

# **FIREWALL-IDs, FILTERED PORTS AND HOW TO BREAK THROUGH**

**CYBERSECURITY  
(TUESDAY & THURSDAY 9 AM CLASS)  
GROUP 2  
PRESENTATION**

# **CONTENTS:**

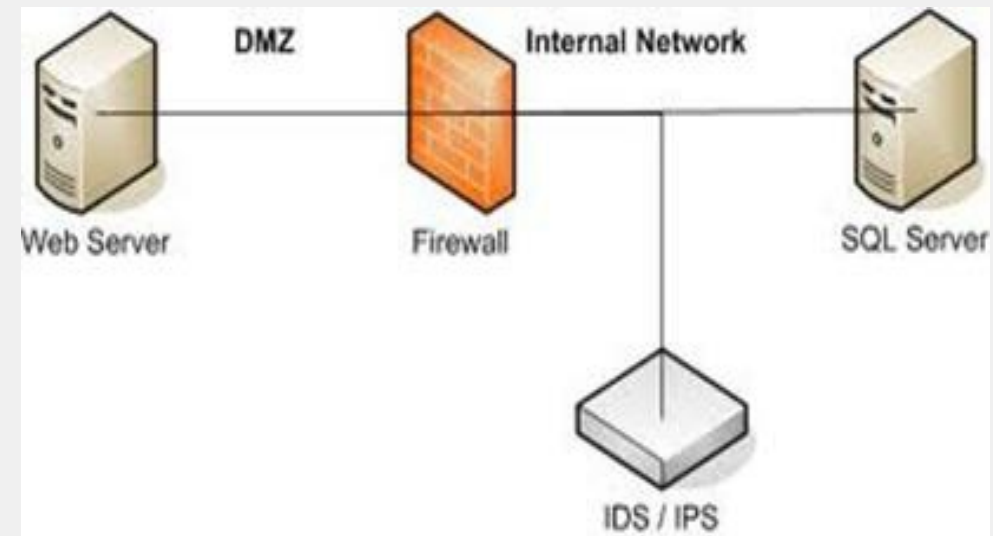
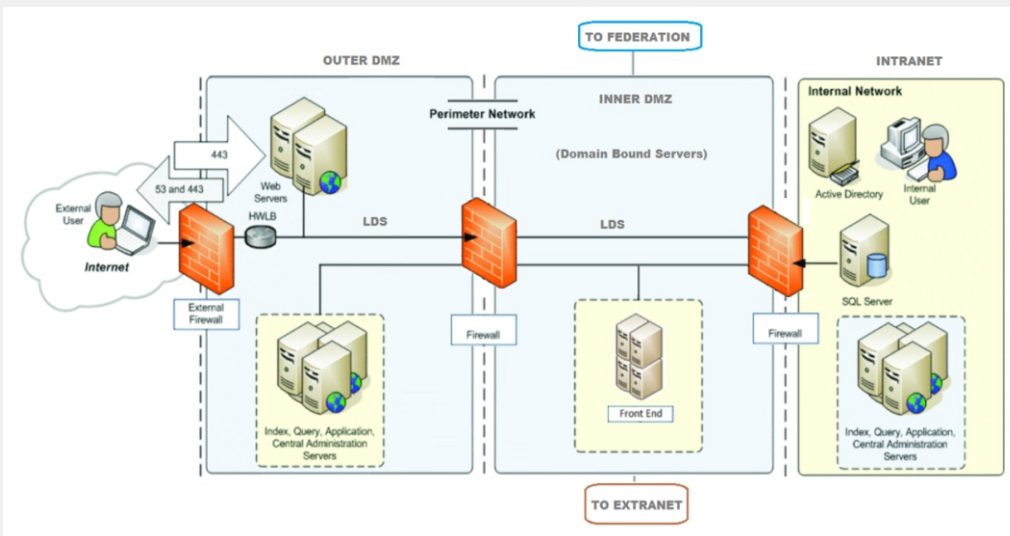
- What Firewalls-IDs
- What Filtered Ports
- Reasons Why People Use Firewalls & Filtered Port
- How to break through firewalls and filtered port

# What is Firewalls?

A firewall is a [network security](#) device that monitors incoming and outgoing network traffic and permits or blocks data [packets](#) based on a set of security rules. Its purpose is to establish a barrier between your internal network and incoming traffic from external sources (such as the internet) in order to block malicious traffic like viruses and hackers.

