Applied!

Data & Network Security

Behnam Amiri

ans.dailysec.ir

aNetSec.github.io

Spring 2025

Network Recap

IP Address

- unique identifier assigned to each device connected to a network
- Public IP Address
- assigned to a device that is directly connected to the internet.
- It is accessible from internet
  - like 8.8.8.8
- Private IP Address
- Used within a private network like home or university
- is not routable on the internet
  - Private IP Address like 192.168.0.2

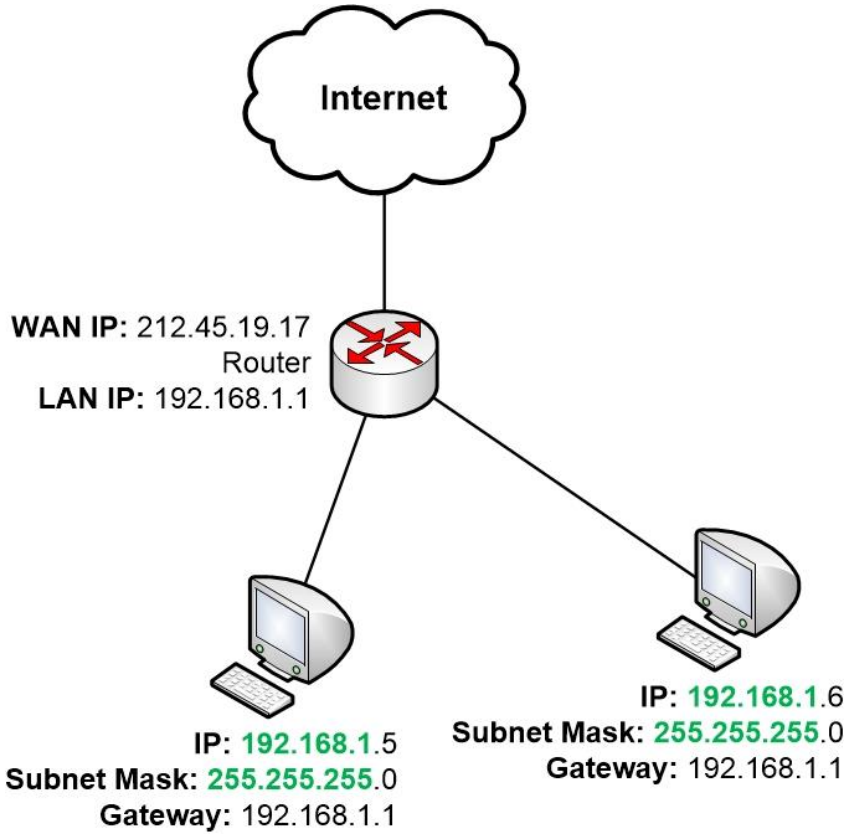
Subnet Mask

- Subnet mask help devices determine whether an IP address is on the same local network or if it needs to be routed to internet
  - Subnet Mask 255.255.255.0

Default Gateway

- Is a device on a network
- Used to send information to a device in another network or the internet

All in one

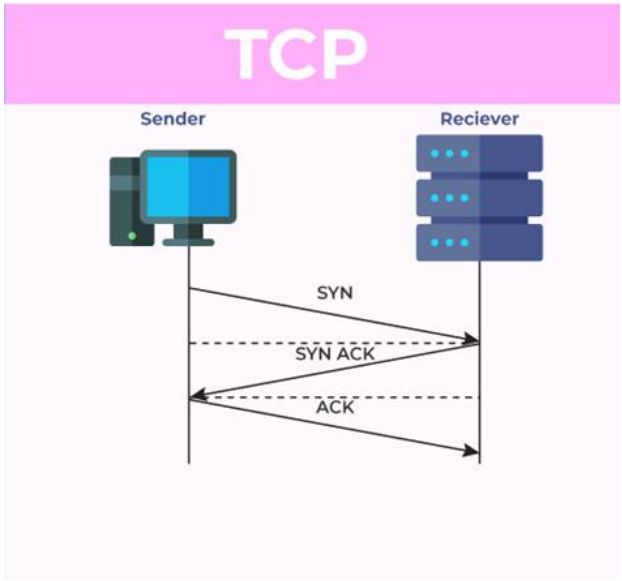

Internet
WAN IP: 212.45.19.17
Router
LAN IP: 192.168.1.1
IP: 192.168.1.5
Subnet Mask: 255.255.255.0
Gateway: 192.168.1.1
IP: 192.168.1.6
Subnet Mask: 255.255.255.0
Gateway: 192.168.1.1

