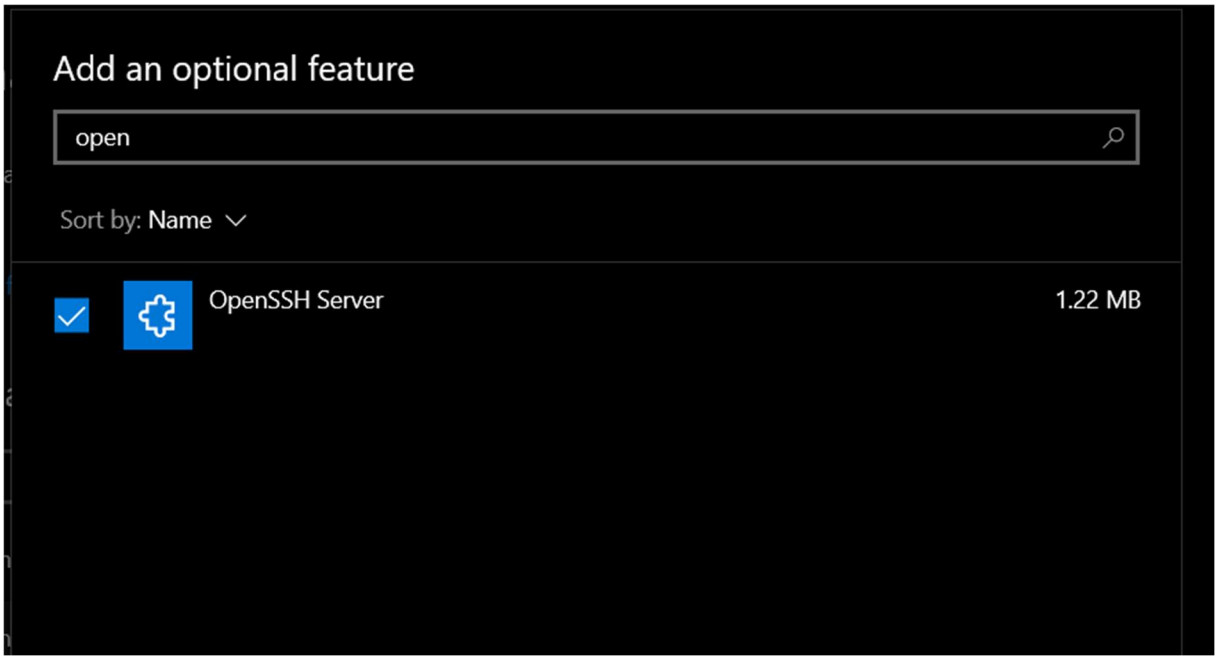
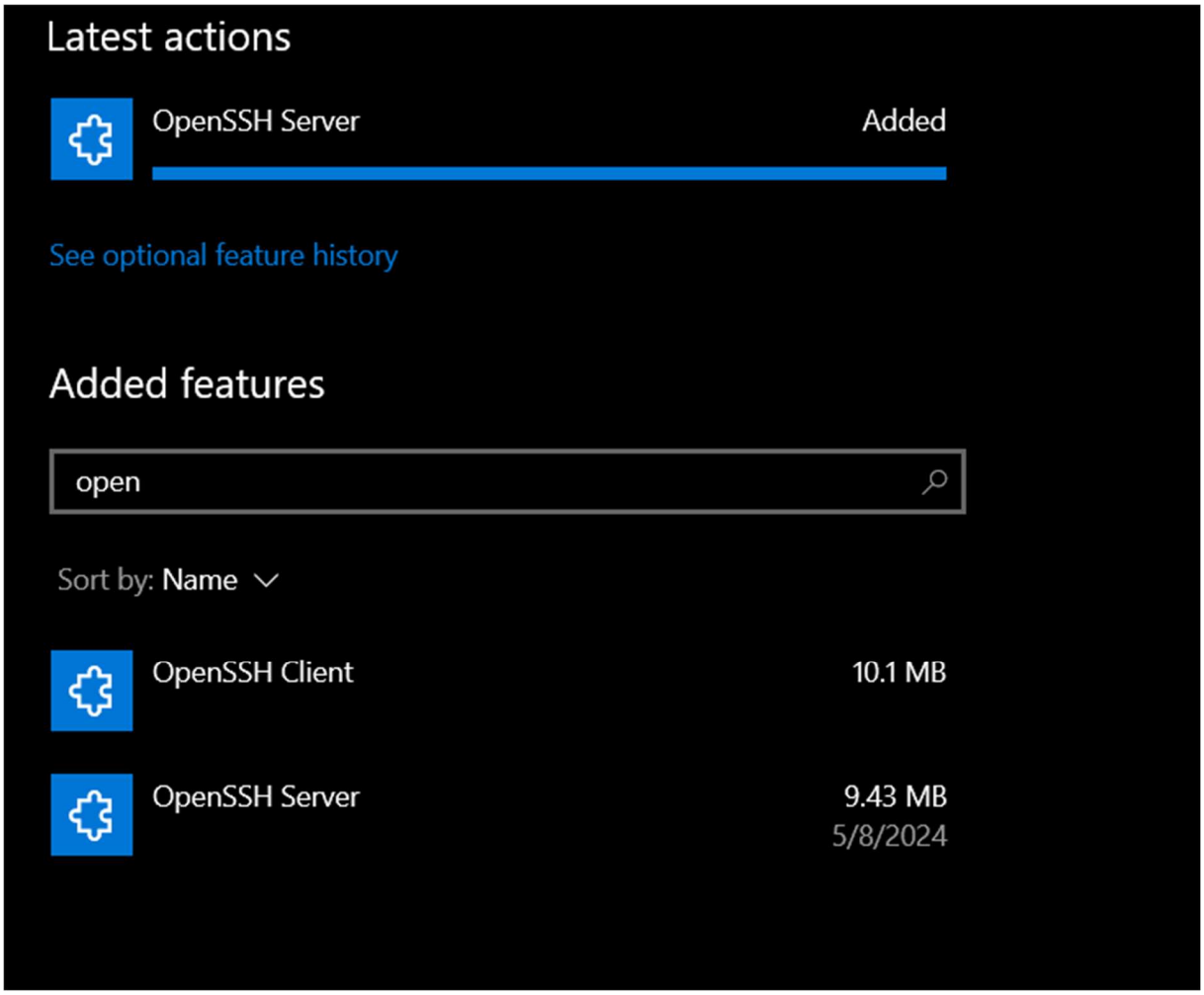
Cyber Security Fundamentals Lab: Stateful Packet Filtering Firewall Configuration et Deployment

Gdoura Ahlem INDP2A

Preliminary configuration of Host 1

1.





2.

```
PS C:\Windows\system32> start-service sshd
```

3.

```
PS C:\Windows\system32> Set-Service -Name sshd -StartupType 'Automatic'
```

4.

```
PS C:\Windows\system32> Get-NetFirewallRule -Name *ssh*


Name                          : OpenSSH-Server-In-TCP
DisplayName                   : OpenSSH SSH Server (sshd)
Description                   : Inbound rule for OpenSSH SSH Server (sshd)
DisplayGroup                  : OpenSSH Server
Group                         : OpenSSH Server
Enabled                       : True
Profile                       : Any
Platform                      : {}
Direction                     : Inbound
Action                        : Allow
EdgeTraversalPolicy           : Block
LooseSourceMapping            : False
LocalOnlyMapping              : False
Owner                         :
PrimaryStatus                 : OK
Status                        : The rule was parsed successfully from the store. (65536)
EnforcementStatus             : NotApplicable
PolicyStoreSource             : PersistentStore
PolicyStoreSourceType         : Local
RemoteDynamicKeywordAddresses :
PolicyAppId                   :
```