## Intrusion detection system (IDS)

Intrusion Detection (ID) is the process of monitoring for and identifying attempted unauthorized system access or manipulation. An ID system gathers and analyzes information from diverse areas within a computer or a network to identify possible security breaches which include both intrusions (attack from outside the organization) and misuse (attack from within the organization).

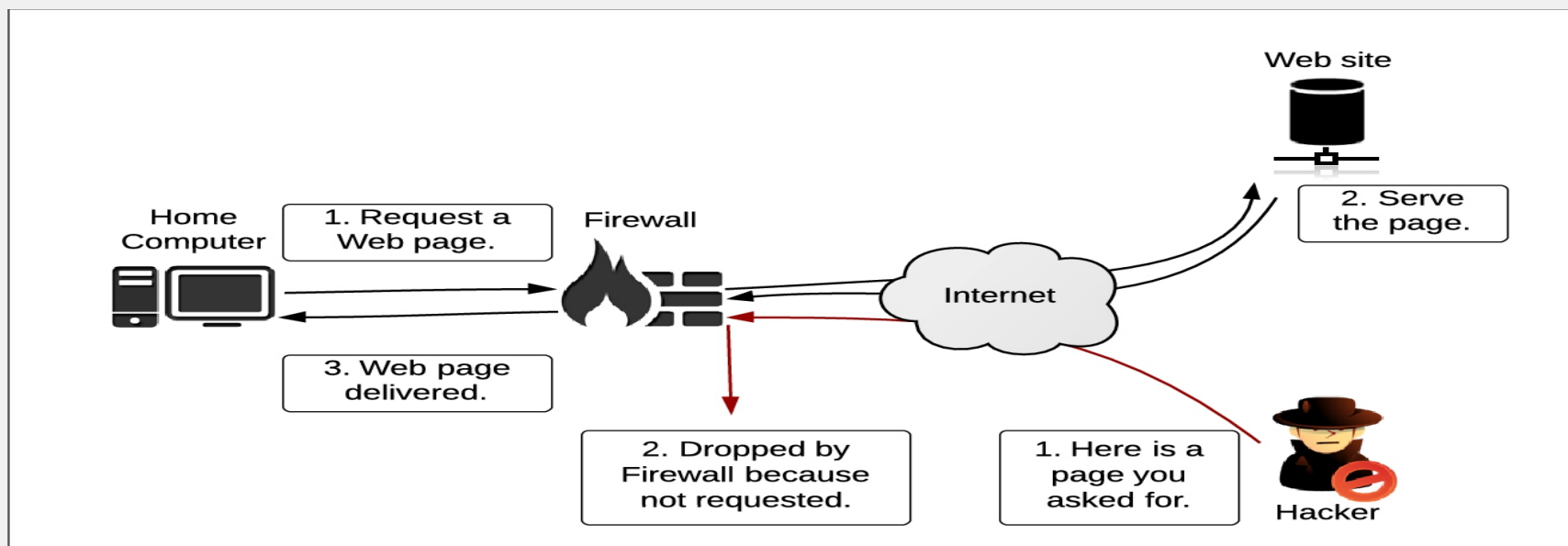


## What is Filtered Port

A filtered port indicates that a firewall, filter, or other network issue is blocking the port. Some standard services that can create a filter port can be, but not limited to, a server or network firewall, router, or security device.