MAC Address

- Physical Address or Network card address
- Example: 01-23-45-67-89-AB
- Usage in switching

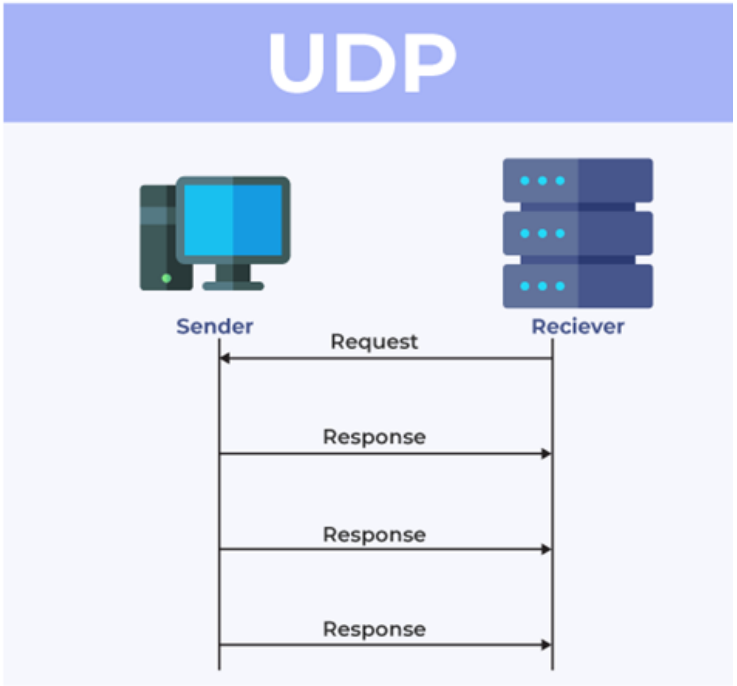
TCP Protocol

- Transmission Control Protocol (TCP)
- TCP is connection oriented
- Data delivery is guaranteed by ACK
- Use 3-Way Handshake



UDP

- User Datagram Protocol (UDP)
- UDP is connection less
- Data delivery is NOT guaranteed
- no Handshake
- Just send data



TCP vs UDP

	TCP	UDP
Protocol	connection-oriented	connection-less
Header Size	20 bytes	Static header 8 bytes
Overhead	Heavy as it needs 3 packets to setup a socket connection	Lightweight as no connections and message ordering tracking
Speed	Slower speed due to re-transmission and reordering	Faster as integrity is checked at the arrival time (via checksum)
Reliability	Guaranteed messages will be delivered in order and no errors	No guarantee that messages will be delivered in order and no errors
Connection	Connection is made before application messages are exchanged	Connection is not made before application messages are exchanged
Acknowledgment	Use handshake protocol (SYN,SYN-ACK,ACK)	No handshake
Error Checking	Performs error checking and resends erroneous packets	Performs basic error checking and discards erroneous packets (no error recovery attempt)
Use	Priority for more reliability and less speed	Priority for more speed and less reliability
Examples	FTP,SMTP,HTTP,TELNET	DNS,DHCP,RTP,TFTP,SNMP

