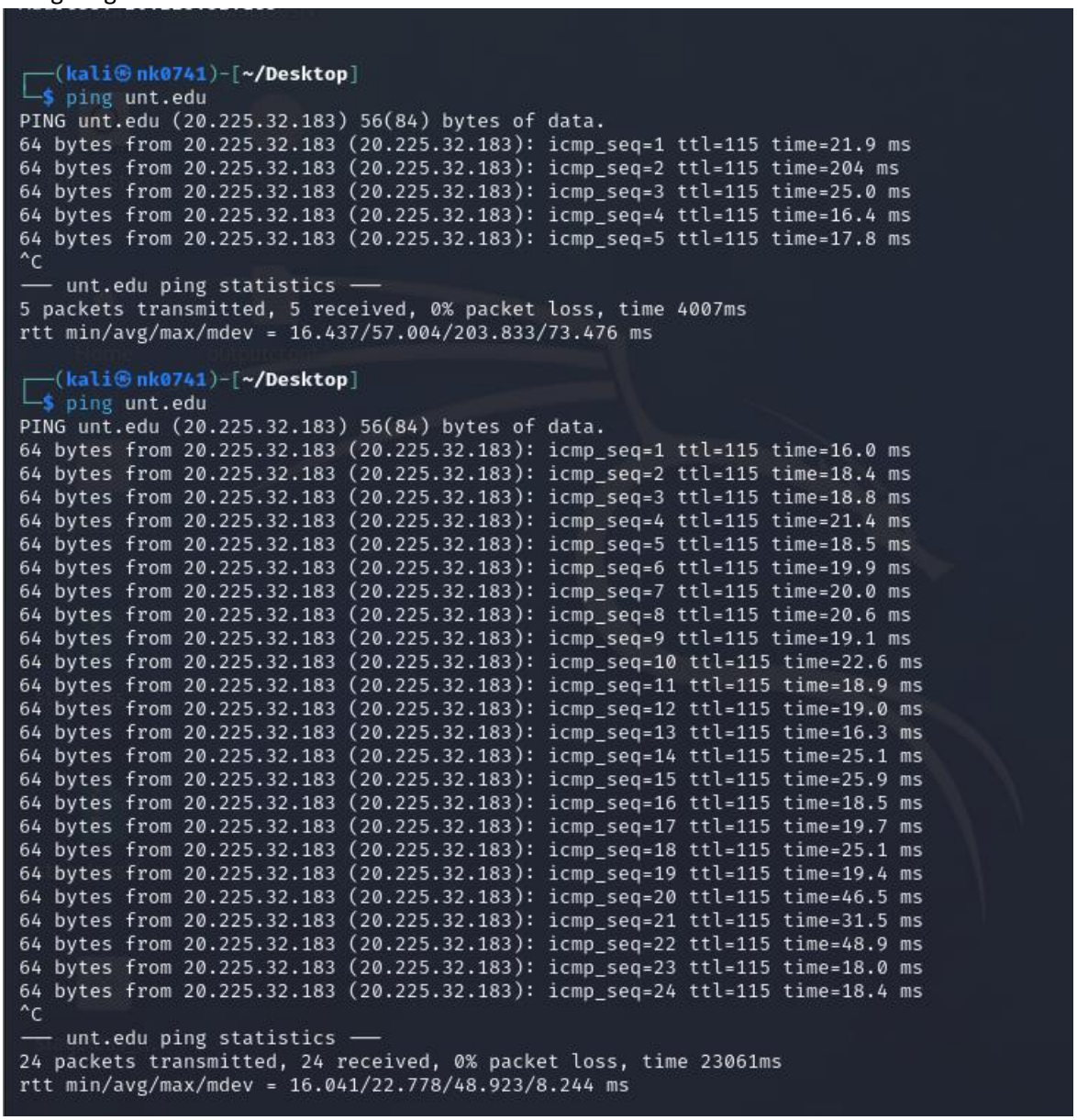
DNS resolution:

We can see the nk0741.com and nk0741.mil doesn't have any server for them. Unt.edu has server has ip address: 20.225.32.183

