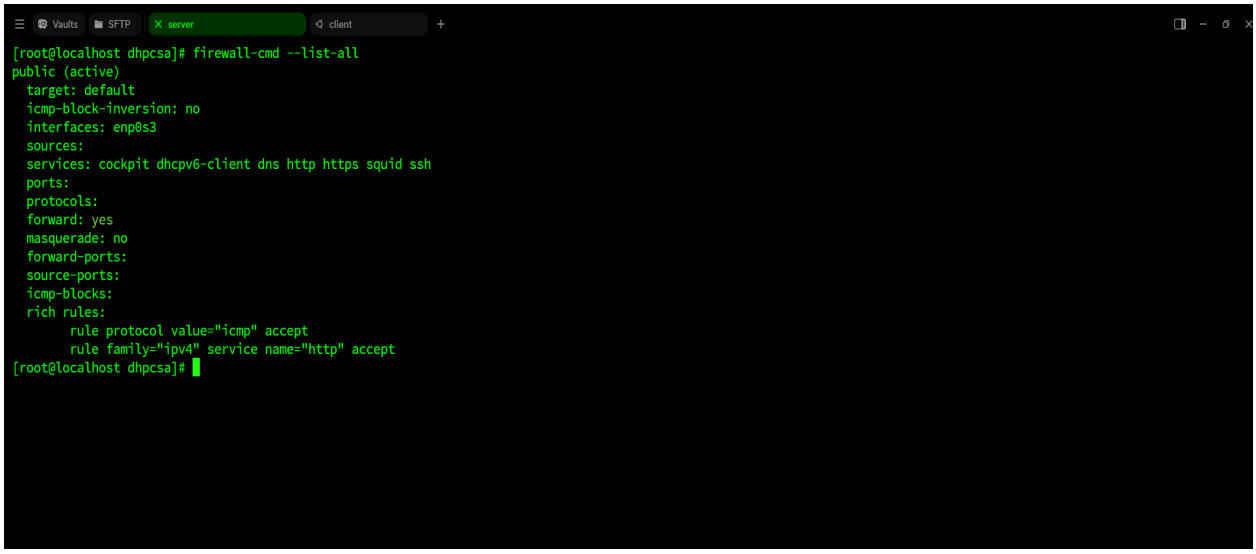
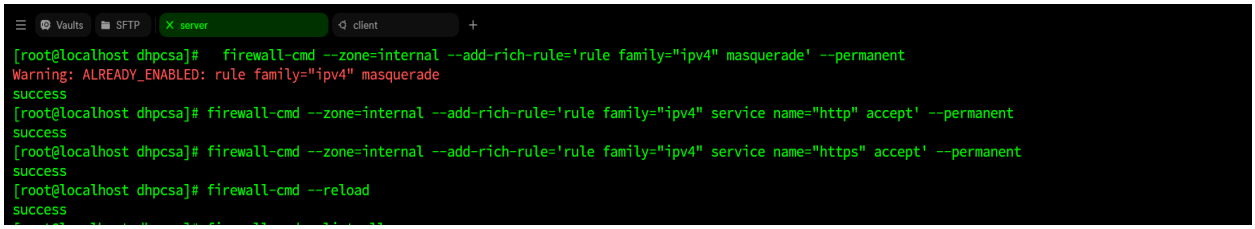
Gaurav Chaudhari
240840127033

1.Write firewall rules for the configuration described below using pfSence or nay other firewall:

Allow ICMP traffic for all LAN IPs



Enable web browsing only from LAN IPs to WAN IPs using the NAT option



```
[root@localhost dhpcsa]# firewall-cmd --zone=public --add-rich-rule='rule family="ipv4" masquerade' --permanent
success
[root@localhost dhpcsa]#  firewall-cmd --zone=public --add-rich-rule='rule family="ipv4" service name="http" accept' --permanent
Warning: ALREADY_ENABLED: rule family="ipv4" service name="http" accept
success
[root@localhost dhpcsa]# firewall-cmd --zone=public --add-rich-rule='rule family="ipv4" service name="https" accept' --permanent
success
[root@localhost dhpcsa]# firewall-cmd --reload
success
[root@localhost dhpcsa]# firewall-cmd --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
  services: cockpit dhcpv6-client dns http https squid ssh
  ports:
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
        rule family="ipv4" service name="https" accept
        rule protocol value="icmp" accept
        rule family="ipv4" service name="http" accept
        rule family="ipv4" masquerade
```

Configure a dmz and forward all incoming traffic on WAN IP port on 443 to a specific local LAN IP