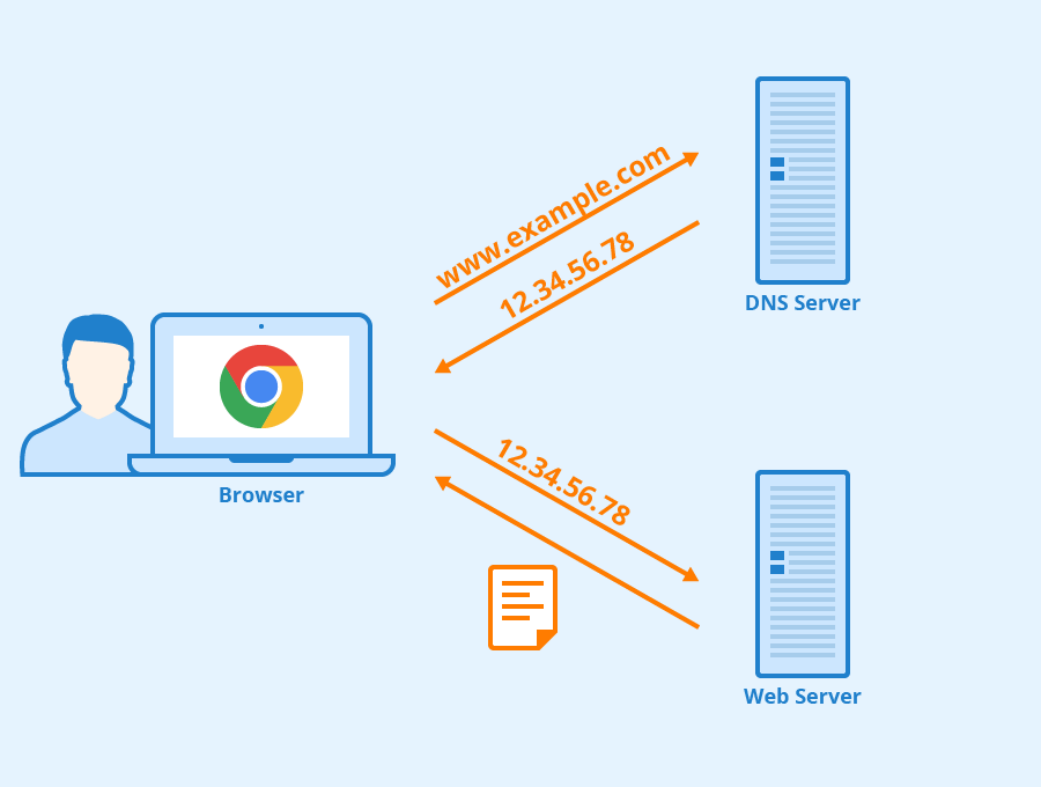
ICMP (Ping)

- Internet Control Message Protocol
- It helps diagnose problems in data transmission
- Utilized through tools like ping and traceroute

DNS

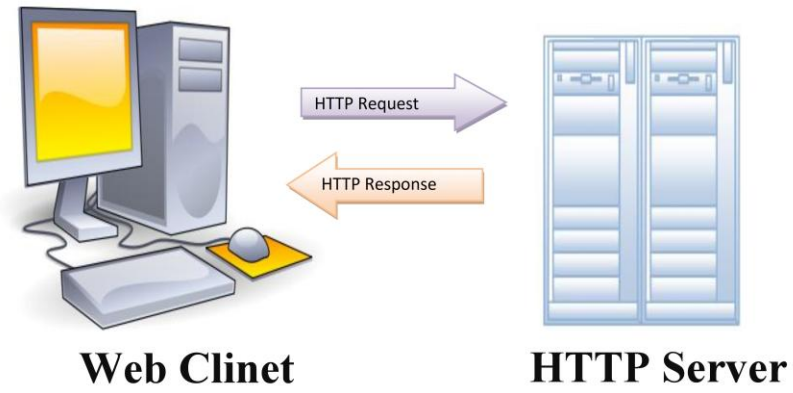
- Domain Name System protocol
- Translates human-readable domain names
- example www.google.com to IP addresses (like 8.7.2.1)
- Use Datagram Protocol (UDP)

