Co-funded by
the European Union

Course: Real time Cyber Threat Detection and Mitigation

Project: Cyber Security 4 ALL(CS4ALL)

Co-funded by
the European Union

Chapter 1: Advanced Network Security

CS4ALL
CYBERSECURITY FOR ALL

Index

Co-funded by
the European Union

Index

Co-funded by the European Union

1.1 Security Through Obscurity

Security approach that relies on keeping details secret to protect systems and data from unauthorized access.

Principles

- **Secrecy**: keeping details confidential
- **Complexity**: more complex a system appears to be
- the more difficult it is for an attacker to understand it.
- **Access Control:** restricting knowledge of the system's workings

Co-funded by the European Union

Advantages

1. Additional Layer of Protection
2. Deterrence for Low-Skill Attackers
3. Short-Term Protection
4. Reduces Exposure

Co-funded by
the European Union

Criticism

1. False Sense of Security
2. Limited Effectiveness
3. Non-Scalability
4. Dependence on Security Measures

Co-funded by
the European Union

Applying Obscurity in System Design

It involves integrating elements of secrecy and complexity to enhance security while maintaining usability and functionality.

1. **Layered Security:** Combine obscurity with other security practices, such as encryption, multi-factor authentication

2.**Code Obfuscation:** make the source code difficult to read and understand

3. **Environment Isolation**: sensitive components are isolated in secure environments

Co-funded by the European Union

Applying Obscurity in System Design

Vulnerability Management: Regularly assess and patch vulnerabilities

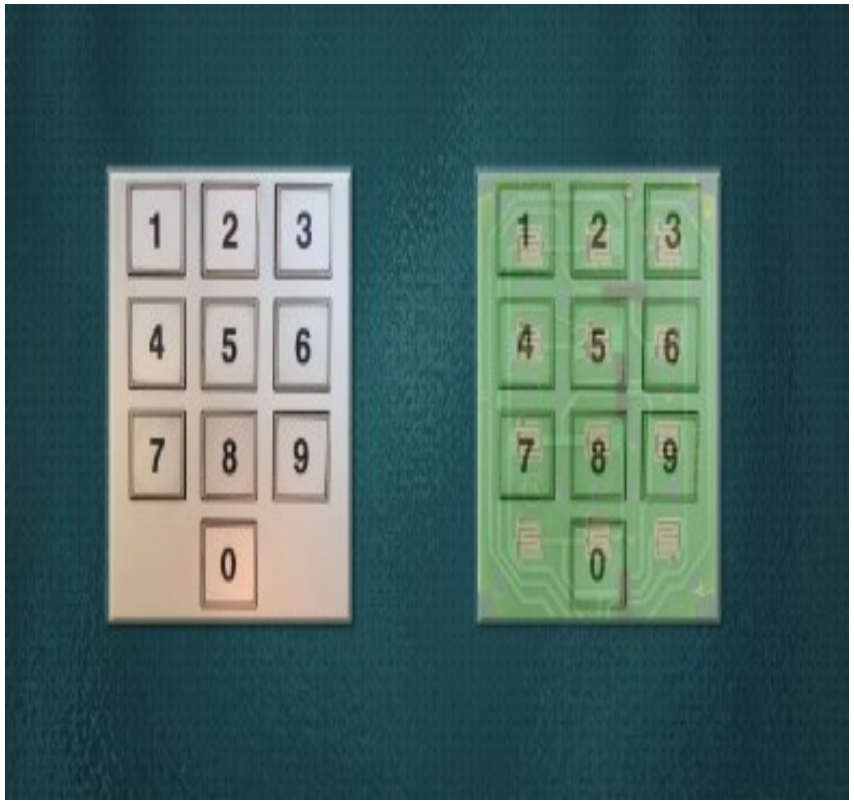
Custom Protocols: communication protocols for internal services

Co-funded by the European Union

Real-World Examples

- **Security Through Software Design:**Code obfuscation in their mobile apps to prevent reverse engineering
- **Network Configuration:** Change default usernames and passwords on devices to obscure the initial access points from attackers.
- **API Security:** use custom endpoint naming conventions

Co-funded by
the European Union



Co-funded by the European Union

Images depicting Obscurity

TCP/IP Model

4	Application	HTTPS, TLS, DNS
3	Transport	TCP, UDP
2	Internet	IPv4, IPv6
1	Network	Ethernet, Wireless LAN

Created by: Rahul Kumar (tecadmin.net)

Co-funded by
the European Union

1.2 TCP/IP Evolution

Origins and Development

1970

DARPA (Defense Advanced Research Projects Agency) designed TCP/IP to connect several research networks into what would eventually become the internet.

Standardization and Expansion

1980

Issued Request for Comments (RFCs) for the two new protocols, TCP and IP, as well as DOD requirements. The onerous job of converting all networks, including ARPANET, to TCP/IP began.

Growth and Global Adoption

1990 - 2012

Commercialization of the Internet & IPv6 Development begin

Modern Era and Continued Evolution

2000s-present

IPv6 adoption has been steadily expanding to meet the growing number of internet-connected devices globally. Major internet service providers, content providers, and businesses have been deploying IPv6 alongside IPv4 in dual-stack settings.

CS4ALL CYBERSECURITY FOR ALL
Co-funded by the European Union

An Evaluation of Security Issues

Vulnerabilities	Security Protocols and Solutions	Addressing Security Challenges	Emerging Threats and Adaptations	Ongoing Improvements
IP Spoofing	IPsec (Internet Protocol Security)	IPv4 Address Exhaustion	IoT Security	Standardization Efforts
Man-in-Middle Attack	TLS (Transport Layer Security)	IPv6 Security Considerations	Cloud Computing and Virtualization	Education and Awareness
Denial of Service (DoS) Attacks				

CS4ALL CYBERSECURITY FOR ALL
Co-funded by the European Union

1.3 TCP/IP Layers

Suite of communication protocols used to interconnect network devices on the internet

1. **Application Layer:** Responsible for network services and end-user interfaces.

   It includes protocols such as:

- **HTTP/HTTPS:** Used for web browsing.
- **FTP:** File Transfer Protocol for transferring files.
- **SMTP/IMAP/POP3:** Email protocols.

Co-funded by the European Union

1.3 TCP/IP Layers

2. Transport Layer: Provides end-to-end communication services.

The main protocols are:

- **TCP (Transmission Control Protocol):** Connection-oriented, ensures reliable data transmission
- **UDP (User Datagram Protocol):** Connectionless, used for applications where speed is critical and reliability is less important

Co-funded by the European Union

1.3 TCP/IP Layers

Internet Layer: handles logical addressing and routing.

Key protocols include:

- **IP (Internet Protocol):** Responsible for addressing and routing packets of data.
- two versions: IPv4 and IPv6.

- **ICMP (Internet Control Message Protocol):** Used for diagnostic and error messages, such as pinging a device.

Co-funded by the European Union

1.3 TCP/IP Layers

Link Layer (Network Interface Layer):

Manages physical network connections and protocols for local network technologies (e.g., Ethernet, Wi-Fi).

Co-funded by the European Union

TCP/IP Operations

Establishing a Connection (TCP)

Three-Way Handshake: process with which Connection is established.

SYN: Client sends a SYN (synchronize) packet to the server to initiate a connection
SYN-ACK: Server responds with a SYN-ACK packet.
ACK: Client sends an ACK packet back to the server, completing the connection

Co-funded by the European Union

TCP/IP Operations

Data Transmission

Segmentation: Data is divided into manageable segments

Adding headers containing sequence numbers and acknowledgment numbers to ensure the correct order and integrity

Flow Control: to manage the rate of data transmission and prevent overwhelming the receiver

Error Detection and Recovery: checksums to detect errors in transmitted segments.

for error, the affected segment is retransmitted.

Co-funded by the European Union

TCP/IP Operations

Closing a Connection

Four-Way Handshake: used to close a TCP connection

FIN: FIN (finish) packet is sent to indicate to close the connection.

ACK: The other side acknowledges the FIN with an ACK.

FIN: The second side sends its own FIN packet.

ACK: The first side acknowledges the second FIN.

Co-funded by the European Union

TCP/IP Operations

Routing and Addressing (IP)

IP Addressing:

Each device on a network is assigned a unique IP address

IPv4 addresses are 32 bits long

IPv6 addresses are 128 bits

Packet Routing: IP packets are routed through various devices across networks

Each router examines the destination IP address

forwards it to the next hop based on its routing table.

Co-funded by the European Union

TCP/IP Operations

Subnetting: divides larger networks into smaller, more manageable segments

allowing for better organization

efficient use of IP addresses.

Co-funded by
the European Union

1.4 IP Spoofing

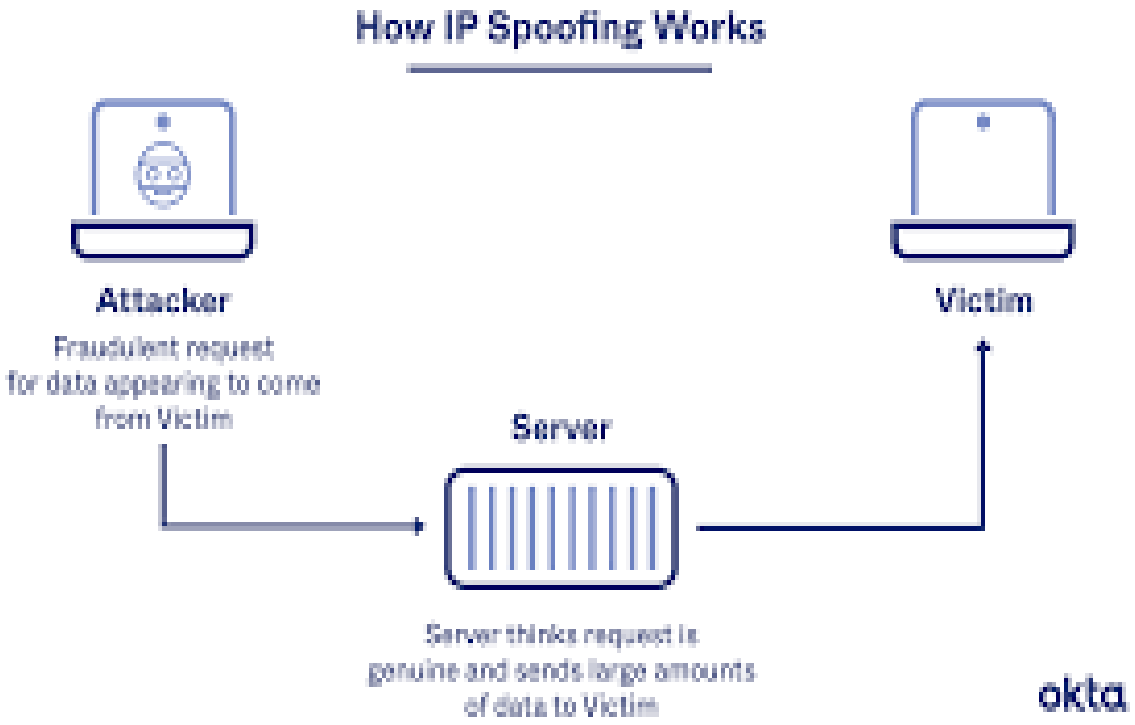
- The act of creating IP packets with a forged source IP address

- Make it appear as though they are coming from a trusted or legitimate source.

Co-funded by
the European Union

How IP Spoofing Works

- Packet Creation
- Transmission
- Target Perception



Co-funded by the European Union

1.5 Packet Flooding

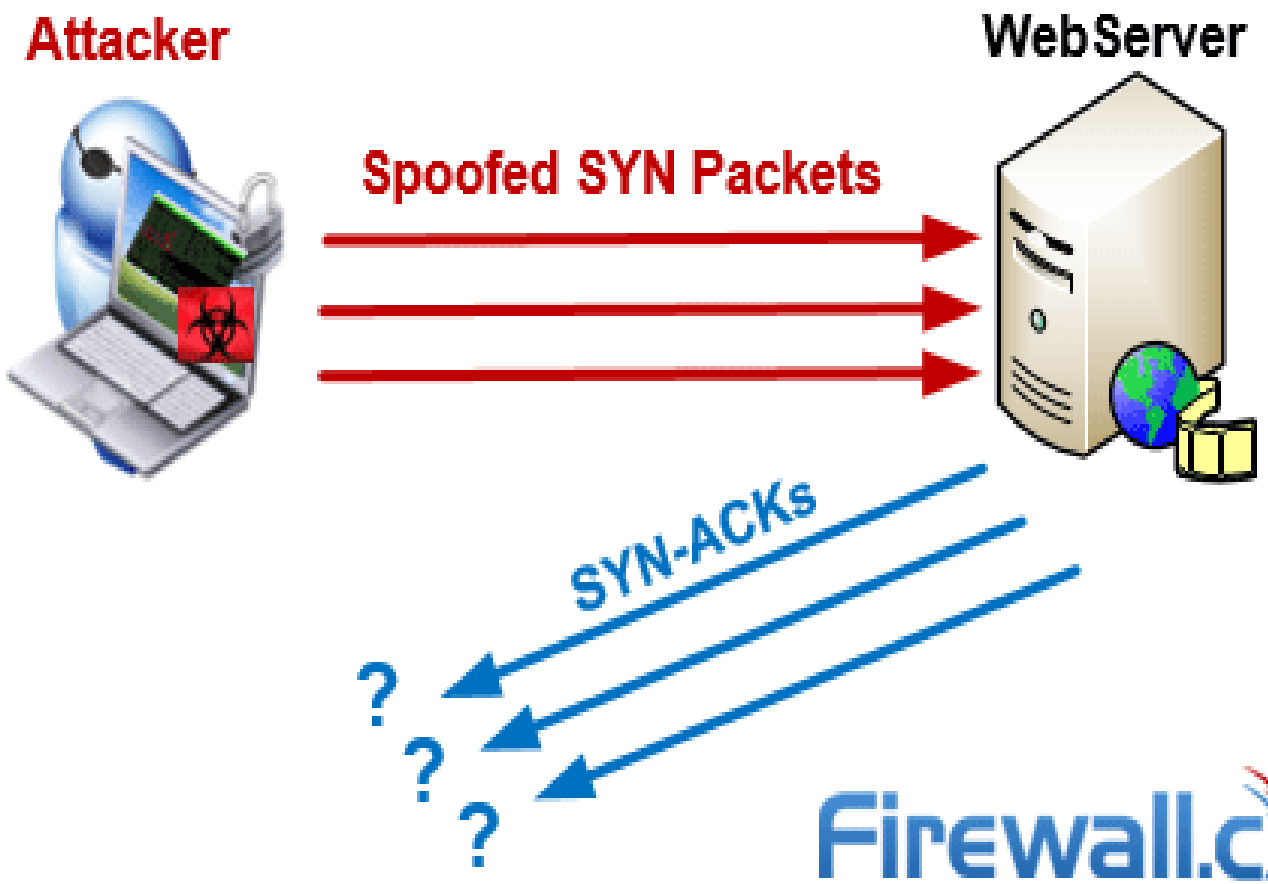
Network attack where a large number of packets are sent to a network or a specific device within the network in a short period of time.

Goal : To overload the target's resources, like internet capacity, computing power, or memory.

Making the service slow down or stop working completely.

Co-funded by
the European Union

Packet Flooding



Co-funded by
the European Union

Packet Characteristics

1. Sending High Volume of Packets

1. Resource Exhaustion

1. Variety of Packets

1. Source of Packets

Co-funded by
the European Union

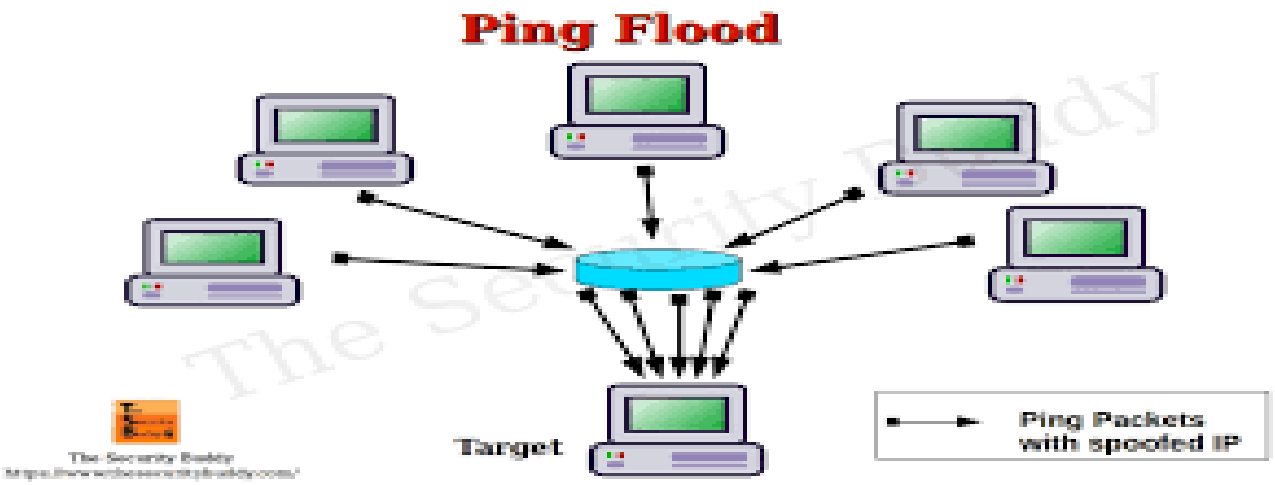
Packet Flooding Attacks

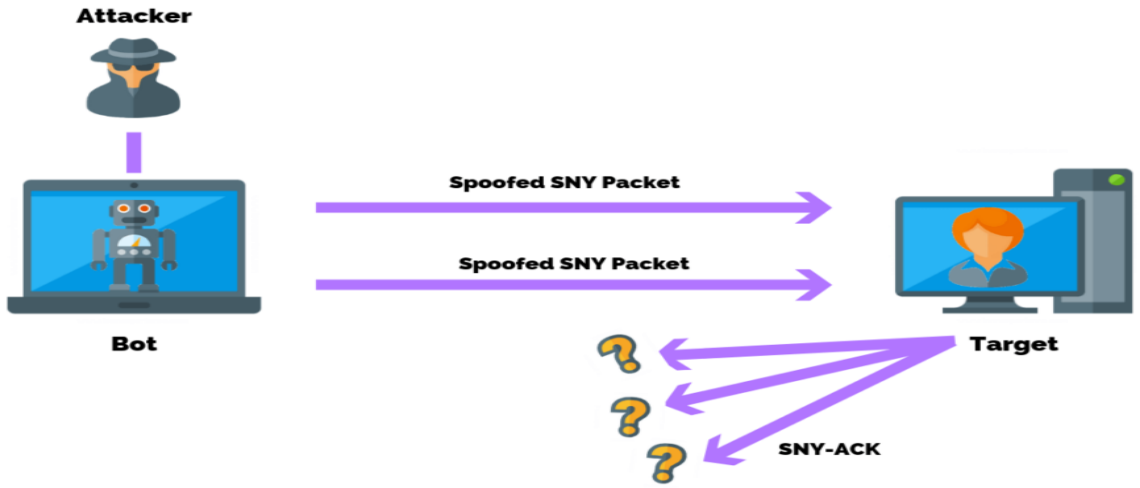
1. **ICMP Flood:** Overwhelms the target with excessive ping requests

