CY-3001 NETWORKS AND CYBERSECURITY II
FALL 2023
ASSIGNMENT 1: Networking

Group members:

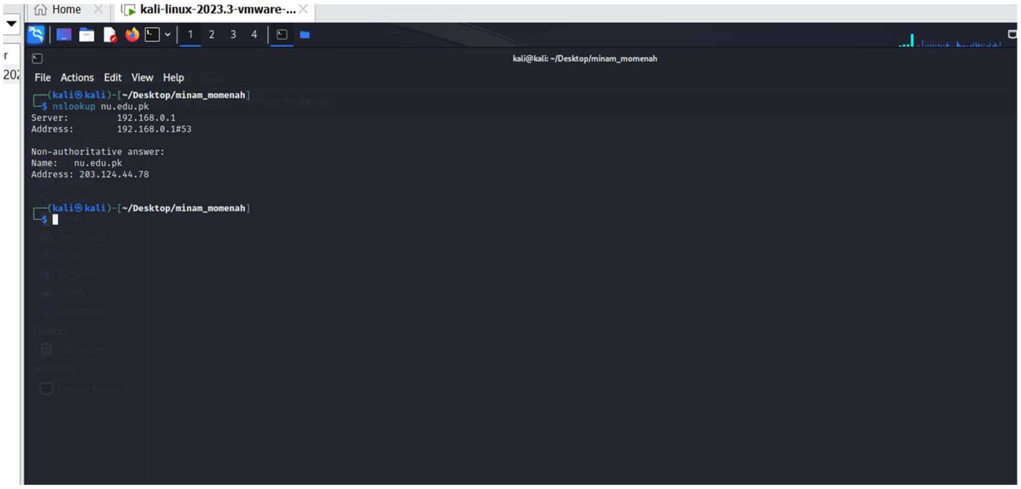
Minam Faisal (21i-1901)
Momenah Saif (21i-1909)

QUESTION# 1:

Nslookup:-

1. Run nslookup to obtain the IP address of the web server for the FAST-NU. What is the IP address of ***nu.edu.pk*?**

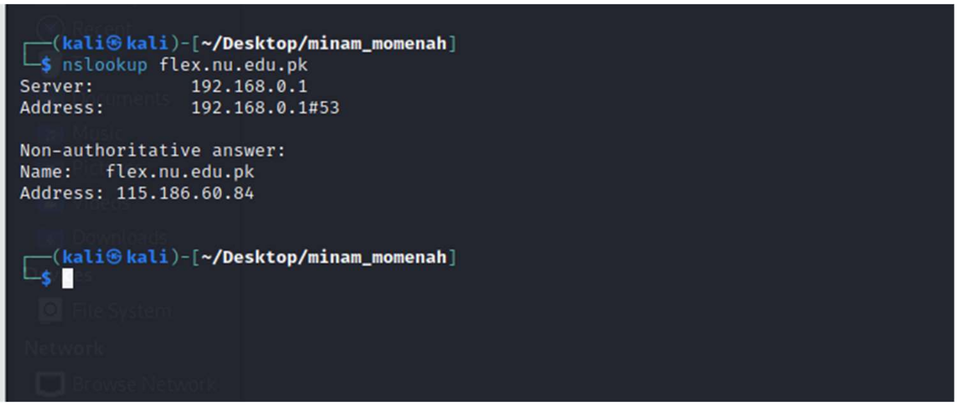
    A. The IP address of the web server for FAST-NU is 192.168.0.1 and the IP address of nu.edu.pk is 203.124.44.78.


Home
kali-linux-2023.3-vmware-...
1
2
3
4
kali@kali: ~/Desktop/minam_momenah
File
Actions
Edit
View
Help

```
┌──(kali㉿kali)-[~/Desktop/minam_momenah]
└─$ nslookup nu.edu.pk
Server:         192.168.0.1
Address:        192.168.0.1#53

Non-authoritative answer:
Name:   nu.edu.pk
Address: 203.124.44.78


┌──(kali㉿kali)-[~/Desktop/minam_momenah]
└─$ 
```

2. Run nslookup to obtain the IP address of the web server for the Flex. What is the IP address of ***flex.nu.edu.pk*?**

A. The IP address for flex.nu.edu.pk is 115.186.6.84.



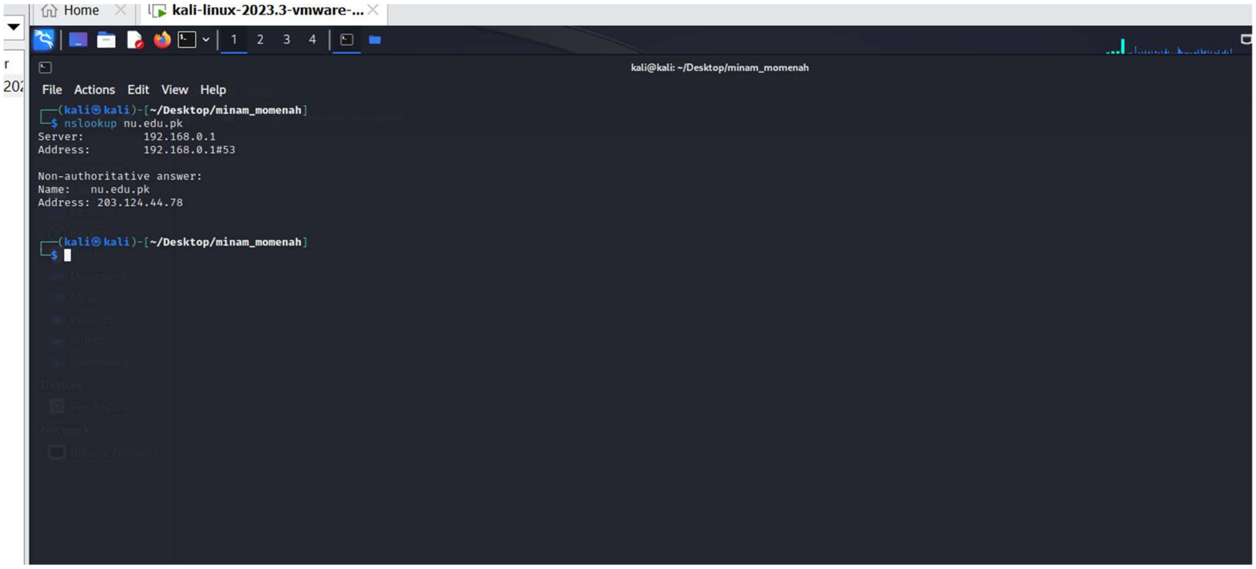
```
┌──(kali㉿kali)-[~/Desktop/minam_momenah]
└─$ nslookup flex.nu.edu.pk
Server:         192.168.0.1
Address:        192.168.0.1#53

Non-authoritative answer:
Name:   flex.nu.edu.pk
Address: 115.186.60.84

┌──(kali㉿kali)-[~/Desktop/minam_momenah]
└─$ █
```

3. What is the IP address of the DNS server that provided the answer to your nslookup command in question 1 above? Also, write the command to get this answer.

A. The IP address for the DNS server that provided the answer in Q1 is "192.168.0.1"

Commands used:

nslookup nu.edu.pk



Home
kali-linux-2023.3-vmware-...
1 2 3 4
kali@kali: ~/Desktop/minam_momenah
File Actions Edit View Help

```
┌──(kali㉿kali)-[~/Desktop/minam_momenah]
└─$ nslookup nu.edu.pk
Server:         192.168.0.1
Address:        192.168.0.1#53

Non-authoritative answer:
Name:   nu.edu.pk
Address: 203.124.44.78


┌──(kali㉿kali)-[~/Desktop/minam_momenah]
└─$ 
```

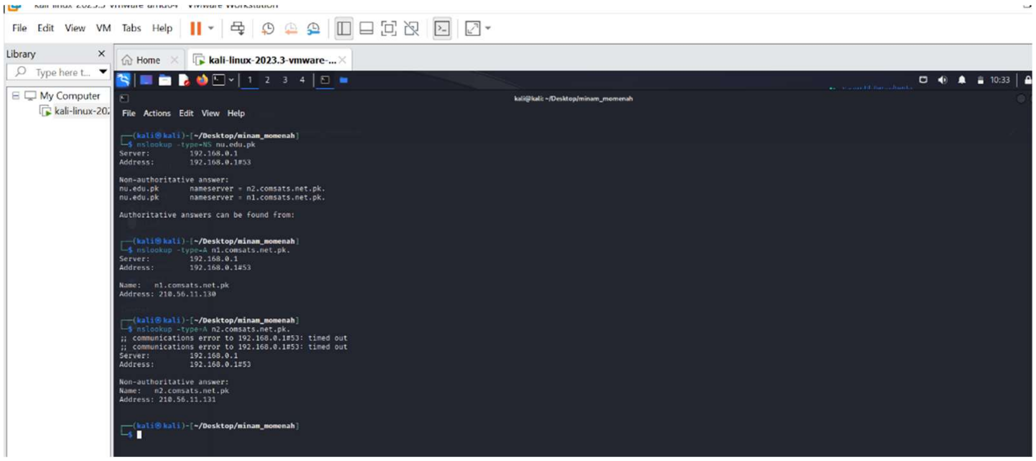
4. Did the answer to your nslookup command in question 1 above come from an authoritative or non-authoritative server?

A. The answer is from “non-authoritative server.”

5. What is the IP address and name of the Authoritative server of nu.edu.pk? Also, write the command to get this answer.

A. The name and IP addresses of Authoritative servers of nu.edu.pk are:
Name: n1.comsats.net.pk **IP address** = 210.56.11.130
Name: n2.comsats.net.pk **IP address** = 210.56.11.131

Command used:
nslookup -type=NS nu.edu.pk

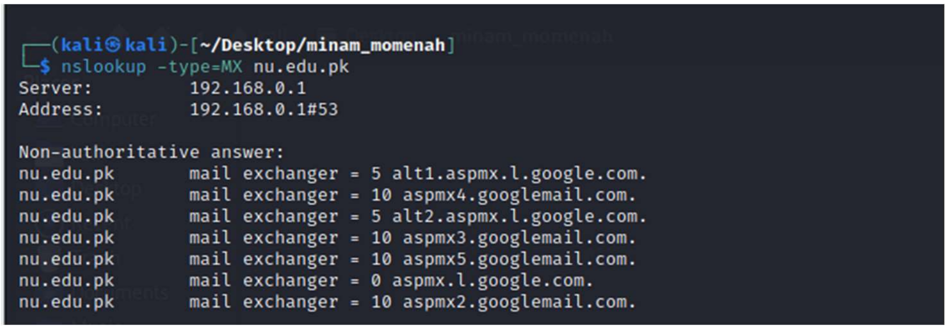


```
┌──(kali㉿kali)-[~/Desktop/minam_momenah]
└─$ nslookup -type=NS nu.edu.pk
Server:         192.168.0.1
Address:        192.168.0.1#53

Non-authoritative answer:
nu.edu.pk       nameserver = n2.comsats.net.pk.
nu.edu.pk       nameserver = n1.comsats.net.pk.

Authoritative answers can be found from:


┌──(kali㉿kali)-[~/Desktop/minam_momenah]
└─$ nslookup -type=A n1.comsats.net.pk.
Server:         192.168.0.1
Address:        192.168.0.1#53

Name:   n1.comsats.net.pk
Address: 210.56.11.130


┌──(kali㉿kali)-[~/Desktop/minam_momenah]
└─$ nslookup -type=A n2.comsats.net.pk.
;; communications error to 192.168.0.1#53: timed out
;; communications error to 192.168.0.1#53: timed out
Server:         192.168.0.1
Address:        192.168.0.1#53

Non-authoritative answer:
Name:   n2.comsats.net.pk
Address: 210.56.11.131


┌──(kali㉿kali)-[~/Desktop/minam_momenah]
└─$ 
```

6. MX records store all relevant Mail Exchange server data. This information is used to route all email requests for the domain to the appropriate mail server. Use the type mx for the domain 'nu.edu.pk' and list down the mail servers used by the nu domain.