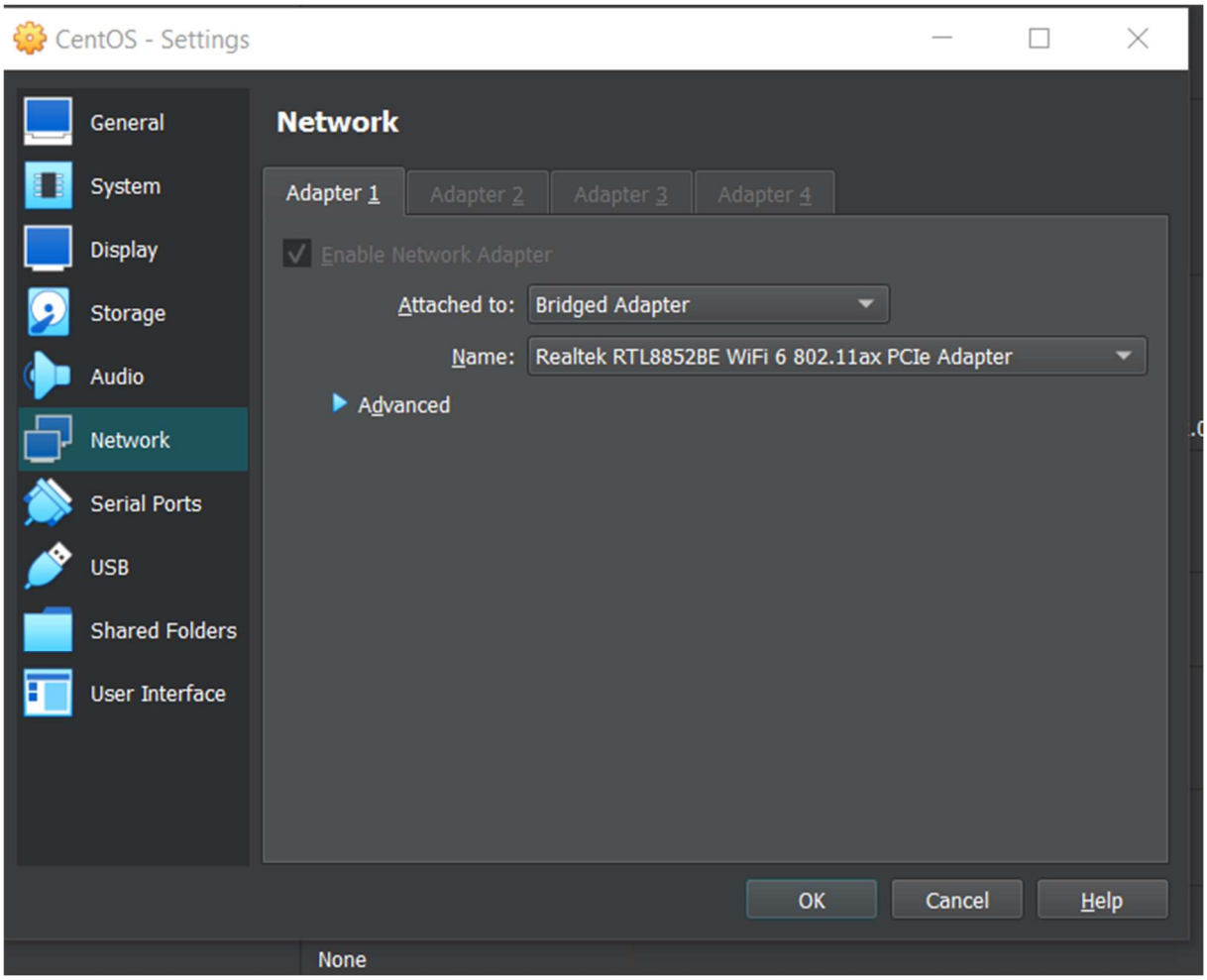
5.

```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . : Home
   Link-local IPv6 Address . . . . . : fe80::15fd:d79:22e0:b931%16
   IPv4 Address. . . . . . . . . . . : 192.168.1.11
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1
```

```
PS C:\Windows\system32> ssh USER@192.168.1.11
The authenticity of host '192.168.1.11 (192.168.1.11)' can't be established.
ECDSA key fingerprint is SHA256:nWcipfJWZ8+Ngw1VDp9OgWvJOjsX4dQgs1M2F71D74A.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.11' (ECDSA) to the list of known hosts.
USER@192.168.1.11's password:
```

```
user@DESKTOP-T8UB7J5 C:\Users\USER>
```

Preliminary configuration of Host 2

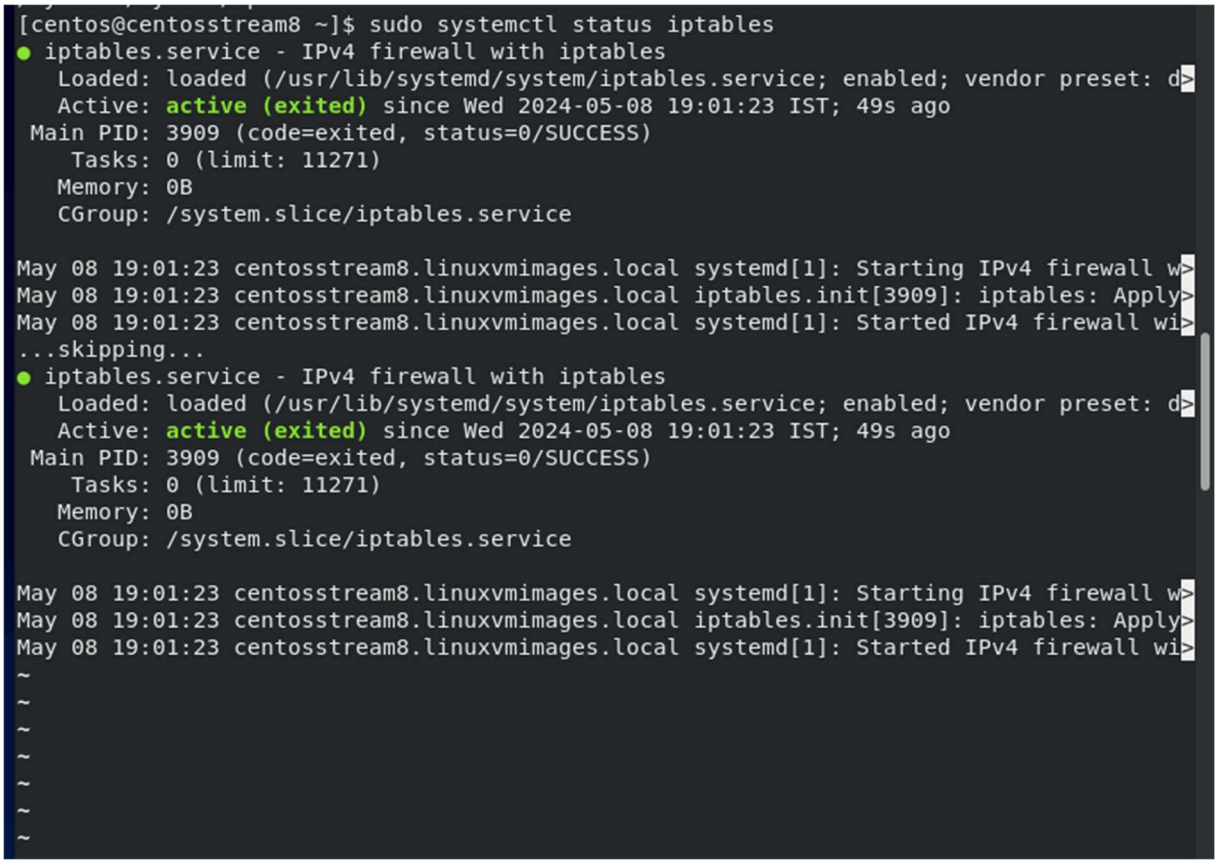

CentOS - Settings
General
System
Display
Storage
Audio
Network
Serial Ports
USB
Shared Folders
User Interface
Network
Adapter 1
Adapter 2
Adapter 3
Adapter 4
Enable Network Adapter
Attached to:
Bridged Adapter
Name:
Realtek RTL8852BE WiFi 6 802.11ax PCIe Adapter
Advanced
OK
Cancel
Help
None

1.