1. **UDP Flood:** Bombards the target with UDP packets to random ports

1. **TCP SYN Flood:** Sends numerous fake TCP connection requests

Co-funded by
the European Union





Co-funded by
the European Union

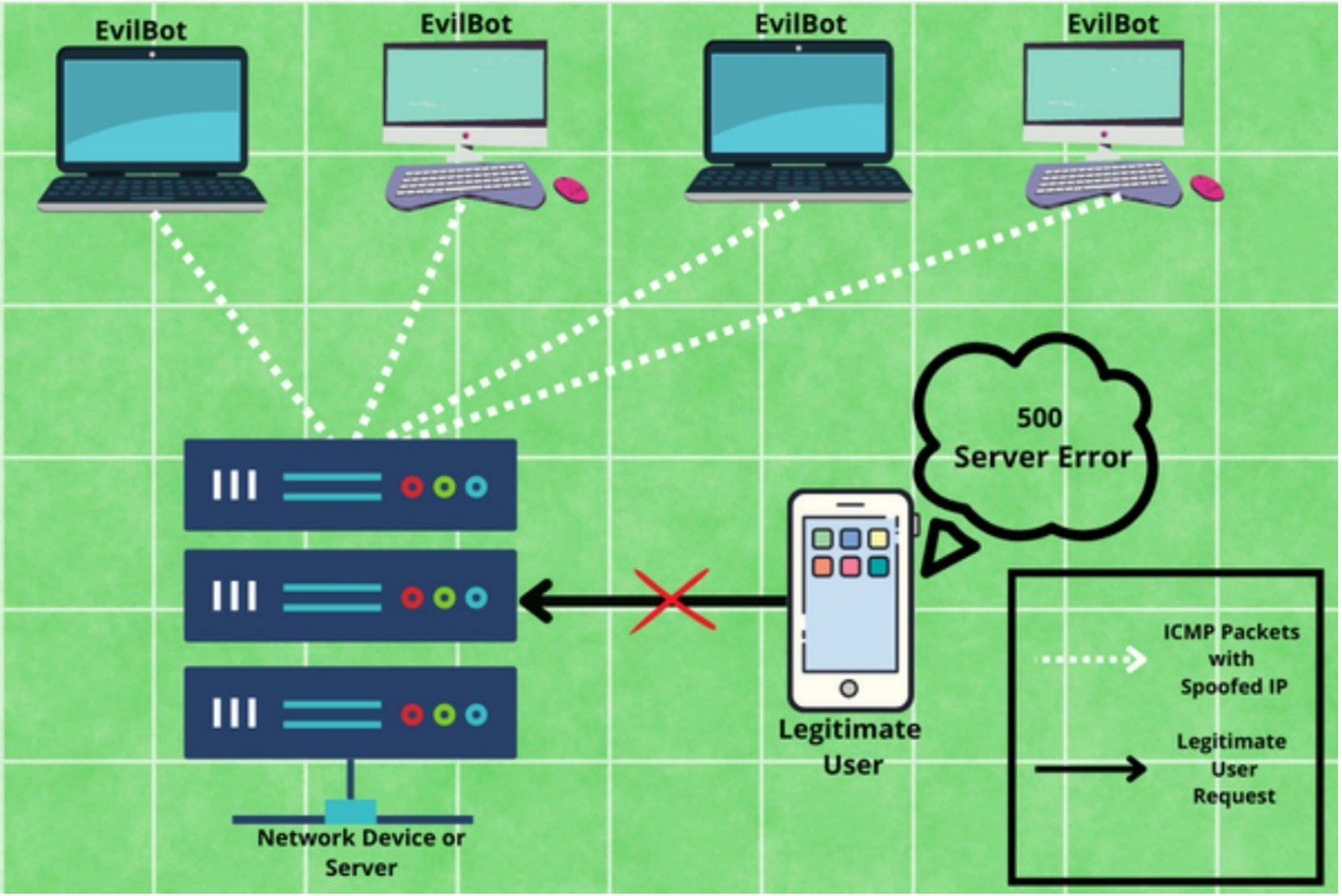
Impact of Packet Flooding

1. **Service Disruption:** Resource exhaustion prevents legitimate users from accessing services

1. **Network Congestion:** Excessive traffic clogs the network, impacting both the target and other users.

1. **Increased Latency:** Network performance degrades, causing slow responses and timeouts

Co-funded by the European Union



Co-funded by
the European Union

ICMP Flood DDOS Attack

1.6 Packet Sniffing Overview

- Involves capturing packets of data that are transmitted over a network
- Technique used for

  Network management

  Security testing

  Troubleshooting to monitor and capture packets of data

- Packet sniffers or network analyzers capture data packets
- Packet sniffing tools

  Wireshark

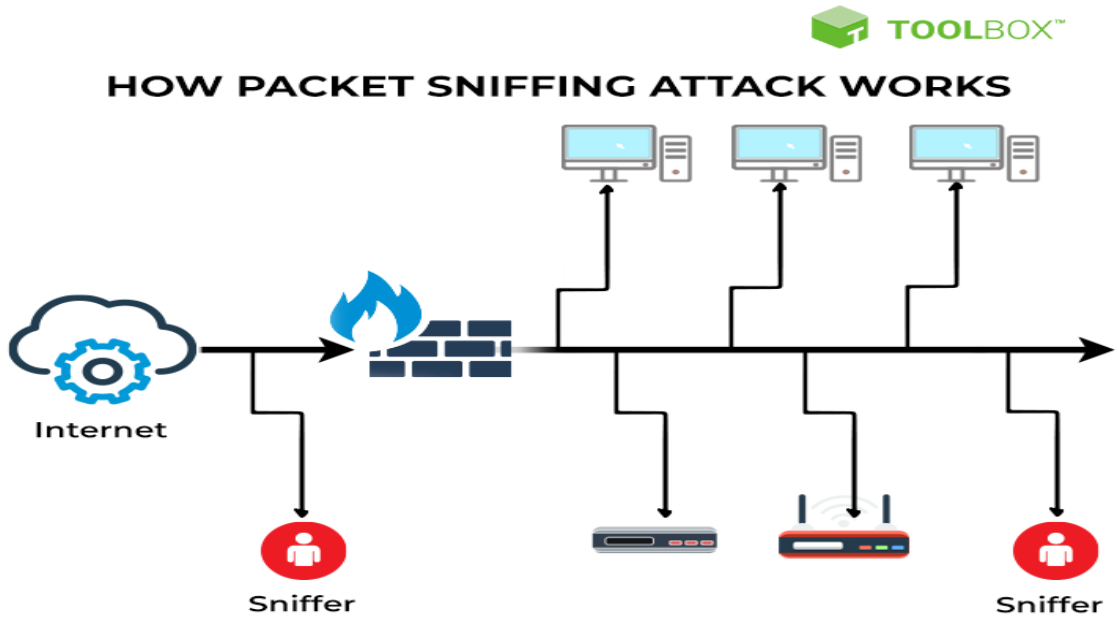
  tcpdump

  Microsoft Network Monitor.

Co-funded by the European Union

What is Packet Sniffing ?

- Data being transmitted over the computer network broken down into smaller units
- Packets- Smallest unit of communication over a computer network
- Capturing data packets across the computer network is called packet sniffing.



Co-funded by the European Union

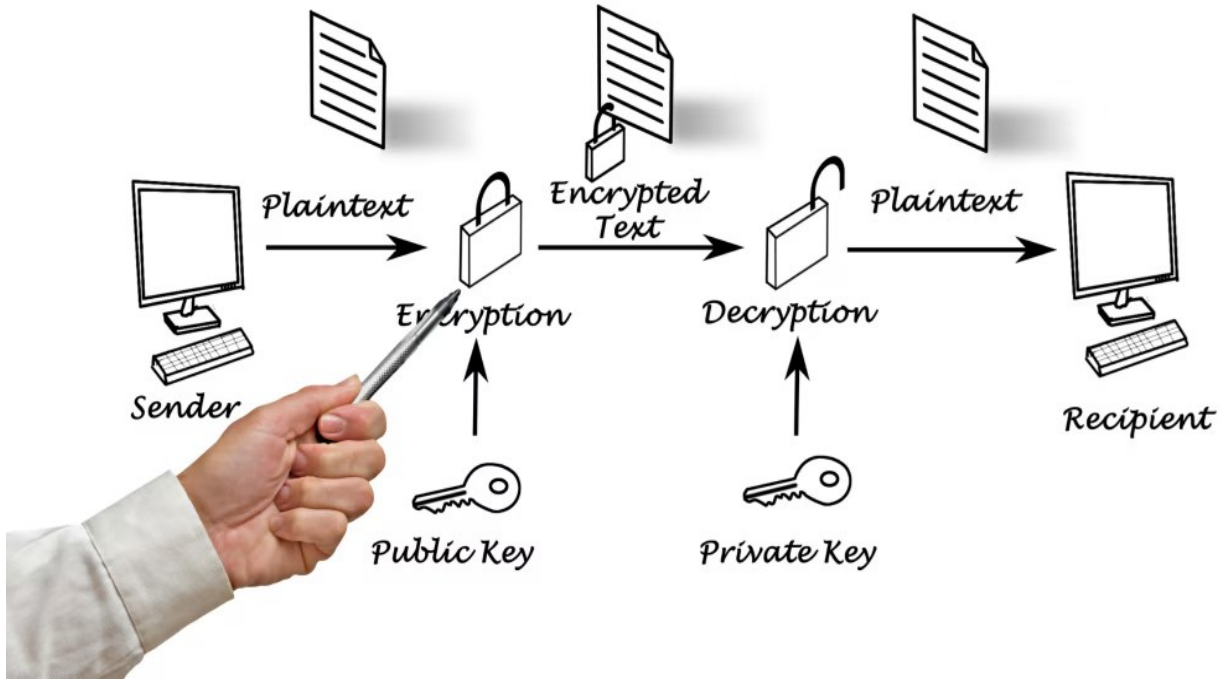
Packet Sniffer

- Packet sniffing tool
- Types: Filtered or Unfiltered.
- Filtered -capturs specific data packets
- Unfiltered -capturs all the data packets
- Examples: WireShark, SmartSniff

Co-funded by
the European Union

How to prevent Packet Sniffing

- Encrypting data you send or receive.
- using trusted Wi-Fi networks.
- Scanning your network for dangers or issues.



Co-funded by the European Union

Advantages

- **Network troubleshooting:** used to identify network problems
- **Security analysis:**used to detect and analyze network intrusions, malware infections, or unauthorized access attempts.

Network Troubleshooting

Co-funded by
the European Union

Advantages

- **Network optimization:** used to optimize network performance
- Identify bottlenecks and optimizing the network configuration.

- **Protocol analysis:** used to analyze network protocols
- identify areas where they can be improved or optimized.

Co-funded by
the European Union

Disadvantages

- **Privacy violations:** Intercepts sensitive information, such as passwords, credit card numbers, or personal information.
- **Legal issues:** illegal without the express consent of all parties involved in the communication

Co-funded by
the European Union

Disadvantages

- **Resource usage:** consume a significant amount of system resources.

- **Complexity:** Complex process, requiring specialized knowledge and tools to analyze network traffic effectively

Co-funded by
the European Union

Packet sniffing using Scapy

- Powerful and versatile packet manipulation tool written in Python
- User will be able to send, sniff, dissect and forge network packets
- Capability to store the sniffed packets in a pcap file
- Facilitates trace routing, probing, scanning, unit tests, and network discovery
- useful for network-based attacks

Co-funded by the European Union

How scapy works

- **Installing Scapy from Source**
- **sudo apt install python3-pip**

git clone https://github.com/secdev/scapy

cd scapy

sudo python3 setup.py install

```
git clone https://github.com/secdev/scapy
cd scapy
sudo python3 setup.py install
```

Co-funded by
the European Union

```
namrata@DESKTOP-2SHAHKI:~$ git clone https://github.com/secdev/scapy
Cloning into 'scapy'...
remote: Enumerating objects: 42427, done.
remote: Counting objects: 100% (1901/1901), done.
remote: Compressing objects: 100% (348/348), done.
remote: Total 42427 (delta 1650), reused 1658 (delta 1552), pack-reused 40526 (from 1
Receiving objects: 100% (42427/42427), 85.57 MiB | 4.97 MiB/s, done.
Resolving deltas: 100% (29305/29305), done.
namrata@DESKTOP-2SHAHKI:~$ cd scapy
namrata@DESKTOP-2SHAHKI:~/scapy$ sudo python3 setup.py install
running install
running bdist_egg
running egg_info
creating UNKNOWN.egg-info
writing UNKNOWN.egg-info/PKG-INFO
writing dependency_links to UNKNOWN.egg-info/dependency_links.txt
writing top-level names to UNKNOWN.egg-info/top_level.txt
writing manifest file 'UNKNOWN.egg-info/SOURCES.txt'
reading manifest file 'UNKNOWN.egg-info/SOURCES.txt'
reading manifest template 'MANIFEST.in'
writing manifest file 'UNKNOWN.egg-info/SOURCES.txt'
installing library code to build/bdist.linux-x86_64/egg
running install_lib
```

Co-funded by
the European Union

```
namrata@DESKTOP-2SHAHKI:~/scapy$ pip show scapy
Name: scapy
Version: 2.6.0
Summary: Scapy: interactive packet manipulation tool
Home-page: None
Author: Philippe BIONDI
Author-email: None
License: GPL-2.0-only
Location: /home/namrata/.local/lib/python3.8/site-packages
Requires:
Required-by:
```

Co-funded by
the European Union

Installing scapy through command prompt

Command Prompt

```
C:\Users\Admin>pip install scapy
Collecting scapy
  Downloading scapy-2.6.0-py3-none-any.whl.metadata (5.6 kB)
Downloading scapy-2.6.0-py3-none-any.whl (2.4 MB)
   ---------------------------------------- 2.4/2.4 MB 3.0 MB/s eta 0:00:00
Installing collected packages: scapy
  WARNING: The script scapy.exe is installed in 'C:\Users\Admin\AppData\Local\Packages\PythonSoftwareFoundation.Python.3
.10_qbz5n2kfra8p0\LocalCache\local-packages\Python310\Scripts' which is not on PATH.
  Consider adding this directory to PATH or, if you prefer to suppress this warning, use --no-warn-script-location.
Successfully installed scapy-2.6.0

[notice] A new release of pip is available: 24.0 -> 24.2
[notice] To update, run: C:\Users\Admin\AppData\Local\Microsoft\WindowsApps\PythonSoftwareFoundation.Python.3.10_qbz5n2k
fra8p0\python.exe -m pip install --upgrade pip

C:\Users\Admin>pip show scapy
Name: scapy
Version: 2.6.0
Summary: Scapy: interactive packet manipulation tool
Home-page:
Author: Philippe BIONDI
Author-email:
License: GPL-2.0-only
Location: c:\users\admin\appdata\local\packages\pythonsoftwarefoundation.python.3.10_qbz5n2kfra8p0\localcache\local-pack
ages\python310\site-packages
Requires:
Required-by:

C:\Users\Admin>
```

Co-funded by
the European Union

Installing scapy through command prompt

pip install scapy

pip show scapy

Co-funded by
the European Union

Sniffing packets using scapy

- **sniff():** returns information about all the packets that has been sniffed

  capture = sniff()

- **summary():** summary of packet responses

  capture.summary()

  capture = sniff(count=5)

Co-funded by
the European Union

sniffing packets with scapy

IDLE Shell 3.10.11

File Edit Shell Debug Options Window Help

```
Python 3.10.11 (tags/v3.10.11:7d4cc5a, Apr  5
4 bit (AMD64)] on win32
Type "help", "copyright", "credits" or "licen
>>> from scapy.all import *
>>> sniff(count=1)
<Sniffed: TCP:1 UDP:0 ICMP:0 Other:0>
>>>
```

Co-funded by
the European Union

sniffing packets with scapy

```
>>> packets = sniff(count=10)
>>> packets.show()
0000 Ether / ARP who has 192.168.0.101 says 192.168.0.1
0001 Ether / IP / TCP 142.250.76.196:https > 192.168.0.102:56895 FA
0002 Ether / IP / TCP 192.168.0.102:56895 > 142.250.76.196:https A
0003 Ether / ARP who has 192.168.0.101 says 192.168.0.1
0004 Ether / IP / TCP 192.168.0.102:56887 > 13.107.246.48:https FA
0005 Ether / :: > ff02::1 (0) / IPv6ExtHdrHopByHop / ICMPv6MLQuery2
0006 Ether / ARP who has 192.168.0.101 says 192.168.0.1
0007 Ether / ARP who has 192.168.0.101 says 192.168.0.1
0008 Ether / ARP who has 192.168.0.101 says 192.168.0.1
0009 Ether / 192.168.0.1 > 239.255.255.250 2 / Raw
>>>
```

Co-funded by
the European Union

sniffing packets with scapy

count=10: Captures 10 packets. You can adjust this number or remove it to capture indefinitely.

packets.show(): Displays details of the captured packets.