A. List of mail-servers used by nu domain are:

alt2.aspmx.l.google.com
alt1.aspmx.l.google.com
aspm5.googlemail.com
aspm3.googlemail.com
aspmx.l.google.com
aspm4.googlemail.com
aspm2.googlemail.com



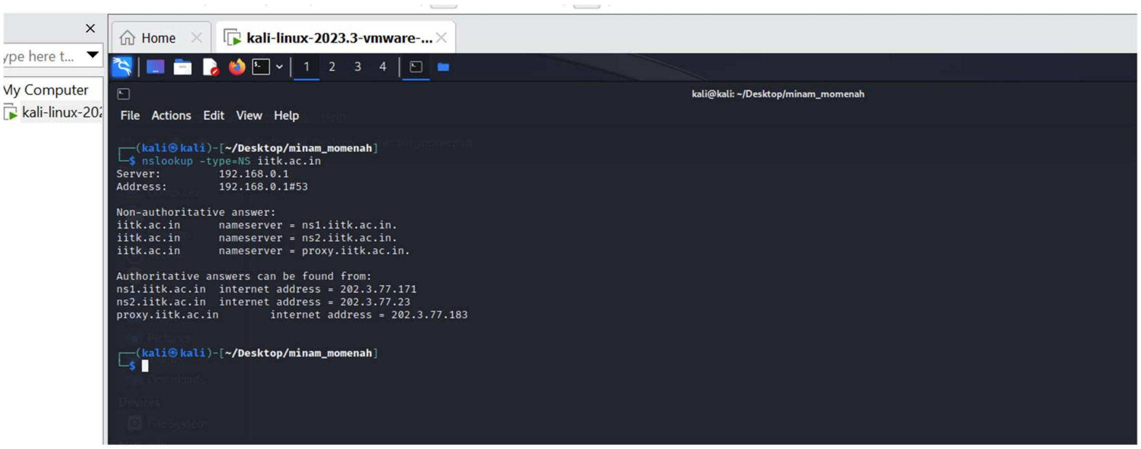
```
┌──(kali㉿kali)-[~/Desktop/minam_momenah]
└─$ nslookup -type=MX nu.edu.pk
Server:         192.168.0.1
Address:        192.168.0.1#53

Non-authoritative answer:
nu.edu.pk       mail exchanger = 5 alt1.aspmx.l.google.com.
nu.edu.pk       mail exchanger = 10 aspmx4.googlemail.com.
nu.edu.pk       mail exchanger = 5 alt2.aspmx.l.google.com.
nu.edu.pk       mail exchanger = 10 aspmx3.googlemail.com.
nu.edu.pk       mail exchanger = 10 aspmx5.googlemail.com.
nu.edu.pk       mail exchanger = 0 aspmx.l.google.com.
nu.edu.pk       mail exchanger = 10 aspmx2.googlemail.com.
```

7. Use the nslookup command to determine the name of the authoritative name server for the iit.ac.in domain. What is that name? (If there are more than one authoritative servers, what

is the name of the first authoritative server returned by nslookup)? If you had to find the IP address of that authoritative name server, how would you do so?

A. There are two authoritative servers of iitk.ac.in:

Name: ns1.iitk.ac.in **IP address**: 203.3.77.171
Name: ns2.iitk.ac.in **IP address:** 203.3.77.23

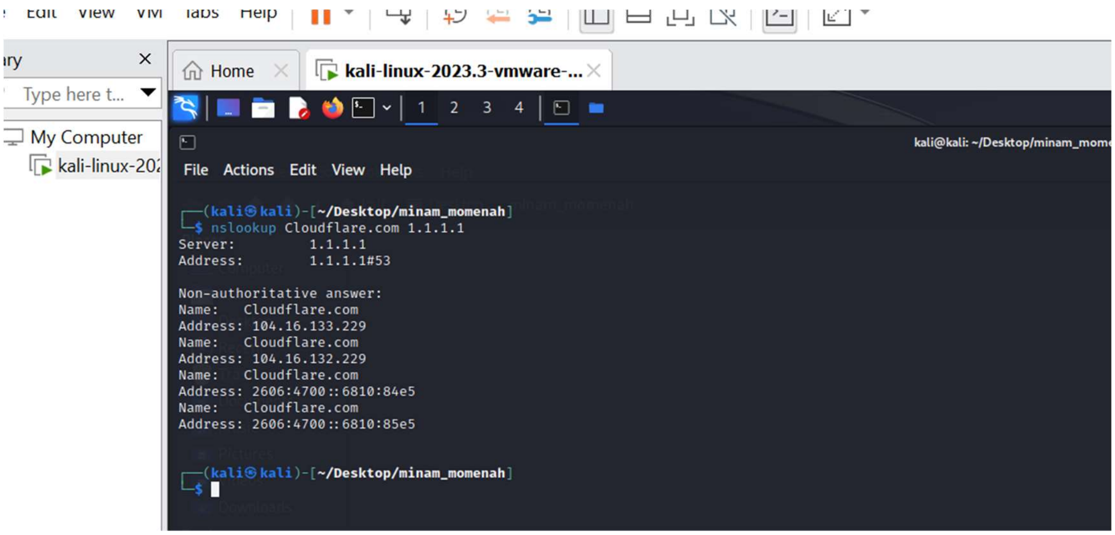

ype here t...
My Computer
kali-linux-202
Home
kali-linux-2023.3-vmware-...
1 2 3 4
kali@kali: ~/Desktop/minam_momenah
File Actions Edit View Help

```
┌──(kali㉿kali)-[~/Desktop/minam_momenah]
└─$ nslookup -type=NS iitk.ac.in
Server:         192.168.0.1
Address:        192.168.0.1#53

Non-authoritative answer:
iitk.ac.in      nameserver = ns1.iitk.ac.in.
iitk.ac.in      nameserver = ns2.iitk.ac.in.
iitk.ac.in      nameserver = proxy.iitk.ac.in.

Authoritative answers can be found from:
ns1.iitk.ac.in  internet address = 202.3.77.171
ns2.iitk.ac.in  internet address = 202.3.77.23
proxy.iitk.ac.in        internet address = 202.3.77.183

┌──(kali㉿kali)-[~/Desktop/minam_momenah]
└─$ 
```

8. In this example, we indicate that we want to the query sent to a DNS server (choose one from the list below) rather than to the default DNS server (dns-dns.google). Thus, the query and reply transaction takes place directly between our querying host and the other DNS server. Write the command for this lookup and also the name/IP of the DNS server used. [4] (syntax: lookup domain name DNS_server_ip/name).

A. Name: Cloudflare.com IP address: 1.1.1.1

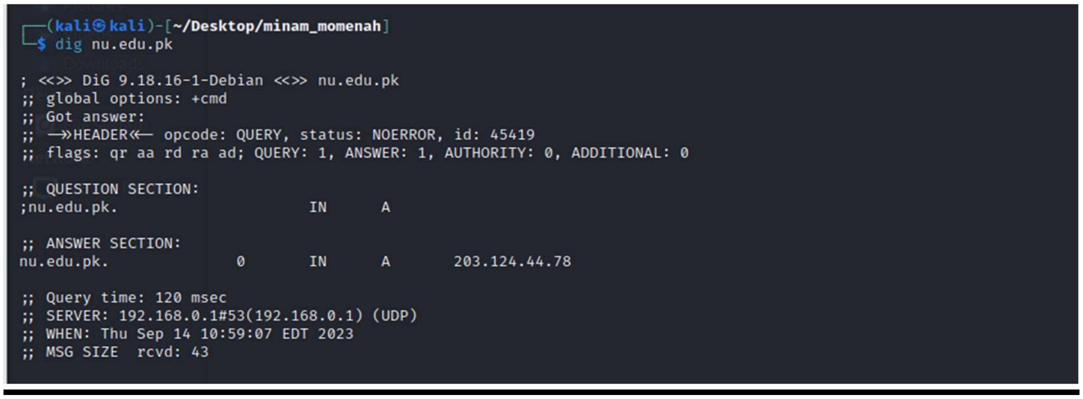
Command used:
nslookup Cloudflare.com 1.1.1.1


Edit View VM Tabs Help
ary
Type here t...
My Computer
kali-linux-202
Home
kali-linux-2023.3-vmware-...
1 2 3 4
kali@kali: ~/Desktop/minam_mome
File Actions Edit View Help

```
┌──(kali㉿kali)-[~/Desktop/minam_momenah]
└─$ nslookup Cloudflare.com 1.1.1.1
Server:         1.1.1.1
Address:        1.1.1.1#53

Non-authoritative answer:
Name:   Cloudflare.com
Address: 104.16.133.229
Name:   Cloudflare.com
Address: 104.16.132.229
Name:   Cloudflare.com
Address: 2606:4700::6810:84e5
Name:   Cloudflare.com
Address: 2606:4700::6810:85e5

┌──(kali㉿kali)-[~/Desktop/minam_momenah]
└─$ ▮
```

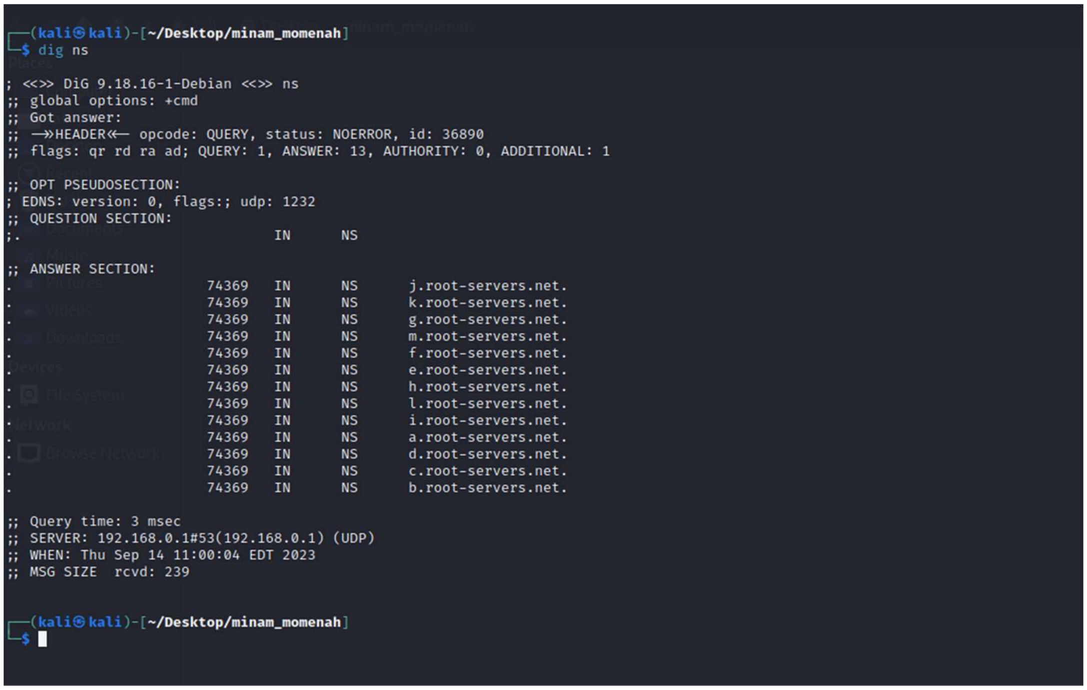
Bind 9:-

1. Use dig command for nu.edu.pk and analyses the query and answer sections. It should provide information on the record type a DNS server returns. Provide a screenshot.

