FIREWALL-IDs, FILTERED PORTS AND HOW TO BREAK THROUGH

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

CONTENTS:

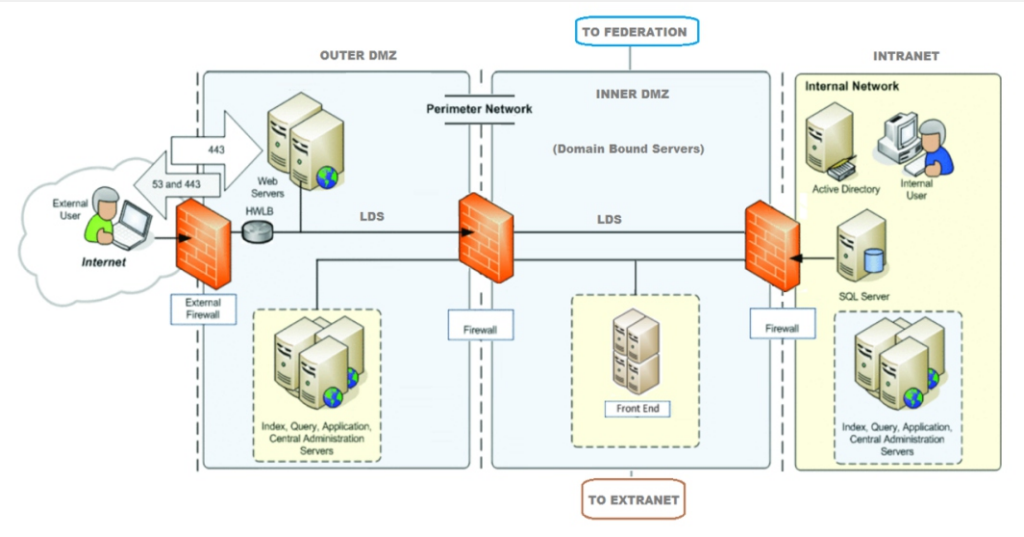
- What Firewalls-IDs
- What Filtered Ports
- Reasons Why People Use Firewalls & Filtered Port
- How to break through firewalls and filtered port

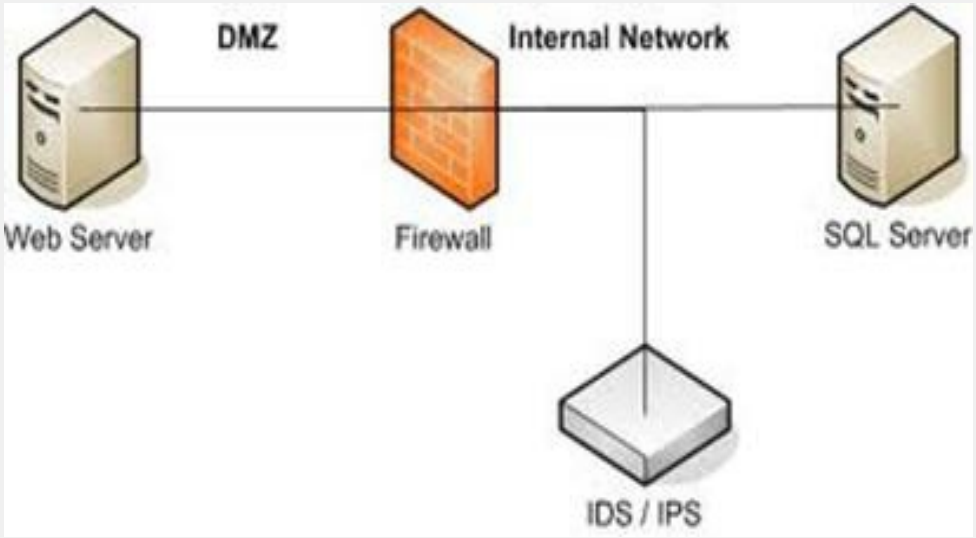
What is Firewalls?

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).



