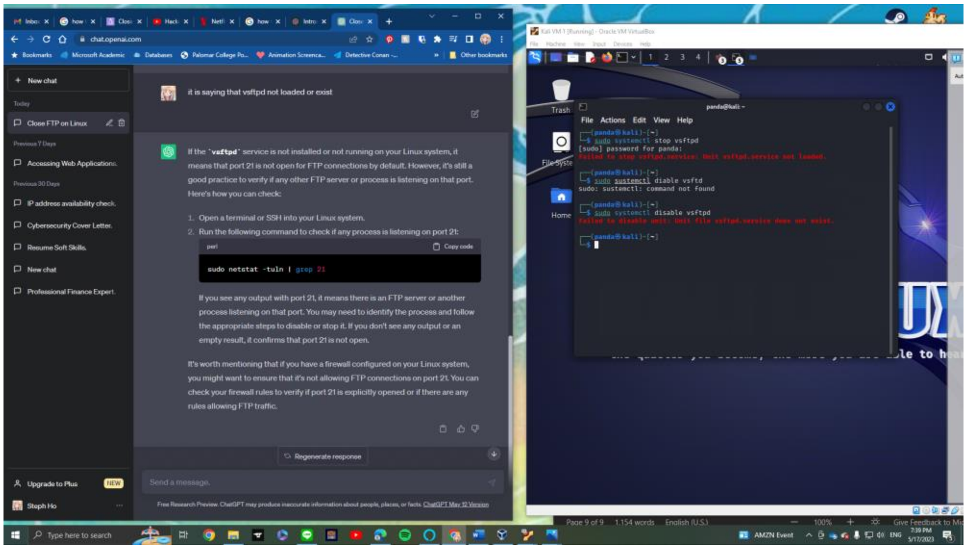


1. Identify the FTP server software: First, determine the FTP server software installed on your Linux system. The most commonly used FTP servers on Linux are `vsftpd` (Very Secure FTP daemon) and `proftpd` (Pro FTP daemon). The method to disable FTP may vary slightly depending on the software.
2. Stop the FTP service: Once you know the FTP server software, you can stop the corresponding service. Open a terminal or SSH into your Linux system, and execute the appropriate command to stop the FTP service.
   For `vsftpd`:
   ```arduino
   sudo systemctl stop vsftpd
   ```
   For `proftpd`:
   ```arduino
   sudo systemctl stop proftpd
   ```
3. Disable the FTP service: To prevent the FTP service from starting automatically on system boot, you can disable it.
   For `vsftpd`:
   ```bash
   sudo systemctl disable vsftpd
   ```
   For `proftpd`:
   ```bash
   sudo systemctl di
   ```

Free Research Preview. ChatGPT may produce inaccurate information about people, places, or facts. ChatGPT May 12 Version

```
┌──(panda㉿kali)-[~]
└─$ sudo systemctl stop vsftpd
[sudo] password for panda:
Failed to stop vsftpd.service: Unit vsftpd.service not loaded.

┌──(panda㉿kali)-[~]
└─$ sudo sustemctl diable vsftd
sudo: sustemctl: command not found

┌──(panda㉿kali)-[~]
└─$ sudo systemctl disable vsftpd
Failed to disable unit: Unit file vsftpd.service does not exist.

┌──(panda㉿kali)-[~]
└─$ 
```

4. Suggests to verify if other FTP server or process is listening on port 21



it is saying that vsftpd not loaded or exist

If the `vsftpd` service is not installed or not running on your Linux system, it means that port 21 is not open for FTP connections by default. However, it's still a good practice to verify if any other FTP server or process is listening on that port. Here's how you can check:

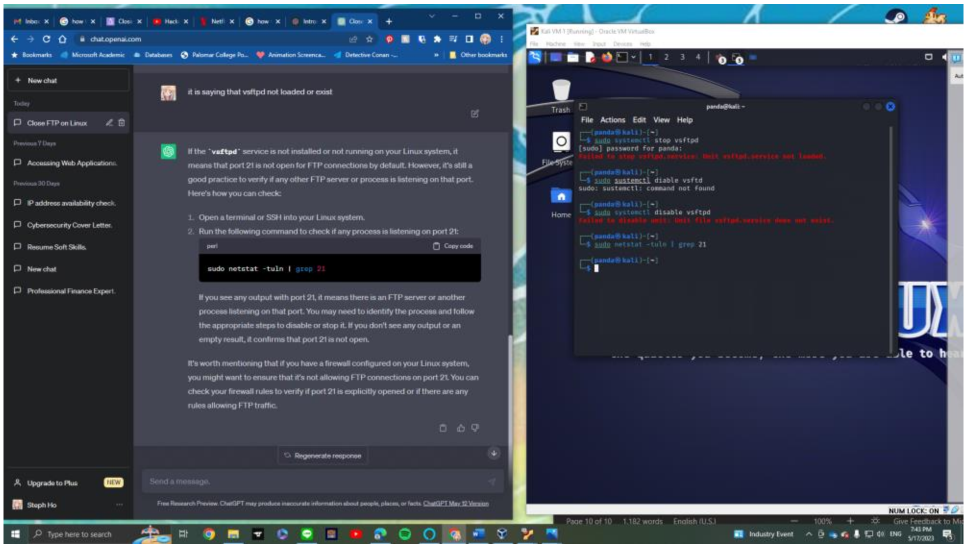
1. Open a terminal or SSH into your Linux system.
2. Run the following command to check if any process is listening on port 21:
   ```perl
   sudo netstat -tuln | grep 21
   ```
   If you see any output with port 21, it means there is an FTP server or another process listening on that port. You may need to identify the process and follow the appropriate steps to disable or stop it. If you don't see any output or an empty result, it confirms that port 21 is not open.

It's worth mentioning that if you have a firewall configured on your Linux system, you might want to ensure that it's not allowing FTP connections on port 21. You can check your firewall rules to verify if port 21 is explicitly opened or if there are any rules allowing FTP traffic.

Free Research Preview. ChatGPT may produce inaccurate information about people, places, or facts. ChatGPT May 12 Version

```
┌──(panda㉿kali)-[~]
└─$ sudo systemctl stop vsftpd
[sudo] password for panda:
Failed to stop vsftpd.service: Unit vsftpd.service not loaded.

┌──(panda㉿kali)-[~]
└─$ sudo sustemctl diable vsftd
sudo: sustemctl: command not found

┌──(panda㉿kali)-[~]
└─$ sudo systemctl disable vsftpd
Failed to disable unit: Unit file vsftpd.service does not exist.

┌──(panda㉿kali)-[~]
└─$ 
```

5. Nothing opened after



it is saying that vsftpd not loaded or exist

If the `vsftpd` service is not installed or not running on your Linux system, it means that port 21 is not open for FTP connections by default. However, it's still a good practice to verify if any other FTP server or process is listening on that port. Here's how you can check:

1. Open a terminal or SSH into your Linux system.
2. Run the following command to check if any process is listening on port 21:

```perl
sudo netstat -tuln | grep 21
```

If you see any output with port 21, it means there is an FTP server or another process listening on that port. You may need to identify the process and follow the appropriate steps to disable or stop it. If you don't see any output or an empty result, it confirms that port 21 is not open.

It's worth mentioning that if you have a firewall configured on your Linux system, you might want to ensure that it's not allowing FTP connections on port 21. You can check your firewall rules to verify if port 21 is explicitly opened or if there are any rules allowing FTP traffic.

Regenerate response
Send a message.
Free Research Preview. ChatGPT may produce inaccurate information about people, places, or facts. ChatGPT May 12 Version
Kali VM 1 [Running] - Oracle VM VirtualBox
Trash
File System
Home
panda@kali: ~
File Actions Edit View Help

```
┌──(panda㉿kali)-[~]
└─$ sudo systemctl stop vsftpd
[sudo] password for panda:
Failed to stop vsftpd.service: Unit vsftpd.service not loaded.

┌──(panda㉿kali)-[~]
└─$ sudo sustemctl diable vsftd
sudo: sustemctl: command not found

┌──(panda㉿kali)-[~]
└─$ sudo systemctl disable vsftpd
Failed to disable unit: Unit file vsftpd.service does not exist.

┌──(panda㉿kali)-[~]
└─$ sudo netstat -tuln | grep 21

┌──(panda㉿kali)-[~]
└─$ 
```

6.