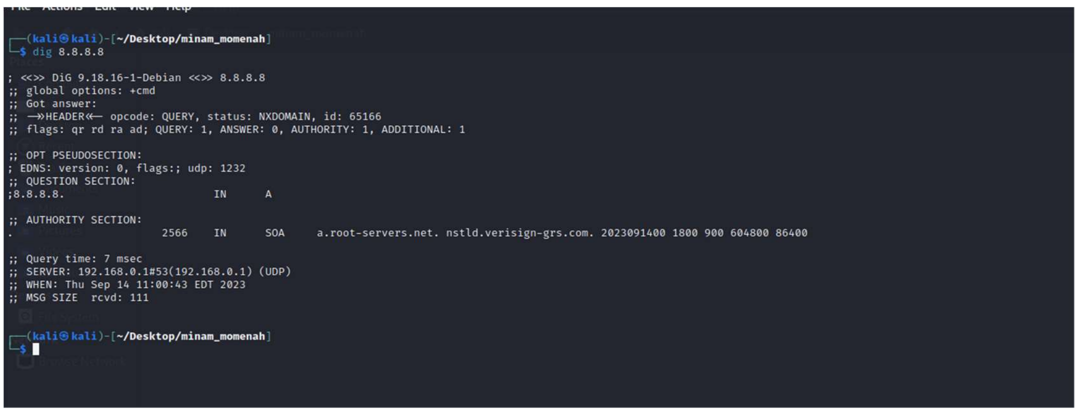


```
┌──(kali㉿kali)-[~/Desktop/minam_momenah]
└─$ dig nu.edu.pk

; <<>> DiG 9.18.16-1-Debian <<>> nu.edu.pk
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 45419
;; flags: qr aa rd ra ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;nu.edu.pk.                     IN      A

;; ANSWER SECTION:
nu.edu.pk.              0       IN      A       203.124.44.78

;; Query time: 120 msec
;; SERVER: 192.168.0.1#53(192.168.0.1) (UDP)
;; WHEN: Thu Sep 14 10:59:07 EDT 2023
;; MSG SIZE  rcvd: 43
```

2. Let’s query our DNS server for information on the Root servers. Just type ‘dig ns’ and should see the list of root servers. If this does not work then use the dig command for dns.google (dig 8.8.8.8). You should see a list of root servers comes for the dns.google. Provide your screenshot.

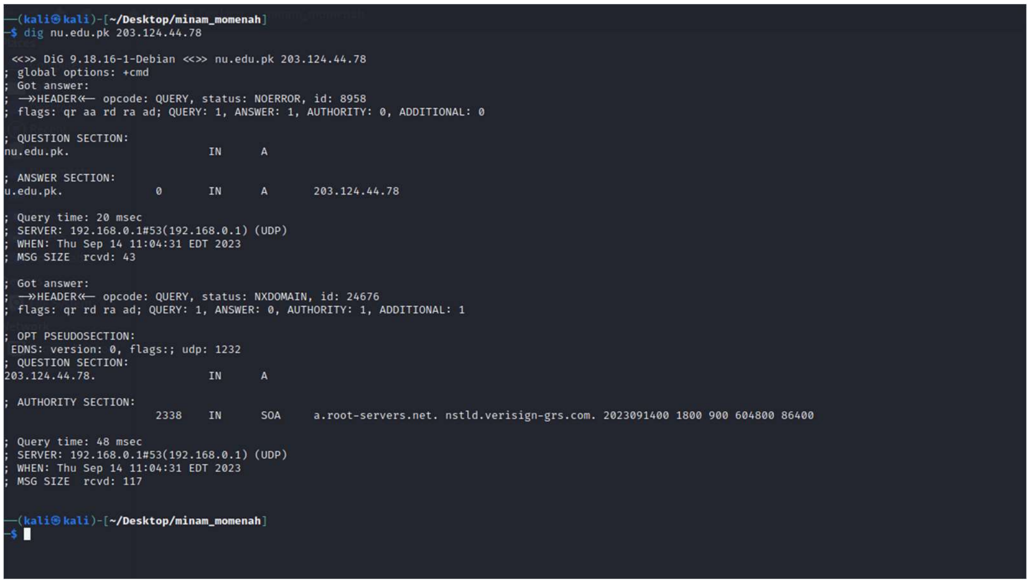


```
┌──(kali㉿kali)-[~/Desktop/minam_momenah]
└─$ dig ns

; <<>> DiG 9.18.16-1-Debian <<>> ns
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 36890
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 13, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;.                              IN      NS

;; ANSWER SECTION:
.                       74369   IN      NS      j.root-servers.net.
.                       74369   IN      NS      k.root-servers.net.
.                       74369   IN      NS      g.root-servers.net.
.                       74369   IN      NS      m.root-servers.net.
.                       74369   IN      NS      f.root-servers.net.
.                       74369   IN      NS      e.root-servers.net.
.                       74369   IN      NS      h.root-servers.net.
.                       74369   IN      NS      l.root-servers.net.
.                       74369   IN      NS      i.root-servers.net.
.                       74369   IN      NS      a.root-servers.net.
.                       74369   IN      NS      d.root-servers.net.
.                       74369   IN      NS      c.root-servers.net.
.                       74369   IN      NS      b.root-servers.net.

;; Query time: 3 msec
;; SERVER: 192.168.0.1#53(192.168.0.1) (UDP)
;; WHEN: Thu Sep 14 11:00:04 EDT 2023
;; MSG SIZE  rcvd: 239


┌──(kali㉿kali)-[~/Desktop/minam_momenah]
└─$ 
```



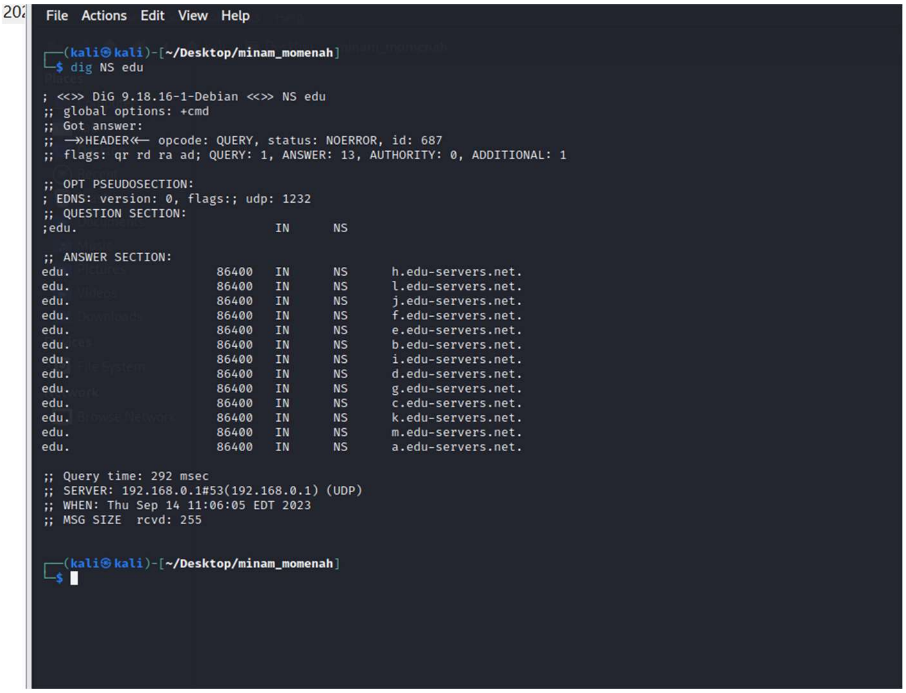
```
┌──(kali㉿kali)-[~/Desktop/minam_momenah]
└─$ dig 8.8.8.8

; <<>> DiG 9.18.16-1-Debian <<>> 8.8.8.8
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 65166
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;8.8.8.8.                       IN      A

;; AUTHORITY SECTION:
.                       2566    IN      SOA     a.root-servers.net. nstld.verisign-grs.com. 2023091400 1800 900 604800 86400

;; Query time: 7 msec
;; SERVER: 192.168.0.1#53(192.168.0.1) (UDP)
;; WHEN: Thu Sep 14 11:00:43 EDT 2023
;; MSG SIZE  rcvd: 111


┌──(kali㉿kali)-[~/Desktop/minam_momenah]
└─$ 
```

3. Let’s directly query about ‘nu.edu.pk’ from its authoritative server and see the output. Provide the screenshot.



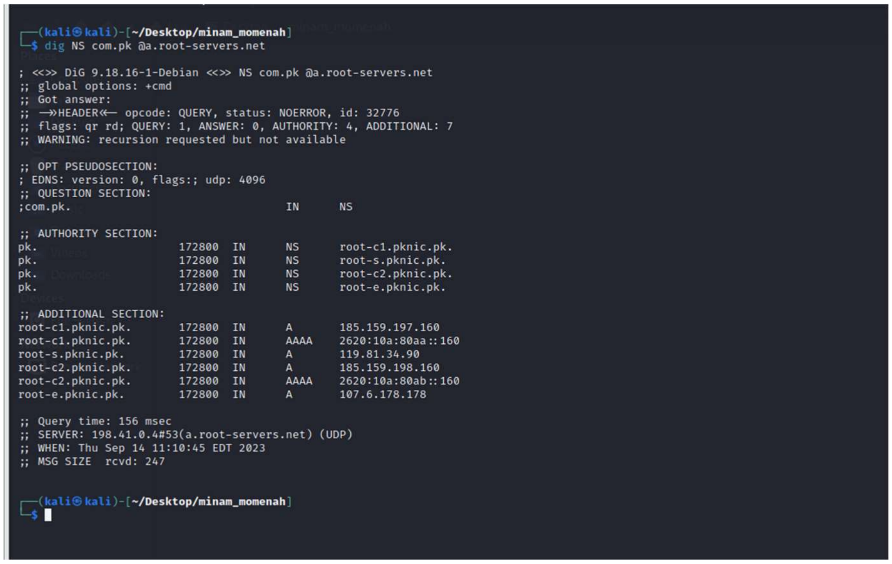
```
—(kali㉿kali)-[~/Desktop/minam_momenah]
—$ dig nu.edu.pk 203.124.44.78

 <<>> DiG 9.18.16-1-Debian <<>> nu.edu.pk 203.124.44.78
; global options: +cmd
; Got answer:
; —»HEADER«— opcode: QUERY, status: NOERROR, id: 8958
; flags: qr aa rd ra ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

; QUESTION SECTION:
nu.edu.pk.                    IN      A

; ANSWER SECTION:
u.edu.pk.             0       IN      A       203.124.44.78

; Query time: 20 msec
; SERVER: 192.168.0.1#53(192.168.0.1) (UDP)
; WHEN: Thu Sep 14 11:04:31 EDT 2023
; MSG SIZE  rcvd: 43

; Got answer:
; —»HEADER«— opcode: QUERY, status: NXDOMAIN, id: 24676
; flags: qr rd ra ad; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

; OPT PSEUDOSECTION:
 EDNS: version: 0, flags:; udp: 1232
; QUESTION SECTION:
203.124.44.78.                IN      A

; AUTHORITY SECTION:
                      2338    IN      SOA     a.root-servers.net. nstld.verisign-grs.com. 2023091400 1800 900 604800 86400

; Query time: 48 msec
; SERVER: 192.168.0.1#53(192.168.0.1) (UDP)
; WHEN: Thu Sep 14 11:04:31 EDT 2023
; MSG SIZE  rcvd: 117


—(kali㉿kali)-[~/Desktop/minam_momenah]
—$
```