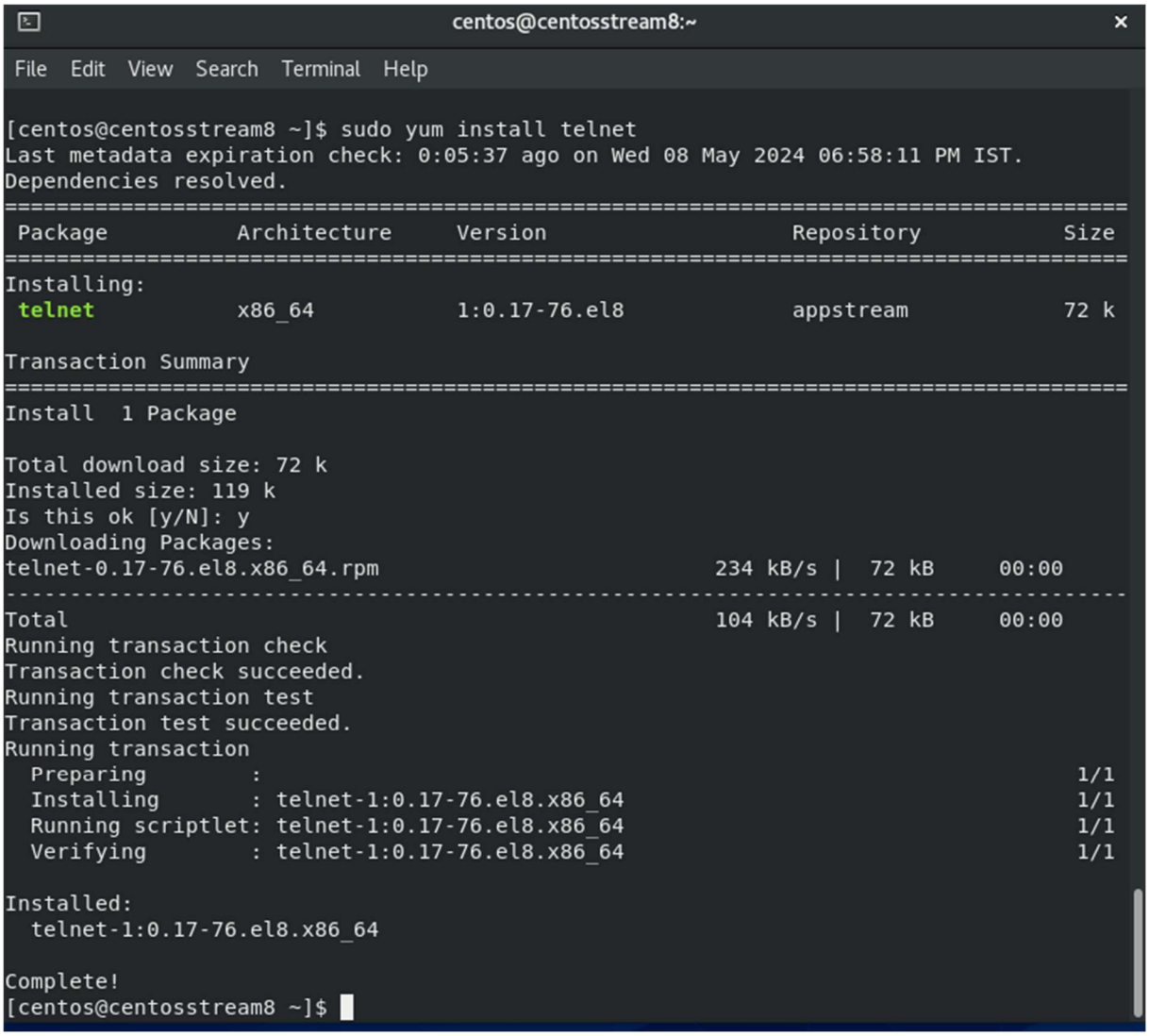
```
[centos@centosstream8 ~]$ sudo yum install iptables-services
CentOS Stream 8 - AppStream                     3.0 MB/s |  28 MB     00:09
CentOS Stream 8 - BaseOS                        2.3 MB/s |  10 MB     00:04
CentOS Stream 8 - Extras                         28 kB/s |  18 kB     00:00
Dependencies resolved.
================================================================================
 Package                 Architecture  Version             Repository     Size
================================================================================
Installing:
 iptables-services       x86_64        1.8.5-11.el8        baseos         65 k
Upgrading:
 iptables                x86_64        1.8.5-11.el8        baseos        671 k
 iptables-ebtables       x86_64        1.8.5-11.el8        baseos         74 k
 iptables-libs           x86_64        1.8.5-11.el8        baseos        103 k

Transaction Summary
================================================================================
Install  1 Package
Upgrade  3 Packages

Total download size: 913 k
Is this ok [y/N]: y
Downloading Packages:
(1/4): iptables-ebtables-1.8.5-11.el8.x86_64.rp 110 kB/s |  74 kB     00:00
(2/4): iptables-services-1.8.5-11.el8.x86_64.rp  87 kB/s |  65 kB     00:00
(3/4): iptables-libs-1.8.5-11.el8.x86_64.rpm    373 kB/s | 103 kB     00:00
(4/4): iptables-1.8.5-11.el8.x86_64.rpm         631 kB/s | 671 kB     00:01
--------------------------------------------------------------------------------
Total                                           637 kB/s | 913 kB     00:01
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
```

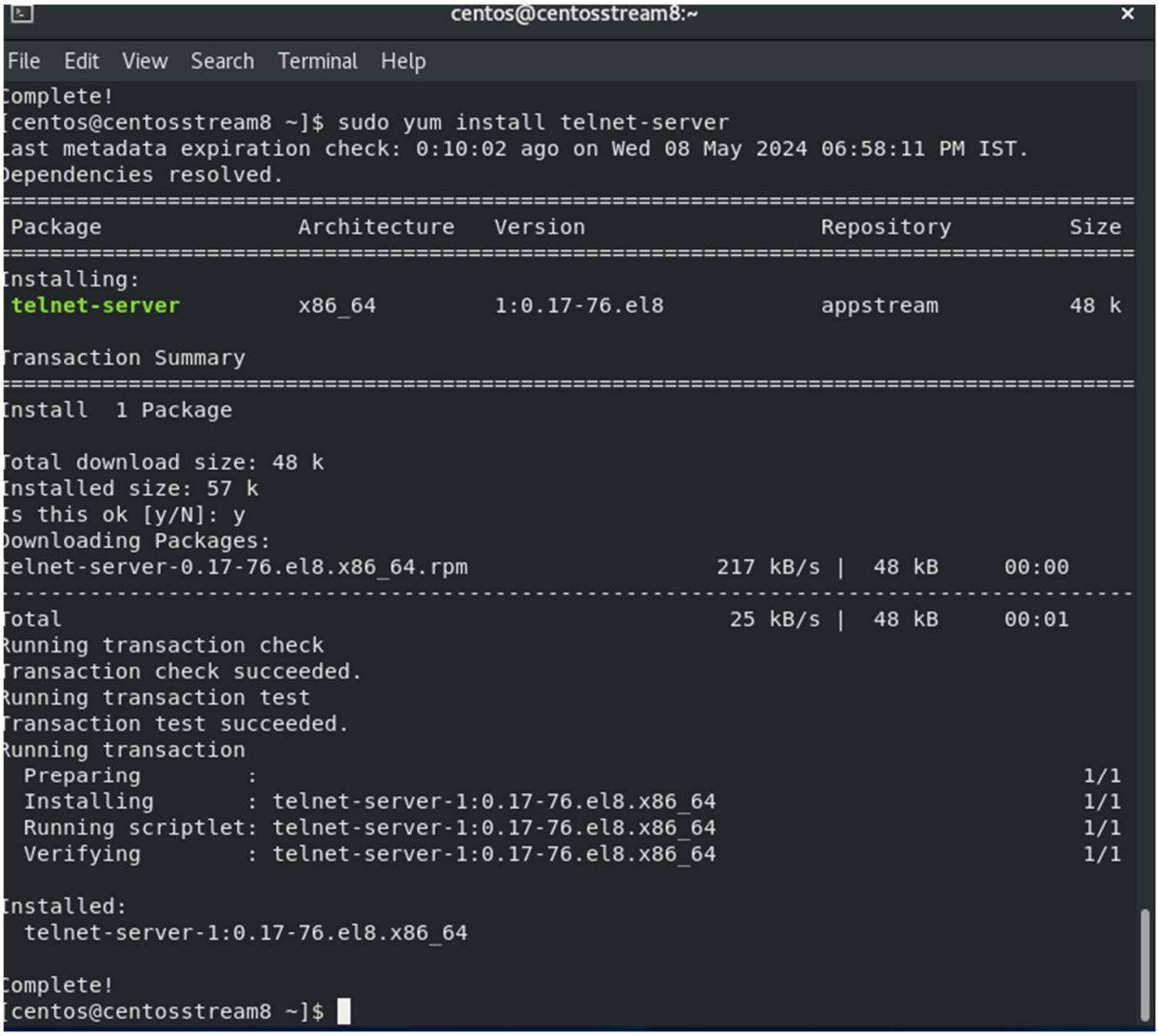
```
[centos@centosstream8 ~]$ sudo systemctl start iptables
[centos@centosstream8 ~]$ sudo systemctl enable iptables
Created symlink /etc/systemd/system/multi-user.target.wants/iptables.service → /usr/lib
/systemd/system/iptables.service.
[centos@centosstream8 ~]$
```

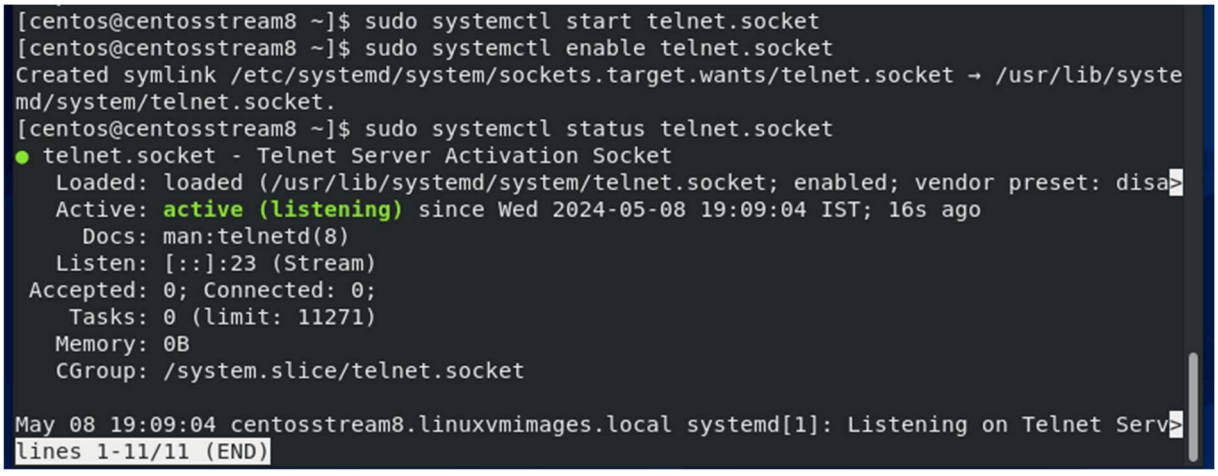
2.