Using Ping command on unt.edu

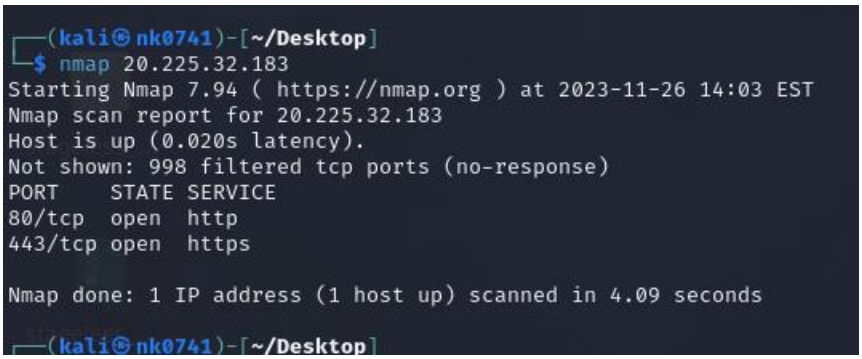


```
┌──(kali㉿nk0741)-[~/Desktop]
└─$ ping unt.edu
PING unt.edu (20.225.32.183) 56(84) bytes of data.
64 bytes from 20.225.32.183 (20.225.32.183): icmp_seq=1 ttl=115 time=21.9 ms
64 bytes from 20.225.32.183 (20.225.32.183): icmp_seq=2 ttl=115 time=204 ms
64 bytes from 20.225.32.183 (20.225.32.183): icmp_seq=3 ttl=115 time=25.0 ms
64 bytes from 20.225.32.183 (20.225.32.183): icmp_seq=4 ttl=115 time=16.4 ms
64 bytes from 20.225.32.183 (20.225.32.183): icmp_seq=5 ttl=115 time=17.8 ms
^C
── unt.edu ping statistics ──
5 packets transmitted, 5 received, 0% packet loss, time 4007ms
rtt min/avg/max/mdev = 16.437/57.004/203.833/73.476 ms

┌──(kali㉿nk0741)-[~/Desktop]
└─$ ping unt.edu
PING unt.edu (20.225.32.183) 56(84) bytes of data.
64 bytes from 20.225.32.183 (20.225.32.183): icmp_seq=1 ttl=115 time=16.0 ms
64 bytes from 20.225.32.183 (20.225.32.183): icmp_seq=2 ttl=115 time=18.4 ms
64 bytes from 20.225.32.183 (20.225.32.183): icmp_seq=3 ttl=115 time=18.8 ms
64 bytes from 20.225.32.183 (20.225.32.183): icmp_seq=4 ttl=115 time=21.4 ms
64 bytes from 20.225.32.183 (20.225.32.183): icmp_seq=5 ttl=115 time=18.5 ms
64 bytes from 20.225.32.183 (20.225.32.183): icmp_seq=6 ttl=115 time=19.9 ms
64 bytes from 20.225.32.183 (20.225.32.183): icmp_seq=7 ttl=115 time=20.0 ms
64 bytes from 20.225.32.183 (20.225.32.183): icmp_seq=8 ttl=115 time=20.6 ms
64 bytes from 20.225.32.183 (20.225.32.183): icmp_seq=9 ttl=115 time=19.1 ms
64 bytes from 20.225.32.183 (20.225.32.183): icmp_seq=10 ttl=115 time=22.6 ms
64 bytes from 20.225.32.183 (20.225.32.183): icmp_seq=11 ttl=115 time=18.9 ms
64 bytes from 20.225.32.183 (20.225.32.183): icmp_seq=12 ttl=115 time=19.0 ms
64 bytes from 20.225.32.183 (20.225.32.183): icmp_seq=13 ttl=115 time=16.3 ms
64 bytes from 20.225.32.183 (20.225.32.183): icmp_seq=14 ttl=115 time=25.1 ms
64 bytes from 20.225.32.183 (20.225.32.183): icmp_seq=15 ttl=115 time=25.9 ms
64 bytes from 20.225.32.183 (20.225.32.183): icmp_seq=16 ttl=115 time=18.5 ms
64 bytes from 20.225.32.183 (20.225.32.183): icmp_seq=17 ttl=115 time=19.7 ms
64 bytes from 20.225.32.183 (20.225.32.183): icmp_seq=18 ttl=115 time=25.1 ms
64 bytes from 20.225.32.183 (20.225.32.183): icmp_seq=19 ttl=115 time=19.4 ms
64 bytes from 20.225.32.183 (20.225.32.183): icmp_seq=20 ttl=115 time=46.5 ms
64 bytes from 20.225.32.183 (20.225.32.183): icmp_seq=21 ttl=115 time=31.5 ms
64 bytes from 20.225.32.183 (20.225.32.183): icmp_seq=22 ttl=115 time=48.9 ms
64 bytes from 20.225.32.183 (20.225.32.183): icmp_seq=23 ttl=115 time=18.0 ms
64 bytes from 20.225.32.183 (20.225.32.183): icmp_seq=24 ttl=115 time=18.4 ms
^C
── unt.edu ping statistics ──
24 packets transmitted, 24 received, 0% packet loss, time 23061ms
rtt min/avg/max/mdev = 16.041/22.778/48.923/8.244 ms
```

Using trace route on unt.edu:

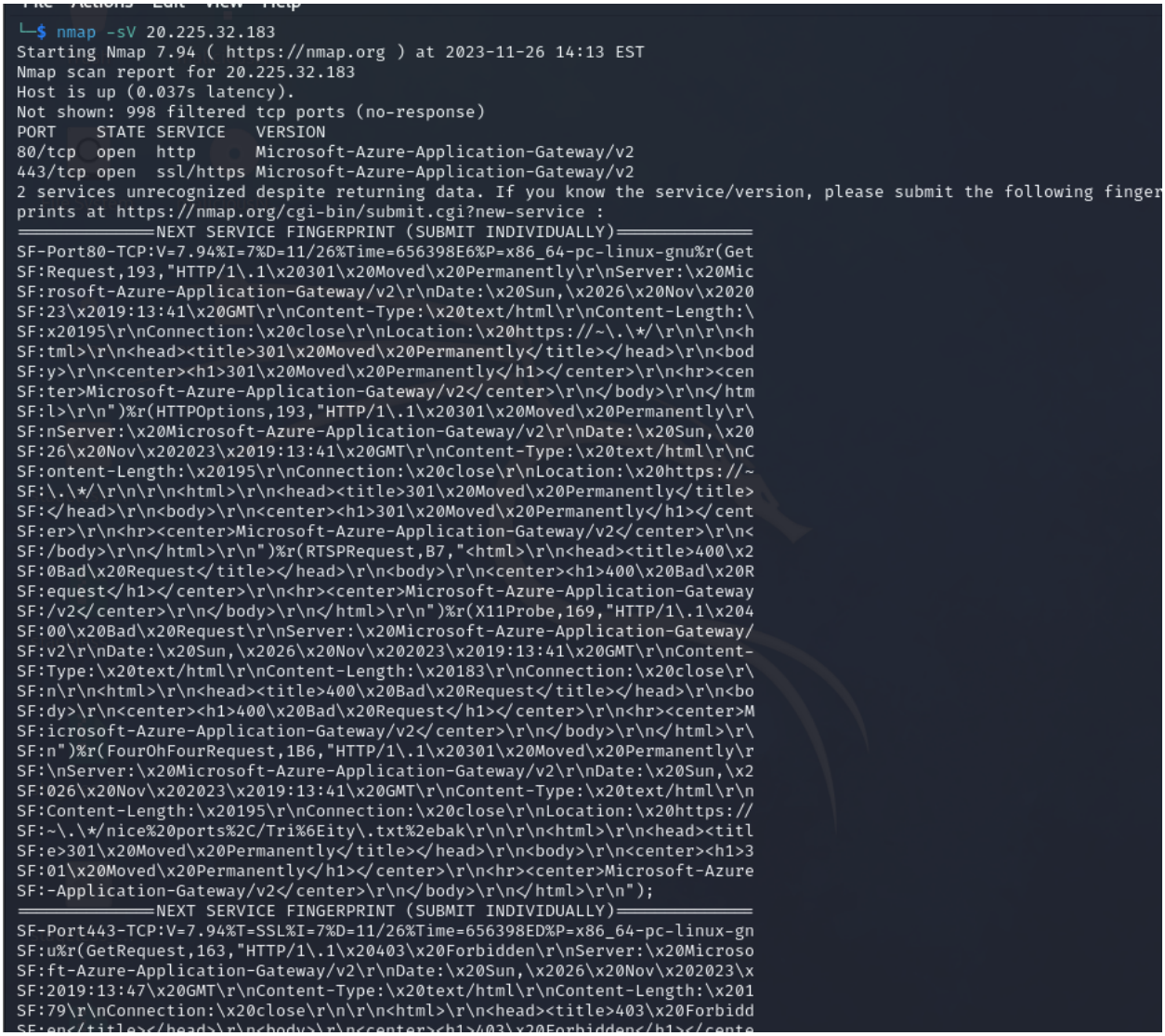
The traceroute shows a connection attempt to unt.edu (20.225.32.183) with no successful hops, likely due to network configurations blocking ICMP packets. The asterisks (*) indicate no response received within the allotted time, possibly due to firewall settings or network congestion. The lack of specific hop details suggests the packets might be getting dropped or filtered at an intermediary network point.

Using nmap on unt.edu:



The nmap command shows that host is up and responsive with a very low latency of 0.020 seconds. The scan revealed two open ports: port 80 for HTTP and port 443 for HTTPS. Additionally, the scan found 998 TCP ports as filtered, suggesting that these ports are likely protected by a firewall or not responding to the scan. Overall, the host seems to be running web services on standard HTTP and HTTPS ports.

Detailed scan using nmap:



```
└─$ nmap -sV 20.225.32.183
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-26 14:13 EST
Nmap scan report for 20.225.32.183
Host is up (0.037s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE   VERSION
80/tcp  open  http      Microsoft-Azure-Application-Gateway/v2
443/tcp open  ssl/https Microsoft-Azure-Application-Gateway/v2
2 services unrecognized despite returning data. If you know the service/version, please submit the following finger
prints at https://nmap.org/cgi-bin/submit.cgi?new-service :
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port80-TCP:V=7.94%I=7%D=11/26%Time=656398E6%P=x86_64-pc-linux-gnu%r(Get
SF:Request,193,"HTTP/1\.1\x20301\x20Moved\x20Permanently\r\nServer:\x20Mic
SF:rosoft-Azure-Application-Gateway/v2\r\nDate:\x20Sun,\x2026\x20Nov\x2020
SF:23\x2019:13:41\x20GMT\r\nContent-Type:\x20text/html\r\nContent-Length:\
SF:x20195\r\nConnection:\x20close\r\nLocation:\x20https://~\.\*/\r\n\r\n<h
SF:tml>\r\n<head><title>301\x20Moved\x20Permanently</title></head>\r\n<bod
SF:y>\r\n<center><h1>301\x20Moved\x20Permanently</h1></center>\r\n<hr><cen
SF:ter>Microsoft-Azure-Application-Gateway/v2</center>\r\n</body>\r\n</htm
SF:l>\r\n")%r(HTTPOptions,193,"HTTP/1\.1\x20301\x20Moved\x20Permanently\r\
SF:nServer:\x20Microsoft-Azure-Application-Gateway/v2\r\nDate:\x20Sun,\x20
SF:26\x20Nov\x202023\x2019:13:41\x20GMT\r\nContent-Type:\x20text/html\r\nC
SF:ontent-Length:\x20195\r\nConnection:\x20close\r\nLocation:\x20https://~
SF:\.\*/\r\n\r\n<html>\r\n<head><title>301\x20Moved\x20Permanently</title>
SF:</head>\r\n<body>\r\n<center><h1>301\x20Moved\x20Permanently</h1></cent
SF:er>\r\n<hr><center>Microsoft-Azure-Application-Gateway/v2</center>\r\n<
SF:/body>\r\n</html>\r\n")%r(RTSPRequest,B7,"<html>\r\n<head><title>400\x2
SF:0Bad\x20Request</title></head>\r\n<body>\r\n<center><h1>400\x20Bad\x20R
SF:equest</h1></center>\r\n<hr><center>Microsoft-Azure-Application-Gateway
SF:/v2</center>\r\n</body>\r\n</html>\r\n")%r(X11Probe,169,"HTTP/1\.1\x204
SF:00\x20Bad\x20Request\r\nServer:\x20Microsoft-Azure-Application-Gateway/
SF:v2\r\nDate:\x20Sun,\x2026\x20Nov\x202023\x2019:13:41\x20GMT\r\nContent-
SF:Type:\x20text/html\r\nContent-Length:\x20183\r\nConnection:\x20close\r\
SF:n\r\n<html>\r\n<head><title>400\x20Bad\x20Request</title></head>\r\n<bo
SF:dy>\r\n<center><h1>400\x20Bad\x20Request</h1></center>\r\n<hr><center>M
SF:icrosoft-Azure-Application-Gateway/v2</center>\r\n</body>\r\n</html>\r\
SF:n")%r(FourOhFourRequest,1B6,"HTTP/1\.1\x20301\x20Moved\x20Permanently\r
SF:\nServer:\x20Microsoft-Azure-Application-Gateway/v2\r\nDate:\x20Sun,\x2
SF:026\x20Nov\x202023\x2019:13:41\x20GMT\r\nContent-Type:\x20text/html\r\n
SF:Content-Length:\x20195\r\nConnection:\x20close\r\nLocation:\x20https://
SF:~\.\*/nice%20ports%2C/Tri%6Eity\.txt%2ebak\r\n\r\n<html>\r\n<head><titl
SF:e>301\x20Moved\x20Permanently</title></head>\r\n<body>\r\n<center><h1>3
SF:01\x20Moved\x20Permanently</h1></center>\r\n<hr><center>Microsoft-Azure
SF:-Application-Gateway/v2</center>\r\n</body>\r\n</html>\r\n");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port443-TCP:V=7.94%T=SSL%I=7%D=11/26%Time=656398ED%P=x86_64-pc-linux-gn
SF:u%r(GetRequest,163,"HTTP/1\.1\x20403\x20Forbidden\r\nServer:\x20Microso
SF:ft-Azure-Application-Gateway/v2\r\nDate:\x20Sun,\x2026\x20Nov\x202023\x
SF:2019:13:47\x20GMT\r\nContent-Type:\x20text/html\r\nContent-Length:\x201
SF:79\r\nConnection:\x20close\r\n\r\n<html>\r\n<head><title>403\x20Forbidd
SF:en</title></head>\r\n<body>\r\n<center><h1>403\x20Forbidden</h1></cente
```