4. Getting the list of TLD servers for .edu (provide a screenshot).



```
┌──(kali㉿kali)-[~/Desktop/minam_momenah]
└─$ dig NS edu

; <<>> DiG 9.18.16-1-Debian <<>> NS edu
;; global options: +cmd
;; Got answer:
;; —»HEADER«— opcode: QUERY, status: NOERROR, id: 687
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 13, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;edu.                           IN      NS

;; ANSWER SECTION:
edu.                    86400   IN      NS      h.edu-servers.net.
edu.                    86400   IN      NS      l.edu-servers.net.
edu.                    86400   IN      NS      j.edu-servers.net.
edu.                    86400   IN      NS      f.edu-servers.net.
edu.                    86400   IN      NS      e.edu-servers.net.
edu.                    86400   IN      NS      b.edu-servers.net.
edu.                    86400   IN      NS      i.edu-servers.net.
edu.                    86400   IN      NS      d.edu-servers.net.
edu.                    86400   IN      NS      g.edu-servers.net.
edu.                    86400   IN      NS      c.edu-servers.net.
edu.                    86400   IN      NS      k.edu-servers.net.
edu.                    86400   IN      NS      m.edu-servers.net.
edu.                    86400   IN      NS      a.edu-servers.net.

;; Query time: 292 msec
;; SERVER: 192.168.0.1#53(192.168.0.1) (UDP)
;; WHEN: Thu Sep 14 11:06:05 EDT 2023
;; MSG SIZE  rcvd: 255


┌──(kali㉿kali)-[~/Desktop/minam_momenah]
└─$
```

5. Getting the list of ‘com.pk’ servers from ‘a.root-servers.net (provide a screenshot).



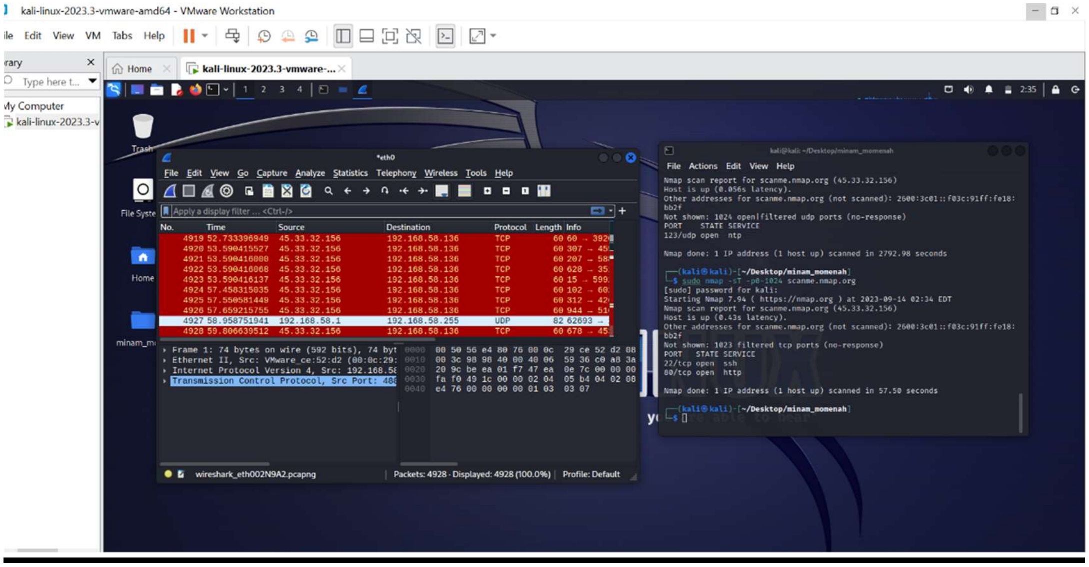
```
┌──(kali㉿kali)-[~/Desktop/minam_momenah]
└─$ dig NS com.pk @a.root-servers.net

; <<>> DiG 9.18.16-1-Debian <<>> NS com.pk @a.root-servers.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 32776
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 4, ADDITIONAL: 7
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;com.pk.                                IN      NS

;; AUTHORITY SECTION:
pk.                     172800  IN      NS      root-c1.pknic.pk.
pk.                     172800  IN      NS      root-s.pknic.pk.
pk.                     172800  IN      NS      root-c2.pknic.pk.
pk.                     172800  IN      NS      root-e.pknic.pk.

;; ADDITIONAL SECTION:
root-c1.pknic.pk.       172800  IN      A       185.159.197.160
root-c1.pknic.pk.       172800  IN      AAAA    2620:10a:80aa::160
root-s.pknic.pk.        172800  IN      A       119.81.34.90
root-c2.pknic.pk.       172800  IN      A       185.159.198.160
root-c2.pknic.pk.       172800  IN      AAAA    2620:10a:80ab::160
root-e.pknic.pk.        172800  IN      A       107.6.178.178

;; Query time: 156 msec
;; SERVER: 198.41.0.4#53(a.root-servers.net) (UDP)
;; WHEN: Thu Sep 14 11:10:45 EDT 2023
;; MSG SIZE  rcvd: 247


┌──(kali㉿kali)-[~/Desktop/minam_momenah]
└─$ █
```

QUESTION # 2

Port scanning:-

1. What is the full command you used to run the TCP port scan (including arguments)?

A. The full command I used to run TCP port scan is:
sudo nmap –sT –p0-1024 scanme.nmap.org

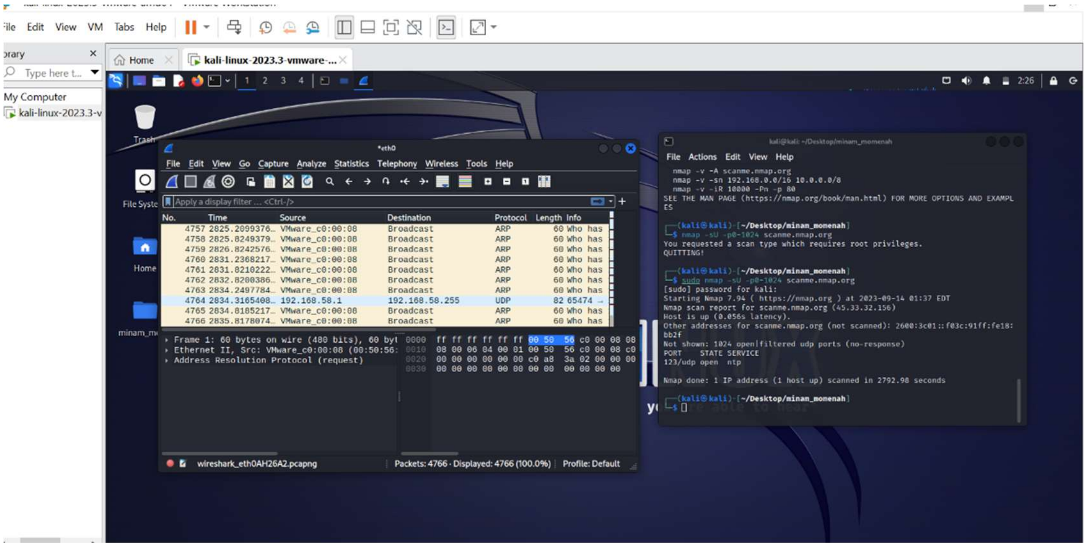

kali-linux-2023.3-vmware-amd64 - VMware Workstation
Home
kali-linux-2023.3-vmware-...
My Computer
kali-linux-2023.3-v
Trash
File System
Home
minam_m
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
kali@kali: ~/Desktop/minam_momenah
File Actions Edit View Help
2:35

```
No.  Time         Source        Destination     Protocol Length Info
4919 52.733396949 45.33.32.156  192.168.58.136  TCP      60 60 → 392
4920 53.590415527 45.33.32.156  192.168.58.136  TCP      60 307 → 45
4921 53.590416808 45.33.32.156  192.168.58.136  TCP      60 207 → 58
4922 53.590416068 45.33.32.156  192.168.58.136  TCP      60 628 → 35
4923 53.590416137 45.33.32.156  192.168.58.136  TCP      60 15 → 599
4924 57.458315035 45.33.32.156  192.168.58.136  TCP      60 102 → 60
4925 57.550581449 45.33.32.156  192.168.58.136  TCP      60 312 → 42
4926 57.659215755 45.33.32.156  192.168.58.136  TCP      60 944 → 51
4927 58.958751941 192.168.58.1  192.168.58.255  UDP      82 62693 →
4928 59.806639512 45.33.32.156  192.168.58.136  TCP      60 678 → 45

› Frame 1: 74 bytes on wire (592 bits), 74 byt   0000  00 50 56 e4 80 76 00 0c  29 ce 52 d2 08
› Ethernet II, Src: VMware_ce:52:d2 (00:0c:29:   0010  00 3c 98 98 40 00 40 06  59 36 c0 a8 3a
› Internet Protocol Version 4, Src: 192.168.58   0020  20 9c be ea 01 f7 47 ea  0e 7c 00 00 00
› Transmission Control Protocol, Src Port: 488   0030  fa f0 49 1c 00 00 02 04  05 b4 04 02 08
                                                 0040  e4 76 00 00 00 00 01 03  03 07

wireshark_eth002N9A2.pcapng | Packets: 4928 · Displayed: 4928 (100.0%) | Profile: Default
```

```
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.056s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:
bb2f
Not shown: 1024 open|filtered udp ports (no-response)
PORT    STATE SERVICE
123/udp open  ntp

Nmap done: 1 IP address (1 host up) scanned in 2792.98 seconds

┌──(kali㉿kali)-[~/Desktop/minam_momenah]
└─$ sudo nmap -sT -p0-1024 scanme.nmap.org
[sudo] password for kali:
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-14 02:34 EDT
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.43s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:
bb2f
Not shown: 1023 filtered tcp ports (no-response)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 57.50 seconds

┌──(kali㉿kali)-[~/Desktop/minam_momenah]
└─$ ▯
```