Co-funded by the European Union

Sniffing and Filtering Packets (Using BPF Filters) You can filter packets based on specific criteria using a Berkeley Packet Filter (BPF):

```
>>> from scapy.all import sniff
>>> packets = sniff(filter="tcp", count=10)
>>> packets.show()
0000 Ether / IP / TCP 192.168.0.102:56915 > 142.250.183.142:https A /
0001 Ether / IP / TCP 142.250.183.142:https > 192.168.0.102:56915 A
0002 Ether / IP / TCP 192.168.0.102:56923 > 23.196.14.121:https FA
0003 Ether / IP / TCP 23.196.14.121:https > 192.168.0.102:56923 PA /
0004 Ether / IP / TCP 192.168.0.102:56923 > 23.196.14.121:https A
0005 Ether / IP / TCP 23.196.14.121:https > 192.168.0.102:56923 FA
0006 Ether / IP / TCP 192.168.0.102:56923 > 23.196.14.121:https A
0007 Ether / IP / TCP 192.168.0.102:56923 > 23.196.14.121:https FA
0008 Ether / IP / TCP 23.196.14.121:https > 192.168.0.102:56923 FA
```

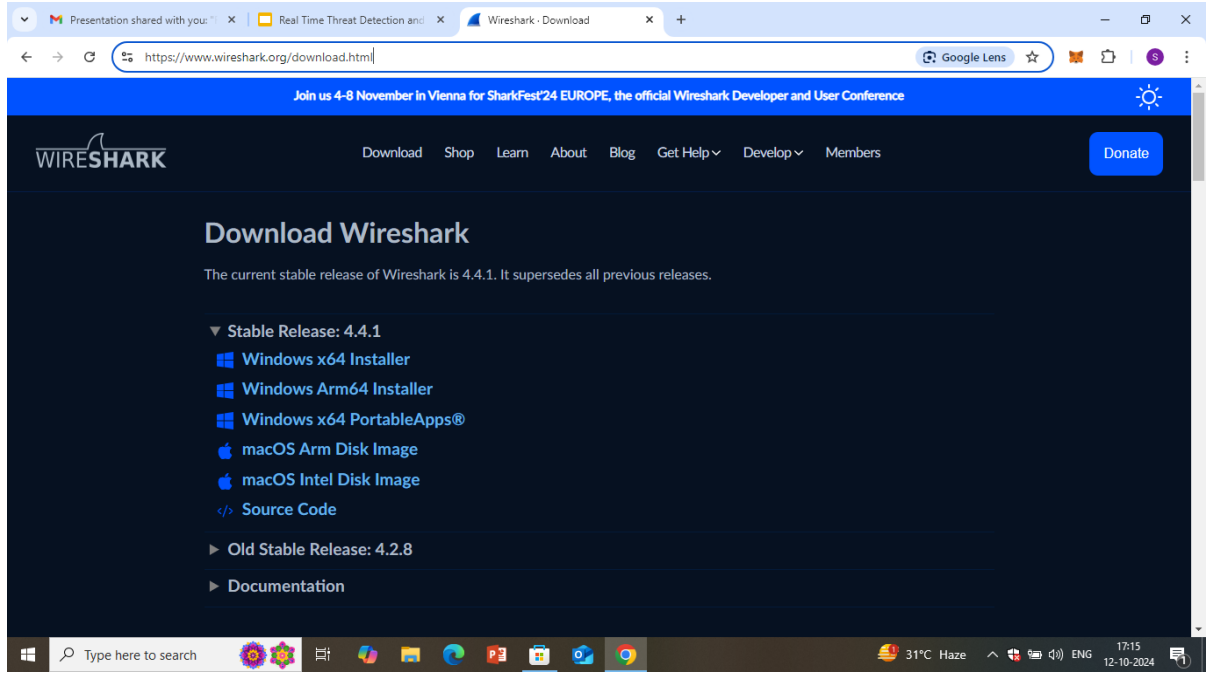
Co-funded by
the European Union

Packet Sniffing and Network Analysis Tool: Wireshark

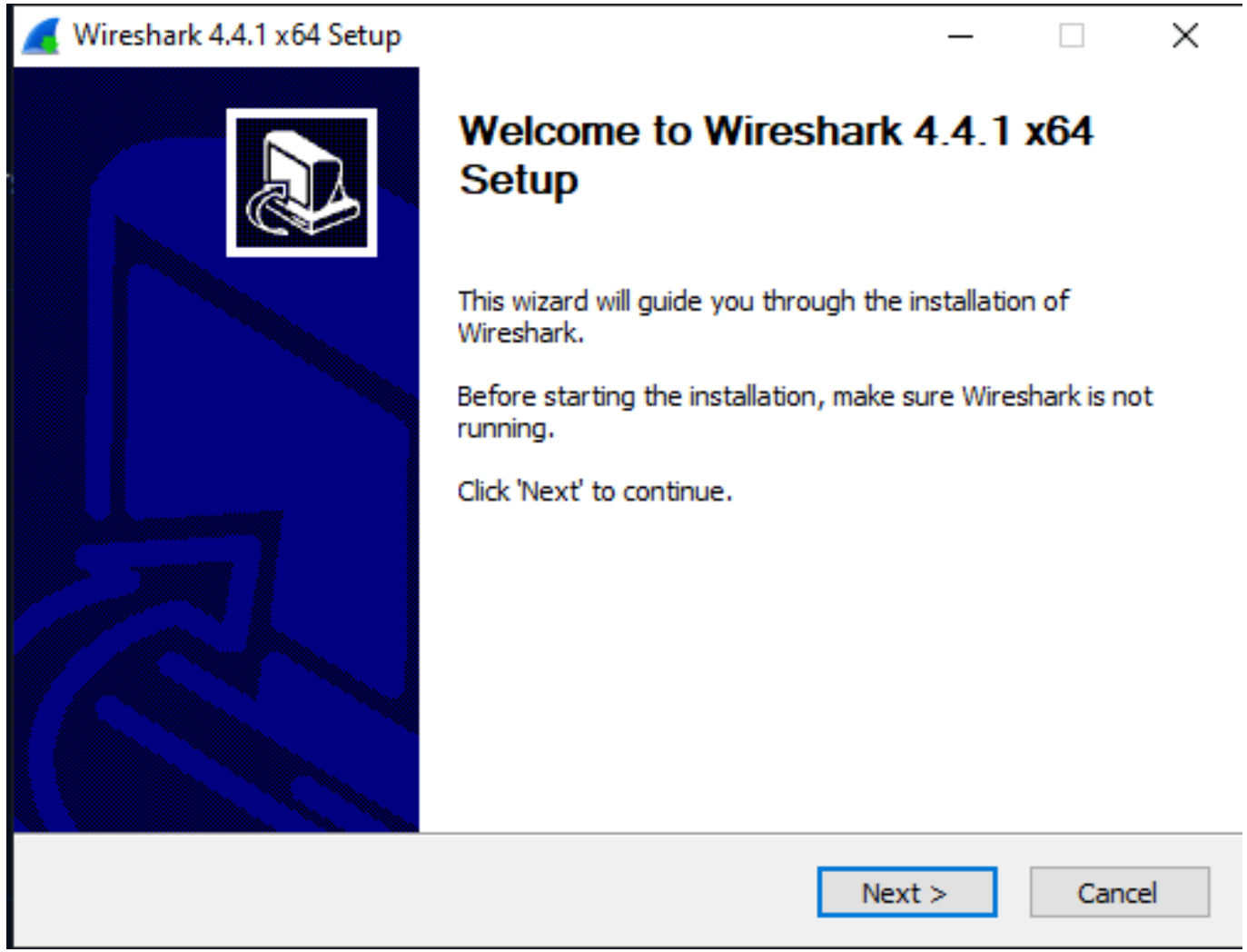
Using Wireshark:

1. Download and Install Wireshark

https://www.wireshark.org/download.html



Co-funded by the European Union



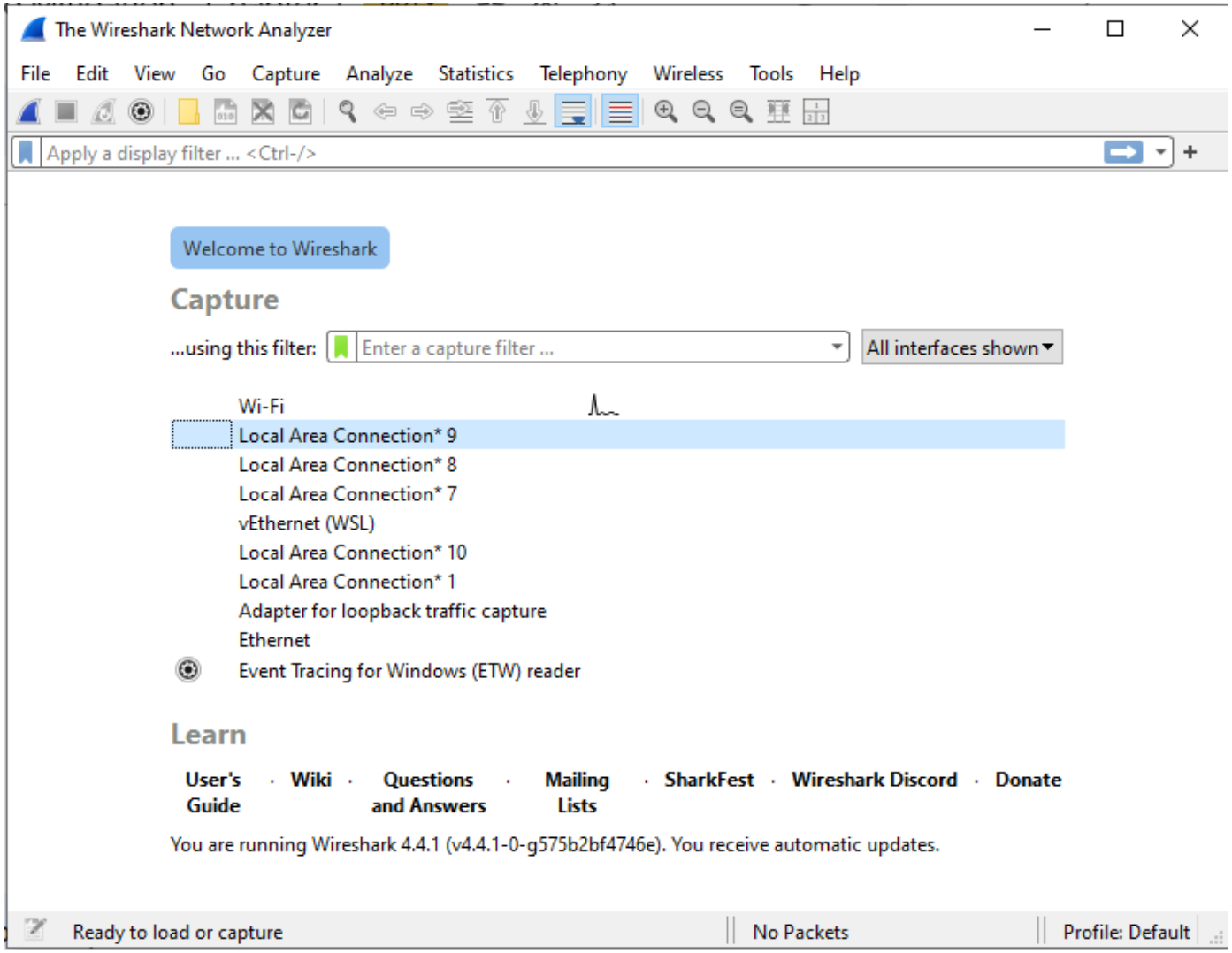
Co-funded by
the European Union

Packet Sniffing with Wireshark

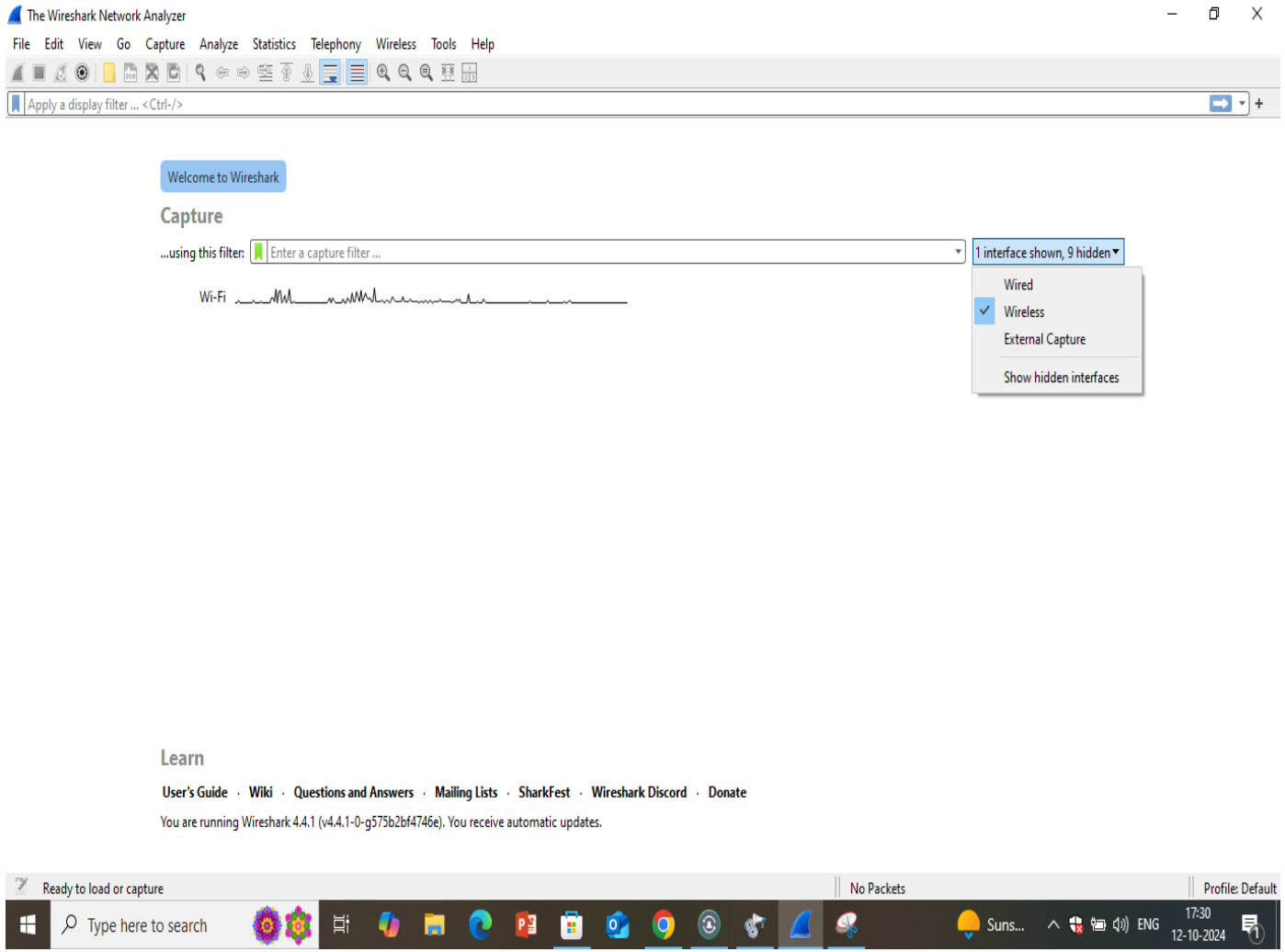
2. Begin Packet Capturing:

- Open Wireshark and choose the network interface from which to begin collecting packets.