## What is Ports?

Ports are an integral part of the internet's communication model. also ports are channel through which applications on the client computer can reach the software on the serve. Examples of ports are ftp, tcp, ssh etc



## Reasons Why People Use Firewalls & Filtered Port

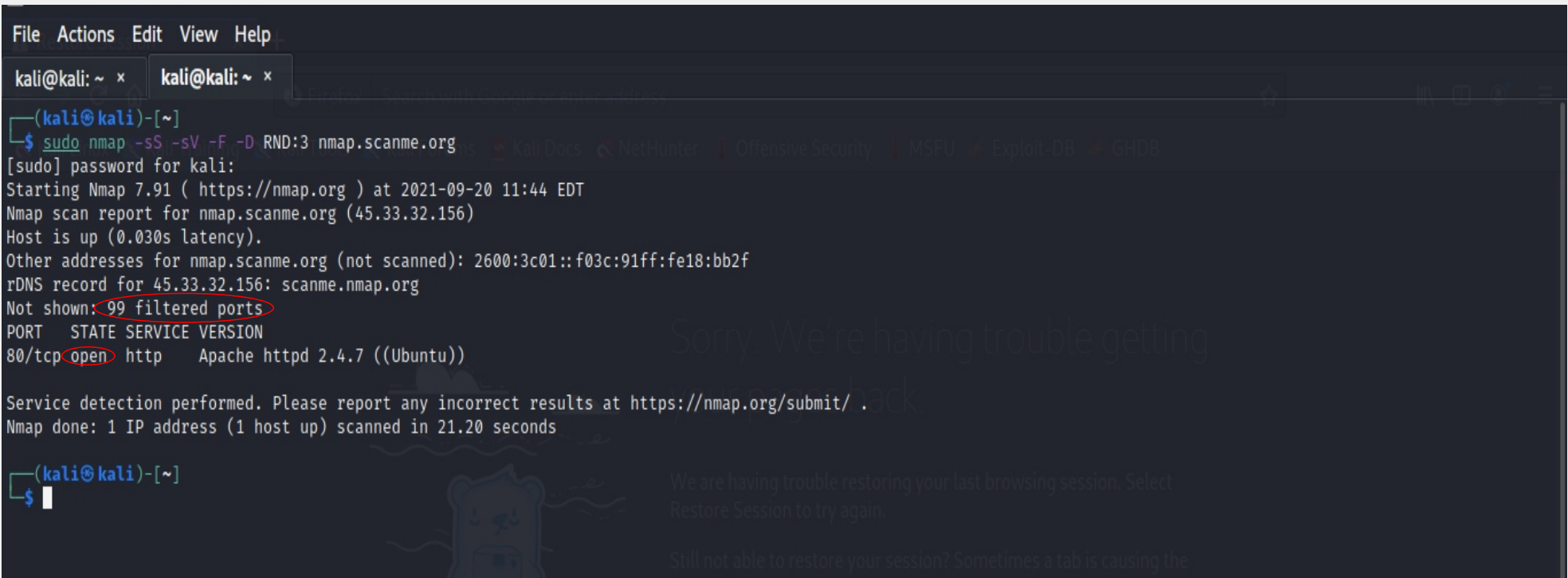
- 1. Cyber Security Attack Prevention:** Cyber security is certainly the top reason to use a firewall. Firewalls can block malicious programs from being installed on users' computers. They can be used as part of a multi-layer [cyber security strategy](#) to protect against distributed denial of service (DDoS) attacks, where a hacker floods your network with unwanted traffic. In some cases, they can also stop intrusions and block unauthorized network use.
- 2. Threat Detection:** A managed service provider (MSP) will configure your firewall to send an alert if something in your network seems amiss. For instance, we can add features that will scan outgoing network traffic for sensitive data such as social security numbers or credit card information. That way, we can spring into action and begin securing data and minimizing the damage from a potential data breach if we [detect suspicious traffic](#).
- 3. Blocking Prohibited Sites:** Although it's nearly impossible to run a business without the internet, the web is also home to plenty of distracting and unsafe websites. Firewall can be configure to block sites you don't want employees visiting, like social media platforms or explicit content.
- 4. Securing Remote or Mobile Workers:** Many modern businesses have workers trying to access internal networks [outside of the office](#). However, once users go outside of your ISP, it can be much harder to protect your network. A firewall can help by securing connections between external users and your internal network. This way, other users on a shared or unsecure internet connection can't interrupt or listen in on your traffic.

# How to break through firewalls and filtered port

There are several methods that can be used to break through firewalls and filtered port, but for the purpose of this demo we are going to be using fragmentation method.