DNS

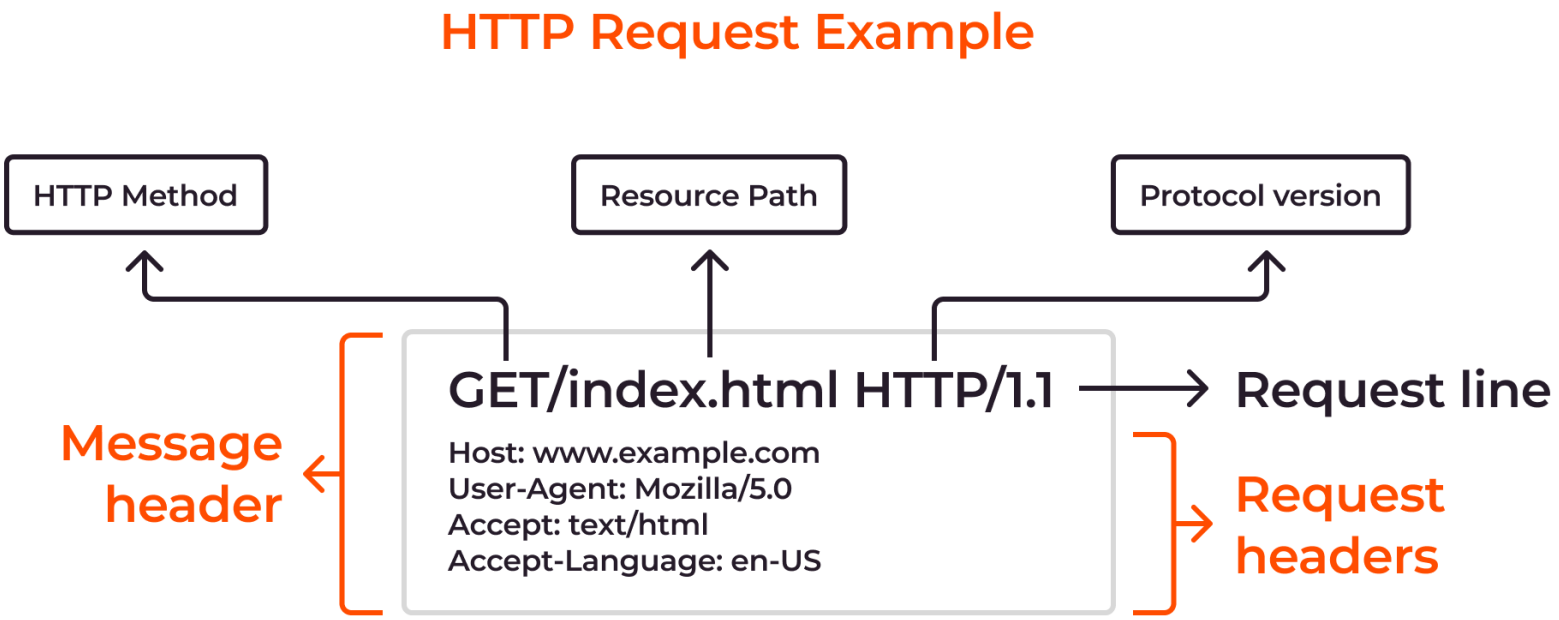

www.example.com
12.34.56.78
DNS Server
Browser
12.34.56.78
Web Server

HTTP

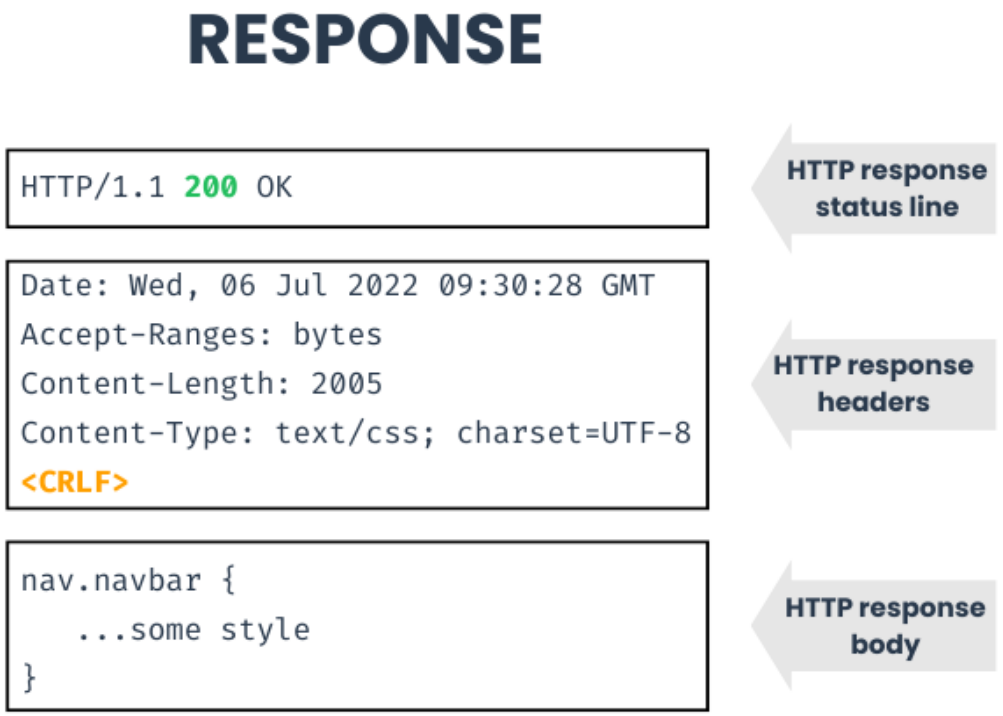
- Hypertext Transfer Protocol
- Used for data communication on the World Wide Web
- Allowing web browsers t
  web pages from servers.
- a request-response prot