Co-funded by
the European Union

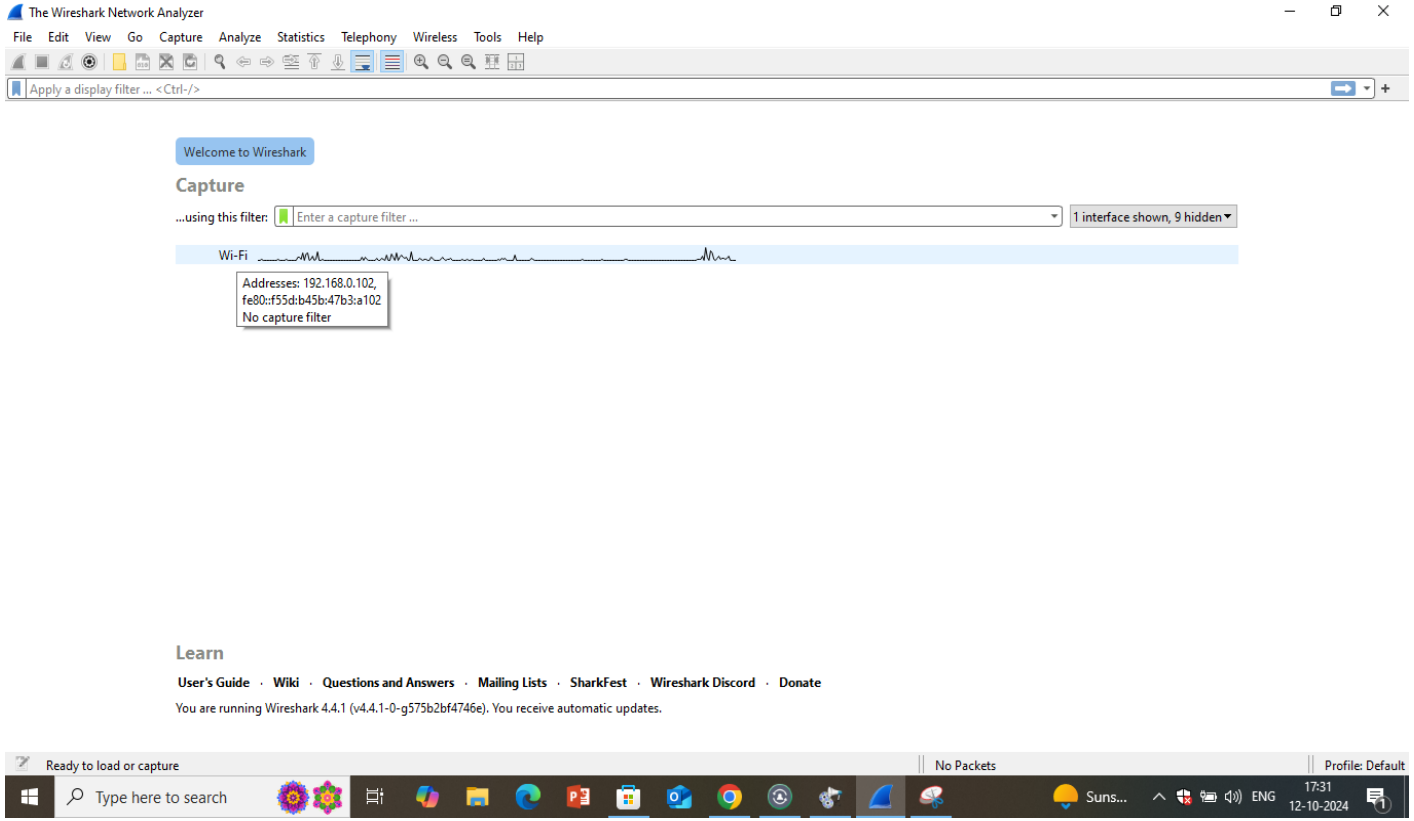


Co-funded by
the European Union

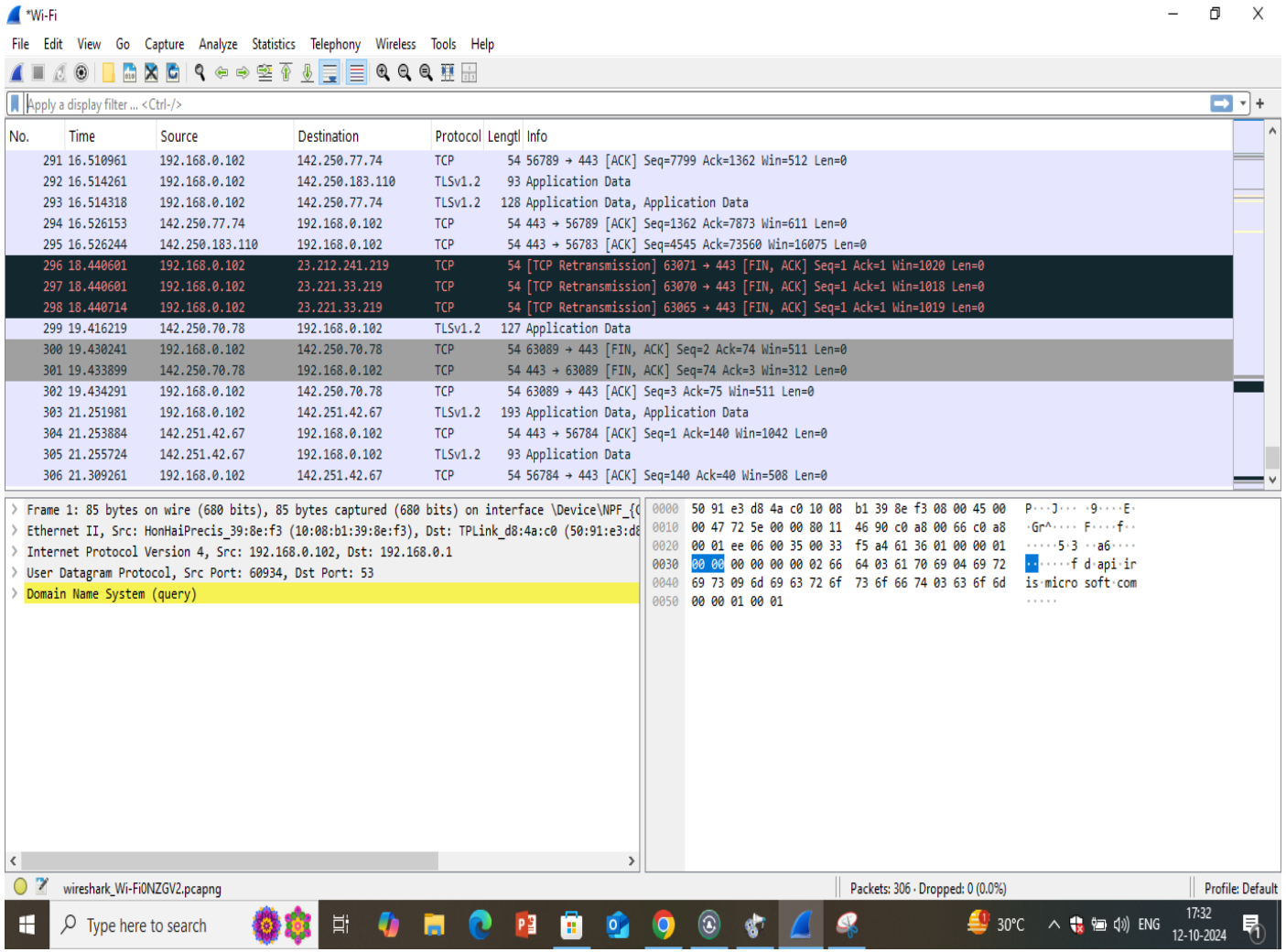


Co-funded by
the European Union

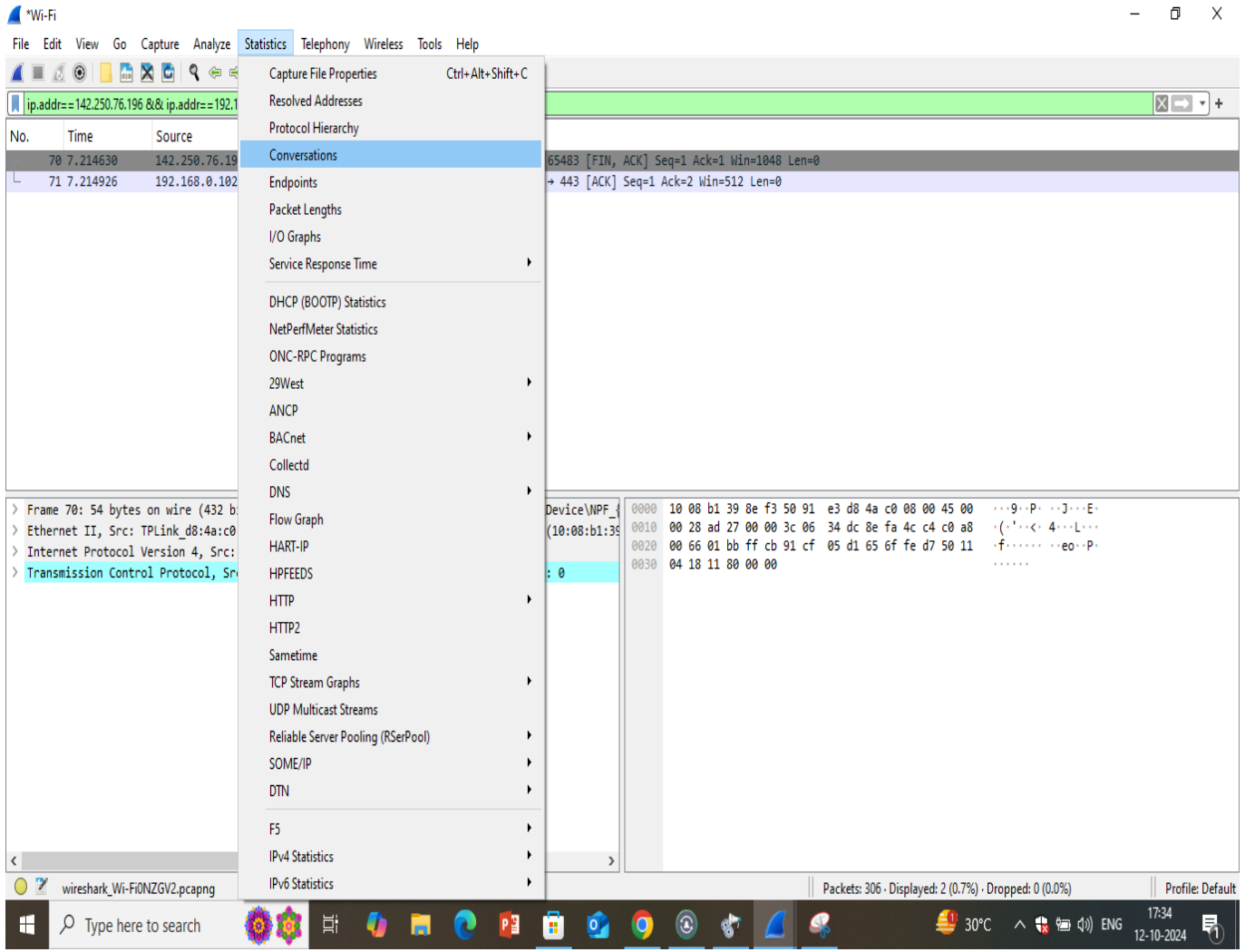
Double click on selected network



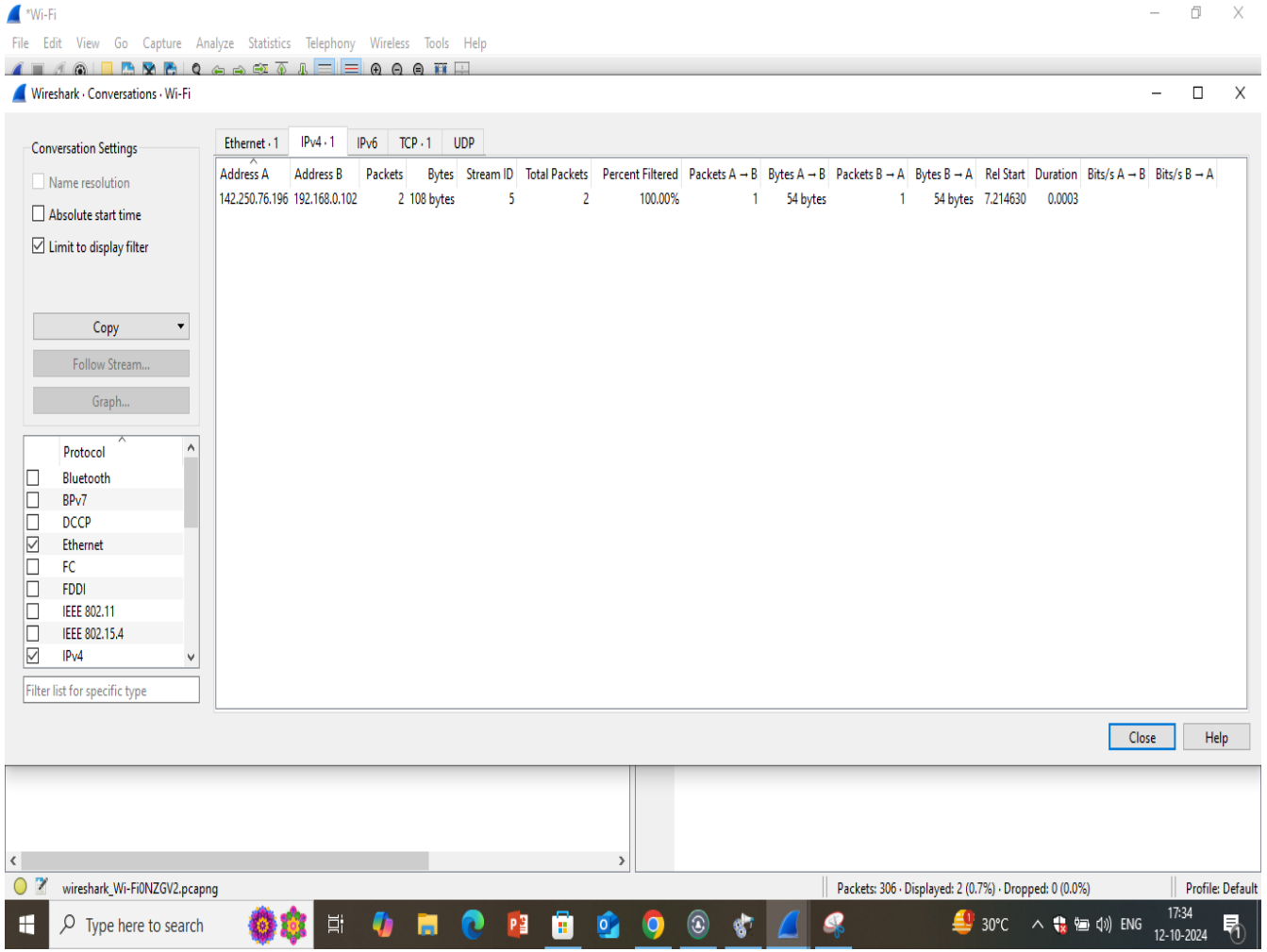
Co-funded by
the European Union



Co-funded by the European Union



Co-funded by the European Union



Co-funded by
the European Union

Presentation shared with you: "C" | Real Time Threat Detection and

Wireshark · Conversations · Wi-Fi

Conversation Settings

- [ ] Name resolution
- [ ] Absolute start time
- [ ] Limit to display filter

Copy

Follow Stream...

Graph...

Protocol	
[ ]	Bluetooth
[ ]	BPv7
[ ]	DCCP
[x]	Ethernet
[ ]	FC
[ ]	FDDI
[ ]	IEEE 802.11
[ ]	IEEE 802.15.4
[x]	IPv4

Filter list for specific type

Ethernet · 3 | IPv4 · 15 | IPv6 | TCP · 19 | UDP · 3

Address A	Address B	Packets	Bytes	Stream ID	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
142.250.76.196	192.168.0.102	2	108 bytes	5	1	54 bytes	1	54 bytes	7.214630	0.0003		
142.250.77.74	192.168.0.102	38	12 kB	10	22	3 kB	16	9 kB	11.409426	5.1167	4263 bits/s	14 kbps
192.168.0.102	20.24.121.134	58	25 kB	1	34	4 kB	24	21 kB	0.019457	1.7959	19 kbps	92 kbps
192.168.0.102	23.212.241.219	6	324 bytes	2	6	324 bytes	0	0 bytes	2.092335	16.3483	158 bits/s	0 bits/s
192.168.0.102	23.221.33.219	10	540 bytes	12	10	540 bytes	0	0 bytes	13.913051	4.5277	954 bits/s	0 bits/s
192.168.0.102	108.177.122.94	4	242 bytes	7	2	110 bytes	2	132 bytes	8.826331	0.3407	2582 bits/s	3099 bits/s
192.168.0.102	142.250.66.10	20	8 kB	13	9	6 kB	11	2 kB	16.363031	0.1187	424 kbps	127 kbps
192.168.0.102	142.250.67.138	2	121 bytes	9	1	55 bytes	1	66 bytes	10.763809	0.0018		
192.168.0.102	142.250.67.238	2	121 bytes	11	1	55 bytes	1	66 bytes	11.529445	0.0023		
192.168.0.102	142.250.70.78	6	410 bytes	3	3	163 bytes	3	247 bytes	4.482566	14.9517	87 bits/s	132 bits/s
192.168.0.102	142.250.183.110	142	86 kB	8	73	78 kB	69	8 kB	8.923643	7.6026	81 kbps	8702 bits/s
192.168.0.102	142.250.192.131	2	121 bytes	4	1	55 bytes	1	66 bytes	5.529462	0.0125	35 kbps	42 kbps
192.168.0.102	142.251.42.67	4	394 bytes	14	2	247 bytes	2	147 bytes	21.251981	0.0573	34 kbps	20 kbps
192.168.0.102	192.168.0.1	4	1 kB	0	2	156 bytes	2	1 kB	0.000000	1.5099	826 bits/s	5711 bits/s
192.168.0.102	192.168.0.255	3	276 bytes	6	3	276 bytes	0	0 bytes	8.744801	1.5035	1468 bits/s	0 bits/s