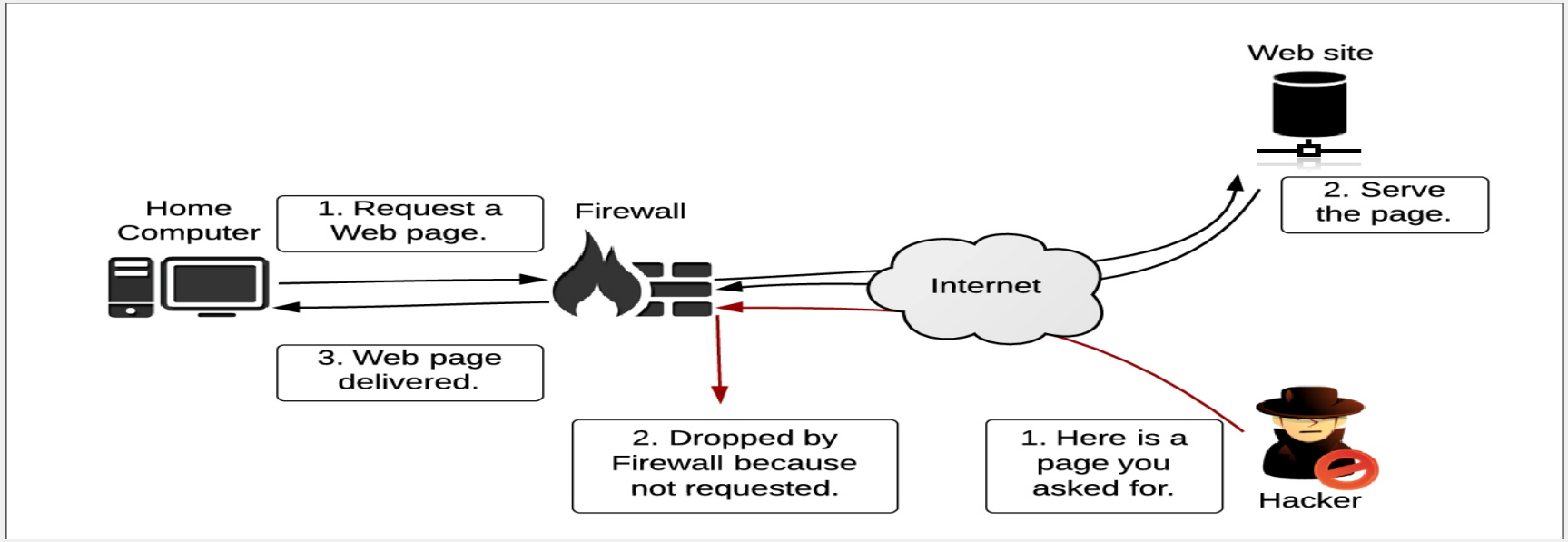


What is Filtered Port

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

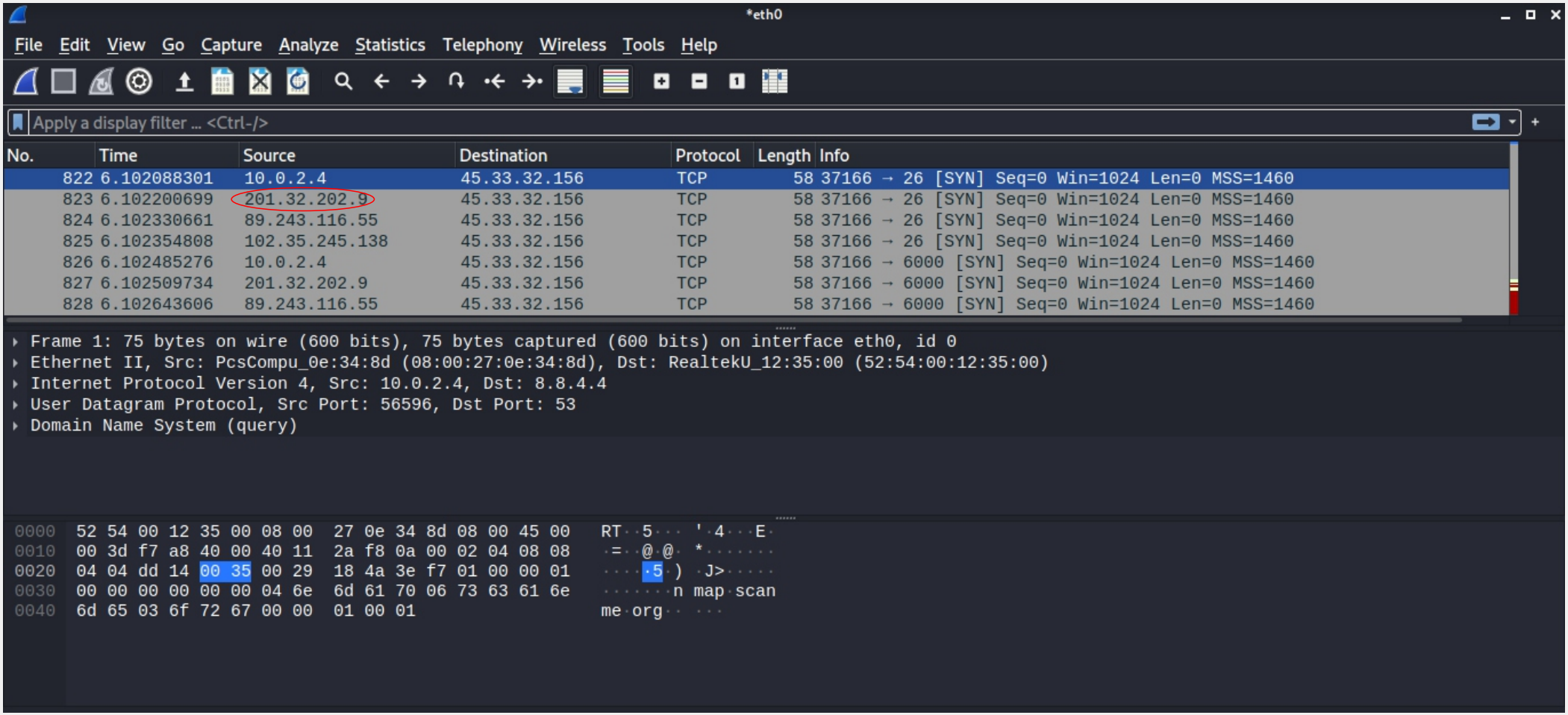
```
File  Actions  Edit  View  Help
kali@kali: ~ ×   kali@kali: ~ ×
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS -sV -F -D RND:3 nmap.scanme.org
[sudo] password for kali:
Starting Nmap 7.91 ( https://nmap.org ) at 2021-09-20 11:44 EDT