[centos@centosstream8 ~]$ sudo systemctl status iptables
● iptables.service - IPv4 firewall with iptables
Loaded: loaded (/usr/lib/systemd/system/iptables.service; enabled; vendor preset: d>
Active: active (exited) since Wed 2024-05-08 19:01:23 IST; 49s ago
Main PID: 3909 (code=exited, status=0/SUCCESS)
Tasks: 0 (limit: 11271)
Memory: 0B
CGroup: /system.slice/iptables.service
May 08 19:01:23 centosstream8.linuxvmimages.local systemd[1]: Starting IPv4 firewall w>
May 08 19:01:23 centosstream8.linuxvmimages.local iptables.init[3909]: iptables: Apply>
May 08 19:01:23 centosstream8.linuxvmimages.local systemd[1]: Started IPv4 firewall wi>
...skipping...
● iptables.service - IPv4 firewall with iptables
Loaded: loaded (/usr/lib/systemd/system/iptables.service; enabled; vendor preset: d>
Active: active (exited) since Wed 2024-05-08 19:01:23 IST; 49s ago
Main PID: 3909 (code=exited, status=0/SUCCESS)
Tasks: 0 (limit: 11271)
Memory: 0B
CGroup: /system.slice/iptables.service
May 08 19:01:23 centosstream8.linuxvmimages.local systemd[1]: Starting IPv4 firewall w>
May 08 19:01:23 centosstream8.linuxvmimages.local iptables.init[3909]: iptables: Apply>
May 08 19:01:23 centosstream8.linuxvmimages.local systemd[1]: Started IPv4 firewall wi>
~
~
~
~
~
~
~

3.


centos@centosstream8:~
File Edit View Search Terminal Help
[centos@centosstream8 ~]$ sudo yum install telnet
Last metadata expiration check: 0:05:37 ago on Wed 08 May 2024 06:58:11 PM IST.
Dependencies resolved.
Package Architecture Version Repository Size
Installing:
telnet x86_64 1:0.17-76.el8 appstream 72 k
Transaction Summary
Install 1 Package
Total download size: 72 k
Installed size: 119 k
Is this ok [y/N]: y
Downloading Packages:
telnet-0.17-76.el8.x86_64.rpm 234 kB/s | 72 kB 00:00
Total 104 kB/s | 72 kB 00:00
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
Preparing : 1/1
Installing : telnet-1:0.17-76.el8.x86_64 1/1
Running scriptlet: telnet-1:0.17-76.el8.x86_64 1/1
Verifying : telnet-1:0.17-76.el8.x86_64 1/1
Installed:
telnet-1:0.17-76.el8.x86_64
Complete!
[centos@centosstream8 ~]$


centos@centosstream8:~
File Edit View Search Terminal Help
Complete!
[centos@centosstream8 ~]$ sudo yum install telnet-server
Last metadata expiration check: 0:10:02 ago on Wed 08 May 2024 06:58:11 PM IST.
Dependencies resolved.
Package Architecture Version Repository Size
Installing:
telnet-server x86_64 1:0.17-76.el8 appstream 48 k
Transaction Summary
Install 1 Package
Total download size: 48 k
Installed size: 57 k
Is this ok [y/N]: y
Downloading Packages:
telnet-server-0.17-76.el8.x86_64.rpm 217 kB/s | 48 kB 00:00
Total 25 kB/s | 48 kB 00:01
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
Preparing : 1/1
Installing : telnet-server-1:0.17-76.el8.x86_64 1/1
Running scriptlet: telnet-server-1:0.17-76.el8.x86_64 1/1
Verifying : telnet-server-1:0.17-76.el8.x86_64 1/1
Installed:
telnet-server-1:0.17-76.el8.x86_64
Complete!
[centos@centosstream8 ~]$


[centos@centosstream8 ~]$ sudo systemctl start telnet.socket
[centos@centosstream8 ~]$ sudo systemctl enable telnet.socket
Created symlink /etc/systemd/system/sockets.target.wants/telnet.socket → /usr/lib/systemd/system/telnet.socket.
[centos@centosstream8 ~]$ sudo systemctl status telnet.socket
● telnet.socket - Telnet Server Activation Socket
Loaded: loaded (/usr/lib/systemd/system/telnet.socket; enabled; vendor preset: disa>
Active: active (listening) since Wed 2024-05-08 19:09:04 IST; 16s ago
Docs: man:telnetd(8)
Listen: [::]:23 (Stream)
Accepted: 0; Connected: 0;
Tasks: 0 (limit: 11271)
Memory: 0B
CGroup: /system.slice/telnet.socket
May 08 19:09:04 centosstream8.linuxvmimages.local systemd[1]: Listening on Telnet Serv>
lines 1-11/11 (END)

4.

```
[centos@centosstream8 ~]$ sudo yum install httpd
Last metadata expiration check: 0:12:20 ago on Wed 08 May 2024 06:58:11 PM IST.
Dependencies resolved.
================================================================================
 Package              Arch     Version                                  Repository   Size
================================================================================
Installing:
 httpd                x86_64   2.4.37-64.module_el8+965+1ad5c49d        appstream   1.6 M
Installing dependencies:
 apr                  x86_64   1.6.3-12.el8                             appstream   129 k
 apr-util             x86_64   1.6.1-9.el8                              appstream   106 k
 centos-logos-httpd   noarch   85.8-2.el8                               appstream    75 k
 httpd-filesystem     noarch   2.4.37-64.module_el8+965+1ad5c49d        appstream    44 k
 httpd-tools          x86_64   2.4.37-64.module_el8+965+1ad5c49d        appstream   112 k
 mod_http2            x86_64   1.15.7-10.module_el8+1009+c203647a       appstream   156 k
Installing weak dependencies:
 apr-util-bdb         x86_64   1.6.1-9.el8                              appstream    25 k
 apr-util-openssl     x86_64   1.6.1-9.el8                              appstream    27 k
Enabling module streams:
 httpd                         2.4

Transaction Summary
================================================================================
Install  9 Packages

Total download size: 2.2 M
Installed size: 5.6 M
Is this ok [y/N]: y
Downloading Packages:
(1/9): apr-util-bdb-1.6.1-9.el8.x86_64.rpm              93 kB/s |  25 kB     00:00
```

```
Installed:
  apr-1.6.3-12.el8.x86_64
  apr-util-1.6.1-9.el8.x86_64
  apr-util-bdb-1.6.1-9.el8.x86_64
  apr-util-openssl-1.6.1-9.el8.x86_64
  centos-logos-httpd-85.8-2.el8.noarch
  httpd-2.4.37-64.module_el8+965+1ad5c49d.x86_64
  httpd-filesystem-2.4.37-64.module_el8+965+1ad5c49d.noarch
  httpd-tools-2.4.37-64.module_el8+965+1ad5c49d.x86_64
  mod_http2-1.15.7-10.module_el8+1009+c203647a.x86_64

Complete!
```

```
[centos@centosstream8 ~]$ sudo systemctl start httpd
[centos@centosstream8 ~]$ sudo systemctl enable httpd
Created symlink /etc/systemd/system/multi-user.target.wants/httpd.service → /usr/lib/sy
stemd/system/httpd.service.
[centos@centosstream8 ~]$ sudo systemctl status httpd
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; enabled; vendor preset: disa>
   Active: active (running) since Wed 2024-05-08 19:11:29 IST; 16s ago
     Docs: man:httpd.service(8)
 Main PID: 5220 (httpd)
   Status: "Running, listening on: port 80"
    Tasks: 213 (limit: 11271)
   Memory: 19.1M
   CGroup: /system.slice/httpd.service
           ├─5220 /usr/sbin/httpd -DFOREGROUND
           ├─5227 /usr/sbin/httpd -DFOREGROUND
           ├─5228 /usr/sbin/httpd -DFOREGROUND
           ├─5229 /usr/sbin/httpd -DFOREGROUND
           └─5230 /usr/sbin/httpd -DFOREGROUND

May 08 19:11:29 centosstream8.linuxvmimages.local systemd[1]: Starting The Apache HTTP>
May 08 19:11:29 centosstream8.linuxvmimages.local systemd[1]: Started The Apache HTTP >
May 08 19:11:29 centosstream8.linuxvmimages.local httpd[5220]: Server configured, list>
lines 1-18/18 (END)
```

5.

```
[centos@centosstream8 ~]$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

6.

```
[centos@centosstream8 ~]$ ssh USER@192.168.1.11
The authenticity of host '192.168.1.11 (192.168.1.11)' can't be established.
ECDSA key fingerprint is SHA256:nWcipfJWZ8+NgwlVDp9OgWvJOjsX4dQgs1M2F71D74A.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.11' (ECDSA) to the list of known hosts.
USER@192.168.1.11's password:
```

```
Microsoft Windows [Version 10.0.19045.4291]
(c) Microsoft Corporation. All rights reserved.

user@DESKTOP-T8UB7J5 C:\Users\USER>
```

7.

```
[centos@centosstream8 ~]$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.12  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::a00:27ff:fe2f:d5f6  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:2f:d5:f6  txqueuelen 1000  (Ethernet)
        RX packets 33107  bytes 46479765 (44.3 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 18411  bytes 1241977 (1.1 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

```
user@DESKTOP-T8UB7J5 C:\Users\USER>ping 192.168.1.12

Pinging 192.168.1.12 with 32 bytes of data:
Reply from 192.168.1.12: bytes=32 time<1ms TTL=64
Reply from 192.168.1.12: bytes=32 time=1ms TTL=64
Reply from 192.168.1.12: bytes=32 time<1ms TTL=64
Reply from 192.168.1.12: bytes=32 time=1ms TTL=64

Ping statistics for 192.168.1.12:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Access control policy implementation on iptables :

9.