2. What is the full command you used to run the UDP port scan (including arguments)?

A. The full command I used to run UDP port scan is:
sudo nmap –sU –p0-1024 scanme.nmap.org

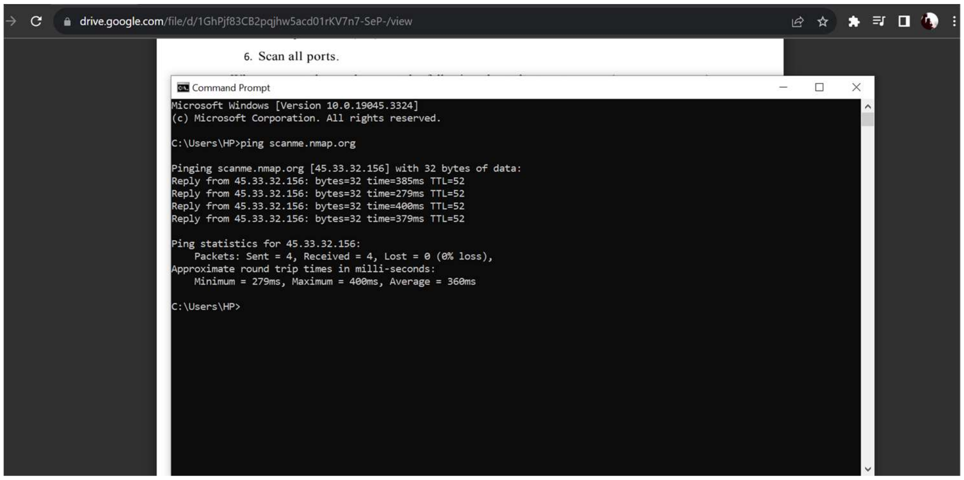

Home
kali-linux-2023.3-vmware-...
My Computer
kali-linux-2023.3-v
Trash
File System
Home
minam_m
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
kali@kali: ~/Desktop/minam_momenah
File Actions Edit View Help
2:26

```
No.  Time           Source           Destination     Protocol Length Info
4757 2825.2099376… VMware_c0:00:08  Broadcast       ARP      60 Who has
4758 2825.8249379… VMware_c0:00:08  Broadcast       ARP      60 Who has
4759 2826.8242576… VMware_c0:00:08  Broadcast       ARP      60 Who has
4760 2831.2368217… VMware_c0:00:08  Broadcast       ARP      60 Who has
4761 2831.8210222… VMware_c0:00:08  Broadcast       ARP      60 Who has
4762 2832.8200386… VMware_c0:00:08  Broadcast       ARP      60 Who has
4763 2834.2497784… VMware_c0:00:08  Broadcast       ARP      60 Who has
4764 2834.3165408… 192.168.58.1     192.168.58.255  UDP      82 65474 →
4765 2834.8185217… VMware_c0:00:08  Broadcast       ARP      60 Who has
4766 2835.8178074… VMware_c0:00:08  Broadcast       ARP      60 Who has

› Frame 1: 60 bytes on wire (480 bits), 60 byt   0000  ff ff ff ff ff ff 00 50  56 c0 00 08 08
› Ethernet II, Src: VMware_c0:00:08 (00:50:56:   0010  08 00 06 04 00 01 00 50  56 c0 00 08 c0
› Address Resolution Protocol (request)          0020  00 00 00 00 00 00 c0 a8  3a 02 00 00 00
                                                 0030  00 00 00 00 00 00 00 00  00 00 00 00

wireshark_eth0AH26A2.pcapng | Packets: 4766 · Displayed: 4766 (100.0%) | Profile: Default
```

```
  nmap -v -A scanme.nmap.org
  nmap -v -sn 192.168.0.0/16 10.0.0.0/8
  nmap -v -iR 10000 -Pn -p 80
SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPL
ES

┌──(kali㉿kali)-[~/Desktop/minam_momenah]
└─$ nmap -sU -p0-1024 scanme.nmap.org
You requested a scan type which requires root privileges.
QUITTING!

┌──(kali㉿kali)-[~/Desktop/minam_momenah]
└─$ sudo nmap -sU -p0-1024 scanme.nmap.org
[sudo] password for kali:
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-14 01:37 EDT
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.056s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:
bb2f
Not shown: 1024 open|filtered udp ports (no-response)
PORT    STATE SERVICE
123/udp open  ntp

Nmap done: 1 IP address (1 host up) scanned in 2792.98 seconds

┌──(kali㉿kali)-[~/Desktop/minam_momenah]
└─$ ▯
```

3. What is the IP address of scanme.nmap.org? Please provide a screenshot of your scan.

A. The IP address of scanme.nmap.org is:
“**45.33.32.156**”


drive.google.com/file/d/1GhPjf83CB2pqjhw5acd01rKV7n7-SeP-/view
Command Prompt

6. Scan all ports.

```
Microsoft Windows [Version 10.0.19045.3324]
(c) Microsoft Corporation. All rights reserved.

C:\Users\HP>ping scanme.nmap.org

Pinging scanme.nmap.org [45.33.32.156] with 32 bytes of data:
Reply from 45.33.32.156: bytes=32 time=385ms TTL=52
Reply from 45.33.32.156: bytes=32 time=279ms TTL=52
Reply from 45.33.32.156: bytes=32 time=400ms TTL=52
Reply from 45.33.32.156: bytes=32 time=379ms TTL=52

Ping statistics for 45.33.32.156:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 279ms, Maximum = 400ms, Average = 360ms

C:\Users\HP>
```

4. What ports are open on the target server? What applications are running on those ports? (For this part, you only need to report the service name printed by nmap.)

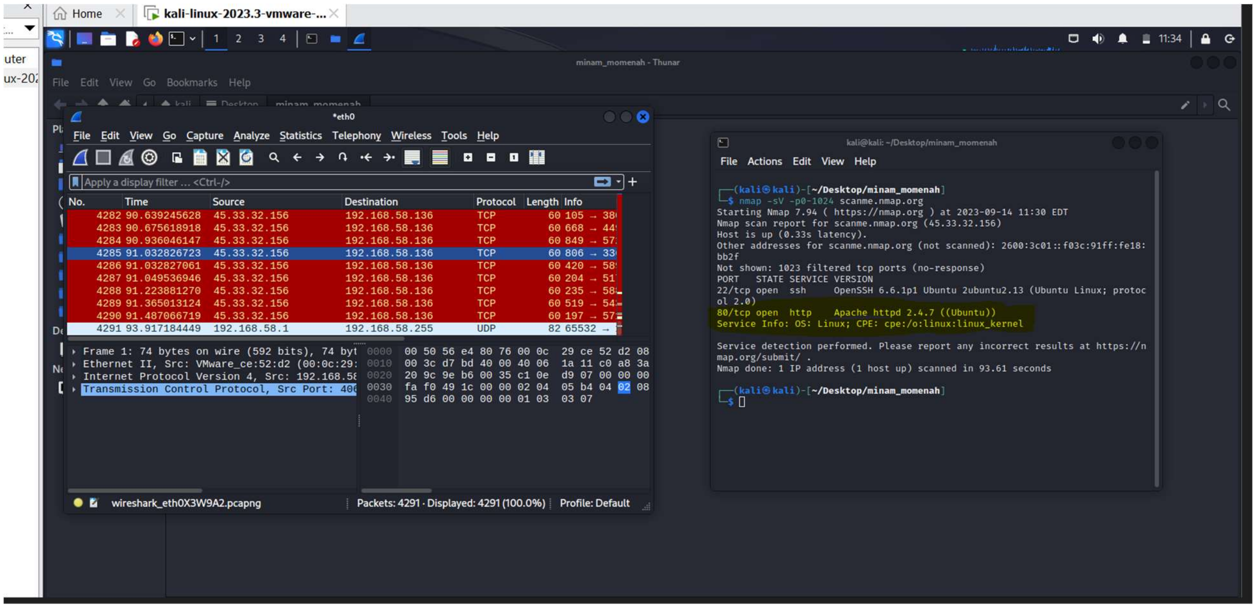
A.

PORT	**SERVICE**
TCP (80)	http
TCP (22)	ssh
UDP (1,2,3)	Compressnet tcpmux

5. The target machine is also running a webserver. What webserver software and version are being used? What ports does it run on? Please provide the full command and the screenshot of your scan.

A. The webserver software and version is used :
On port 80/tcp. Apache http webserver software with version 2.4.7 (Ubuntu).
Command used:

sudo nmap –sV –p0-1024 scanme.nmap.org



Home
kali-linux-2023.3-vmware-...
minam_momenah - Thunar
File Edit View Go Bookmarks Help
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
kali@kali: ~/Desktop/minam_momenah
File Actions Edit View Help
11:34

```
No.  Time         Source        Destination     Protocol Length Info
4282 90.639245628 45.33.32.156  192.168.58.136  TCP          60 105 → 38
4283 90.675618918 45.33.32.156  192.168.58.136  TCP          60 668 → 44
4284 90.936046147 45.33.32.156  192.168.58.136  TCP          60 849 → 57
4285 91.032826723 45.33.32.156  192.168.58.136  TCP          60 806 → 33
4286 91.032827061 45.33.32.156  192.168.58.136  TCP          60 420 → 58
4287 91.049536946 45.33.32.156  192.168.58.136  TCP          60 204 → 51
4288 91.223881270 45.33.32.156  192.168.58.136  TCP          60 235 → 58
4289 91.365013124 45.33.32.156  192.168.58.136  TCP          60 519 → 54
4290 91.487066719 45.33.32.156  192.168.58.136  TCP          60 197 → 57
4291 93.917184449 192.168.58.1  192.168.58.255  UDP          82 65532 →

› Frame 1: 74 bytes on wire (592 bits), 74 byt   0000  00 50 56 e4 80 76 00 0c  29 ce 52 d2 08
› Ethernet II, Src: VMware_ce:52:d2 (00:0c:29:   0010  00 3c d7 bd 40 00 40 06  1a 11 c0 a8 3a
› Internet Protocol Version 4, Src: 192.168.58   0020  20 9c 9e b6 00 35 c1 0e  d9 07 00 00 00
› Transmission Control Protocol, Src Port: 40    0030  fa f0 49 1c 00 00 02 04  05 b4 04 02 08
                                                 0040  95 d6 00 00 00 00 01 03  03 07

wireshark_eth0X3W9A2.pcapng    Packets: 4291 · Displayed: 4291 (100.0%)    Profile: Default
```

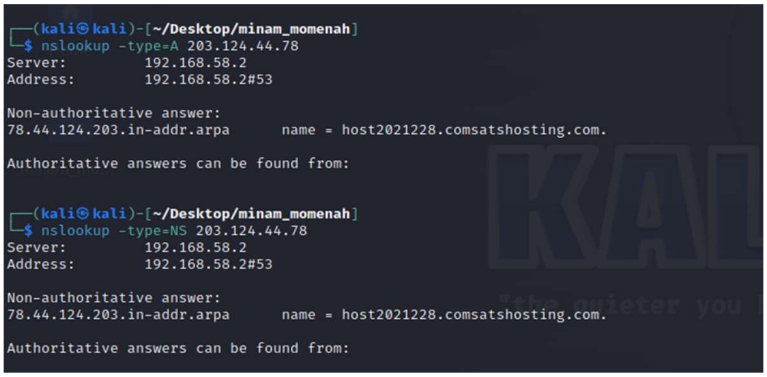
```
┌──(kali㉿kali)-[~/Desktop/minam_momenah]
└─$ nmap -sV -p0-1024 scanme.nmap.org
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-14 11:30 EDT
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.33s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:
bb2f
Not shown: 1023 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protoc
ol 2.0)
80/tcp open  http    Apache httpd 2.4.7 ((Ubuntu))
Service Info: OS: 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 93.61 seconds

┌──(kali㉿kali)-[~/Desktop/minam_momenah]
└─$ 
```

6. Find the IP of the nu.edu.pk web server. Then use the nslookup on this IP to find out the name of the server's name. Please provide the full command and the screenshot of your scan.