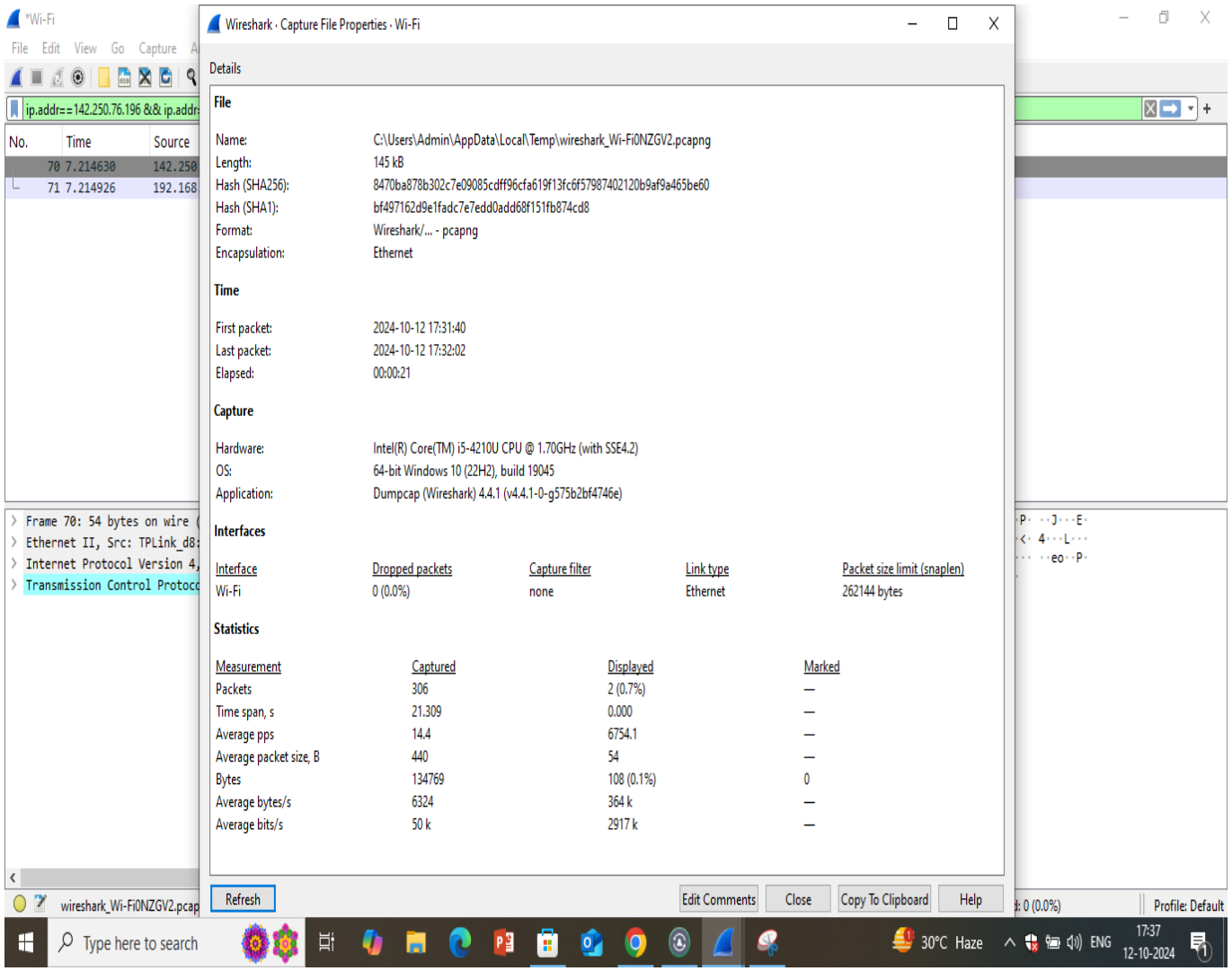
Close | Help

Click to add speaker notes

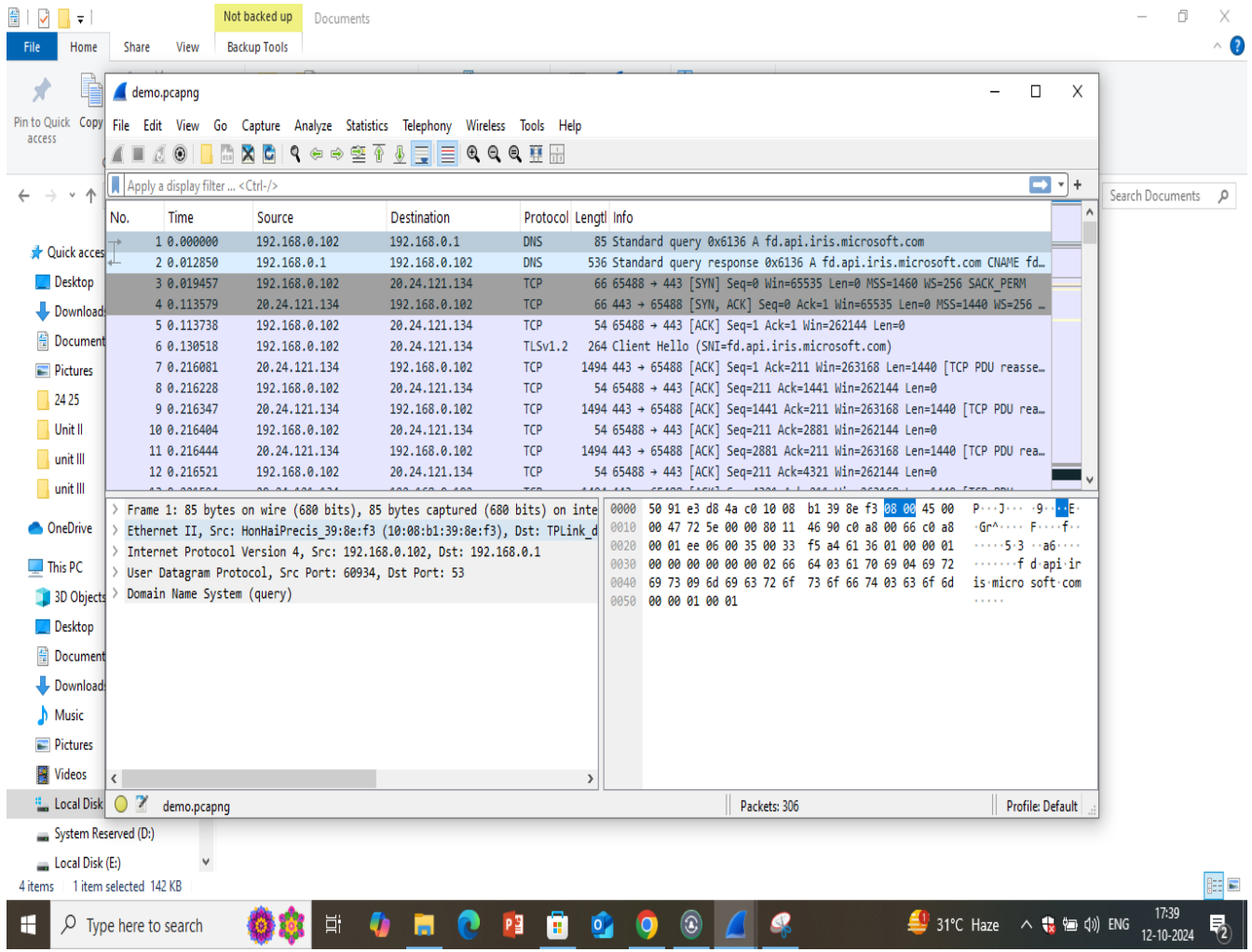
Type here to search

30°C ENG 17:35 12-10-2024

Co-funded by the European Union



Co-funded by the European Union



Co-funded by
the European Union

Packet Sniffing with Wireshark

3. Analyze Packets:

- Wireshark will show packets as they come through the chosen interface in real time.

- To limit the packets that are shown based on parameters such as source, destination, protocol, etc., you can apply filters.

Co-funded by
the European Union

Packet Sniffing with tcpdump

- 1. Install tcpdump

sudo apt-get install tcpdump

Co-funded by
the European Union

namrata@DESKTOP-2SHAHKI: ~

```
namrata@DESKTOP-2SHAHKI:~$ sudo apt-get install tcpdump
[sudo] password for namrata:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages will be upgraded:
  tcpdump
1 upgraded, 0 newly installed, 0 to remove and 149 not upgraded.
Need to get 370 kB of archives.
After this operation, 0 B of additional disk space will be used.
Get:1 http://archive.ubuntu.com/ubuntu focal-updates/main amd64 tcpdump amd64 4.9.3
Fetched 370 kB in 24s (15.2 kB/s)
(Reading database ... 38812 files and directories currently installed.)
Preparing to unpack .../tcpdump_4.9.3-4ubuntu0.3_amd64.deb ...
Unpacking tcpdump (4.9.3-4ubuntu0.3) over (4.9.3-4ubuntu0.2) ...
Setting up tcpdump (4.9.3-4ubuntu0.3) ...
Installing new version of config file /etc/apparmor.d/usr.sbin.tcpdump ...
Processing triggers for man-db (2.9.1-1) ...
namrata@DESKTOP-2SHAHKI:~$
```

Co-funded by
the European Union

sudo tcpdump

By default, tcpdump listens to the first available interface

```
namrata@DESKTOP-2SHAHKI:~$ sudo tcpdump
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
21:18:05.856266 IP 172.19.68.22.38574 > api.snapcraft.io.https: Flags [FP.], sec
win 501, options [nop,nop,TS val 1065135596 ecr 2959490897], length 24
21:18:05.856828 IP 172.19.68.22.45543 > DESKTOP-2SHAHKI.mshome.net.domain: 1343+
21:18:05.858337 IP DESKTOP-2SHAHKI.mshome.net.mdns > mdns.mcast.net.mdns: 0 PTR
 (51)
21:18:05.859086 IP6 DESKTOP-2SHAHKI.mdns > ff02::fb.mdns: 0 PTR (QM)? 50.188.12
```

Co-funded by
the European Union

tcpdump

capture packets on a specific network interface (e.g., eth0)

```
namrata@DESKTOP-2SHAHKI:~$ sudo tcpdump -i eth0
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
```

Co-funded by
the European Union

tcpdump

limit the number of packets captured by using the -c option

sudo tcpdump -i eth0 -c 10

```
namrata@DESKTOP-2SHAHKI:~$ sudo tcpdump -i eth0 -c 10
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
```

Co-funded by
the European Union

Save Captured Packets to a File

Save the captured packets to a .pcap file

```
namrata@DESKTOP-2SHAHKI:~$ sudo tcpdump -i eth0 -c 100 -w capture.pcap
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
```

Co-funded by
the European Union

Applying Filters

Capture Only TCP Packets

To capture only TCP packets:

sudo tcpdump -i eth0 tcp

```
namrata@DESKTOP-2SHAHKI:~$ sudo tcpdump -i eth0 tcp
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
```

Co-funded by
the European Union

Applying Filters

To capture only UDP packets

sudo tcpdump -i eth0 udp

```
namrata@DESKTOP-2SHAHKI:~$ sudo tcpdump -i eth0 udp
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
```

tcpdump will continue to capture packets until you stop it manually. To stop tcpdump, press Ctrl + C in the terminal where it's running

Co-funded by the European Union

1.7 SYN Packets for Access Control

- SYN packets- part of the **TCP three-way handshake**

- Used to establish a connection between a client and a server

Co-funded by the European Union

Basics of TCP

- **Handshake SYN Packet:** Initiates a connection.
- The client sends a SYN packet to the server.

- **SYN-ACK Packet:** The server responds with a SYN-ACK
- acknowledging the receipt of the SYN

- **ACK Packet:** The client responds with an ACK packet
- completing the handshake and establishing the connection.

Co-funded by
the European Union

TCP 3-Way Handshake Process

- Fundamental process that establishes a reliable connection between two devices over a TCP/IP network

- It involves three steps: SYN (Synchronize), SYN-ACK (Synchronize-Acknowledge), and ACK (Acknowledge).

- The client and server exchange initial sequence numbers and confirm the connection establishment.

Co-funded by the European Union

Using SYN Packets for Access Control

- a system could be configured to recognize and respond to SYN packets as part of an access control strategy

- a firewall or network device might check for specific SYN packet characteristics to grant or deny access.

Co-funded by the European Union

Challenges and Limitations

- **Simplicity:** Do not carry authentication or user identification data
- **Spoofing:**Can be spoofed or faked,
- Relying on them for security would be risky.
- **Limited Information:** do not contain application-level information
- using them for complex access control would be challenging.

Co-funded by
the European Union

Possible Approaches

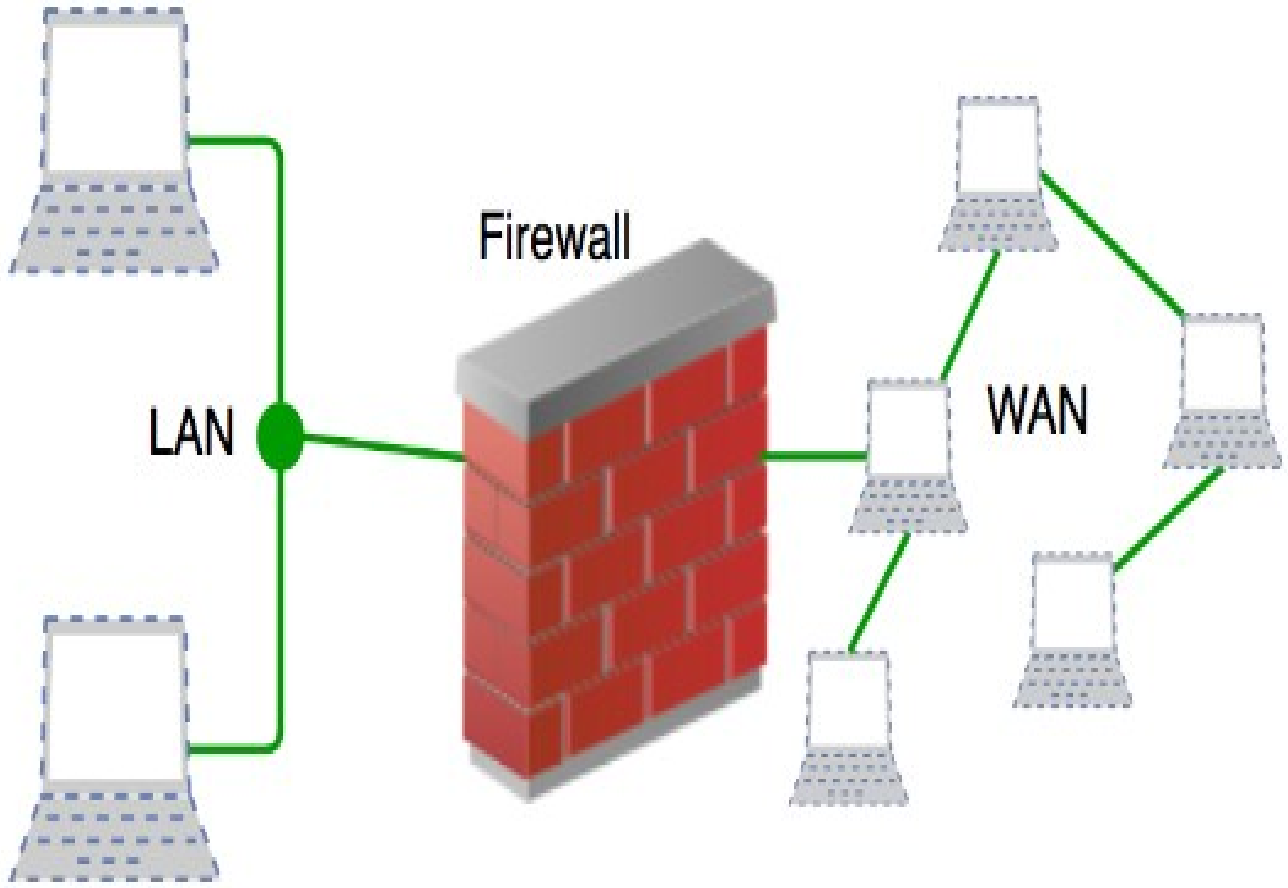
- **Firewall Rules:** Some firewalls might filter traffic based on SYN packets to block or allow connections from certain IP addresses
- **Rate Limiting:** Implementing rate limiting based on the number of SYN packets received to mitigate SYN flood attacks.
- **Custom Protocols:**a custom protocol might be designed where SYN packets play a role in an initial handshake for more complex authentication.

Co-funded by
the European Union

1.8 What is Firewall?

- A network security device or software that monitors and controls incoming and outgoing network traffic based on predetermined security rules
- Designed to block unauthorized access while allowing safe data to pass through
- Helps keep your digital world safe from unwanted visitors and potential threats

Co-funded by the European Union



Co-funded by
the European Union

Types of Firewalls

- **Network Firewalls:** Typically used to protect internal networks
- filters traffic based on IP addresses, ports, and protocols

- **Host-Based Firewalls**: Installed on individual devices to protect from threats
- Monitor and control network traffic to and from the device.

Co-funded by the European Union

Types of Firewalls

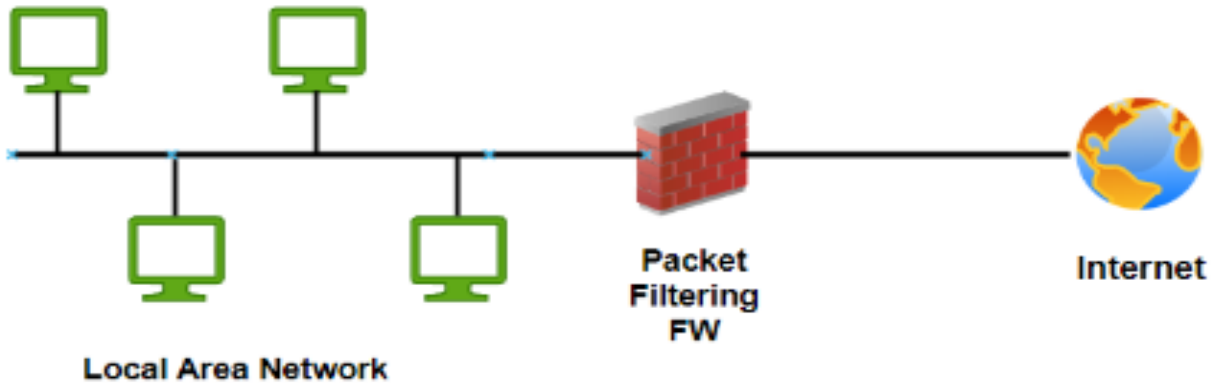
- **Proxy Firewalls:** Intercept all incoming and outgoing traffic between a network and the internet,
- acts as an intermediary.

- **Next-Generation Firewalls (NGFWs):** Combine traditional firewall capabilities with advanced features like application awareness, intrusion prevention, and threat intelligence integration.

Co-funded by the European Union

Packet Filters

- Technique used to control network access by monitoring outgoing and incoming packets
- Allows to pass or halt based on the source and destination Internet Protocol (IP) addresses, protocols, and ports.



Packet Filter Firwall

Stateful Inspection Firewalls

- Packet filtering that is used to control data packets move through a firewall.
- can inspect if the packet belongs to a particular session or not.
- It only permits communication if the session is perfectly established between two endpoints else it will block the communication.

Co-funded by
the European Union

Application Layer Firewalls

- can examine application layer (of OSI model) information like an HTTP request.
- If finds suspicious application that can be responsible for harming our network or that is not safe for our network then it gets blocked right away.

Co-funded by the European Union

Next-generation Firewalls

- Intelligent firewalls.
- Includes additional features like application awareness and control, integrated intrusion prevention, a cloud-delivered threat intelligence
- Combine traditional firewall capabilities with advanced features
- Provide more granular control over network traffic.

Co-funded by
the European Union

How Firewalls Work

- Examine packets of data as they enter or leave a network.
- Use a set of predefined rules
- Determine whether the packets should be allowed through or blocked.

Co-funded by the European Union

How Firewalls Work

Rules can be based on various factors, including:

- IP Addresses
- Ports and Protocols
- Content Filtering
- Stateful Inspection

Co-funded by
the European Union

Benefits of Firewalls

- Enhanced Security
- Network Monitoring
- Access Control
- Improved Privacy

Co-funded by
the European Union

Disadvantages

- Cost
- Restricts User
- Issues With The Speed of The Network
- Maintenance

Co-funded by the European Union

1.8 Stateless vs Stateful Packet Filtering Firewalls

- Check the source and destination IP addresses, protocols UDP and TCP, and port addresses
- If both IP addresses match, the packet is considered secured and verified

- *Two* categories :
- **Stateless packet filtering firewalls**
- **Stateful packet filtering firewalls**

Co-funded by the European Union

Stateful firewalls

- Keeps track of the state of network connections
- Traffic approved by a stateful firewall added to a state table.
- The state table entries are created for TCP streams or UDP that are allowed to communicate through the firewall
- If no traffic is seen for a specified time the connection is removed from the state table.

Co-funded by
the European Union

Stateless firewalls

- Does not store information on the connection state
- Applicable to the network and physical layers
- When the sender sends a packet gets filtered through a firewall
- device checks for matches ACL rules that are configured in the firewall
- then drops or rejects the packet accordingly.

Co-funded by
the European Union

Differences between Stateless and Stateful firewalls

- The stateless firewalls are designed to protect networks based on static information such as source and destination.

  Stateful firewalls filter packets based on the full context of the connection.

- Stateful firewalls are more secure as compared to stateless firewalls.

Co-funded by the European Union

Cont..

- Stateful firewalls are Expensive where as stateless firewalls are Cheaper
- Stateful firewalls are Slower in speed when compared to Stateless firewall.
- a stateless firewall could be a better option for small business hereas For larger enterprises, a stateful firewall would be a smarter option.

Co-funded by
the European Union

1.9 Packet Filtering

- Essential to designing secure and efficient network infrastructures.

- Technique used in network security to control which packets are allowed to enter or leave a network based on predefined rules

Co-funded by
the European Union

Packet Filtering

- Rules are defined based on various criteria such as IP addresses, port numbers, and protocols.

- Rule might specify that only packets with a source IP of 192.168.1.1 and destination port 80 (HTTP) are allowed.