```
[centos@centosstream8 ~]$ sudo iptables -P INPUT DROP
[centos@centosstream8 ~]$ sudo iptables -P OUTPUT DROP
```

10.

```
[centos@centosstream8 ~]$ sudo iptables -L --line-num
Chain INPUT (policy DROP)
num  target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
num  target     prot opt source               destination

Chain OUTPUT (policy DROP)
num  target     prot opt source               destination
[centos@centosstream8 ~]$
```

11.

```
user@DESKTOP-T8UB7J5 C:\Users\USER>ping 192.168.1.12

Pinging 192.168.1.12 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.12:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

12.

```
[centos@centosstream8 ~]$ sudo iptables -A OUTPUT -p tcp -s 192.168.1.12 -d 192.168.1.11 --dport 22
-j ACCEPT
```

13.

```
[centos@centosstream8 ~]$ sudo iptables -A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
```

14.

```
[centos@centosstream8 ~]$ sudo iptables -L --line-num
Chain INPUT (policy DROP)
num  target     prot opt source               destination
1    ACCEPT     all  --  anywhere             anywhere             state RELATED,ESTABLISHED

Chain FORWARD (policy ACCEPT)
num  target     prot opt source               destination

Chain OUTPUT (policy DROP)
num  target     prot opt source               destination
1    ACCEPT     tcp  --  centosstream8.linuxvmimages.local  192.168.1.11         tcp dpt:ssh
```

15.

```
[centos@centosstream8 ~]$ ssh USER@192.168.1.11
USER@192.168.1.11's password:
```

```
Microsoft Windows [Version 10.0.19045.4291]
(c) Microsoft Corporation. All rights reserved.

user@DESKTOP-T8UB7J5 C:\Users\USER>
```

16.

```
user@DESKTOP-T8UB7J5 C:\Users\USER> nslookup www.portquiz.net
Server:  UnKnown
Address:  193.95.57.20

Non-authoritative answer:
Name:    portquiz.net
Address:  35.180.139.74
Aliases:  www.portquiz.net
```

17.

```
[centos@centosstream8 ~]$ sudo iptables -A OUTPUT -s 192.168.1.11 -d 35.180.139.
74 -j DROP
```

```
[centos@centosstream8 ~]$ sudo iptables -A OUTPUT -s 192.168.1.12 -p TCP -m mult
iport --dports 443,80 -j ACCEPT
```

18.

Why did we choose to deny all traffic going to www.portquiz.net rather

than TCP traffic on ports 80 and 443?

to prevent access to other services (there could be more than just http and

https)

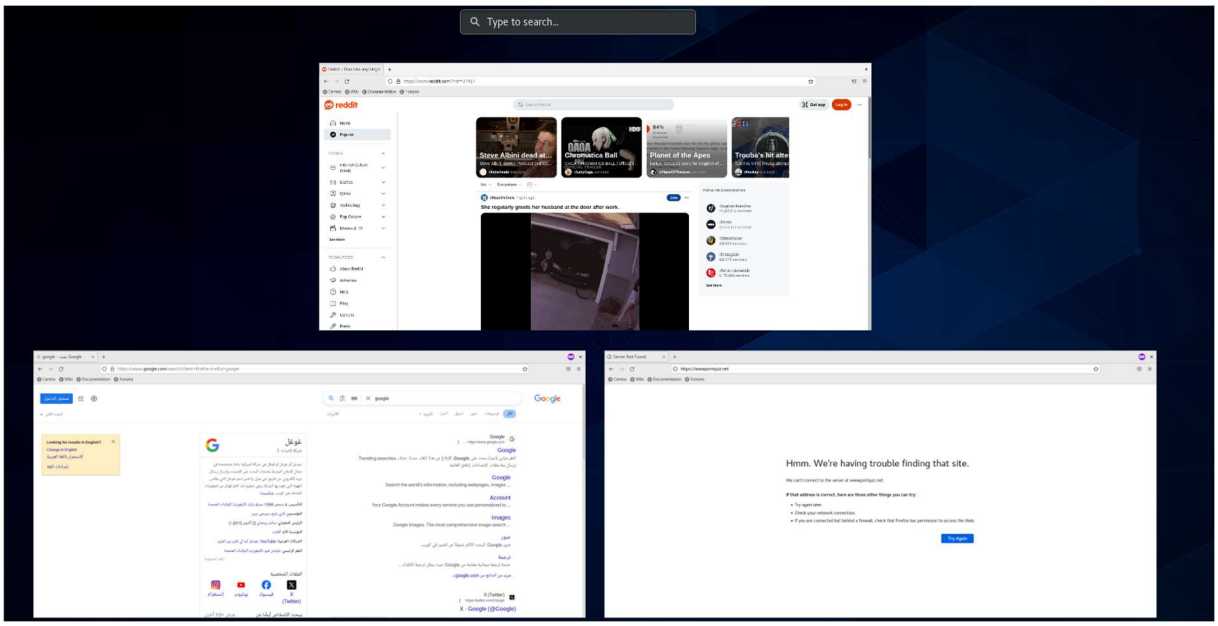
19.

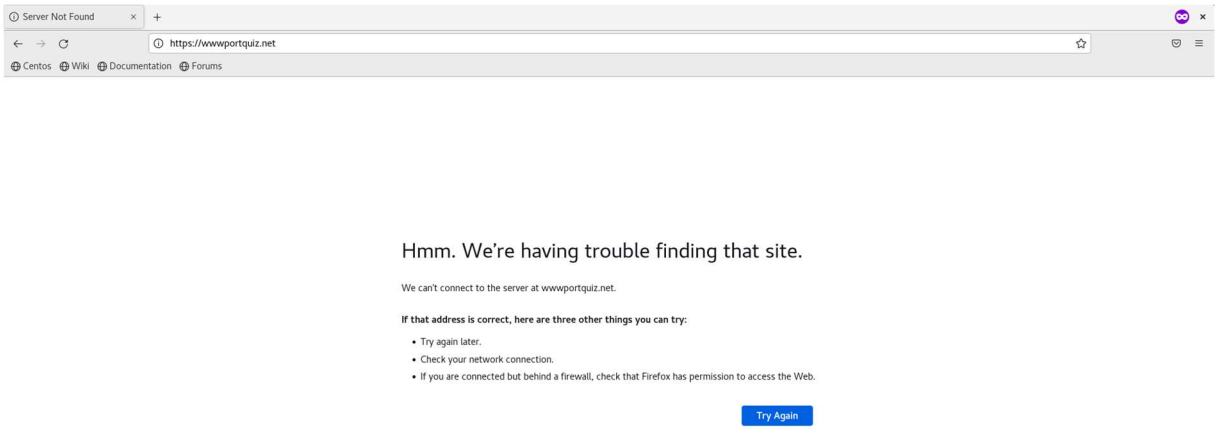
```
[centos@centosstream8 ~]$ sudo iptables -A OUTPUT -p udp -s 192.168.1.12 -d 193.
95.57.20 --dport 53 -j ACCEPT
```

20.

```
[centos@centosstream8 ~]$ host www.portquiz.net
www.portquiz.net is an alias for portquiz.net.
portquiz.net has address 35.180.139.74
portquiz.net mail is handled by 1 mx4.mail.ovh.net.
portquiz.net mail is handled by 10 mx3.mail.ovh.net.
[centos@centosstream8 ~]$
```

21.





22.

```
[centos@centosstream8 ~]$ sudo iptables -nvL
Chain INPUT (policy DROP 1166 packets, 163K bytes)
 pkts bytes target     prot opt in     out     source               destination
  477  191K ACCEPT     all  --  *      *       0.0.0.0/0            0.0.0.0/0           state RELATED,ESTABLISHED

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy DROP 113 packets, 8465 bytes)
 pkts bytes target     prot opt in     out     source               destination
   24  3553 ACCEPT     tcp  --  *      *       192.168.1.12         192.168.1.11        tcp dpt:22
    0     0 DROP       all  --  *      *       192.168.1.11         35.180.139.74
  338 54680 ACCEPT     tcp  --  *      *       192.168.1.12         0.0.0.0/0           multiport dports 443,80
  103  7094 ACCEPT     udp  --  *      *       192.168.1.12         193.95.57.20        udp dpt:53
```

23.

```
[centos@centosstream8 ~]$ sudo iptables -A INPUT -p icmp --icmp-type echo-request -d
 192.168.1.12 -j LOG --log-prefix "echo request received"
```

```
[centos@centosstream8 ~]$ sudo iptables -L --line-num
Chain INPUT (policy DROP)
num  target     prot opt source               destination
1    ACCEPT     all  --  anywhere             anywhere             state RELATED,ESTABLISHED
2    LOG        icmp --  anywhere             centosstream8.linuxvmimages.local  icmp echo-request LOG level warning prefix "echo request receiv
ed"

Chain FORWARD (policy ACCEPT)
num  target     prot opt source               destination

Chain OUTPUT (policy DROP)
num  target     prot opt source               destination
1    ACCEPT     tcp  --  centosstream8.linuxvmimages.local  192.168.1.11         tcp dpt:ssh
2    DROP       all  --  192.168.1.11         ec2-35-180-139-74.eu-west-3.compute.amazonaws.com
3    ACCEPT     tcp  --  centosstream8.linuxvmimages.local  anywhere             multiport dports https,http
4    ACCEPT     udp  --  centosstream8.linuxvmimages.local  193.95.57.20         udp dpt:domain
[centos@centosstream8 ~]$
```

24.

```
user@DESKTOP-T8UB7J5 C:\Users\USER>ping 192.168.1.12

Pinging 192.168.1.12 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.12:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

25.