Open a terminal.

```
kali@kali> sudo nmap -sS -sV -F -p nmap.scanme.org
```

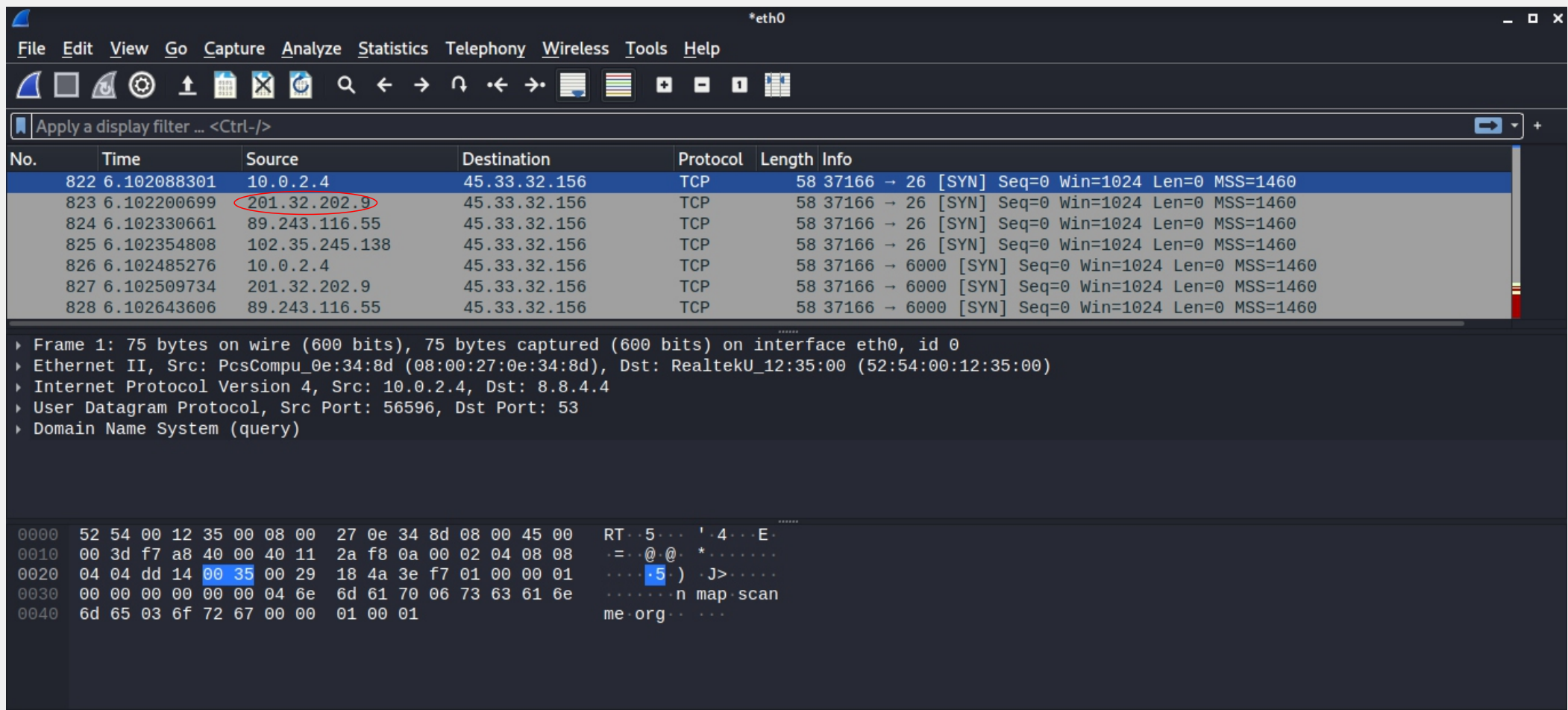


```
File Actions Edit View Help
kali@kali: ~ x kali@kali: ~ x
(kali@kali)-[~]
$ sudo nmap -sS -sV -F -D RND:3 nmap.scanme.org
[sudo] password for kali:
Starting Nmap 7.91 ( https://nmap.org ) at 2021-09-20 11:44 EDT
Nmap scan report for nmap.scanme.org (45.33.32.156)
Host is up (0.030s latency).
Other addresses for nmap.scanme.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
rDNS record for 45.33.32.156: scanme.nmap.org
Not shown: 99 filtered ports
PORT      STATE SERVICE VERSION
80/tcp    open  http      Apache httpd 2.4.7 ((Ubuntu))

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.20 seconds

(kali@kali)-[~]
$
```