Co-funded by
the European Union

Cont…

- **Packet Inspection:**The device inspects the packet's header to determine if it matches any of the rules.
- **Action Decision:** Based on the rules, the packet is either allowed to pass through, dropped, or denied.
- Not examining the packet's payload, making packet filtering relatively fast and efficient

Co-funded by
the European Union

Example of Packet Filtering Rule:

- Allow incoming traffic from 192.168.1.10 to 10.0.0.5 on port 22 (SSH).
- Deny all incoming traffic from 0.0.0.0/0 to port 23 (Telnet).

Co-funded by the European Union

1.10 Sample Packet Filtering and Reference Architecture

- **Reference Architecture**
- provides a standardized framework for designing and implementing network and security solutions
- outlines best practices, components, and their interactions to achieve specific goals.

Co-funded by the European Union

Reference Architecture Component

- **Components:** routers, firewalls, intrusion detection/prevention systems (IDS/IPS), and load balancers.
- **Interactions:** Specifies how these components should interact to ensure optimal performance and security.

Co-funded by the European Union

Reference Architecture Component

- **Best Practices:** Includes guidelines for deployment, configuration, and management.

- **Layered Security:** including perimeter defenses (firewalls), network segmentation, and endpoint protection.

Co-funded by the European Union

Example of a Reference Architecture for a Corporate Network:

- **Perimeter Security:** Firewalls and IDS/IPS systems at the network edge to monitor and control external traffic.

- **Internal Segmentation:** Separate VLANs or subnets for different departments (e.g., HR, Finance) to restrict lateral movement in case of a breach.

Co-funded by the European Union

Example of a Reference Architecture for a Corporate Network:

- **Access Controls:** Role-based access control (RBAC) and multi-factor authentication (MFA) to secure access to critical systems.

- **Monitoring and Logging:** Centralized logging and monitoring to detect and respond to security incidents promptly.

Co-funded by the European Union

1.11 Default firewall block

- Security policy or configuration setting in a firewall where all incoming or outgoing traffic is blocked unless explicitly allowed by a set of rules.

- Used to ensure that only authorized traffic can traverse the firewall, enhancing security by default

Co-funded by
the European Union

How Default Firewall Block Works

- Implicit Deny: The firewall operates on the principle of "implicit deny" or "default deny."

- If a packet does not match any of the firewall's predefined allow rules, it is automatically blocked.

Co-funded by
the European Union

Cont…

- **Rule Configuration:** Explicit rules to permit specific types of traffic

- **Granular Control:**
- The default block setting
- permits only the necessary services, applications, and users, minimizing the attack surface

Co-funded by
the European Union

Advantages of Default Firewall Block

- **Enhanced Security:**
- Reduces the risk of unauthorized access.
- Only traffic that is explicitly permitted by rules can pass through

- **Controlled Access:**
- Ensures allowed traffic is intentional and documented
- helping to maintain a secure and well-managed network environment

Co-funded by the European Union

Advantages of Default Firewall Block

- **Minimized Attack Surface:** Prevents the potential exploitation of services or ports that are not explicitly needed

- **Compliance:** Supports compliance with security policies and regulations that require a restrictive approach to network access.

Co-funded by the European Union

1.12 Firewall Rules to Allow Outbound Web Browsing

What is Outbound Web Browsing?

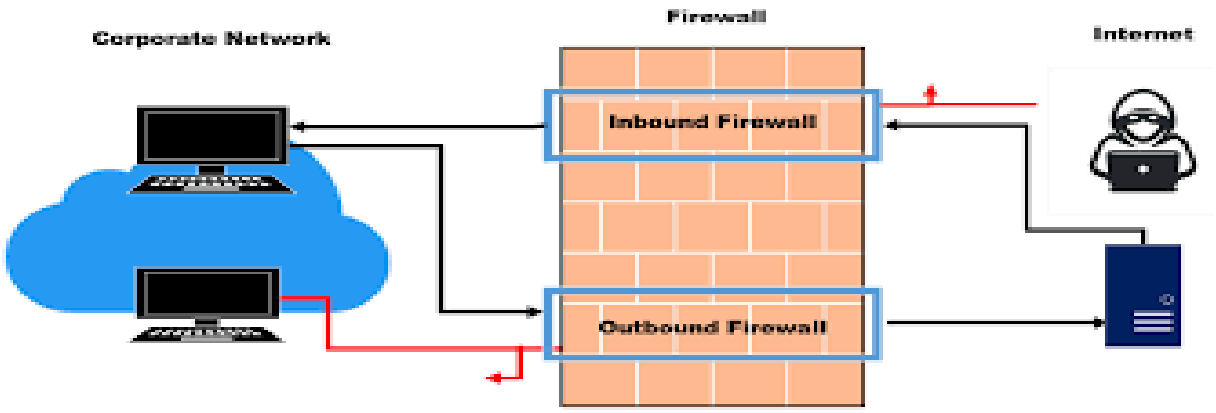
- Process where a device on a network initiates requests to access websites or web-based resources on the internet.
- Device sending requests to web servers and receiving responses
- HTTP Requests: For standard web pages (port 80).
- HTTPS Requests: For secure web pages (port 443).

Co-funded by the European Union

1.12 Firewall Rules to Allow Outbound Web Browsing

- Firewall Rules to Allow Outbound Web Browsing

  Need to configure firewall to permit traffic leaving the network to access the internet over specific ports used for web traffic.



Co-funded by the European Union

cont…

- **Outbound Traffic:**
- Requests that originate from within the internal network to external web servers.

- **Inbound Traffic:**
- Responses from external servers to the internal network
- replies to the initial outbound requests.

Co-funded by
the European Union

Allowing HTTP Traffic (port 80)

- **Outbound Rule:**Allows outgoing traffic using the TCP protocol to port 80, the standard port for unencrypted web traffic (HTTP).
- **Inbound Rule:**Allows the firewall to accept traffic from port 80 on the server side, but only if the connection is ESTABLISHED.
- Incoming traffic must be part of an existing session initiated by the internal client
- Prevents unsolicited inbound traffic from being

```
# Outbound HTTP rule
iptables -A OUTPUT -p tcp --dport 80 -m state --state NEW,ESTABLISHED -j ACCEPT

# Inbound HTTP rule (response)
iptables -A INPUT -p tcp --sport 80 -m state --state ESTABLISHED -j ACCEPT
```

Co-funded by
the European Union

1.13 Firewall Rules to Allow Telnet and Other TCP Services

- Need to create rules that permit traffic on the specific ports used by these services.

- **Understanding Telnet and TCP Services**

  Telnet: Protocol used to remotely access and manage devices over a network.

  operates on TCP port **23**.

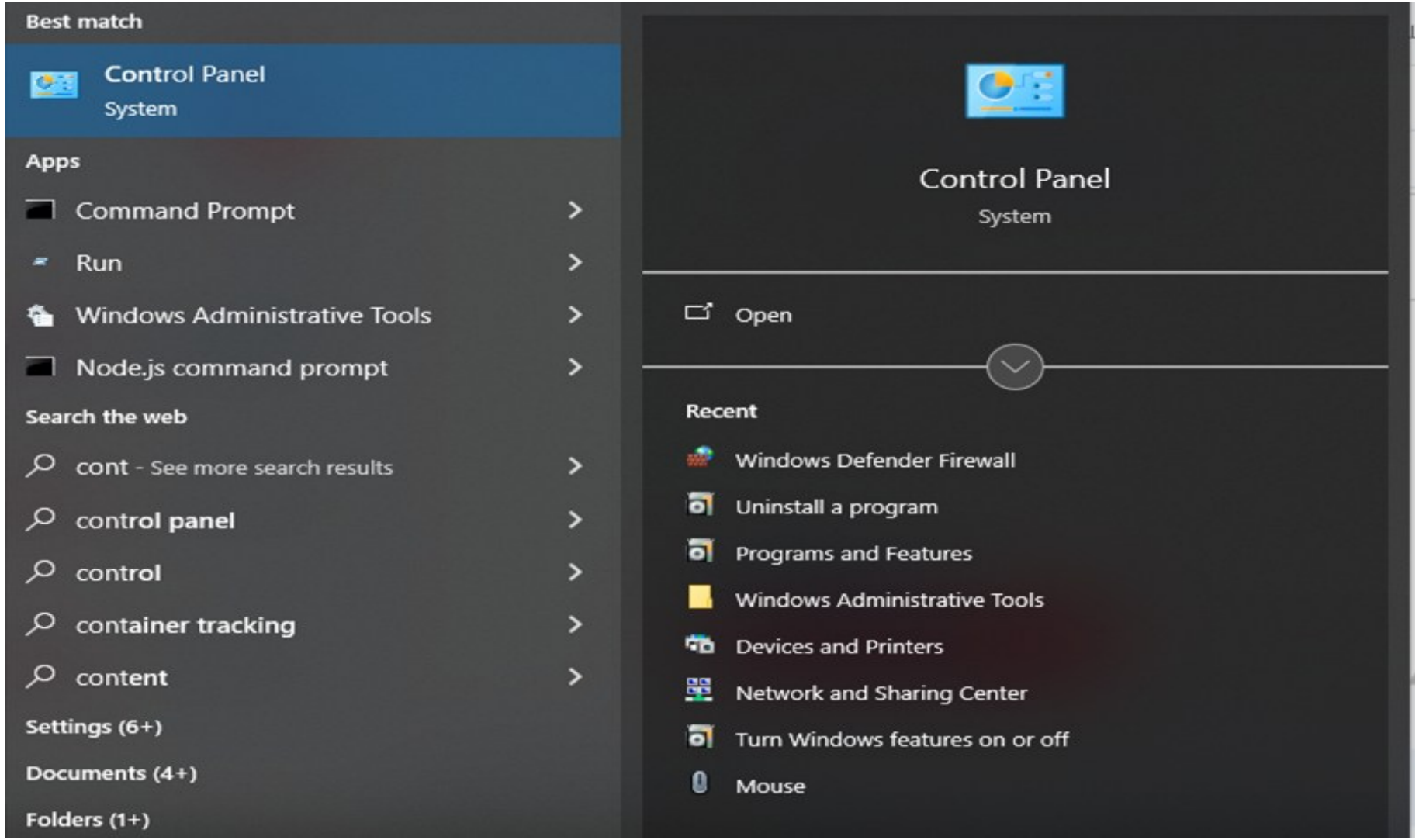
- **Other TCP Services**: Other services might use various TCP ports
- Need to create rules for each specific port or range of ports as required.

Co-funded by the European Union

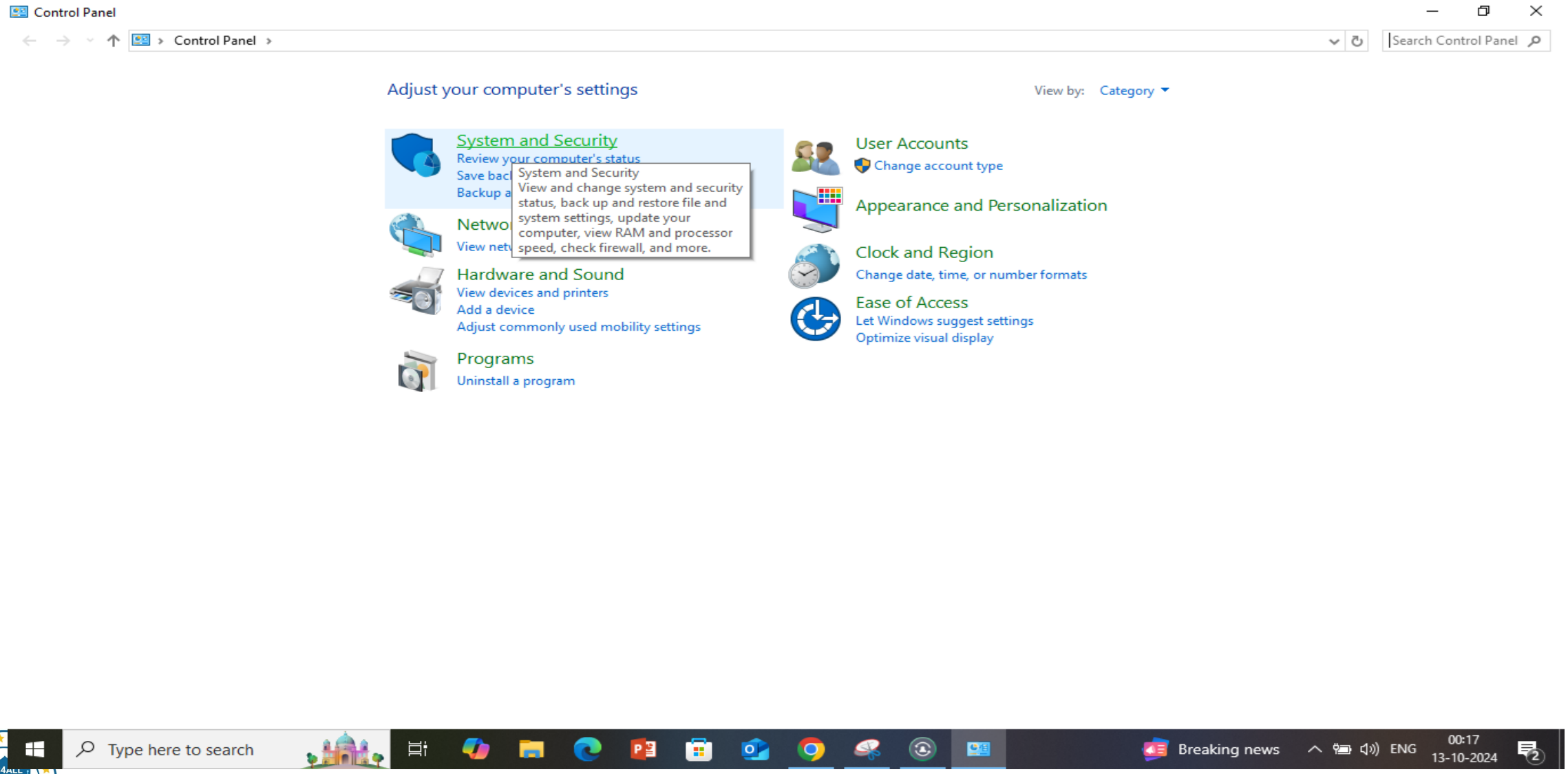
1.13 Firewall Rules to Allow Telnet and Other TCP Services

- Firewall Rules Configuration For Windows Firewall (Software Firewall)
- Open Windows Firewall:
- Navigate to Control Panel > System and Security > Windows Defender Firewall.
- Click on Advanced settings to open the Windows Firewall with Advanced Security window.

Co-funded by the European Union



Co-funded by
the European Union



Co-funded by
the European Union

System and Security

Control Panel › System and Security

- Control Panel Home
- **System and Security**
- Network and Internet
- Hardware and Sound
- Programs
- User Accounts
- Appearance and Personalization
- Clock and Region
- Ease of Access

Security and Maintenance
Review your computer's status and resolve issues | Change User Account Control settings |
Troubleshoot common computer problems

Windows Defender Firewall
Check firewall status | Allow an app through Windows Firewall

Windows Defender Firewall
Set firewall security options to help protect your computer from hackers and malicious software.

System
View amount of R emote access | Launch remote assistance |
See the name of th

Power Options
Change battery settings | Change what the power buttons do | Change when the computer sleeps

File History
Save backup copies of your files with File History | Restore your files with File History

Backup and Restore (Windows 7)
Backup and Restore (Windows 7) | Restore files from backup

BitLocker Drive Encryption
Manage BitLocker

Storage Spaces
Manage Storage Spaces

Work Folders
Manage Work Folders

Administrative Tools
Free up disk space | Defragment and optimize your drives | Create and format hard disk partitions |
View event logs | Schedule tasks

Co-funded by the European Union

Windows Defender Firewall

Control Panel › System and Security › Windows Defender Firewall

Control Panel Home

Allow an app or feature through Windows Defender Firewall

Change notification settings

Turn Windows Defender Firewall on or off

Restore defaults

Advanced settings

Troubleshoot my network

Help protect your PC with Windows Defender Firewall

Windows Defender Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network.

Private networks — Not connected

Guest or public networks — Connected

Networks in public places such as airports or coffee shops

Windows Defender Firewall state:	On
Incoming connections:	Block all connections to apps that are not on the list of allowed apps
Active public networks:	Prathvik 2
Notification state:	Notify me when Windows Defender Firewall blocks a new app

Co-funded by the European Union

Windows Defender Firewall with Advanced Security

File Action View Help

Windows Defender Firewall witl
- Inbound Rules
- Outbound Rules
- Connection Security Rules
- Monitoring

Windows Defender Firewall with Advanced Security on Local Computer

Windows Defender Firewall with Advanced Security provides network security for Windows computers.

Overview

Domain Profile

- Windows Defender Firewall is on.
- Inbound connections that do not match a rule are blocked.
- Outbound connections that do not match a rule are allowed.

Private Profile

- Windows Defender Firewall is on.
- Inbound connections that do not match a rule are blocked.
- Outbound connections that do not match a rule are allowed.

Public Profile is Active

- Windows Defender Firewall is on.
- Inbound connections that do not match a rule are blocked.
- Outbound connections that do not match a rule are allowed.