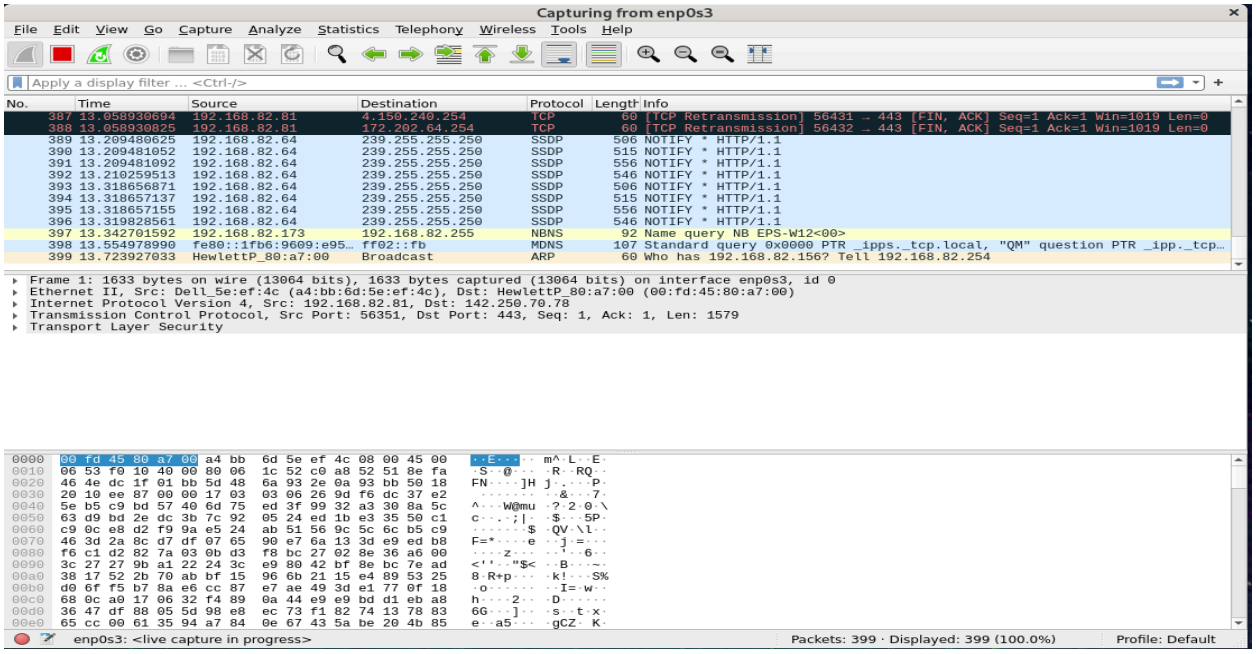
```
Vaults  SFTP  server  client  client (1)
[root@localhost dhpcsa]#  firewall-cmd --zone=public --add-rich-rule='rule family="ipv4" forward-port port="443" protocol="tcp" to-addr="192.168.82.97" to-port="443"' --per
manent
success
[root@localhost dhpcsa]#  firewall-cmd --zone=dmz --add-rich-rule='rule family="ipv4" service name="https" accept' --permanent
success
[root@localhost dhpcsa]# firewall-cmd --reload
success
[root@localhost dhpcsa]# firewall-cmd --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
  services: cockpit dhcpv6-client dns http https squid ssh
  ports:
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
        rule protocol value="icmp" accept
        rule family="ipv4" service name="https" accept
        rule family="ipv4" forward-port port="443" protocol="tcp" to-port="443" to-addr="192.168.82.97"
        rule family="ipv4" service name="http" accept
        rule family="ipv4" masquerade
[root@localhost dhpcsa]#
```

All rules set successfully

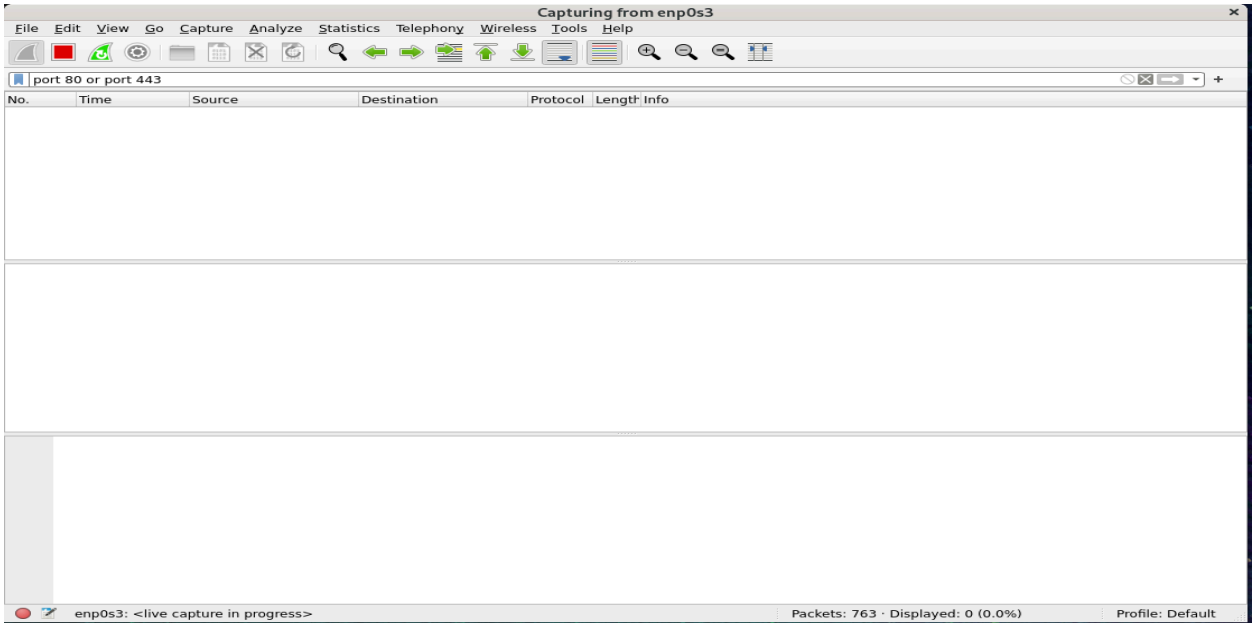
```
Vaults  SFTP  server  client  client (1)
[root@localhost dhpcsa]# firewall-cmd --list-rich-rules
rule protocol value="icmp" accept
rule family="ipv4" service name="https" accept
rule family="ipv4" forward-port port="443" protocol="tcp" to-port="443" to-addr="192.168.82.97"
rule family="ipv4" service name="http" accept
rule family="ipv4" masquerade
[root@localhost dhpcsa]#
```