```
[centos@centosstream8 ~]$ sudo tail -f /var/log/messages
May 19 16:43:34 centosstream8 journal[2307]: g_hash_table_foreach: assertion 'version == hash_table->ver
sion' failed
May 19 16:43:34 centosstream8 journal[2526]: unable to get EDID for xrandr-Virtual-1: unable to get EDID
 for output
May 19 16:44:04 centosstream8 journal[2307]: g_hash_table_foreach: assertion 'version == hash_table->ver
sion' failed
May 19 16:44:04 centosstream8 journal[2526]: unable to get EDID for xrandr-Virtual-1: unable to get EDID
 for output
May 19 16:48:47 centosstream8 journal[2526]: unable to get EDID for xrandr-Virtual-1: unable to get EDID
 for output
May 19 16:48:48 centosstream8 journal[2526]: unable to get EDID for xrandr-Virtual-1: unable to get EDID
 for output
May 19 16:49:10 centosstream8 kernel: echo request receivedIN=enp0s3 OUT= MAC=08:00:27:2f:d5:f6:b8:1e:a4
:43:6a:a5:08:00 SRC=192.168.1.11 DST=192.168.1.12 LEN=60 TOS=0x00 PREC=0x00 TTL=128 ID=6269 PROTO=ICMP T
YPE=8 CODE=0 ID=1 SEQ=814
May 19 16:49:16 centosstream8 kernel: echo request receivedIN=enp0s3 OUT= MAC=08:00:27:2f:d5:f6:b8:1e:a4
:43:6a:a5:08:00 SRC=192.168.1.11 DST=192.168.1.12 LEN=60 TOS=0x00 PREC=0x00 TTL=128 ID=6270 PROTO=ICMP T
YPE=8 CODE=0 ID=1 SEQ=815
May 19 16:49:21 centosstream8 kernel: echo request receivedIN=enp0s3 OUT= MAC=08:00:27:2f:d5:f6:b8:1e:a4
:43:6a:a5:08:00 SRC=192.168.1.11 DST=192.168.1.12 LEN=60 TOS=0x00 PREC=0x00 TTL=128 ID=6271 PROTO=ICMP T
YPE=8 CODE=0 ID=1 SEQ=816
May 19 16:49:27 centosstream8 kernel: echo request receivedIN=enp0s3 OUT= MAC=08:00:27:2f:d5:f6:b8:1e:a4
:43:6a:a5:08:00 SRC=192.168.1.11 DST=192.168.1.12 LEN=60 TOS=0x00 PREC=0x00 TTL=128 ID=6272 PROTO=ICMP T
YPE=8 CODE=0 ID=1 SEQ=817
```

26. Why the VM does not respond to the received echo-request commands:

because we didn't alllow any input icmp traffic

27.

```
[centos@centosstream8 ~]$ sudo iptables -A INPUT -p icmp --icmp-type echo-request -d 192.168.1.12 -j ACC
EPT
```

28.

```
[centos@centosstream8 ~]$ sudo iptables -A OUTPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
```

29.

```
user@DESKTOP-T8UB7J5 C:\Users\USER>ping 192.168.1.12

Pinging 192.168.1.12 with 32 bytes of data:
Reply from 192.168.1.12: bytes=32 time<1ms TTL=64
Reply from 192.168.1.12: bytes=32 time<1ms TTL=64
Reply from 192.168.1.12: bytes=32 time<1ms TTL=64
Reply from 192.168.1.12: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.1.12:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

30.

```
[centos@centosstream8 ~]$ sudo iptables -A INPUT -s 192.168.1.11 -d 192.168.1.12 -p TCP -m multiport --d
ports 443,80 -j DROP
```

```
[centos@centosstream8 ~]$ sudo iptables -A INPUT -s 192.168.1.0/24 -d 192.168.1.100 -p TCP -m multiport
--dports 443,80 -j ACCEPT
```

31.

```
[centos@centosstream8 ~]$ sudo iptables -A INPUT -i lo -j ACCEPT
[centos@centosstream8 ~]$ sudo iptables -A OUTPUT -o lo -j ACCEPT
```

32.

```
[centos@centosstream8 ~]$ sudo iptables -nvL --line-numbers
Chain INPUT (policy DROP 1934 packets, 266K bytes)
num   pkts bytes target     prot opt in     out     source               destination
1      488  192K ACCEPT     all  --  *      *       0.0.0.0/0            0.0.0.0/0           state RELATED,ESTABLISHED
2        5   300 LOG        icmp --  *      *       0.0.0.0/0            192.168.1.12        icmptype 8 LOG flags 0 level 4 prefix "echo request received"
3        1    60 ACCEPT     icmp --  *      *       0.0.0.0/0            192.168.1.12        icmptype 8
4        0     0 DROP       tcp  --  *      *       192.168.1.11         192.168.1.12        multiport dports 443,80
5        0     0 ACCEPT     tcp  --  *      *       192.168.1.0/24       192.168.1.100       multiport dports 443,80
6        0     0 ACCEPT     all  --  lo     *       0.0.0.0/0            0.0.0.0/0

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
num   pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy DROP 177 packets, 13329 bytes)
num   pkts bytes target     prot opt in     out     source               destination
1       24  3553 ACCEPT     tcp  --  *      *       192.168.1.12         192.168.1.11        tcp dpt:22
2        0     0 DROP       all  --  *      *       192.168.1.11         35.180.139.74
3      338 54680 ACCEPT     tcp  --  *      *       192.168.1.12         0.0.0.0/0           multiport dports 443,80
4      111  7663 ACCEPT     udp  --  *      *       192.168.1.12         193.95.57.20        udp dpt:53
5        4   240 ACCEPT     all  --  *      *       0.0.0.0/0            0.0.0.0/0           state RELATED,ESTABLISHED
6        0     0 ACCEPT     all  --  *      lo      0.0.0.0/0            0.0.0.0/0
[centos@centosstream8 ~]$
```

33.

1-testing loopback rules icmp echo request and http get.

```
[centos@centosstream8 ~]$ ping -c 4 127.0.0.1
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.039 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.059 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.057 ms
64 bytes from 127.0.0.1: icmp_seq=4 ttl=64 time=0.042 ms

--- 127.0.0.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3049ms
rtt min/avg/max/mdev = 0.039/0.049/0.059/0.010 ms
[centos@centosstream8 ~]$
```

```
[centos@centosstream8 ~]$ curl http://127.0.0.1
<!DOCTYPE html>
<html lang="en">
<head>
  <meta name="generator" content="HTML Tidy for HTML5 for Linux version 5.7.28">
  <title>HTTP Server Test Page powered by CentOS</title>
  <meta charset="utf-8">
  <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no">
  <link rel="shortcut icon" href="http://www.centos.org/favicon.ico">
  <style type="text/css">
      /*<![CDATA[*/
      /*!
       * Bootstrap v4.3.1 (https://getbootstrap.com/)
       * Copyright 2011-2019 The Bootstrap Authors
       * Copyright 2011-2019 Twitter, Inc.
       * Licensed under MIT (https://github.com/twbs/bootstrap/blob/master/LICENSE)
       */:root{--blue:#007bff;--indigo:#6610f2;--purple:#6f42c1;--pink:#e83e8c;--red:#dc3545;--orange:#fd7e14;--y
ellow:#ffc107;--green:#28a745;--teal:#20c997;--cyan:#17a2b8;--white:#fff;--gray:#6c757d;--gray-dark:#343a40;--pri
mary:#007bff;--secondary:#6c757d;--success:#28a745;--info:#17a2b8;--warning:#ffc107;--danger:#dc3545;--light:#f8f
9fa;--dark:#343a40;--breakpoint-xs:0;--breakpoint-sm:576px;--breakpoint-md:768px;--breakpoint-lg:992px;--breakpoi
nt-xl:1200px;--font-family-sans-serif:-apple-system,BlinkMacSystemFont,"Segoe UI",Roboto,"Helvetica Neue",Arial,"
Noto Sans",sans-serif,"Apple Color Emoji","Segoe UI Emoji","Segoe UI Symbol","Noto Color Emoji";--font-family-mon
ospace:SFMono-Regular,Menlo,Monaco,Consolas,"Liberation Mono","Courier New",monospace}*,::after,::before{box-sizi
ng:border-box}html{font-family:sans-serif;line-height:1.15;-webkit-text-size-adjust:100%;-webkit-tap-highlight-co
lor:transparent}article,aside,figcaption,figure,footer,header,hgroup,main,nav,section{display:block}body{margin:0
```

2- testing http connection from host 1

```
user@DESKTOP-T8UB7J5 C:\Users\USER>curl 192.168.1.12
curl: (28) Failed to connect to 192.168.1.12 port 80 after 21002 ms: Couldn't connect to server
```

VII. Evading the Firewall :

35.