Explanation:

The Nmap scan conducted on the IP address 20.225.32.183 confirmed that the target system is active and promptly responsive, indicating a quick round-trip time (latency) of 0.020 seconds. This implies that the system is online and accessible. Regarding the ports, the scan identified two ports that are open and accepting connections: port 80 (HTTP) and port 443 (HTTPS). These ports are commonly used for web services, suggesting that the host likely hosts web servers or web-based applications utilizing HTTP and HTTPS protocols. Furthermore, the scan reported 998 TCP ports as "filtered," meaning that these ports did not respond to the scan. This situation typically occurs when ports are protected by a firewall or when the scanned ports do not provide any response, possibly indicating they are closed or not actively listening for connections.

Trying to detect OS used in unt.edu using nmap: (Requires root access)

```
┌──(kali㉿nk0741)-[~/Desktop]
└─$ sudo nmap -O 20.225.32.183
[sudo] password for kali:
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-26 14:22 EST
Nmap scan report for 20.225.32.183
Host is up (0.0090s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: bridge|general purpose
Running (JUST GUESSING): Oracle Virtualbox (98%), QEMU (94%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu
Aggressive OS guesses: Oracle Virtualbox (98%), QEMU user mode network gateway (94%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.64 seconds
```

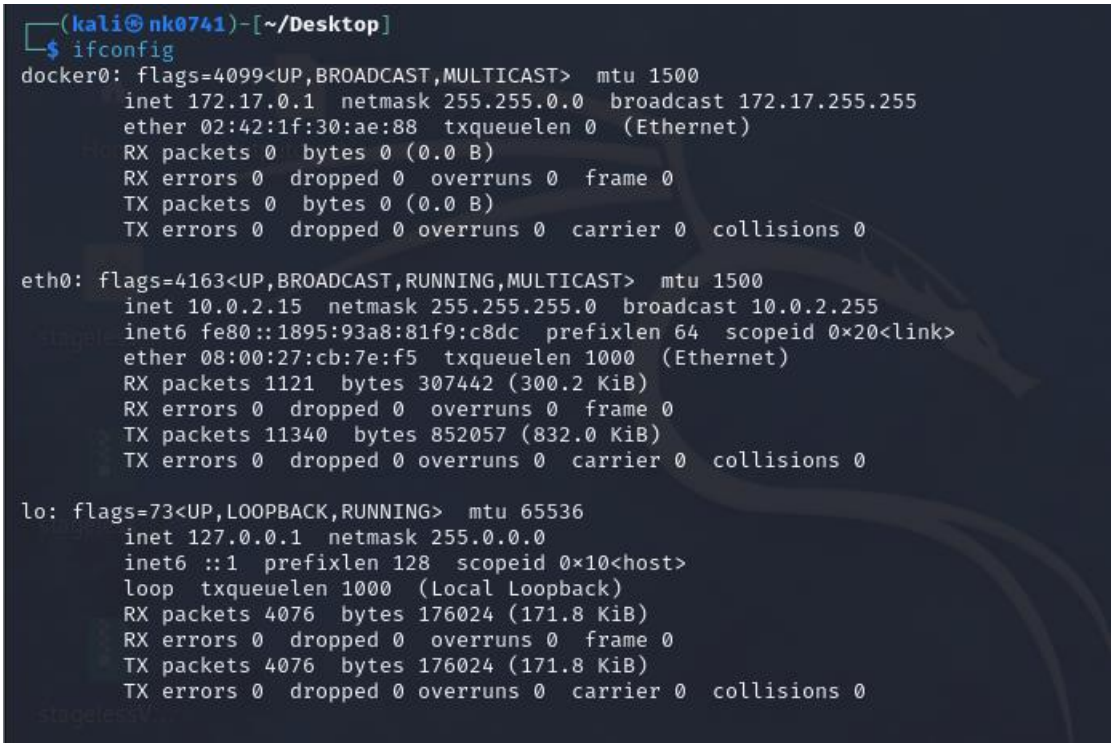
Scanning only specific ports using nmap:

```
┌──(kali㉿nk0741)-[~/Desktop]
└─$ nmap -p 1-1000 20.225.32.183

Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-26 14:18 EST
Nmap scan report for 20.225.32.183
Host is up (0.034s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https
```