A. The IP address of nu.edu.pk webserver is "**203.124.44.78**"

Name: host2021228.comsatshosting.com
IP address: 78.44.124.203

Command used:
nslookup -type=NS 203.124.44.78

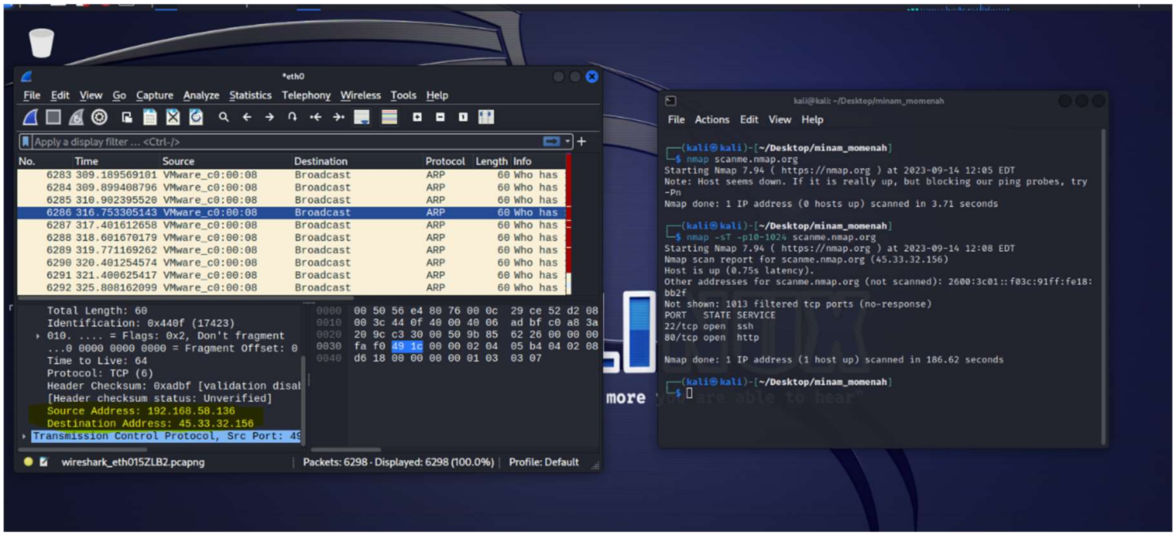


```
┌──(kali㉿kali)-[~/Desktop/minam_momenah]
└─$ nslookup -type=A 203.124.44.78
Server:         192.168.58.2
Address:        192.168.58.2#53

Non-authoritative answer:
78.44.124.203.in-addr.arpa      name = host2021228.comsatshosting.com.

Authoritative answers can be found from:


┌──(kali㉿kali)-[~/Desktop/minam_momenah]
└─$ nslookup -type=NS 203.124.44.78
Server:         192.168.58.2
Address:        192.168.58.2#53

Non-authoritative answer:
78.44.124.203.in-addr.arpa      name = host2021228.comsatshosting.com.

Authoritative answers can be found from:
```

Wireshark:-

1. Write down the IP address of your machine and the IP address of destination server. Also, provide a screenshot with Highlighted IP addresses.

A. Source IP:
192.168.58.136
Destination IP:
45.33.32.156



*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
wireshark_eth015ZLB2.pcapng
Packets: 6298 · Displayed: 6298 (100.0%)
Profile: Default
kali@kali: ~/Desktop/minam_momenah
File Actions Edit View Help

```
No.  Time            Source             Destination  Protocol Length Info
6283 309.189569101 VMware_c0:00:08 Broadcast    ARP      60 Who has
6284 309.899408796 VMware_c0:00:08 Broadcast    ARP      60 Who has
6285 310.902395520 VMware_c0:00:08 Broadcast    ARP      60 Who has
6286 316.753305143 VMware_c0:00:08 Broadcast    ARP      60 Who has
6287 317.401612658 VMware_c0:00:08 Broadcast    ARP      60 Who has
6288 318.601670179 VMware_c0:00:08 Broadcast    ARP      60 Who has
6289 319.771169262 VMware_c0:00:08 Broadcast    ARP      60 Who has
6290 320.401254574 VMware_c0:00:08 Broadcast    ARP      60 Who has
6291 321.400625417 VMware_c0:00:08 Broadcast    ARP      60 Who has
6292 325.808162099 VMware_c0:00:08 Broadcast    ARP      60 Who has
```

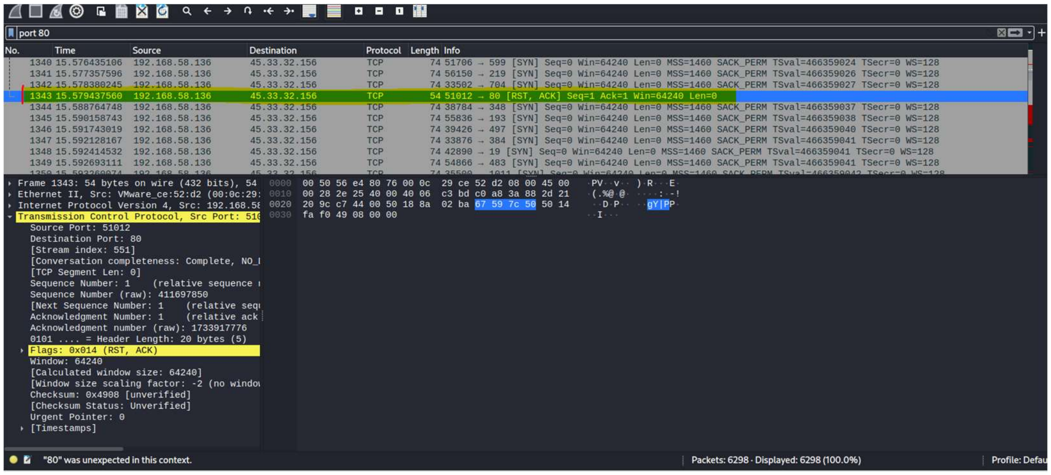
```
    Total Length: 60
    Identification: 0x440f (17423)
  › 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: TCP (6)
    Header Checksum: 0xadbf [validation disal
    [Header checksum status: Unverified]
    Source Address: 192.168.58.136
    Destination Address: 45.33.32.156
› Transmission Control Protocol, Src Port: 49
```

```
0000  00 50 56 e4 80 76 00 0c  29 ce 52 d2 08
0010  00 3c 44 0f 40 00 40 06  ad bf c0 a8 3a
0020  20 9c c3 30 00 50 9b 85  62 26 00 00 00
0030  fa f0 49 1c 00 00 02 04  05 b4 04 02 08
0040  d6 18 00 00 00 00 01 03  03 07
```

```
┌──(kali㉿kali)-[~/Desktop/minam_momenah]
└─$ nmap scanme.nmap.org
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-14 12:05 EDT
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 3.71 seconds

┌──(kali㉿kali)-[~/Desktop/minam_momenah]
└─$ nmap -sT -p10-1024 scanme.nmap.org
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-14 12:08 EDT
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.75s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:
bb2f
Not shown: 1013 filtered tcp ports (no-response)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 186.62 seconds

┌──(kali㉿kali)-[~/Desktop/minam_momenah]
└─$ 
```

2. What does it mean for a port on scanme.nmap.org to be "closed?" More specifically, what is the TCP packet type, if any, the server gives in response to a SYN packet sent to port that is "closed?" Justify your answer with the screenshots from the captured file in wireshark.

A. A "closed" port results in the server responding to a SYN packet with a TCP RST message, indicating it's not available for incoming connections. In contrast, "open" ports reply with a SYN-ACK to show readiness for connection. In this case, port 80 is confirmed as closed.



port 80

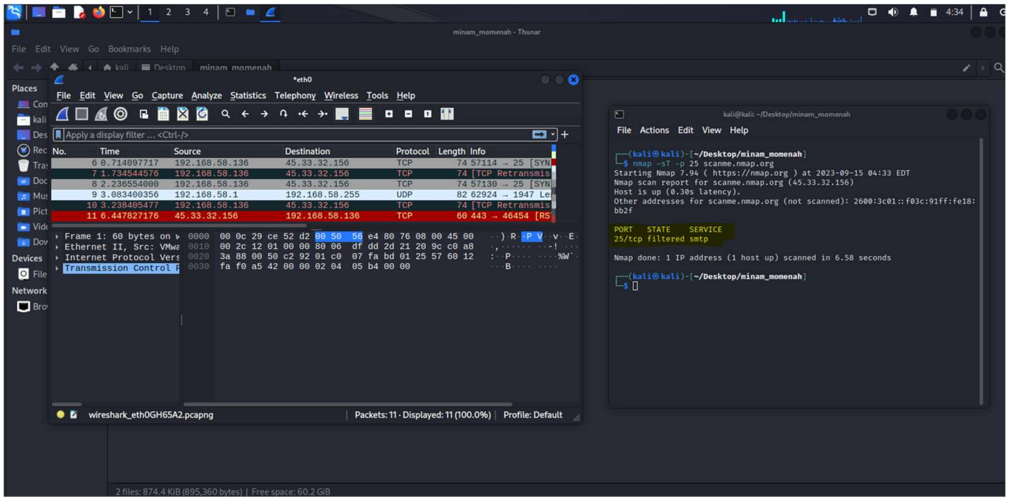
```
No.  Time           Source          Destination   Protocol Length Info
1340 15.576435106   192.168.58.136  45.33.32.156  TCP      74 51706 → 599 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=466359024 TSecr=0 WS=128
1341 15.577357596   192.168.58.136  45.33.32.156  TCP      74 56150 → 219 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=466359026 TSecr=0 WS=128
1342 15.578380245   192.168.58.136  45.33.32.156  TCP      74 33502 → 704 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=466359027 TSecr=0 WS=128
1343 15.579437560   192.168.58.136  45.33.32.156  TCP      54 51012 → 80 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
1344 15.588764748   192.168.58.136  45.33.32.156  TCP      74 38784 → 348 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=466359037 TSecr=0 WS=128
1345 15.590158743   192.168.58.136  45.33.32.156  TCP      74 55836 → 193 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=466359038 TSecr=0 WS=128
1346 15.591743019   192.168.58.136  45.33.32.156  TCP      74 39426 → 497 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=466359040 TSecr=0 WS=128
1347 15.592128167   192.168.58.136  45.33.32.156  TCP      74 33876 → 384 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=466359041 TSecr=0 WS=128
1348 15.592414532   192.168.58.136  45.33.32.156  TCP      74 42890 → 19 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=466359041 TSecr=0 WS=128
1349 15.592693111   192.168.58.136  45.33.32.156  TCP      74 54866 → 483 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=466359041 TSecr=0 WS=128
```

```
› Frame 1343: 54 bytes on wire (432 bits), 54      0000  00 50 56 e4 80 76 00 0c  29 ce 52 d2 08 00 45 00   ·PV··v·· )·R···E·
› Ethernet II, Src: VMware_ce:52:d2 (00:0c:29:     0010  00 28 2e 25 40 00 40 06  c3 bd c0 a8 3a 88 2d 21   ·(.%@·@· ····:·-!
› Internet Protocol Version 4, Src: 192.168.58     0020  20 9c c7 44 00 50 18 8a  02 ba 67 59 7c 50 50 14    ··D·P·· ··gY|PP·
⌄ Transmission Control Protocol, Src Port: 510     0030  fa f0 49 08 00 00                                  ··I···
    Source Port: 51012
    Destination Port: 80
    [Stream index: 551]
    [Conversation completeness: Complete, NO_I
    [TCP Segment Len: 0]
    Sequence Number: 1    (relative sequence
    Sequence Number (raw): 411697850
    [Next Sequence Number: 1    (relative seq
    Acknowledgment Number: 1    (relative ack
    Acknowledgment number (raw): 1733917776
    0101 .... = Header Length: 20 bytes (5)
  › Flags: 0x014 (RST, ACK)
    Window: 64240
    [Calculated window size: 64240]
    [Window size scaling factor: -2 (no windo
    Checksum: 0x4908 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  › [Timestamps]
```