HTTP Request



HTTP Response



Wireshark

- https://www.wireshark.org
- Free & open-source network protocol analyzer
- Capture and interactively browse the traffic running on a computer network

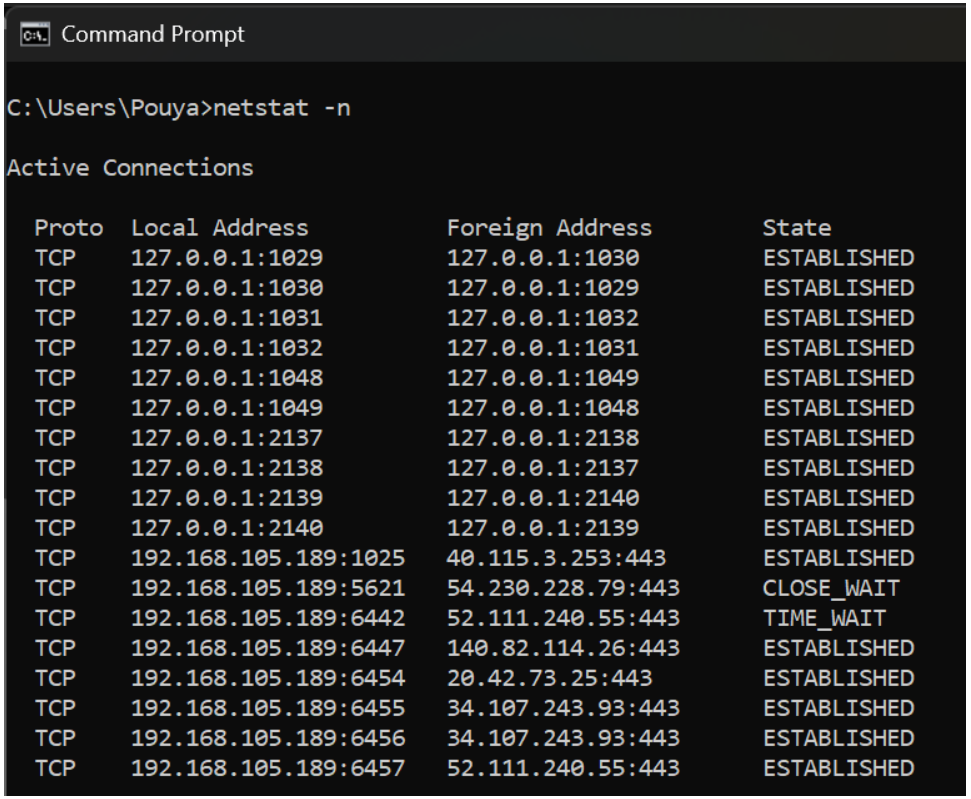
Port

- A port number is a number assigned to uniquely identify a connection endpoint and to direct data to a specific service.