Using nmap to do the script scanning:

```
┌──(kali㉿nk0741)-[~/Desktop]
└─$ nmap --script=default 20.225.32.183

Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-26 14:19 EST
Nmap scan report for 20.225.32.183
Host is up (0.029s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https
| ssl-cert: Subject: commonName=unt.edu/organizationName=University of North Texas System/stateOrProvinceName=Texas
/countryName=US
| Subject Alternative Name: DNS:unt.edu, DNS:*.admin.unt.edu, DNS:*.art.unt.edu, DNS:*.ci.unt.edu, DNS:*.clear.unt.
edu, DNS:*.cmht.unt.edu, DNS:*.cob.unt.edu, DNS:*.coe.unt.edu, DNS:*.courses.unt.edu, DNS:*.cse.unt.edu, DNS:*.cvad
.unt.edu, DNS:*.cws.unt.edu, DNS:*.datacomm.unt.edu, DNS:*.distanceeducation.com, DNS:*.dpdcn.unt.edu, DNS:*.engine
ering.unt.edu, DNS:*.enrollment.unt.edu, DNS:*.essc.unt.edu, DNS:*.gabdcn.its.unt.edu, DNS:*.gabdcn.unt.edu, DNS:*.
gallery.unt.edu, DNS:*.healthcenter.unt.edu, DNS:*.hps.unt.edu, DNS:*.hsc.unt.edu, DNS:*.informationscience.unt.edu
, DNS:*.it.unt.edu, DNS:*.itss.untsystem.edu, DNS:*.jazz.unt.edu, DNS:*.journalism.unt.edu, DNS:*.learningtechnolog
ies.unt.edu, DNS:*.library.hsc.unt.edu, DNS:*.lt.unt.edu, DNS:*.mdr.unt.edu, DNS:*.music.unt.edu, DNS:*.online.unt.
edu, DNS:*.pacs.unt.edu, DNS:*.pdi.org, DNS:*.president.unt.edu, DNS:*.recsports.unt.edu, DNS:*.research.unt.edu, D
NS:*.sharepoint.unt.edu, DNS:*.studentaffairs.unt.edu, DNS:*.texasleadershipscholars.org, DNS:*.unt.edu, DNS:*.untd
allas.edu, DNS:*.untdallas.unt.edu, DNS:*.unthsc.edu, DNS:*.untsystem.edu, DNS:*.vpaa.unt.edu, DNS:*.wdc.unt.edu, D
NS:distanceeducation.com, DNS:global.wildcard.unt.edu, DNS:inspirefrisco.com, DNS:inspirefrisco.net, DNS:inspirefri
sco.org, DNS:library-apps.hsc.unt.edu, DNS:ntdaily.com, DNS:ntdaily.net, DNS:pdi.org, DNS:resnet.hsl.unt.edu, DNS:t
edxunt.org, DNS:texasleadershipscholars.org, DNS:tgs.unt.edu, DNS:themayborn.com, DNS:twu-unt-msw.com, DNS:twu-unt-
msw.org, DNS:untdallas.edu, DNS:untfbtickets.com, DNS:unthstickets.com, DNS:untsystem.edu, DNS:www.dining.unt.edu,
DNS:www.emergency.unt.edu, DNS:www.inspirefrisco.com, DNS:www.inspirefrisco.net, DNS:www.inspirefrisco.org, DNS:ww
.ntdaily.com, DNS:www.ntdaily.net, DNS:www.police.unt.edu, DNS:www.studentactivities.unt.edu, DNS:www.tedxunt.org,
DNS:www.themayborn.com, DNS:www.untfbtickets.com, DNS:www.unthstickets.com
| Not valid before: 2023-09-29T00:00:00
|_Not valid after:  2024-09-28T23:59:59
| tls-nextprotoneg:
|_  http/1.1

Nmap done: 1 IP address (1 host up) scanned in 34.53 seconds
```

Using ifonfig to get machince’s ip address:



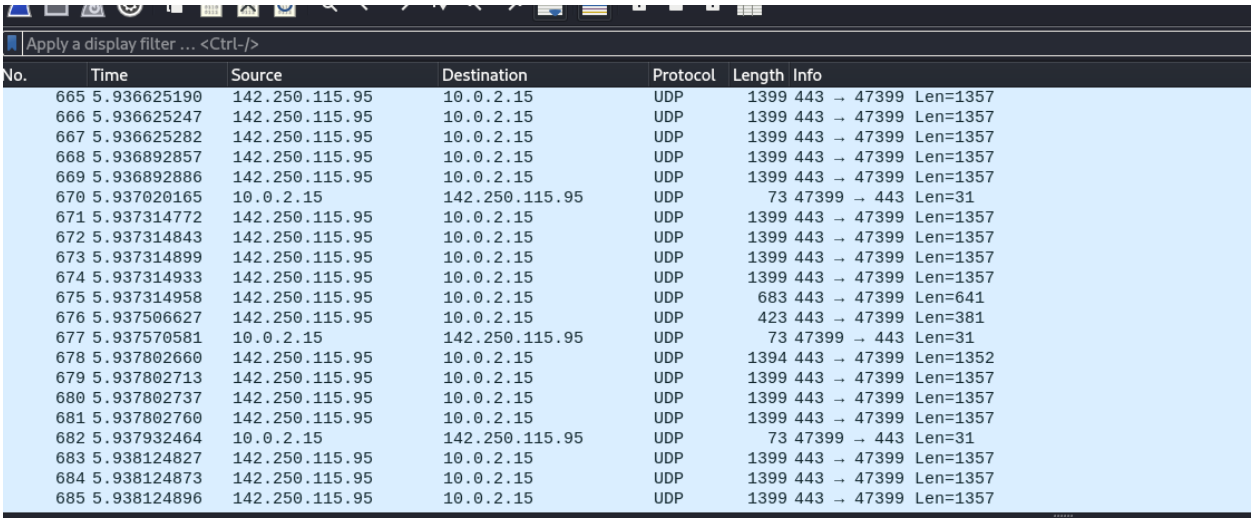
Nmap scan on local OS:

```
┌──(kali㉿nk0741)-[~/Desktop]
└─$ sudo nmap -O 172.17.0.1
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-26 14:27 EST
Nmap scan report for 172.17.0.1
Host is up (0.000075s latency).
All 1000 scanned ports on 172.17.0.1 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.56 seconds

┌──(kali㉿nk0741)-[~/Desktop]
└─$ nmap 10.0.2.15
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-26 14:27 EST
Nmap scan report for 10.0.2.15
Host is up (0.000052s latency).
All 1000 scanned ports on 10.0.2.15 are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Nmap done: 1 IP address (1 host up) scanned in 0.08 seconds

┌──(kali㉿nk0741)-[~/Desktop]
└─$ nmap 172.17.0.1
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-26 14:27 EST
Nmap scan report for 172.17.0.1
Host is up (0.000057s latency).
All 1000 scanned ports on 172.17.0.1 are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Nmap done: 1 IP address (1 host up) scanned in 0.08 seconds

┌──(kali㉿nk0741)-[~/Desktop]
└─$  nmap 127.0.0.1
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-26 14:27 EST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000045s latency).
All 1000 scanned ports on localhost (127.0.0.1) are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Nmap done: 1 IP address (1 host up) scanned in 0.02 seconds
```

The vm has 3 ip address one for docker, other for brigded eth0 connection and last one is localhost/loopback address.

Running wireshark on youtube:

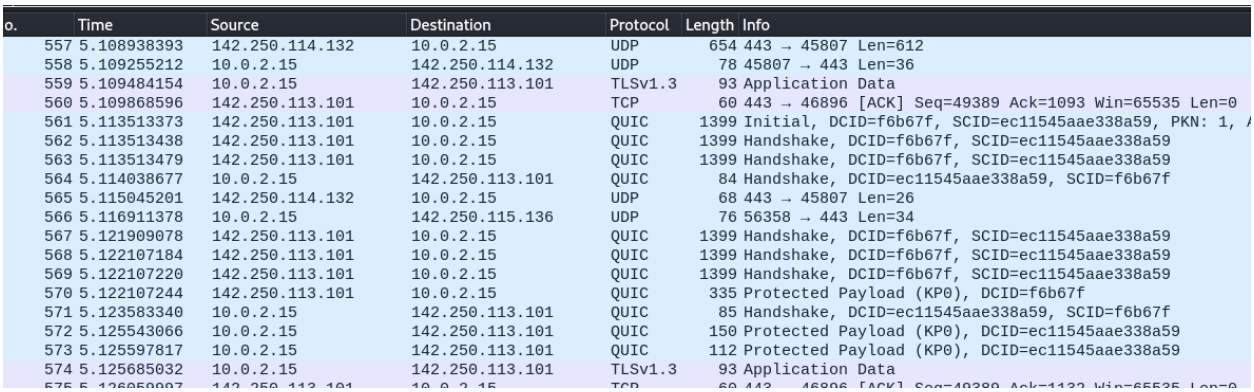
Protocol used- udp:



Apply a display filter … <Ctrl-/>

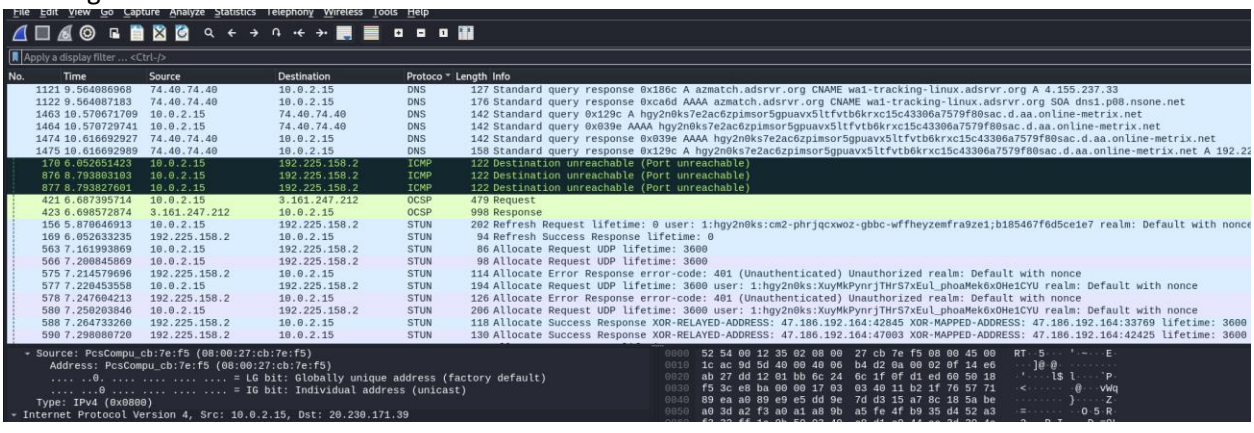
No.	Time	Source	Destination	Protocol	Length	Info
665	5.936625190	142.250.115.95	10.0.2.15	UDP	1399	443 → 47399 Len=1357
666	5.936625247	142.250.115.95	10.0.2.15	UDP	1399	443 → 47399 Len=1357
667	5.936625282	142.250.115.95	10.0.2.15	UDP	1399	443 → 47399 Len=1357
668	5.936892857	142.250.115.95	10.0.2.15	UDP	1399	443 → 47399 Len=1357
669	5.936892886	142.250.115.95	10.0.2.15	UDP	1399	443 → 47399 Len=1357
670	5.937020165	10.0.2.15	142.250.115.95	UDP	73	47399 → 443 Len=31
671	5.937314772	142.250.115.95	10.0.2.15	UDP	1399	443 → 47399 Len=1357
672	5.937314843	142.250.115.95	10.0.2.15	UDP	1399	443 → 47399 Len=1357
673	5.937314899	142.250.115.95	10.0.2.15	UDP	1399	443 → 47399 Len=1357
674	5.937314933	142.250.115.95	10.0.2.15	UDP	1399	443 → 47399 Len=1357
675	5.937314958	142.250.115.95	10.0.2.15	UDP	683	443 → 47399 Len=641
676	5.937506627	142.250.115.95	10.0.2.15	UDP	423	443 → 47399 Len=381
677	5.937570581	10.0.2.15	142.250.115.95	UDP	73	47399 → 443 Len=31
678	5.937802660	142.250.115.95	10.0.2.15	UDP	1394	443 → 47399 Len=1352
679	5.937802713	142.250.115.95	10.0.2.15	UDP	1399	443 → 47399 Len=1357
680	5.937802737	142.250.115.95	10.0.2.15	UDP	1399	443 → 47399 Len=1357
681	5.937802760	142.250.115.95	10.0.2.15	UDP	1399	443 → 47399 Len=1357
682	5.937932464	10.0.2.15	142.250.115.95	UDP	73	47399 → 443 Len=31
683	5.938124827	142.250.115.95	10.0.2.15	UDP	1399	443 → 47399 Len=1357
684	5.938124873	142.250.115.95	10.0.2.15	UDP	1399	443 → 47399 Len=1357
685	5.938124896	142.250.115.95	10.0.2.15	UDP	1399	443 → 47399 Len=1357

Protocol used- QUIC:



o.	Time	Source	Destination	Protocol	Length	Info
557	5.108938393	142.250.114.132	10.0.2.15	UDP	654	443 → 45807 Len=612
558	5.109255212	10.0.2.15	142.250.114.132	UDP	78	45807 → 443 Len=36
559	5.109484154	10.0.2.15	142.250.113.101	TLSv1.3	93	Application Data
560	5.109868596	142.250.113.101	10.0.2.15	TCP	60	443 → 46896 [ACK] Seq=49389 Ack=1093 Win=65535 Len=0
561	5.113513373	142.250.113.101	10.0.2.15	QUIC	1399	Initial, DCID=f6b67f, SCID=ec11545aae338a59, PKN: 1, A
562	5.113513438	142.250.113.101	10.0.2.15	QUIC	1399	Handshake, DCID=f6b67f, SCID=ec11545aae338a59
563	5.113513479	142.250.113.101	10.0.2.15	QUIC	1399	Handshake, DCID=f6b67f, SCID=ec11545aae338a59
564	5.114038677	10.0.2.15	142.250.113.101	QUIC	84	Handshake, DCID=ec11545aae338a59, SCID=f6b67f
565	5.115045201	142.250.114.132	10.0.2.15	UDP	68	443 → 45807 Len=26
566	5.116911378	10.0.2.15	142.250.115.136	UDP	76	56358 → 443 Len=34
567	5.121909078	142.250.113.101	10.0.2.15	QUIC	1399	Handshake, DCID=f6b67f, SCID=ec11545aae338a59
568	5.122107184	142.250.113.101	10.0.2.15	QUIC	1399	Handshake, DCID=f6b67f, SCID=ec11545aae338a59
569	5.122107220	142.250.113.101	10.0.2.15	QUIC	1399	Handshake, DCID=f6b67f, SCID=ec11545aae338a59
570	5.122107244	142.250.113.101	10.0.2.15	QUIC	335	Protected Payload (KP0), DCID=f6b67f
571	5.123583340	10.0.2.15	142.250.113.101	QUIC	85	Handshake, DCID=ec11545aae338a59, SCID=f6b67f
572	5.125543066	10.0.2.15	142.250.113.101	QUIC	150	Protected Payload (KP0), DCID=ec11545aae338a59
573	5.125597817	10.0.2.15	142.250.113.101	QUIC	112	Protected Payload (KP0), DCID=ec11545aae338a59
574	5.125685032	10.0.2.15	142.250.113.101	TLSv1.3	93	Application Data