"80" was unexpected in this context. | Packets: 6298 · Displayed: 6298 (100.0%) | Profile: Defau

3. What does it mean for a port on scanme.nmap.org to be "filtered?" More specifically, what is the TCP packet type, if any, the server gives in response to a SYN packet sent to port that is "filtered?" [hint: look for port: 25 with full TCP handshake (- sT), -p can scan only a specific port for specified host). Justify your answer with the screenshots from the captured file in wireshark.

A. A filtered port in nmap signifies that it couldn't ascertain its open or closed status due to a lack of response from the target. Firewalls often block SYN packets, leading to this ambiguity. Nmap expects a SYN/ACK or RESET response but receives neither when a port is filtered.



1 2 3 4
minam_momenah - Thunar
File Edit View Go Bookmarks Help
kali Desktop minam_momenah
Places
Con
kali
Des
Rec
Tras
Doc
Mus
Pict
Vide
Dow
Devices
File
Network
Bro
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
4:34

```
No.  Time         Source          Destination     Protocol Length Info
   6 0.714097717  192.168.58.136  45.33.32.156    TCP      74 57114 → 25 [SYN
   7 1.734544576  192.168.58.136  45.33.32.156    TCP      74 [TCP Retransmis
   8 2.236554000  192.168.58.136  45.33.32.156    TCP      74 57130 → 25 [SYN
   9 3.083400356  192.168.58.1    192.168.58.255  UDP      82 62924 → 1947 Le
  10 3.238405477  192.168.58.136  45.33.32.156    TCP      74 [TCP Retransmis
  11 6.447827176  45.33.32.156    192.168.58.136  TCP      60 443 → 46454 [RS
```

```
› Frame 1: 60 bytes on w     0000  00 0c 29 ce 52 d2 00 50  56 e4 80 76 08 00 45 00   ··)·R··P V··v··E·
› Ethernet II, Src: VMwa     0010  00 2c 12 01 00 00 80 06  df dd 2d 21 20 9c c0 a8   ·,······ ··-! ···
› Internet Protocol Vers     0020  3a 88 00 50 c2 92 01 c0  07 fa bd 01 25 57 60 12   :··P···· ····%W`·
› Transmission Control P     0030  fa f0 a5 42 00 00 02 04  05 b4 00 00               ···B···· ····
```

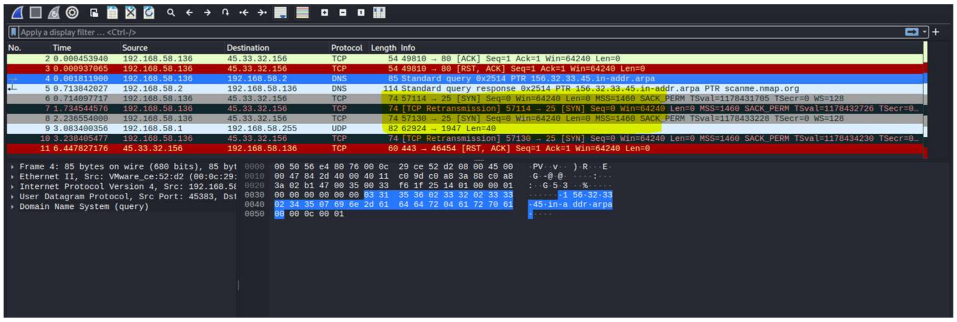
wireshark_eth0GH65A2.pcapng | Packets: 11 · Displayed: 11 (100.0%) | Profile: Default

kali@kali: ~/Desktop/minam_momenah

File Actions Edit View Help

```
┌──(kali㉿kali)-[~/Desktop/minam_momenah]
└─$ nmap -sT -p 25 scanme.nmap.org
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-15 04:33 EDT
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.30s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:
bb2f

PORT   STATE    SERVICE
25/tcp filtered smtp

Nmap done: 1 IP address (1 host up) scanned in 6.58 seconds

┌──(kali㉿kali)-[~/Desktop/minam_momenah]
└─$ 
```

2 files: 874.4 KiB (895,360 bytes) | Free space: 60.2 GiB

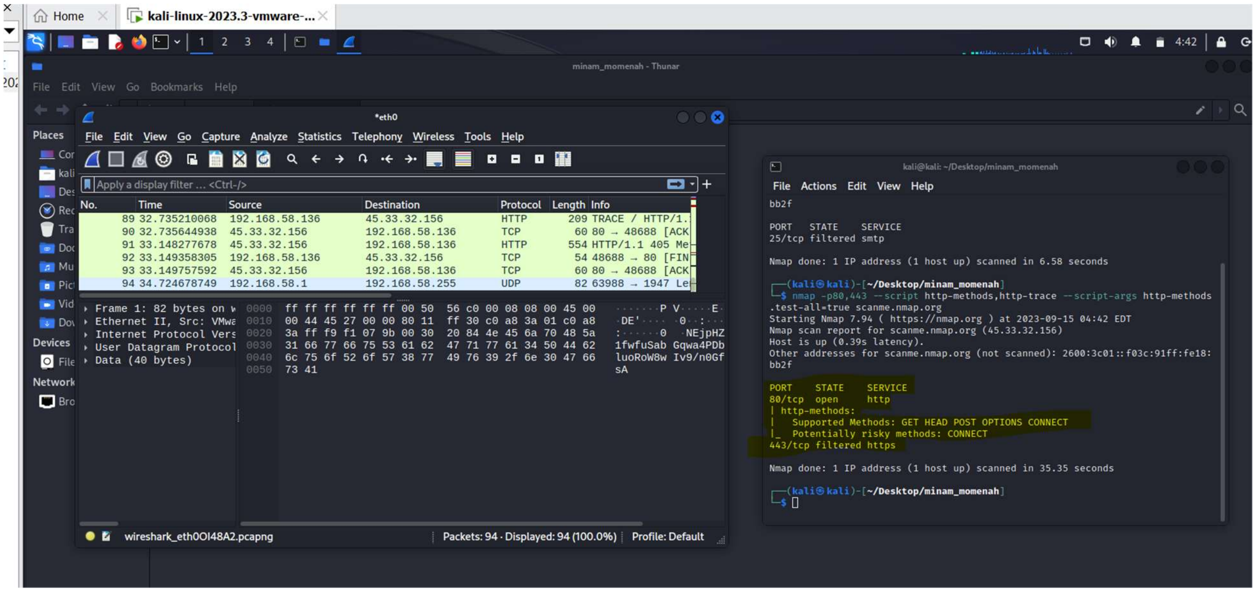


```
No.   Time         Source          Destination     Protocol Length Info
    2 0.000453940  192.168.58.136  45.33.32.156    TCP       54 49810 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
    3 0.000937065  192.168.58.136  45.33.32.156    TCP       54 49810 → 80 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
    4 0.001811900  192.168.58.136  192.168.58.2    DNS       85 Standard query 0x2514 PTR 156.32.33.45.in-addr.arpa
    5 0.713842027  192.168.58.2    192.168.58.136  DNS      114 Standard query response 0x2514 PTR 156.32.33.45.in-addr.arpa PTR scanme.nmap.org
    6 0.714097717  192.168.58.136  45.33.32.156    TCP       74 57114 → 25 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1178431705 TSecr=0 WS=128
    7 1.734544576  192.168.58.136  45.33.32.156    TCP       74 [TCP Retransmission] 57114 → 25 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1178432726 TSecr=0…
    8 2.236554000  192.168.58.136  45.33.32.156    TCP       74 57130 → 25 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1178433228 TSecr=0 WS=128
    9 3.083400356  192.168.58.1    192.168.58.255  UDP       82 62924 → 1947 Len=40
   10 3.238405477  192.168.58.136  45.33.32.156    TCP       74 [TCP Retransmission] 57130 → 25 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1178434230 TSecr=0…
   11 6.447827176  45.33.32.156    192.168.58.136  TCP       60 443 → 46454 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
```

```
› Frame 4: 85 bytes on wire (680 bits), 85 byt   0000  00 50 56 e4 80 76 00 0c  29 ce 52 d2 08 00 45 00   ·PV··v·· )·R···E·
› Ethernet II, Src: VMware_ce:52:d2 (00:0c:29:   0010  00 47 84 2d 40 00 40 11  c0 9d c0 a8 3a 88 c0 a8   ·G·-@·@· ····:···
› Internet Protocol Version 4, Src: 192.168.58   0020  3a 02 b1 47 00 35 00 33  f6 1f 25 14 01 00 00 01   :··G·5·3 ··%·····
› User Datagram Protocol, Src Port: 45383, Dst   0030  00 00 00 00 00 00 03 31  35 36 02 33 32 02 33 33   ······1 56·32·33
› Domain Name System (query)                     0040  02 34 35 07 69 6e 2d 61  64 64 72 04 61 72 70 61   ·45·in-a ddr·arpa
                                                 0050  00 00 0c 00 01                                     ·····
```