Open a new terminal to lunch your wireshark in to capture packets.  
kali@kali> wireshark



Wireshark interface showing a packet capture on interface eth0. The packet list shows several TCP SYN packets from 10.0.2.4 to 45.33.32.156. The packet details pane shows the structure of the first packet: Ethernet II, Internet Protocol Version 4, User Datagram Protocol, and Domain Name System (query). The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
822	6.102088301	10.0.2.4	45.33.32.156	TCP	58	37166 → 26 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
823	6.102200699	201.32.202.9	45.33.32.156	TCP	58	37166 → 26 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
824	6.102330661	89.243.116.55	45.33.32.156	TCP	58	37166 → 26 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
825	6.102354808	102.35.245.138	45.33.32.156	TCP	58	37166 → 26 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
826	6.102485276	10.0.2.4	45.33.32.156	TCP	58	37166 → 6000 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
827	6.102509734	201.32.202.9	45.33.32.156	TCP	58	37166 → 6000 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
828	6.102643606	89.243.116.55	45.33.32.156	TCP	58	37166 → 6000 [SYN] Seq=0 Win=1024 Len=0 MSS=1460

Frame 1: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface eth0, id 0  
Ethernet II, Src: PcsCompu\_0e:34:8d (08:00:27:0e:34:8d), Dst: RealtekU\_12:35:00 (52:54:00:12:35:00)  
Internet Protocol Version 4, Src: 10.0.2.4, Dst: 8.8.4.4  
User Datagram Protocol, Src Port: 56596, Dst Port: 53  
Domain Name System (query)

```
0000  52 54 00 12 35 00 08 00 27 0e 34 8d 08 00 45 00  RT...5...'.4...E.
0010  00 3d f7 a8 40 00 40 11 2a f8 0a 00 02 04 08 08  .=..@..@.*.....
0020  04 04 dd 14 00 35 00 29 18 4a 3e f7 01 00 00 01  ....5.)..J>.....
0030  00 00 00 00 00 00 04 6e 6d 61 70 06 73 63 61 6e  ....n map scan
0040  6d 65 03 6f 72 67 00 00 01 00 01                me.org..
```