Windows Defender Firewall Properties

Co-funded by
the European Union

Windows Defender Firewall with Advanced Security

File Action View Help

Windows Defender Firewall witl
- Inbound Rules
- Outbound Rules
- Connection Security Rules
- Monitoring

Inbound Rules

Name	Group	Profile	Enabled	Acti
Microsoft Lync UcMapi		Public	Yes	Allo
Microsoft Lync UcMapi		Public	Yes	Allo
Microsoft Office Outlook		Public	Yes	Allo
Net Protector Total Internet Security		Public	Yes	Allo
Net Protector Total Internet Security		Public	Yes	Allo
Net Protector Total Internet Security		Private	Yes	Allo
Net Protector Total Internet Security		Private	Yes	Allo
NPAV EmailScn		All	Yes	Allo
NPAV Remote		Public	Yes	Allo
NPAV Remote		Public	Yes	Allo
NPAV Remote		Private	Yes	Allo
NPAV Remote		Private	Yes	Allo
NPAV Vunerability Scanner		Private	Yes	Allo
NPAV Vunerability Scanner		Public	Yes	Allo
NPAV Vunerability Scanner		Public	Yes	Allo
NPAV Vunerability Scanner		Private	Yes	Allo
Port 3306		All	Yes	Allo
Port 33060		All	Yes	Allo
Search Update Server		Public	Yes	Allo
Search Update Server		Private	Yes	Allo

Actions

Inbound Rules
- New Rule...
- Filter by Profile
- Filter by State
- Filter by Group
- View
- Refresh
- Export List...
- Help

BLOCK IP ADDRESS - 101.99.91.210
- Disable Rule
- Cut
- Copy
- Delete
- Properties
- Help

Co-funded by
the European Union

Windows Defender Firewall with Advanced Security

File Action View Help

Windows Defender Firewall wit
- Inbound Rules
- Outbound Rules
- Connection Security Rules
- Monitoring

Outbound Rules

Name	Group	Profile	Enabled	Acti
BranchCache Hosted Cache Client (HTTP...	BranchCache - Hosted Cach...	All	No	Allo
BranchCache Hosted Cache Server(HTTP...	BranchCache - Hosted Cach...	All	No	Allo
BranchCache Peer Discovery (WSD-Out)	BranchCache - Peer Discove...	All	No	Allo
Captive Portal Flow	Captive Portal Flow	All	Yes	Allo
Cast to Device functionality (qWave-TCP...	Cast to Device functionality	Private...	Yes	Allo
Cast to Device functionality (qWave-UDP...	Cast to Device functionality	Private...	Yes	Allo
Cast to Device streaming server (RTP-Stre...	Cast to Device functionality	Public	Yes	Allo
Cast to Device streaming server (RTP-Stre...	Cast to Device functionality	Private	Yes	Allo
Cast to Device streaming server (RTP-Stre...	Cast to Device functionality	Domain	Yes	Allo
Cloud Identity (TCP-Out)	Cloud Identity	All	Yes	Allo
Connected Devices Platform - Wi-Fi Dire...	Connected Devices Platform	Public	Yes	Allo
Connected Devices Platform (TCP-Out)	Connected Devices Platform	Domai...	Yes	Allo
Connected Devices Platform (UDP-Out)	Connected Devices Platform	Domai...	Yes	Allo
Core Networking - DNS (UDP-Out)	Core Networking	All	Yes	Allo
Core Networking - Dynamic Host Config...	Core Networking	All	Yes	Allo
Core Networking - Dynamic Host Config...	Core Networking	All	Yes	Allo
Core Networking - Group Policy (LSASS-...	Core Networking	Domain	Yes	Allo
Core Networking - Group Policy (NP-Out)	Core Networking	Domain	Yes	Allo
Core Networking - Group Policy (TCP-Out)	Core Networking	Domain	Yes	Allo
Core Networking - Internet Group Mana...	Core Networking	All	Yes	Allo
Core Networking - IPHTTPS (TCP-Out)	Core Networking	All	Yes	Allo
Core Networking - IPv6 (IPv6-Out)	Core Networking	All	Yes	Allo
Core Networking - Multicast Listener Do...	Core Networking	All	Yes	Allo
Core Networking - Multicast Listener Qu...	Core Networking	All	Yes	Allo
Core Networking - Multicast Listener Rep...	Core Networking	All	Yes	Allo
Core Networking - Multicast Listener Rep...	Core Networking	All	Yes	Allo
Core Networking - Neighbor Discovery A...	Core Networking	All	Yes	Allo
Core Networking - Neighbor Discovery S...	Core Networking	All	Yes	Allo
Core Networking - Packet Too Big (ICMP...	Core Networking	All	Yes	Allo

Actions

Outbound Rules
- New Rule...
- Filter by Profile
- Filter by State
- Filter by Group
- View
- Refresh
- Export List...
- Help

Co-funded by the European Union

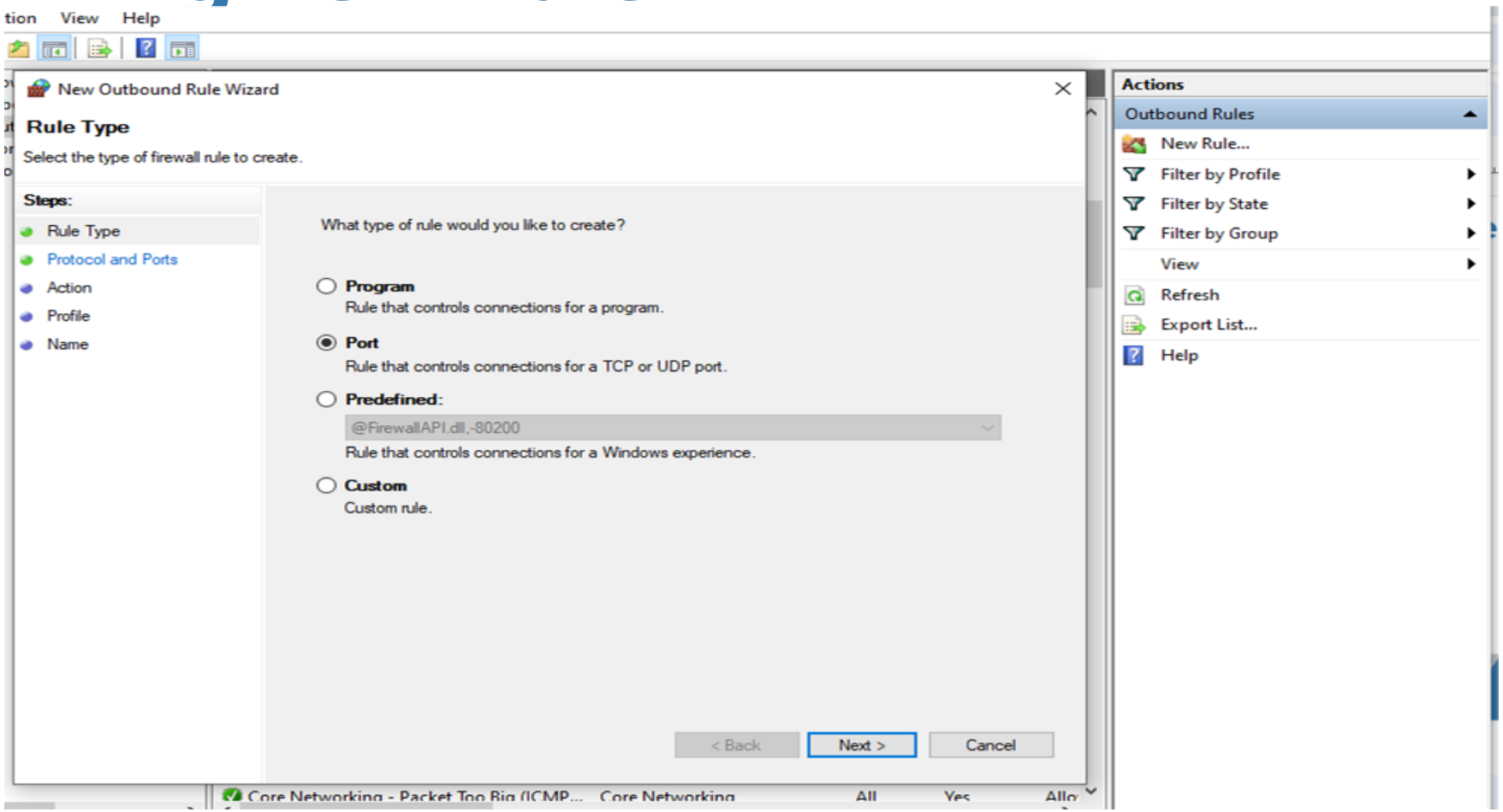
1.13 Firewall Rules to Allow Telnet and Other TCP Services

- **Create Outbound Rule**:
- Click on Outbound Rules in the left pane.
- Click on New Rule… in the right pane.

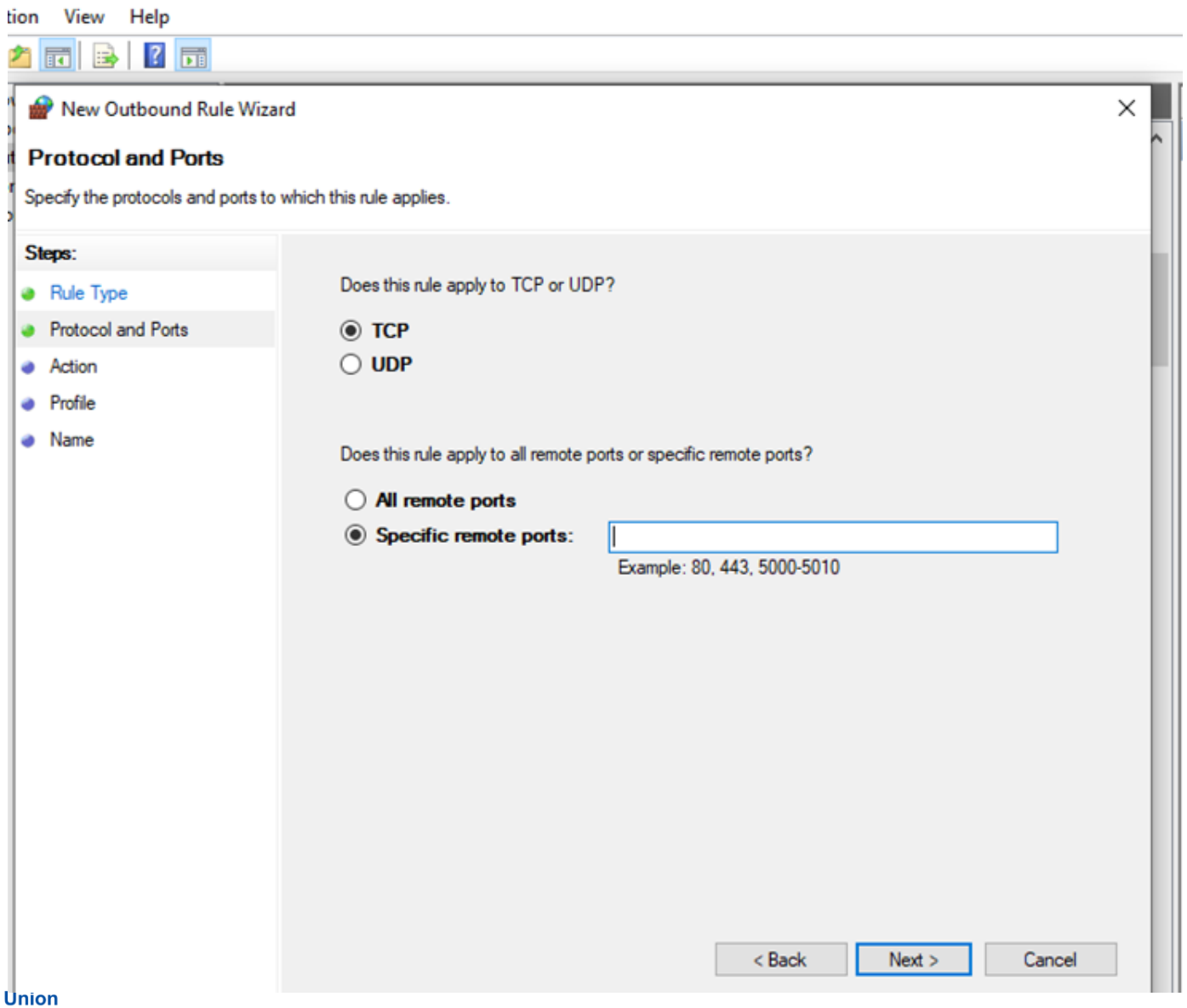
- **Define Rule Type**:
- **Select Port** and click Next.

Co-funded by
the European Union

Defining new Rule



Co-funded by
the European Union



Co-funded by
the European Union

1.13 Firewall Rules to Allow Telnet and Other TCP Services

- **Specify Protocol and Ports**:
- **Choose TCP** as the protocol.
- **Specific local ports**: Enter the port number 23 for Telnet, or other specific TCP ports as needed.
- Need to specify multiple ports or a range, use commas (e.g., 23, 22 for Telnet and SSH) or specify a range (e.g., 1000-2000).

Co-funded by the European Union

1.13 Firewall Rules to Allow Telnet and Other TCP Services

- **Allow the Connection**:
- **Choose Allow the connection** and click Next.
- **Select Profiles**:
  - Choose the network profiles where this rule applies (Domain, Private, Public) and click Next.
- **Name the Rule**:
  - Enter a name like "Allow Telnet" or "Allow TCP Services" and click Finish.
- **Create Additional Rules**:
  - Repeat the process to create additional rules for other TCP services by specifying different ports as required.

Co-funded by the European Union

File Action View Help

New Outbound Rule Wizard

Action

Specify the action to be taken when a connection matches the conditions specified in the rule.

Steps:

- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

What action should be taken when a connection matches the specified conditions?

- (●) **Allow the connection**
  This includes connections that are protected with IPsec as well as those are not.
- ( ) **Allow the connection if it is secure**
  This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.
  Customize...
- ( ) **Block the connection**

< Back | Next > | Cancel

Actions

Outbound Rules

- New Rule...
- Filter by Profile
- Filter by State
- Filter by Group
- View
- Refresh
- Export List...
- Help

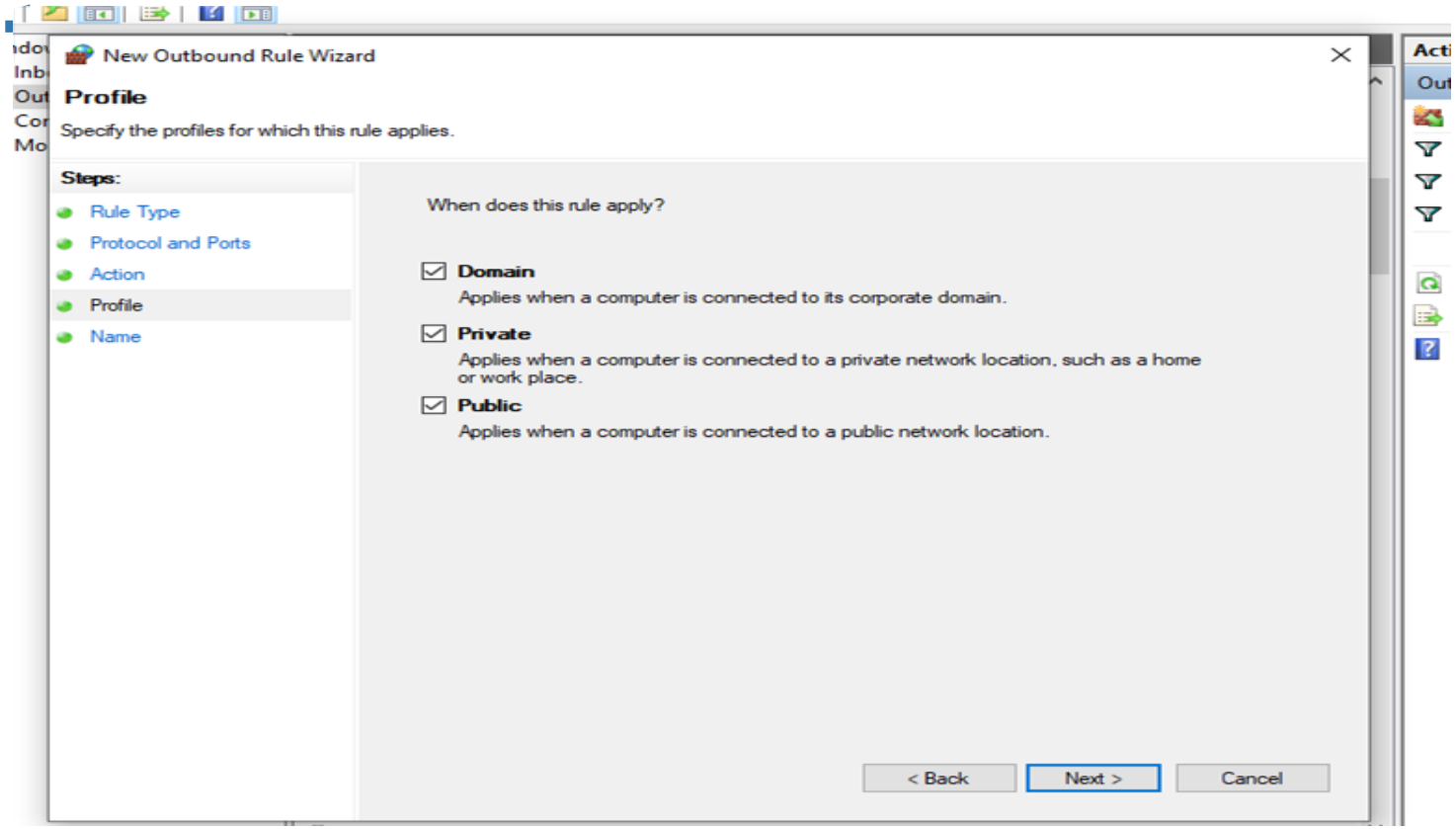
125

126

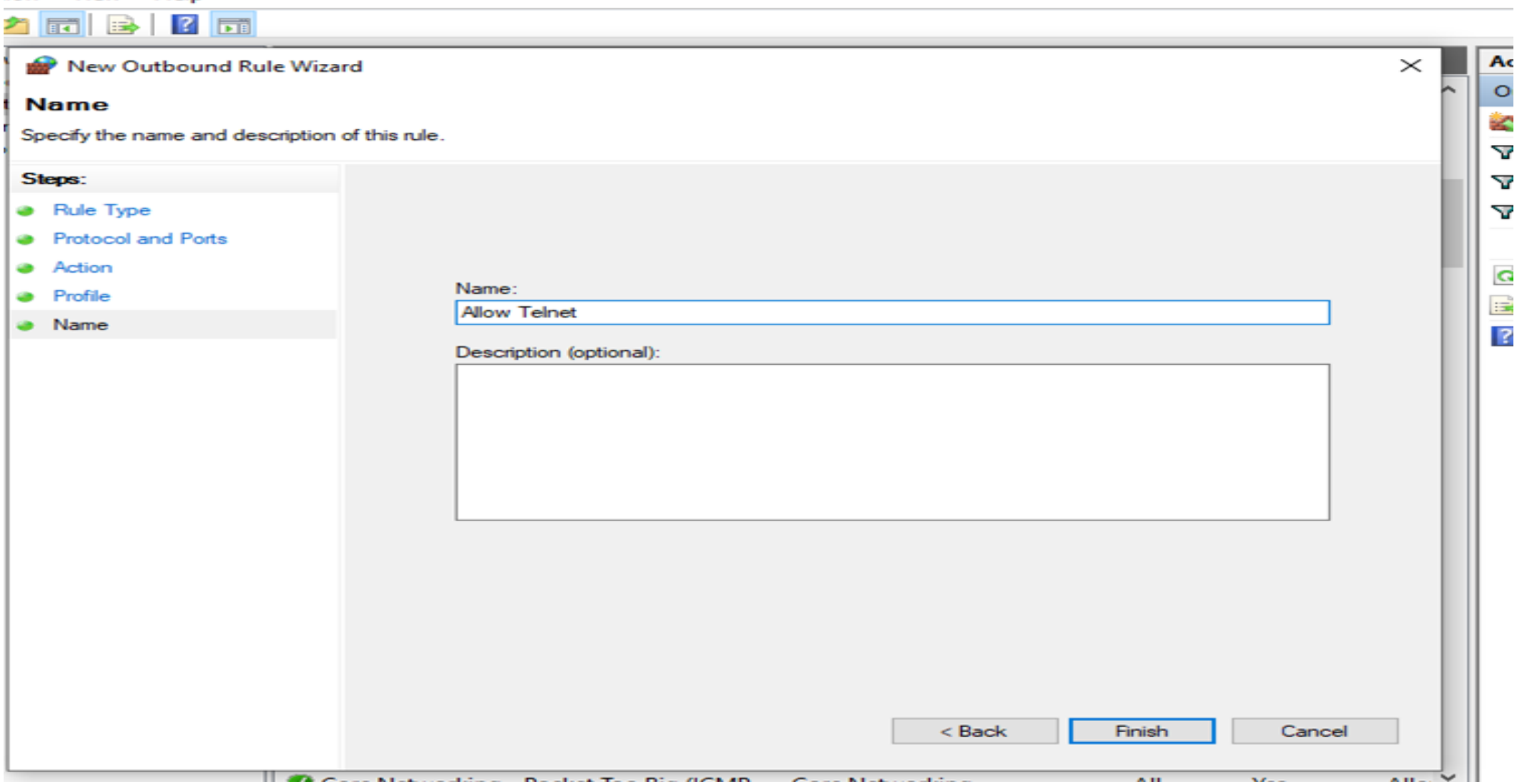
127

128

Domain To be selected as public and priva



Co-funded by
the European Union



Co-funded by
the European Union

1.14 Establishing Corporate Policy Rules

- Involves creating guidelines for how employees should use company resources and handle various situations

- **Steps to Establish Corporate Policy Rules**
- **Set Goals:**
- **Why:** Decide what you want to achieve with the policies.