4. In addition to performing an HTTP GET request to the webserver, what other http request types does Nmap send?

A. The other http request type does NMAP send is
“GET POST HEAD”



Home
kali-linux-2023.3-vmware-...
1 2 3 4
4:42
minam_momenah - Thunar
File Edit View Go Bookmarks Help
Places
Cor
kali
Des
Rec
Tra
Doc
Mu
Pict
Vid
Dov
Devices
File
Network
Bro
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.   Time          Source          Destination     Protocol Length Info
   89 32.735210068  192.168.58.136  45.33.32.156    HTTP      209 TRACE / HTTP/1.
   90 32.735644938  45.33.32.156    192.168.58.136  TCP        60 80 → 48688 [ACK
   91 33.148277678  45.33.32.156    192.168.58.136  HTTP      554 HTTP/1.1 405 Me
   92 33.149358305  192.168.58.136  45.33.32.156    TCP        54 48688 → 80 [FIN
   93 33.149757592  45.33.32.156    192.168.58.136  TCP        60 80 → 48688 [ACK
   94 34.724678749  192.168.58.1    192.168.58.255  UDP        82 63988 → 1947 Le
```

```
› Frame 1: 82 bytes on w    0000  ff ff ff ff ff ff 00 50  56 c0 00 08 08 00 45 00   ······P V·····E·
› Ethernet II, Src: VMwa    0010  00 44 45 27 00 00 80 11  ff 30 c0 a8 3a 01 c0 a8   ·DE'····  ·0··:···
› Internet Protocol Vers    0020  3a ff f9 f1 07 9b 00 30  20 84 4e 45 6a 70 48 5a   :······0  ·NEjpHZ
› User Datagram Protocol    0030  31 66 77 66 75 53 61 62  47 71 77 61 34 50 44 62   1fwfuSab Gqwa4PDb
› Data (40 bytes)           0040  6c 75 6f 52 6f 57 38 77  49 76 39 2f 6e 30 47 66   luoRoW8w Iv9/n0Gf
                            0050  73 41                                              sA
```

wireshark_eth0OI48A2.pcapng
Packets: 94 · Displayed: 94 (100.0%)
Profile: Default
kali@kali: ~/Desktop/minam_momenah
File Actions Edit View Help

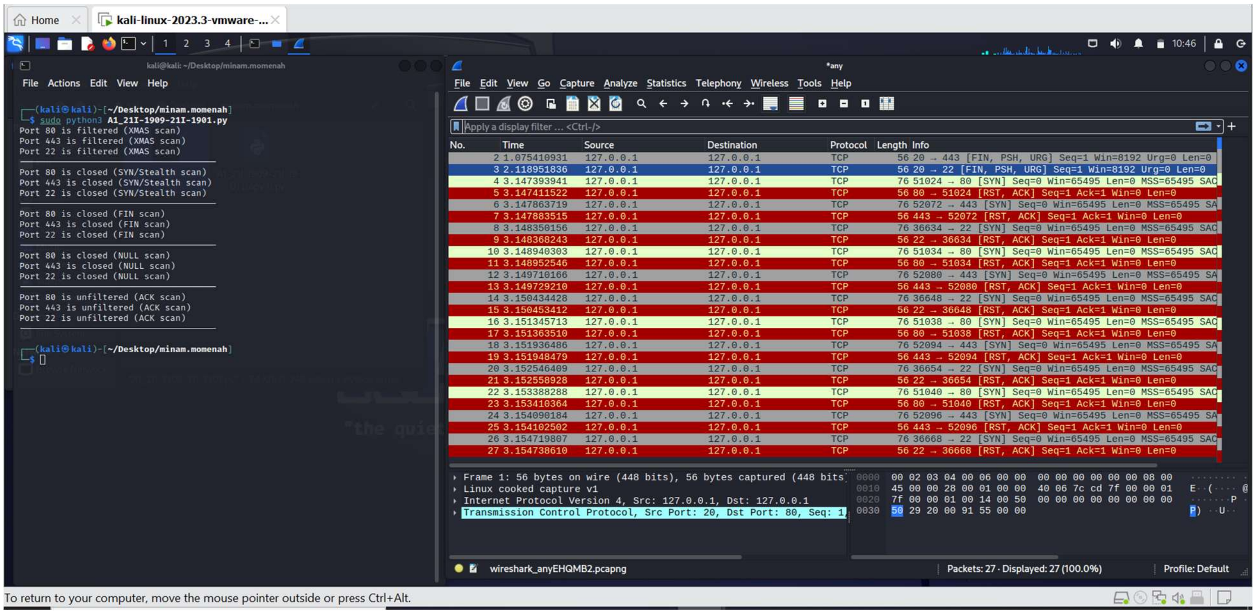
```
bb2f

PORT   STATE    SERVICE
25/tcp filtered smtp

Nmap done: 1 IP address (1 host up) scanned in 6.58 seconds

┌──(kali㉿kali)-[~/Desktop/minam_momenah]
└─$ nmap -p80,443 --script http-methods,http-trace --script-args http-methods
.test-all=true scanme.nmap.org
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-15 04:42 EDT
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.39s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:
bb2f

PORT    STATE    SERVICE
80/tcp  open     http
| http-methods:
|   Supported Methods: GET HEAD POST OPTIONS CONNECT
|_  Potentially risky methods: CONNECT
443/tcp filtered https

Nmap done: 1 IP address (1 host up) scanned in 35.35 seconds

┌──(kali㉿kali)-[~/Desktop/minam_momenah]
└─$ 
```

QUESTION#3

Now that you know what port scanning is and have used Nmap. Your next task is to implement a basic port scanner that performs the following scans:

□ XMAS Scan
□ SYN/Stealth Scan
□ FIN Scan
□ NULL Scan
□ ACK Scan

Research the different flags that must be on in the packet and what particular response indicates that a port is open. Along with the code, attach a screenshot of the network traffic (using Wireshark) during the port scan.



Home
kali-linux-2023.3-vmware-...
1 2 3 4
10:46
kali@kali: ~/Desktop/minam.momenah
File Actions Edit View Help
*any
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
┌──(kali㉿kali)-[~/Desktop/minam.momenah]
└─$ sudo python3 A1_21I-1909-21I-1901.py
Port 80 is filtered (XMAS scan)
Port 443 is filtered (XMAS scan)
Port 22 is filtered (XMAS scan)
──────────────────────────────────────
Port 80 is closed (SYN/Stealth scan)
Port 443 is closed (SYN/Stealth scan)
Port 22 is closed (SYN/Stealth scan)
──────────────────────────────────────
Port 80 is closed (FIN scan)
Port 443 is closed (FIN scan)
Port 22 is closed (FIN scan)
──────────────────────────────────────
Port 80 is closed (NULL scan)
Port 443 is closed (NULL scan)
Port 22 is closed (NULL scan)
──────────────────────────────────────
Port 80 is unfiltered (ACK scan)
Port 443 is unfiltered (ACK scan)
Port 22 is unfiltered (ACK scan)
──────────────────────────────────────

┌──(kali㉿kali)-[~/Desktop/minam.momenah]
└─$ 
```

No.	Time	Source	Destination	Protocol	Length	Info
2	1.075410931	127.0.0.1	127.0.0.1	TCP	56	20 → 443 [FIN, PSH, URG] Seq=1 Win=8192 Urg=0 Len=0
3	2.118951836	127.0.0.1	127.0.0.1	TCP	56	20 → 22 [FIN, PSH, URG] Seq=1 Win=8192 Urg=0 Len=0
4	3.147393941	127.0.0.1	127.0.0.1	TCP	76	51024 → 80 [SYN] Seq=0 Win=65495 Len=0 MSS=65495 SAC
5	3.147411522	127.0.0.1	127.0.0.1	TCP	56	80 → 51024 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
6	3.147863719	127.0.0.1	127.0.0.1	TCP	76	52072 → 443 [SYN] Seq=0 Win=65495 Len=0 MSS=65495 SA
7	3.147883515	127.0.0.1	127.0.0.1	TCP	56	443 → 52072 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
8	3.148350156	127.0.0.1	127.0.0.1	TCP	76	36634 → 22 [SYN] Seq=0 Win=65495 Len=0 MSS=65495 SAC
9	3.148368243	127.0.0.1	127.0.0.1	TCP	56	22 → 36634 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
10	3.148940303	127.0.0.1	127.0.0.1	TCP	76	51034 → 80 [SYN] Seq=0 Win=65495 Len=0 MSS=65495 SAC
11	3.148952546	127.0.0.1	127.0.0.1	TCP	56	80 → 51034 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
12	3.149710166	127.0.0.1	127.0.0.1	TCP	76	52080 → 443 [SYN] Seq=0 Win=65495 Len=0 MSS=65495 SA
13	3.149729210	127.0.0.1	127.0.0.1	TCP	56	443 → 52080 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
14	3.150434428	127.0.0.1	127.0.0.1	TCP	76	36648 → 22 [SYN] Seq=0 Win=65495 Len=0 MSS=65495 SAC
15	3.150453412	127.0.0.1	127.0.0.1	TCP	56	22 → 36648 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
16	3.151345713	127.0.0.1	127.0.0.1	TCP	76	51038 → 80 [SYN] Seq=0 Win=65495 Len=0 MSS=65495 SAC
17	3.151363510	127.0.0.1	127.0.0.1	TCP	56	80 → 51038 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
18	3.151936486	127.0.0.1	127.0.0.1	TCP	76	52094 → 443 [SYN] Seq=0 Win=65495 Len=0 MSS=65495 SA
19	3.151948479	127.0.0.1	127.0.0.1	TCP	56	443 → 52094 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
20	3.152546409	127.0.0.1	127.0.0.1	TCP	76	36654 → 22 [SYN] Seq=0 Win=65495 Len=0 MSS=65495 SAC
21	3.152558928	127.0.0.1	127.0.0.1	TCP	56	22 → 36654 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
22	3.153388288	127.0.0.1	127.0.0.1	TCP	76	51040 → 80 [SYN] Seq=0 Win=65495 Len=0 MSS=65495 SAC
23	3.153410364	127.0.0.1	127.0.0.1	TCP	56	80 → 51040 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
24	3.154090184	127.0.0.1	127.0.0.1	TCP	76	52096 → 443 [SYN] Seq=0 Win=65495 Len=0 MSS=65495 SA
25	3.154102502	127.0.0.1	127.0.0.1	TCP	56	443 → 52096 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
26	3.154719807	127.0.0.1	127.0.0.1	TCP	76	36668 → 22 [SYN] Seq=0 Win=65495 Len=0 MSS=65495 SAC
27	3.154738610	127.0.0.1	127.0.0.1	TCP	56	22 → 36668 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

```
› Frame 1: 56 bytes on wire (448 bits), 56 bytes captured (448 bits
› Linux cooked capture v1
› Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
› Transmission Control Protocol, Src Port: 20, Dst Port: 80, Seq: 1,
```

```
0000  00 02 03 04 00 06 00 00  00 00 00 00 00 00 08 00   ········ ······
0010  45 00 00 28 00 01 00 00  40 06 7c cd 7f 00 00 01   E··(···· @
0020  7f 00 00 01 00 14 00 50  00 00 00 00 00 00 00 00   ·······P ·
0030  50 29 20 00 91 55 00 00                           P) ··U··
```

wireshark_anyEHQMB2.pcapng | Packets: 27 · Displayed: 27 (100.0%) | Profile: Default

To return to your computer, move the mouse pointer outside or press Ctrl+Alt.