Nmap scan report for nmap.scanme.org (45.33.32.156)
Host is up (0.030s latency).
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



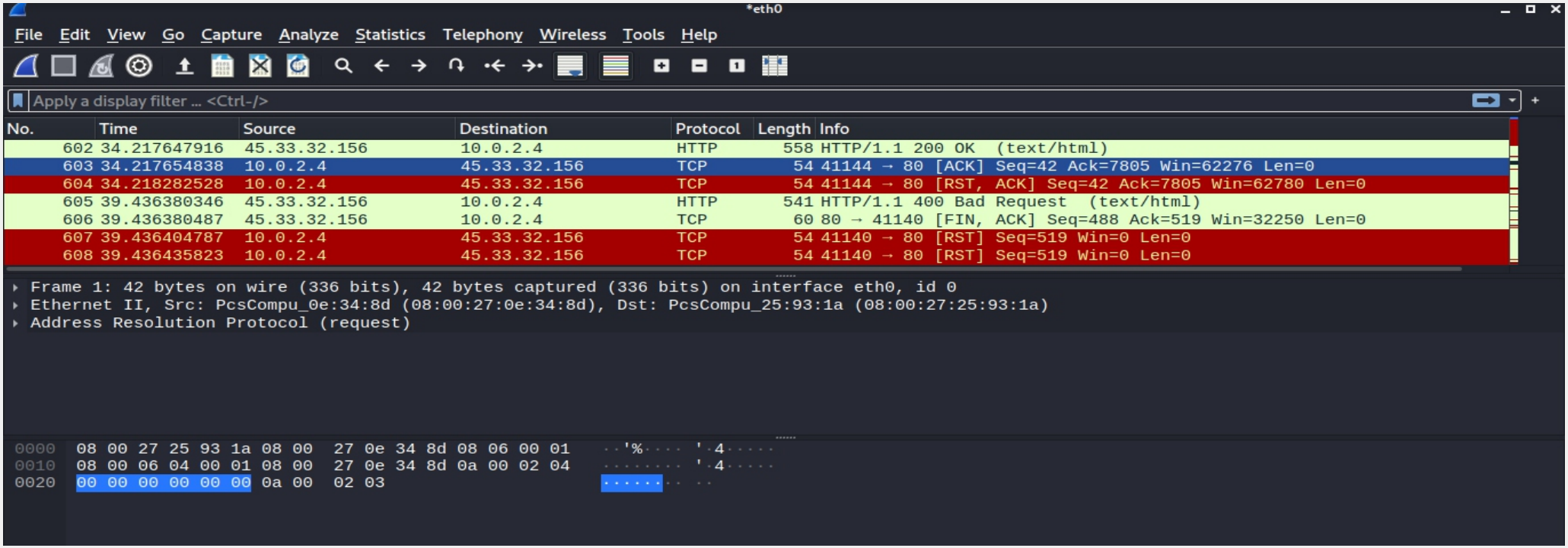
On your terminal do a new scan with the IP address which is the IP after your own IP gotten from wireshark packets.

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



THANK YOU