Co-funded by the European Union

1.14 Establishing Corporate Policy Rules

Create Policy Categories:

Types: Think about different areas where rules are needed, like:

Security: How to protect company data.

Internet Use: What’s okay and not okay to do online using company resources.

Compliance: Following legal and industry regulations.

Operations: Daily tasks and handling of equipment.

Co-funded by the European Union

1.14 Establishing Corporate Policy Rules

Write the Rules:

What: rules are clear and easy to understand. Include:

Purpose: Why the rule exists.

Scope: Who it applies to (e.g., all employees).

Specific Rules: What exactly is allowed or not allowed.

Responsibilities: What employees need to do to follow the rules.

Consequences: What happens if someone doesn't follow the rules

Co-funded by the European Union

1.14 Establishing Corporate Policy Rules

- **Review and Approve:**
  - **Check**: Have the rules reviewed by key people in the company, like managers or the legal team.
  - **Approval**: Get the final okay from top management.
- **Communicate:**
  - **Inform**: Share the rules with everyone in the company. Provide training if needed so everyone understands the new rules.

Co-funded by the European Union

1.14 Establishing Corporate Policy Rules

- **Put into Practice:**
  - **Implement**: Set up any tools or processes needed to enforce the rules (e.g., security software).
- **Monitor and Enforce:**
  - **Check**: Regularly check to make sure everyone is following the rules.
  - **Act**: Take action if someone breaks the rules.
- **Update:**
  - **Revise**: Periodically review and update the rules to keep them relevant as things change in the company or industry.

Co-funded by the European Union

1.14 Establishing Corporate Policy Rule

Example

Internet Use Policy:

Purpose: To make sure employees use the internet responsibly.

Rules:

- Only use company devices for work-related activities.
- Don’t visit inappropriate or illegal websites.
- Personal use of the internet should be limited and not interfere with work.

Co-funded by the European Union

1.14 Establishing Corporate Policy Rule

Responsibilities: Employees must follow these rules and report any issues

Co-funded by the European Union

1.15 Firewall Rules for FTP

- Involves configuring firewall to allow or block FTP traffic.
- FTP uses specific ports to transfer files between a client and a server
- configuring these rules ensures that legitimate FTP traffic can pass through while keeping the network secure.
- **Understanding FTP and Ports**
- **FTP Protocol:**
- Control Connection: Uses TCP port 21 for commands and responses between the client and server
- Data Connection: Uses TCP ports 20 for active mode data transfers, or a range of ports in passive mode.

Co-funded by
the European Union

cont…

Modes of FTP:

Active Mode: The client opens a random port for data transfer, and the server connects back to this port.

Passive Mode: The server opens a random port and the client connects to this port for data transfer.

Co-funded by
the European Union

1.15 Firewall Rules for FTP

- **Firewall Rules for FTP- Windows Firewall**
- Open Windows Firewall:
- Go to Control Panel > System and Security > Windows Defender Firewall.
- Click on Advanced settings to open the Windows Firewall with Advanced Security window.
- Create New Inbound Rule:
- Click on Inbound Rules in the left pane.
- Click on New Rule… in the right pane.

Co-funded by the European Union

1.15 Firewall Rules for FTP

- **Define Rule Type:**
- Select Port and click Next.
- Specify Protocol and Ports:
- Protocol: Choose TCP.
- Specific local ports: Enter 21 for the FTP control connection.
- To allow passive FTP mode, you may need to open a range of ports. For example, if passive mode uses ports 50000-51000, specify this range.

Co-funded by
the European Union

1.15 Firewall Rules for FTP

- **Allow the Connection:**
- Choose Allow the connection and click Next.
- Select Profiles:
- Choose the network profiles where this rule applies (Domain, Private, Public) and click Next.
- **Name the Rule:**
- Enter a name like "Allow FTP" and click Finish.
- **Create Additional Rules:**
- Repeat the steps to create inbound rules for passive FTP port ranges if needed.

Co-funded by the European Union

1.16 Application Proxy Filtering

- Technique used in network security to control and monitor application-level traffic.
- Involves using a proxy server to inspect, filter, and manage data exchanged between users and web applications
- **What is Application Proxy Filtering?**
- involves placing a proxy server between users and the internet to:
- **Inspect Traffic**: Examine the data being sent and received
- **Filter Content:** Block or allow access to specific applications or types of content
- **Manage Applications:** Control which applications can be used and how they are accessed.

Co-funded by
the European Union

1.16 Application Proxy Filtering

- **How It Works**
- **Proxy Server:** Acts as an intermediary between a client (like a web browser) and the internet.
- All requests from the client go through the proxy server.
- **Traffic Inspection:** The proxy server inspects and understands the types of applications or content being accessed.

Co-funded by the European Union

1.16 Application Proxy Filtering

- **Filtering Rules:** Proxy server decides whether to allow or block certain requests or data.
- These rules can be set based on:
- Application Type:
- Content Type:
- User:
- **Forwarding or Blocking:** If a request is allowed, the proxy server forwards it to the intended destination.
- If blocked, the proxy server prevents the request from reaching the internet.

Co-funded by the European Union

Benefits of Application Proxy Filtering

Enhanced Security:

Threat Protection

Data Loss Prevention

Access Control:

Application Management:

Bandwidth Management:

Compliance:

Regulatory Adherence:

Monitoring and Reporting:

Usage Tracking:

Co-funded by the European Union

Example Use Cases

- **Corporate Environment:**
  - Block access to social media sites during work hours while allowing access to business-related applications.
- **Educational Institutions:**
  - filter out inappropriate content and limit access to entertainment sites
- **Public Wi-Fi:**
  - block access to potentially harmful sites and manage network performance.

Co-funded by
the European Union

1.17 Forward and Reverse Proxies

- **<u>Forward Proxy</u>**
- Acts as an intermediary between a client (like a web browser) and the internet.
- **How It Works:**
- **Client Request:** goes to the forward proxy server first.
- **Proxy Handling:** forward proxy server forwards the request to the target server (e.g., the website).
- **Response Handling:** The target server sends the response back to the forward proxy.
- **Client Response:** The forward proxy then sends the response back to the client.

Co-funded by the European Union

Key Features:

- **Anonymity:** Hides the client's IP address from the destination server.
- **Content Filtering:** Can block access to specific sites or content.
- **Caching:** Stores frequently accessed content to speed up future requests.
- **Access Control:** Restricts access to certain websites or applications.

Co-funded by
the European Union

Reverse Proxy

- intermediary between the internet and a server or servers within a network.
- **How It Works:**
- Client Request: goes to the reverse proxy server.
- **Proxy Handling:** forwards the request to the appropriate server within the internal network.
- **Response Handling:** The server sends the response back to the reverse proxy.
- **Client Response:** The reverse proxy then forwards the response to the client.

Co-funded by
the European Union

Key Features

- **Load Balancing:** Distributes incoming traffic across multiple servers
- **Security:** Hides the internal server architecture from the outside world
  Caching: Stores frequently accessed content to reduce load on internal servers and speed up response times.
- **Compression:** Compresses outbound data to save bandwidth and speed up transmission.

Co-funded by
the European Union

Example Use Cases:

- Web Hosting:
- Content Delivery Networks (CDNs)

Co-funded by
the European Union

Understanding Forward and Reverse Proxies

- **<u>Forward Proxy</u>**:
- **Client-side**: Used by clients to access the internet.
- **Features**: Anonymity, content filtering, caching, access control.
- **Example**: Company employees accessing external websites through a corporate proxy server.

- **<u>Reverse Proxy</u>**:
- **Server-side**: Used by servers to manage incoming requests from the internet.
- **Features**: Load balancing, security, caching, compression.
- **Example**: A website using a reverse proxy to balance traffic across multiple web servers and enhance security.

Co-funded by the European Union

Learning Outcome

- Students will be able to explain the concept of STO and how it adds a layer of protection by hiding system details to prevent unauthorized access and exploitation.
- Students will learn how the TCP/IP model underpins modern networking, enabling reliable data exchange across diverse networks.
- Students will develop the ability to use packet sniffing as a network analysis tool, capturing and examining data packets to monitor and troubleshoot network traffic.
- Students will be able to describe the critical function of firewalls as a security mechanism that blocks unauthorized access and safeguards sensitive data.
- Students will understand how application proxy filtering works and be able to configure a proxy server to control access to applications and

Question no 01

What is the primary function of a firewall?

A) To encrypt data

B) To monitor and control network traffic

C) To provide antivirus protection

D) To optimize network speed

Co-funded by
the European Union

Question no 02

Which type of firewall is designed to protect individual devices like computers or servers?

A) Network Firewall

B) Host-Based Firewall

C) Proxy Firewall

D) Cloud Firewall

Co-funded by the European Union

Question no 03

Which of the following is a common method firewalls use to filter traffic?

A) Content delivery

B) Port blocking

C) Traffic doubling

D) IP hiding

Co-funded by the European Union

Question no 04

What role does a firewall play in a corporate network?

A) Acts as the main server

B) Encrypts all internal data

C) Filters incoming and outgoing traffic based on security rules

D) Provides a backup of all corporate data

Co-funded by the European Union

Question no 05

A firewall that acts as an intermediary between the internal network and the internet is called a:

A) Stateful Inspection Firewall

B) Host-Based Firewall

C) Proxy Firewall

D) Unified Threat Management (UTM) Firewall

Co-funded by the European Union

Question no 06

What is the primary function of a SYN packet in TCP communication?

A) To terminate a connection

B) To initiate a connection

C) To acknowledge data transfer

D) To encrypt data

Co-funded by the European Union

Question no 07

In the TCP three-way handshake, what is the correct sequence of packets exchanged between a client and server?

A) SYN, ACK, SYN-ACK

B) SYN, SYN-ACK, ACK

C) ACK, SYN, SYN-ACK

D) SYN-ACK, SYN, ACK

Co-funded by the European Union

Question no 08

Which network security measure is commonly used to protect against SYN flood attacks?

A) Rate Limiting

B) Encryption

C) VPNs

D) Port Scanning

Co-funded by the European Union

Question no 09

What protocol does Telnet use, which can be managed by firewall rules?

A) HTTP

B) FTP

C) TCP

D) DNS

Co-funded by
the European Union

Question no 10

What is the function of an application proxy in firewall rules?

A) Directly connects users to external servers

B) Filters and controls application-level traffic

C) Allows unrestricted access to all apps

D) Monitors DNS queries

Co-funded by the European Union

Question no 11

What is the primary function of a reverse proxy in network security?

A) Allowing outbound web traffic

B) Filtering internal traffic to external websites

C) Providing resources from internal servers to external users

D) Blocking incoming traffic from external servers

Co-funded by the European Union

Question no 12

What does "outbound web browsing" involve?

A) Accessing local network resources

B) Sending requests to and receiving responses from web servers on the internet

C) Blocking incoming traffic from external sources

D) Encrypting data stored on the device

Co-funded by the European Union

Question no 13

What is the primary function of a forward proxy?

A) To balance the load between multiple servers

B) To hide the internal server architecture from external clients

C) To act as an intermediary between a client and the internet

D) To cache frequently accessed content on the server

Co-funded by the European Union

Answers

1. B) To monitor and control network traffic
2. B) Host-Based Firewall
3. B) Port blocking
4. C) Filters incoming and outgoing traffic based on security rules
5. C) Proxy Firewall
6. B) To initiate a connection
7. B) SYN, SYN-ACK, ACK
8. A) Rate Limiting
9. C) TCP
10. B) Filters and controls application-level traffic
11. C) Providing resources from internal servers to external users
12. C) Blocking incoming traffic from external sources
13. C) To act as an intermediary between a client and the internet

Co-funded by
the European Union

Resources

List the resources you used for your research:

1. https://www.geeksforgeeks.org/what-is-packet-sniffing/
2. https://www.geeksforgeeks.org/types-of-network-firewall/
3. https://www.youtube.com/watch?v=2QGgEk20RXM
4. https://www.youtube.com/watch?v=5oioSbgBQ8I
5. https://www.youtube.com/watch?v=kDEX1HXybrU
6. https://www.youtube.com/watch?v=aUPoA3MSajU&t=138s

Co-funded by
the European Union

Resources

1. https://www.google.com/url?sa=i&url=https%3A%2F%2Fcybertalents.com%2Fblog%2Fsecurity-through-obscurity&psig=AOvVaw1jVkQmJhVaeWZG-m8Xeh07&ust=1728465846637000&source=images&cd=vfe&opi=89978449&ved=0CBQQjRxqFwoTCOi3vKa7_ogDFQAAAAAdAAAAABAE

1. https://www.google.com/imgres?q=Security%20Through%20Obscurity%20Criticism&imgurl=https%3A%2F%2Fupload.wikimedia.org%2Fwikipedia%2Fcommons%2Fthumb%2Ff%2Ff1%2FSecurity_through_obscurity_hiding_a_key_on_a_car_tyre.jpg%2F800px-Security_through_obscurity_hiding_a_key_on_a_car_tyre.jpg&imgrefurl=https%3A%2F%2Fen.wikipedia.org%2Fwiki%2FSecurity_through_obscurity&docid=CsRzfeqZEweBJM&tbnid=ZumjYCP63Ss6WM&vet=12ahUKEwiRlvPSu_6IAxUc1jgGHfBHBRIQM3oECE4QAA..i&w=800&h=951&hcb=2&ved=2ahUKEwiRlvPSu_6IAxUc1jgGHfBHBRIQM3oECE4QAA

Co-funded by the European Union

Resources

1. https://www.google.com/url?sa=i&url=https%3A%2F%2Fwww.appsealing.com%2Fcode-obfuscation%2F&psig=AOvVaw2mef8h3lXVMbDMmfkTvYu1&ust=1728466767080000&source=images&cd=vfe&opi=89978449&ved=0CBQQjRxqFwoTCKC0qdC-_ogDFQAAAAAdAAAAABAP

1. https://www.google.com/url?sa=i&url=https%3A%2F%2Fwww.firewall.cx%2Ftools-tips-reviews%2Fnetwork-protocol-analyzers%2Fperforming-tcp-syn-flood-attack-and-detecting-it-with-wireshark.html&psig=AOvVaw1j3b6XktUwjCSNEpE4_3Pc&ust=1728489944114000&source=images&cd=vfe&opi=89978449&ved=0CBQQjRxqFwoTCMjr0JCV_4gDFQAAAAAdAAAAABAK

Co-funded by the European Union

Resources

1. https://www.google.com/imgres?q=WireShark&imgurl=https%3A%2F%2Fmiro.medium.com%2Fv2%2Fresize%3Afit%3A990%2F1*nWfidPwQZkK0sRWJS8UeSQ.png&imgrefurl=https%3A%2F%2Fsecuritywithblue.medium.com%2Fhow-to-analyze-the-https-traffic-using-wireshark-fd3eb652ef89&docid=BqOsAdFMPV1HsM&tbnid=GwMhkDAcRKRPKM&vet=12ahUKEwjuoPOlv4OJAxUpzjgGHZvBENkQM3oECHkQAA..i&w=990&h=989&hcb=2&ved=2ahUKEwjuoPOlv4OJAxUpzjgGHZvBENkQM3oECHkQAA

1. https://www.google.com/url?sa=i&url=https%3A%2F%2Fin.norton.com%2Fblog%2Fprivacy%2Fwhat-is-packet-sniffing-and-ways-to-protect-against-sniffing&psig=AOvVaw2NFFZE52RmT0ug5NwKbdB9&ust=1728638880468000&source=images&cd=vfe&opi=89978449&ved=0CBQQjRxqFwoTCNiNpO6_g4kFQAAAAAdAAAAABAE

Co-funded by the European Union

Resources

1. https://www.google.com/url?sa=i&url=https%3A%2F%2Fnordvpn.com%2Fblog%2Fstoring-your-credit-card-details%2F&psig=AOvVaw0z1tU_drcH62Uinz2MWdVD&ust=1728639472215000&source=images&cd=vfe&opi=89978449&ved=0CBQQjRxqFwoTCJiH2rHCg4kDFQAAAAAdAAAAABAK

Co-funded by the European Union

Reference Book

- "Network Security: Private Communication in a Public World" by Charlie Kaufman, Radia Perlman, and Mike Speciner, 2nd Edition, Prentice Hall PTR Publication
- "Firewall Fundamentals" by Wes Noonan, Ido Dubrawsky, 1st Edition, Cisco Press (6/2/2006) publication
- "The Web Application Hacker's Handbook" by Dafydd Stuttard and Marcus Pinto,Wiley Publishing
- "Practical Packet Analysis: Using Wireshark to Solve Real-World Network Problems" by Chris Sanders, 2nd Edition, William Pollock.

Co-funded by
the European Union