36.

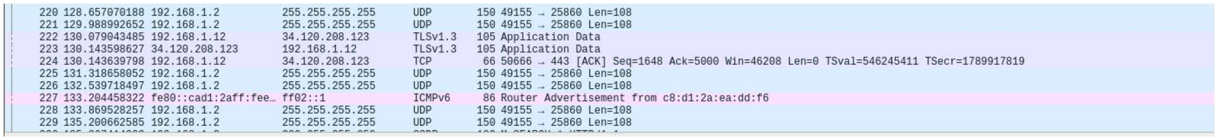
```
[centos@centosstream8 ~]$ ssh -L 1234:www.portquiz.net:80 USER@192.168.1.11
USER@192.168.1.11's password:
```

```
Microsoft Windows [Version 10.0.19045.4291]
(c) Microsoft Corporation. All rights reserved.

user@DESKTOP-T8UB7J5 C:\Users\USER>
```

37.

```
[centos@centosstream8 ~]$ curl http://localhost:1234
Port test successful!
Your IP: 41.225.159.75
[centos@centosstream8 ~]$
```

38.

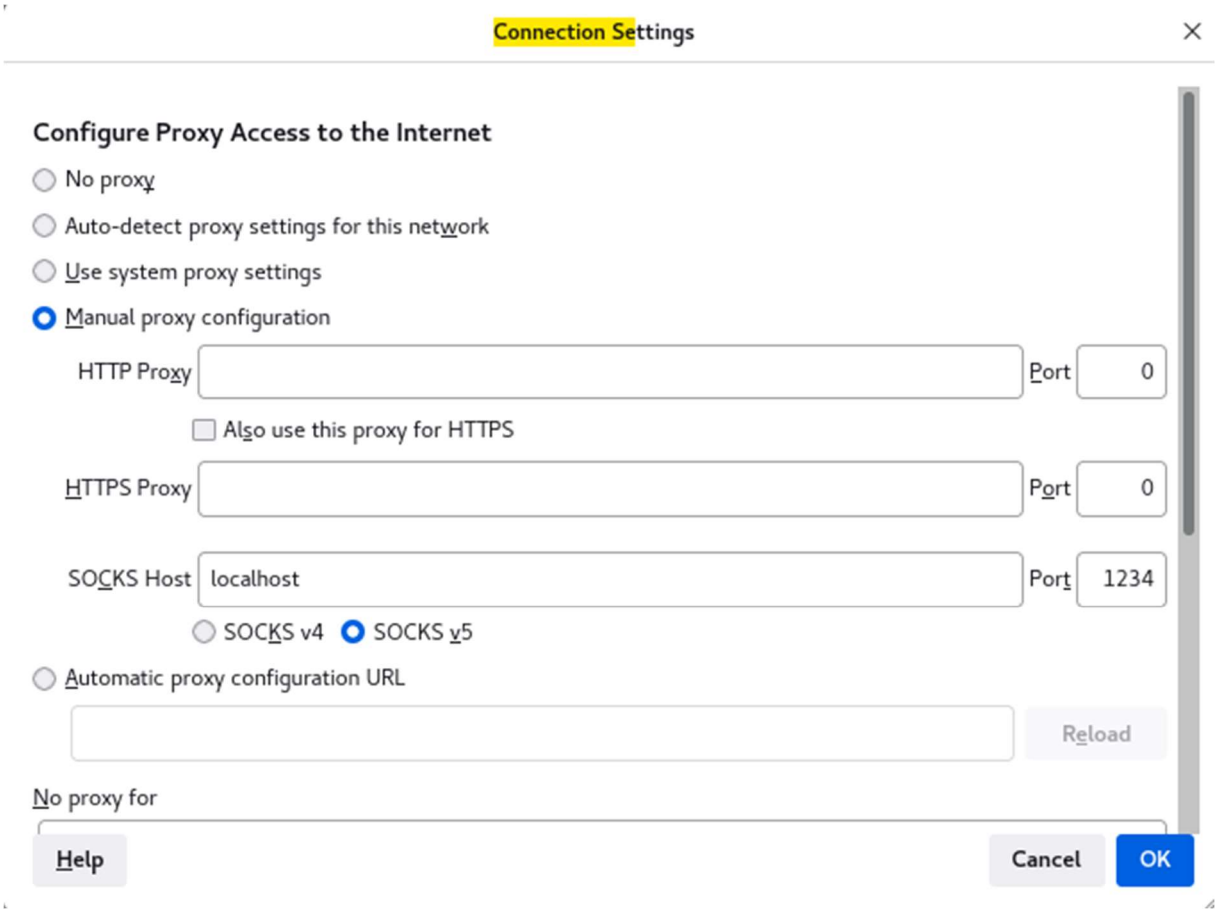


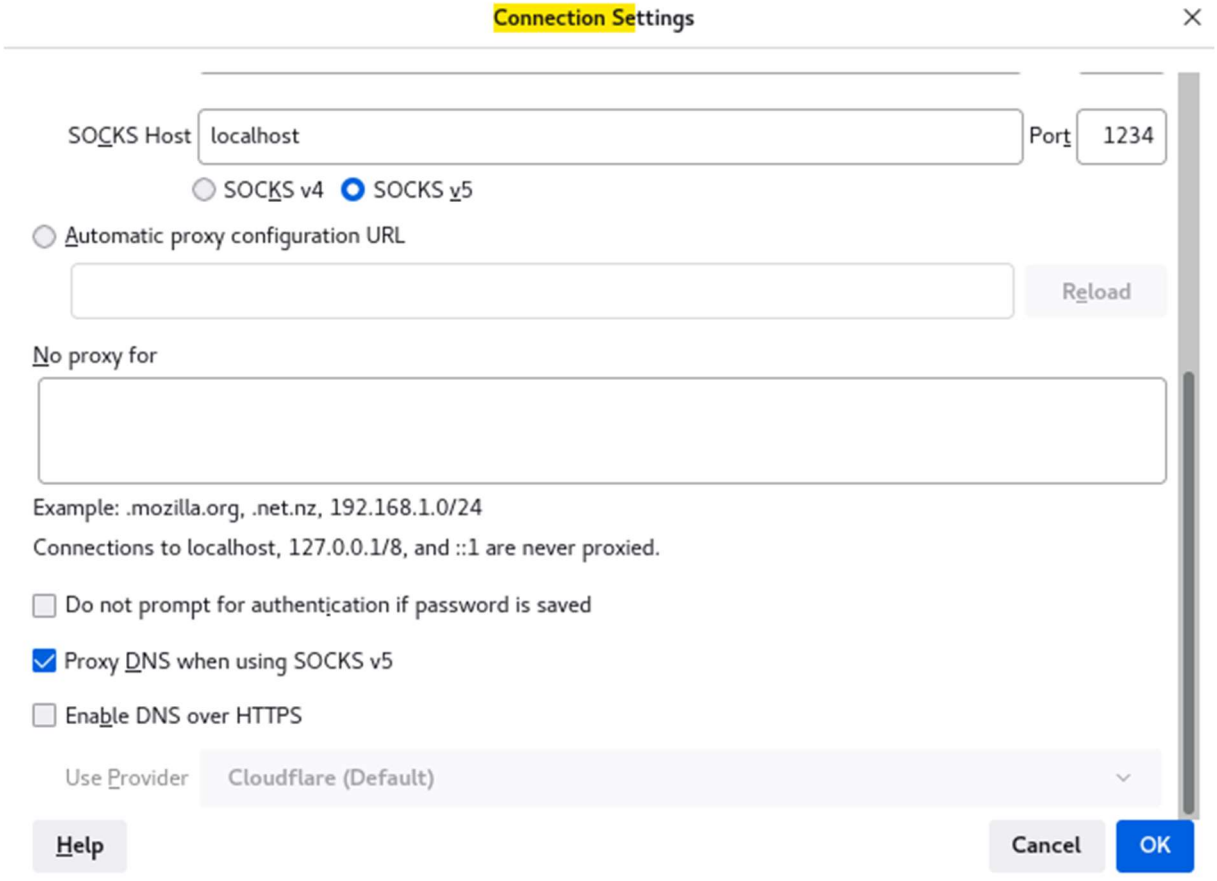
220	128.657070188	192.168.1.2	255.255.255.255	UDP	150 49155 → 25860 Len=108
221	129.988992652	192.168.1.2	255.255.255.255	UDP	150 49155 → 25860 Len=108
222	130.079043485	192.168.1.12	34.120.208.123	TLSv1.3	105 Application Data
223	130.143598627	34.120.208.123	192.168.1.12	TLSv1.3	105 Application Data
224	130.143639798	192.168.1.12	34.120.208.123	TCP	66 50666 → 443 [ACK] Seq=1648 Ack=5000 Win=46208 Len=0 TSval=546245411 TSecr=1789917819
225	131.318658052	192.168.1.2	255.255.255.255	UDP	150 49155 → 25860 Len=108
226	132.539718497	192.168.1.2	255.255.255.255	UDP	150 49155 → 25860 Len=108
227	133.204458322	fe80::cad1:2aff:fee…	ff02::1	ICMPv6	86 Router Advertisement from c8:d1:2a:ea:dd:f6
228	133.869528257	192.168.1.2	255.255.255.255	UDP	150 49155 → 25860 Len=108
229	135.200662585	192.168.1.2	255.255.255.255	UDP	150 49155 → 25860 Len=108