Common Ports

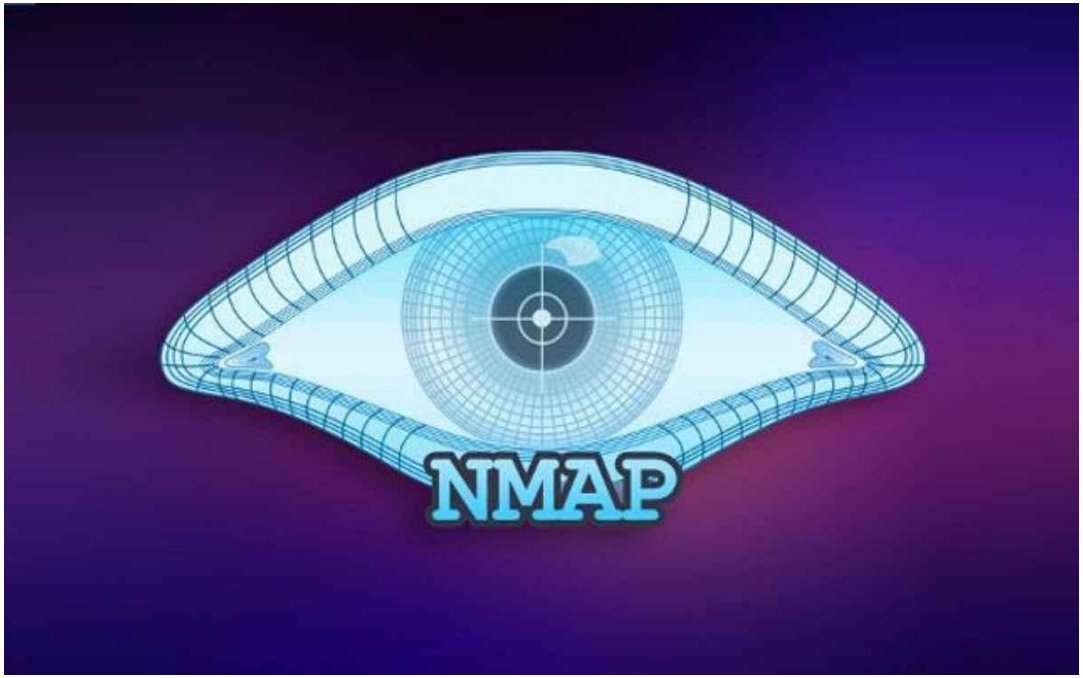
Port Number	Protocol	Usage
20	TCP	File Transfer Protocol (FTP) Data Transfer
21	TCP	FTP Command Control
22	TCP	Secure Shell (SSH)
23	TCP	Telnet - Remote login service, unencrypted text messages
25	TCP	Simple Mail Transfer Protocol (SMTP) E-mail Routing
53	TCP and UDP	Domain Name System (DNS)
67 and 68	UDP	Dynamic Host Configuration Protocol (DHCP)
69	UDP	Trivial File Transfer Protocol (TFTP)
80	TCP	Hypertext Transfer Protocol (HTTP)
110	TCP	Post Office Protocol (POP3) used by e-mail clients to retrieve e-mail from a server
119	TCP and UDP	Network News Transfer Protocol (NNTP)
123	UDP	Network Time Protocol (NTP)
137 and 138 and 139	TCP and UDP	NetBIOS
143	TCP	Internet Message Access Protocol (IMAP) Management of Digital Mail
161 and 162	TCP and UDP	Simple Network Management Protocol (SNMP)
194	TCP and UDP	Internet Relay Chat (IRC)
389	TCP and UDP	Lightweight Directory Access Protocol (LDAP)
443	TCP	HTTP Secure (HTTPS) HTTP over TLS/SSL
3389	TCP and UDP	Microsoft Terminal Server (RDP)