Running wire shark on Walmart.com



File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter … <Ctrl-/>

No.	Time	Source	Destination	Protoco	Length	Info
1121	9.564086968	74.40.74.40	10.0.2.15	DNS	127	Standard query response 0x186c A azmatch.adsrvr.org CNAME wa1-tracking-linux.adsrvr.org A 4.155.237.33
1122	9.564087183	74.40.74.40	10.0.2.15	DNS	176	Standard query response 0xca6d AAAA azmatch.adsrvr.org CNAME wa1-tracking-linux.adsrvr.org SOA dns1.p08.nsone.net
1463	10.570671709	10.0.2.15	74.40.74.40	DNS	142	Standard query 0x129c A hgy2n0ks7e2ac6zpimsor5gpuavx5ltfvtb6krxc15c43306a7579f80sac.d.aa.online-metrix.net
1464	10.570729741	10.0.2.15	74.40.74.40	DNS	142	Standard query 0x039e AAAA hgy2n0ks7e2ac6zpimsor5gpuavx5ltfvtb6krxc15c43306a7579f80sac.d.aa.online-metrix.net
1474	10.616692927	74.40.74.40	10.0.2.15	DNS	142	Standard query response 0x039e AAAA hgy2n0ks7e2ac6zpimsor5gpuavx5ltfvtb6krxc15c43306a7579f80sac.d.aa.online-metrix.net
1475	10.616692989	74.40.74.40	10.0.2.15	DNS	158	Standard query response 0x129c A hgy2n0ks7e2ac6zpimsor5gpuavx5ltfvtb6krxc15c43306a7579f80sac.d.aa.online-metrix.net A 192.2
170	6.052651423	10.0.2.15	192.225.158.2	ICMP	122	Destination unreachable (Port unreachable)
876	8.793803103	10.0.2.15	192.225.158.2	ICMP	122	Destination unreachable (Port unreachable)
877	8.793827601	10.0.2.15	192.225.158.2	ICMP	122	Destination unreachable (Port unreachable)
421	6.687395714	10.0.2.15	3.161.247.212	OCSP	479	Request
423	6.698572874	3.161.247.212	10.0.2.15	OCSP	998	Response
156	5.870646913	10.0.2.15	192.225.158.2	STUN	202	Refresh Request lifetime: 0 user: 1:hgy2n0ks:cm2-phrjqcxwoz-gbbc-wffheyzemfra9ze1;b185467f6d5ce1e7 realm: Default with nonce
169	6.052633235	192.225.158.2	10.0.2.15	STUN	94	Refresh Success Response lifetime: 0
563	7.161993869	10.0.2.15	192.225.158.2	STUN	86	Allocate Request UDP lifetime: 3600
566	7.200845869	10.0.2.15	192.225.158.2	STUN	98	Allocate Request UDP lifetime: 3600
575	7.214579696	192.225.158.2	10.0.2.15	STUN	114	Allocate Error Response error-code: 401 (Unauthenticated) Unauthorized realm: Default with nonce
577	7.220453558	10.0.2.15	192.225.158.2	STUN	194	Allocate Request UDP lifetime: 3600 user: 1:hgy2n0ks:XuyMkPynrjTHrS7xEul_phoaMek6xOHe1CYU realm: Default with nonce
578	7.247604213	192.225.158.2	10.0.2.15	STUN	126	Allocate Error Response error-code: 401 (Unauthenticated) Unauthorized realm: Default with nonce
580	7.250203846	10.0.2.15	192.225.158.2	STUN	206	Allocate Request UDP lifetime: 3600 user: 1:hgy2n0ks:XuyMkPynrjTHrS7xEul_phoaMek6xOHe1CYU realm: Default with nonce
588	7.264733260	192.225.158.2	10.0.2.15	STUN	118	Allocate Success Response XOR-RELAYED-ADDRESS: 47.186.192.164:42845 XOR-MAPPED-ADDRESS: 47.186.192.164:33769 lifetime: 3600
590	7.298080720	192.225.158.2	10.0.2.15	STUN	130	Allocate Success Response XOR-RELAYED-ADDRESS: 47.186.192.164:47003 XOR-MAPPED-ADDRESS: 47.186.192.164:42425 lifetime: 3600

▾ Source: PcsCompu_cb:7e:f5 (08:00:27:cb:7e:f5)
  Address: PcsCompu_cb:7e:f5 (08:00:27:cb:7e:f5)
  .... ..0. .... = LG bit: Globally unique address (factory default)
  ....0 .... = IG bit: Individual address (unicast)
Type: IPv4 (0x0800)
▾ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 20.230.171.39

0000 52 54 00 12 35 02 08 00 27 cb 7e f5 08 00 45 00 RT··5··· '·~···E·
0010 1c ac 9d 5d 40 00 40 06 b4 d2 0a 00 02 0f 14 e6 ···]@·@· ····
0020 ab 27 dd 12 01 bb 6c 24 6c 1f 0f d1 ed 60 50 18 ·'····l$ l····`P·
0030 f5 3c e8 ba 00 00 17 03 03 40 11 b2 1f 76 57 71 ·<····· ·@···vWq
0040 89 ea a0 89 e9 e5 dd 9e 7d d3 15 a7 8c 18 5a be ········ }·····Z·
0050 a0 3d a2 f3 a0 a1 a8 9b a5 fe 4f b9 35 d4 52 a3 ·=····· ··O·5·R·

I found many different protocols like dns, icmp, ocsp, stun, tcp, TLSv1.2, udp. It didn't use quic protocol.