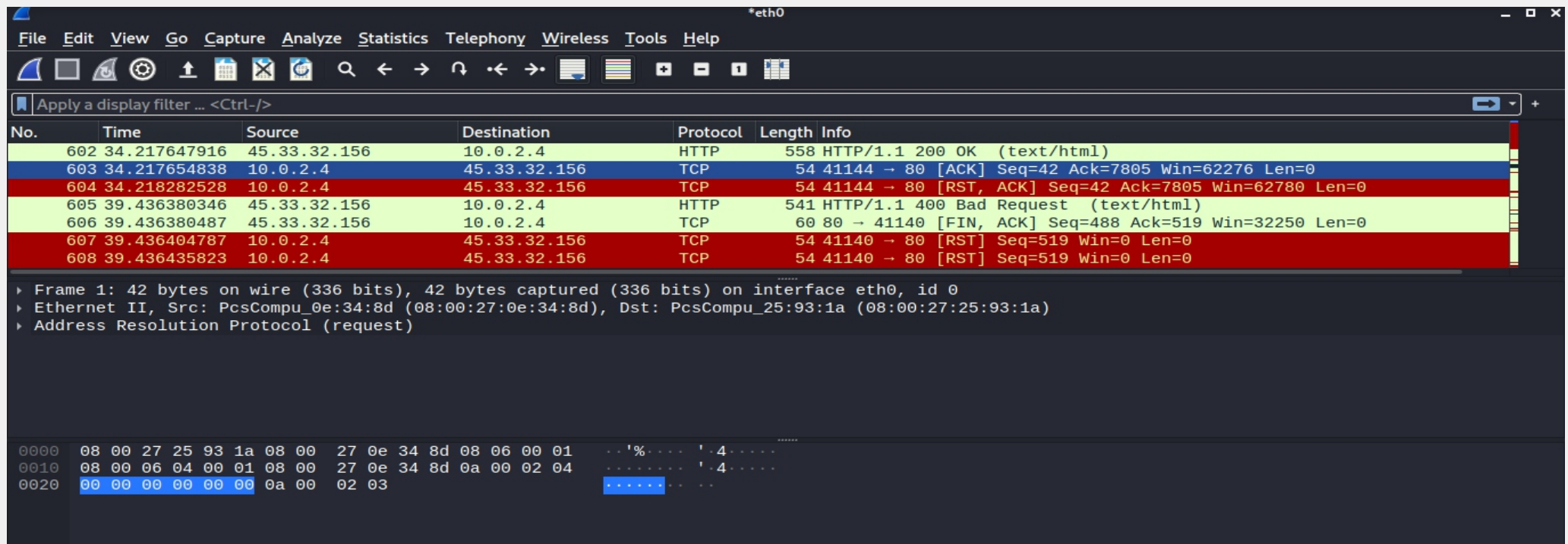
On your terminal do a new scan with the IP address which is the IP after your own IP gotten from wireshark packets.

```
kali@kali> sudo nmap -sS -sV -F -D 201.32.202.9 nmap.scanme.org
```

```
(kali@kali)-[~]  
$ sudo nmap -sS -sV -F -D 201.32.202.9 nmap.scanme.org  
Starting Nmap 7.91 ( https://nmap.org ) at 2021-09-20 11:52 EDT  
Nmap scan report for nmap.scanme.org (45.33.32.156)  
Host is up (0.063s latency).  
Other addresses for nmap.scanme.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f  
rDNS record for 45.33.32.156: scanme.nmap.org  
Not shown: 98 filtered ports  
PORT      STATE SERVICE      VERSION  
22/tcp    open  tcpwrapped  
80/tcp    open  http         Apache httpd 2.4.7 ((Ubuntu))  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 32.42 seconds
```



# Recapture packets using wireshark



The image shows the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with various icons for file operations, capture control, and analysis. A display filter bar shows "Apply a display filter ... <Ctrl-/>".

The main packet list pane displays the following data:

No.	Time	Source	Destination	Protocol	Length	Info
602	34.217647916	45.33.32.156	10.0.2.4	HTTP	558	HTTP/1.1 200 OK (text/html)
603	34.217654838	10.0.2.4	45.33.32.156	TCP	54	41144 → 80 [ACK] Seq=42 Ack=7805 Win=62276 Len=0
604	34.218282528	10.0.2.4	45.33.32.156	TCP	54	41144 → 80 [RST, ACK] Seq=42 Ack=7805 Win=62780 Len=0
605	39.436380346	45.33.32.156	10.0.2.4	HTTP	541	HTTP/1.1 400 Bad Request (text/html)
606	39.436380487	45.33.32.156	10.0.2.4	TCP	60	80 → 41140 [FIN, ACK] Seq=488 Ack=519 Win=32250 Len=0
607	39.436404787	10.0.2.4	45.33.32.156	TCP	54	41140 → 80 [RST] Seq=519 Win=0 Len=0
608	39.436435823	10.0.2.4	45.33.32.156	TCP	54	41140 → 80 [RST] Seq=519 Win=0 Len=0

The packet details pane for the selected packet (No. 602) shows:

- Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface eth0, id 0
- Ethernet II, Src: PcsCompu\_0e:34:8d (08:00:27:0e:34:8d), Dst: PcsCompu\_25:93:1a (08:00:27:25:93:1a)
- Address Resolution Protocol (request)

The packet bytes pane shows the raw data in hexadecimal and ASCII:

```
0000  08 00 27 25 93 1a 08 00 27 0e 34 8d 08 06 00 01  ..'%. . . .'-4. . . .
0010  08 00 06 04 00 01 08 00 27 0e 34 8d 0a 00 02 04  . . . . .'-4. . . .
0020  00 00 00 00 00 00 0a 00 02 03  . . . . .
```

THANK  
YOU