SSH Tunneling through dynamic port forwarding

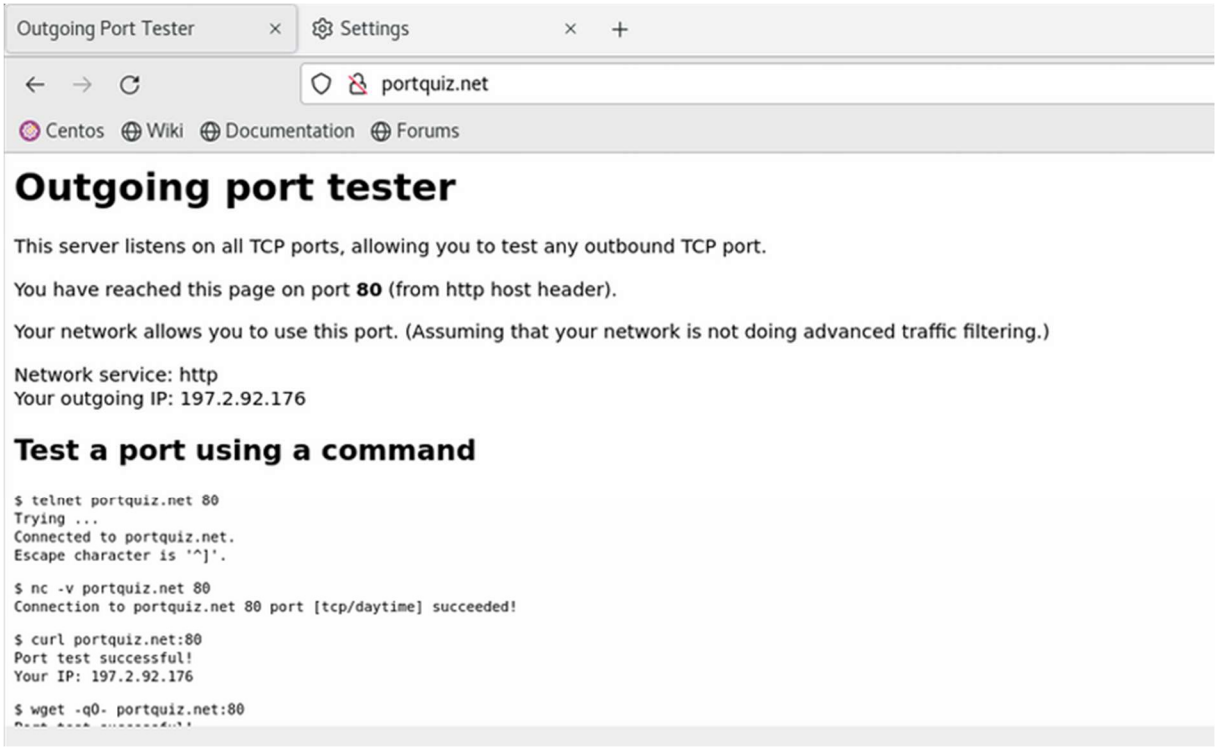
39.

```
[centos@centosstream8 ~]$ ssh -D 1234 -C USER@192.168.1.11
USER@192.168.1.11's password:
```

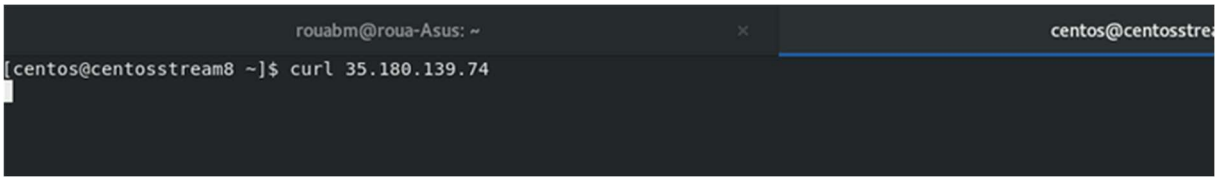

Connection Settings
Configure Proxy Access to the Internet
No proxy
Auto-detect proxy settings for this network
Use system proxy settings
Manual proxy configuration
HTTP Proxy
Port
0
Also use this proxy for HTTPS
HTTPS Proxy
Port
0
SOCKS Host
localhost
Port
1234
SOCKS v4
SOCKS v5
Automatic proxy configuration URL
Reload
No proxy for
Help
Cancel
OK


Connection Settings
SOCKS Host
localhost
Port
1234
SOCKS v4
SOCKS v5
Automatic proxy configuration URL
Reload
No proxy for
Example: .mozilla.org, .net.nz, 192.168.1.0/24
Connections to localhost, 127.0.0.1/8, and ::1 are never proxied.
Do not prompt for authentication if password is saved
Proxy DNS when using SOCKS v5
Enable DNS over HTTPS
Use Provider
Cloudflare (Default)
Help
Cancel
OK

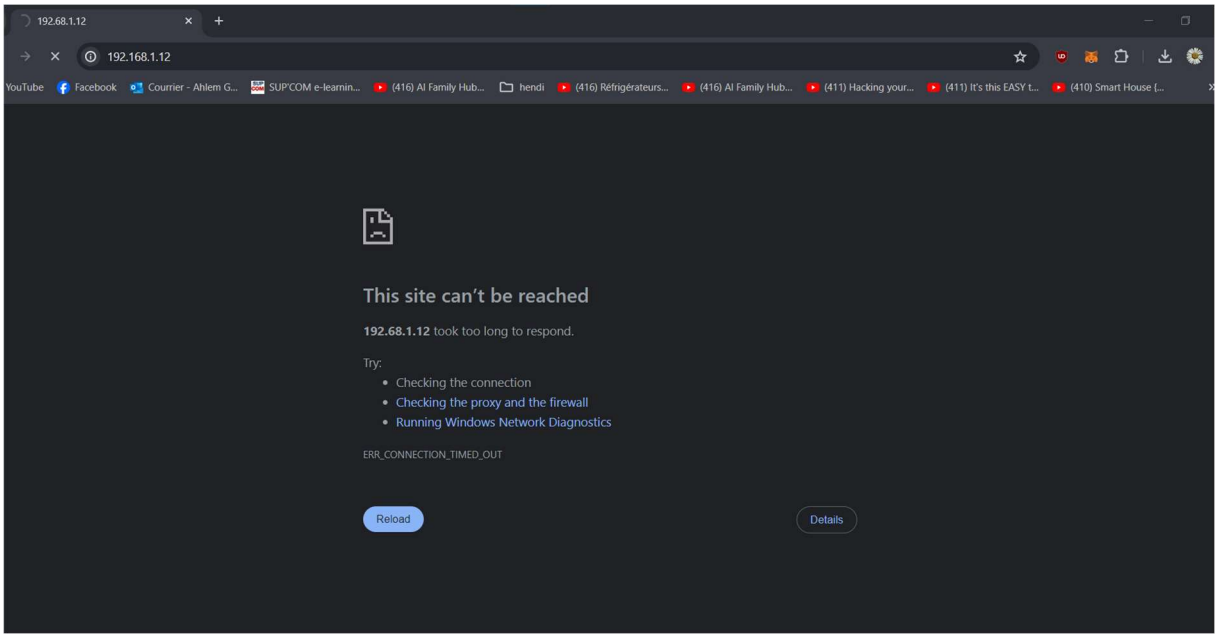
40.


Outgoing Port Tester
Settings
portquiz.net
Centos
Wiki
Documentation
Forums
Outgoing port tester
This server listens on all TCP ports, allowing you to test any outbound TCP port.
You have reached this page on port 80 (from http host header).
Your network allows you to use this port. (Assuming that your network is not doing advanced traffic filtering.)
Network service: http
Your outgoing IP: 197.2.92.176
Test a port using a command
$ telnet portquiz.net 80
Trying ...
Connected to portquiz.net.
Escape character is '^]'.
$ nc -v portquiz.net 80
Connection to portquiz.net 80 port [tcp/daytime] succeeded!
$ curl portquiz.net:80
Port test successful!
Your IP: 197.2.92.176
$ wget -q0- portquiz.net:80

41.


rouabm@roua-Asus: ~
centos@centosstre
[centos@centosstream8 ~]$ curl 35.180.139.74

43.


192.68.1.12
192.168.1.12
YouTube
Facebook
Courrier - Ahlem G...
SUP'COM e-learnin...
(416) Al Family Hub...
hendi
(416) Réfrigérateurs...
(416) Al Family Hub...
(411) Hacking your...
(411) It's this EASY t...
(410) Smart House (...
This site can't be reached
192.68.1.12 took too long to respond.
Try:
Checking the connection
Checking the proxy and the firewall
Running Windows Network Diagnostics
ERR_CONNECTION_TIMED_OUT
Reload
Details

44.

```
[centos@centosstream8 ~]$ ssh -R 4321:192.168.1.12:80 USER@192.168.1.11
USER@192.168.1.11's password:
```

45.