3.Configure Wireshark to capture traffic on port 80 and simulate a web browser request to capture the data of the page being browsed by the user

Installig wireshark and start the wireshark using sudo or root permission

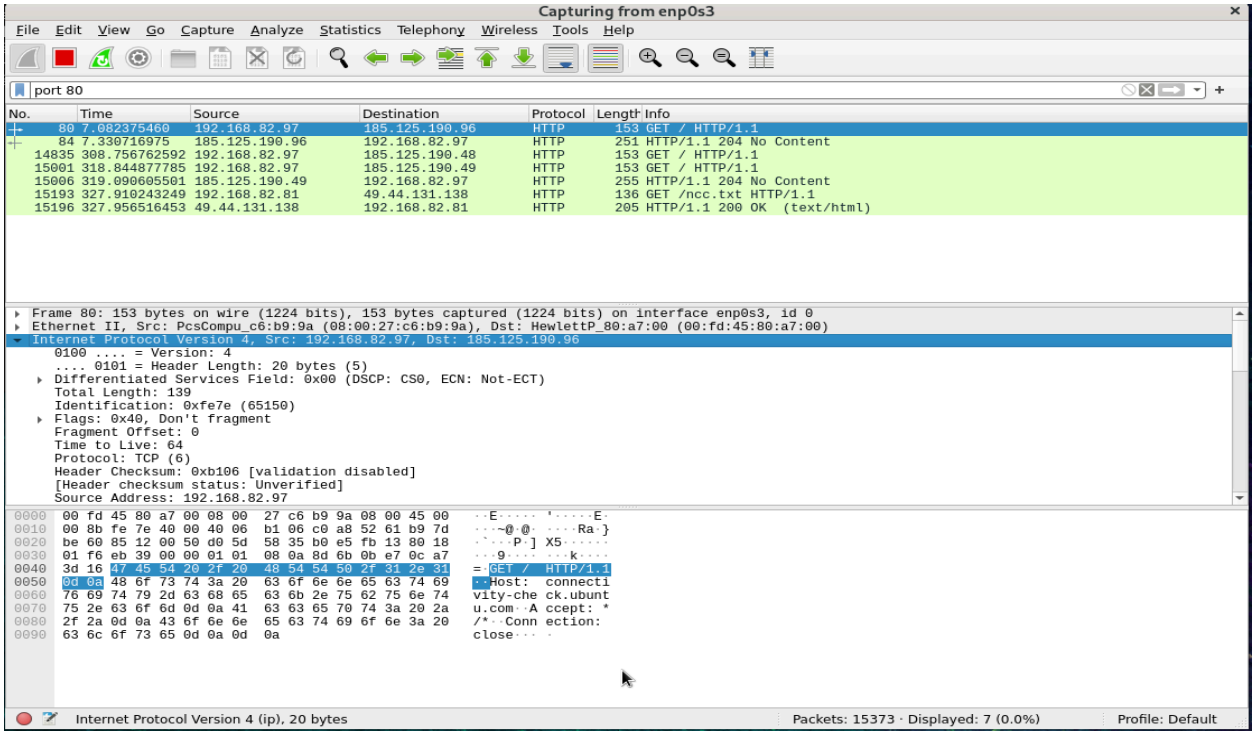


Filter port on 80 or port 443



Web page hosted on server open from client machine or user machine

Http packet captured successfully



Also using ip address and port to see the traffic on http port