



WIRESHARK

Res. Asst. Melek ŞENTÜRK





WHAT IS A DDOS ATTACK?



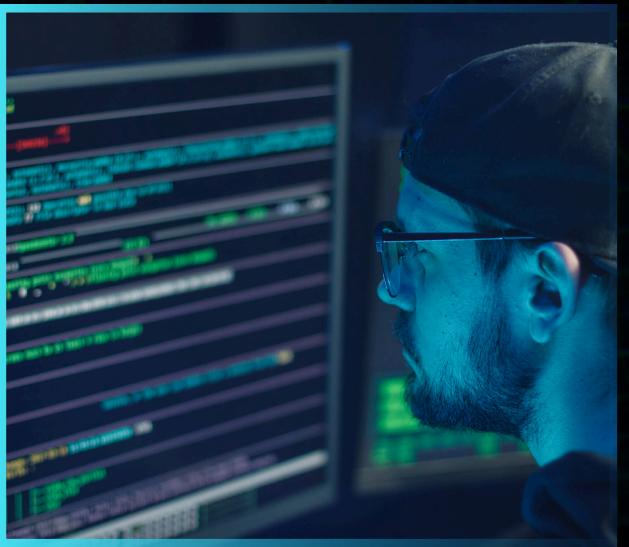
DDoS stands for Distributed Denial of Service attack.

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

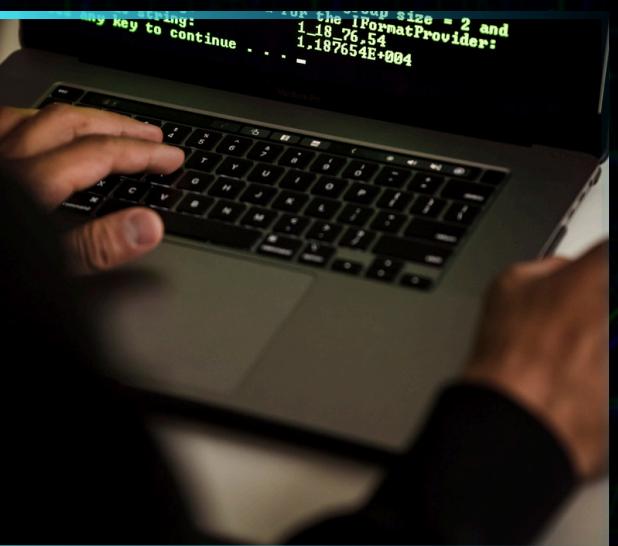




The purpose of a DDoS attack: To crash or make the target inaccessible.



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





HOW DOES IT 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 AGAINST 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 (WINDOWS SUBSYSTEM FOR LINUX)

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 INSTALLATION

Open PowerShell as Administrator:

```
Administrator: Windows PowerShell  
Windows PowerShell  
Copyright (C) Microsoft Corporation. All rights reserved.  
Try the new cross-platform PowerShell https://aka.ms/pscore6  
PS C:\WINDOWS\system32> wsl --install
```

Restart the computer after the process is complete.





APACHE WEB SERVER

On Ubuntu:

```
elek@DESKTOP-KN9BFE4: ~  
/home/elek/.hushlogin file.  
elek@DESKTOP-KN9BFE4:~$ sudo apt update  
[sudo] password for elek:  
Get:1 http://security.ubuntu.com/ubuntu noble-security InRelease  
Hit:2 http://archive.ubuntu.com/ubuntu noble InRelease  
Get:3 http://archive.ubuntu.com/ubuntu noble-updates InRelease
```

Then:

```
elek@DESKTOP-KN9BFE4:~$ sudo apt install apache2
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
```

```
elek@DESKTOP-KN9BFE4:~$ (sudo service apache2 start)
```





APACHE WEB SERVER

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

The screenshot shows a web browser window titled "localhost". The main content is the "Apache2 Default Page". It features the Ubuntu logo (a white circle with three dots) and the word "Ubuntu" in large black letters. To the right of "Ubuntu" is a red button with the white text "It works!". Below this, there is descriptive text about the default welcome page and configuration details. At the bottom, there is a section titled "Configuration Overview" with more information about the configuration files.

localhost

 **Apache2 Default Page**

Ubuntu **It works!**

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in `/usr/share/doc/apache2/README.Debian.gz`**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the apache2-doc package was installed on this server.

The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

`/etc/apache2/`





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.





WIRESHARK SIDE

tcp.flags.syn == 1 && tcp.flags.ack == 0

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	::1	::1	TCP	76	51998 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=6547
4	0.000236	::1	::1	TCP	76	51999 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=6547
15	9.956555	::1	::1	TCP	76	52000 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=6547
62	34.606807	::1	::1	TCP	76	52003 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=6547
119	121.039312	::1	::1	TCP	76	52016 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=6547
122	121.039591	::1	::1	TCP	76	52017 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=6547

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.