Netstat

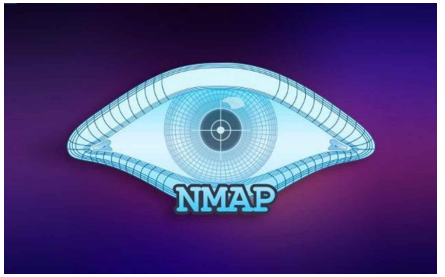

Command Prompt
C:\Users\Pouya>netstat -n
Active Connections
Proto Local Address Foreign Address State
TCP 127.0.0.1:1029 127.0.0.1:1030 ESTABLISHED
TCP 127.0.0.1:1030 127.0.0.1:1029 ESTABLISHED
TCP 127.0.0.1:1031 127.0.0.1:1032 ESTABLISHED
TCP 127.0.0.1:1032 127.0.0.1:1031 ESTABLISHED
TCP 127.0.0.1:1048 127.0.0.1:1049 ESTABLISHED
TCP 127.0.0.1:1049 127.0.0.1:1048 ESTABLISHED
TCP 127.0.0.1:2137 127.0.0.1:2138 ESTABLISHED
TCP 127.0.0.1:2138 127.0.0.1:2137 ESTABLISHED
TCP 127.0.0.1:2139 127.0.0.1:2140 ESTABLISHED
TCP 127.0.0.1:2140 127.0.0.1:2139 ESTABLISHED
TCP 192.168.105.189:1025 40.115.3.253:443 ESTABLISHED
TCP 192.168.105.189:5621 54.230.228.79:443 CLOSE_WAIT
TCP 192.168.105.189:6442 52.111.240.55:443 TIME_WAIT
TCP 192.168.105.189:6447 140.82.114.26:443 ESTABLISHED
TCP 192.168.105.189:6454 20.42.73.25:443 ESTABLISHED
TCP 192.168.105.189:6455 34.107.243.93:443 ESTABLISHED
TCP 192.168.105.189:6456 34.107.243.93:443 ESTABLISHED
TCP 192.168.105.189:6457 52.111.240.55:443 ESTABLISHED

Port Scan

- Find Open ports
- Find Services



Port Scan




```
┌──(kali㉿kali)-[~/Desktop]
└─$ nmap -v -sT 10.10.2.144
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-04 07:03 EDT
Initiating Ping Scan at 07:03
Scanning 10.10.2.144 [2 ports]
Completed Ping Scan at 07:03, 0.20s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 07:03
Completed Parallel DNS resolution of 1 host. at 07:03, 0.03s elapsed
Initiating Connect Scan at 07:03
Scanning 10.10.2.144 [1000 ports]
Discovered open port 21/tcp on 10.10.2.144
Discovered open port 53/tcp on 10.10.2.144
Discovered open port 80/tcp on 10.10.2.144
Discovered open port 3389/tcp on 10.10.2.144
Discovered open port 135/tcp on 10.10.2.144
Completed Connect Scan at 07:04, 11.39s elapsed (1000 total ports)
Nmap scan report for 10.10.2.144
Host is up (0.19s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT     STATE SERVICE
21/tcp   open  ftp
53/tcp   open  domain
80/tcp   open  http
135/tcp  open  msrpc
3389/tcp open  ms-wbt-server

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 11.74 seconds
```

Find Service Version

```
~/StationX  nmap -iL ip-addresses.txt -sV -oN common_services.txt

Starting Nmap 7.94 ( https://nmap.org ) at 2023-07-29 11:39 EDT
Nmap scan report for 192.168.52.2
Host is up (0.00088s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
53/tcp open  domain  ISC BIND

Nmap scan report for 192.168.52.131
Host is up (0.0028s latency).
Not shown: 994 closed tcp ports (conn-refused)
PORT     STATE SERVICE  VERSION
22/tcp   open  ssh      OpenSSH 3.9p1 (protocol 1.99)
80/tcp   open  http     Apache httpd 2.0.52 ((CentOS))
111/tcp  open  rpcbind  2 (RPC #100000)
443/tcp  open  ssl/http Apache httpd 2.0.52 ((CentOS))
631/tcp  open  ipp      CUPS 1.1
3306/tcp open  mysql    MySQL (unauthorized)

Nmap scan report for 192.168.52.132
Host is up (0.00094s latency).
Not shown: 995 closed tcp ports (conn-refused)
PORT    STATE SERVICE     VERSION
22/tcp  open  ssh         OpenSSH 7.4p1 Debian 10+deb9u6 (protocol 2.0)
25/tcp  open  smtp        Postfix smtpd
80/tcp  open  http        Apache httpd 2.4.25 ((Debian))
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
Service Info: Hosts:  symfonos.localdomain, SYMFONOS; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 192.168.52.129
```

CIA Triangle

Confidentiality

- Ensuring that sensitive data is accessed only by authorized individuals or systems
- prevents unauthorized access
- confidential information should remain hidden from unauthorized users
- Example: When transmitting data over a network hackers, eavesdroppers data.
- Best Practices: Encryption for sensitive data.

Integrity

- Ensuring data remains accurate, consistent, and unaltered during transmission or storage
- prevents unauthorized changes
- Integrity guarantees that the information received without any unauthorized modifications, deletions, or additions
- Example: Add 0 to user banking account balance!
- Best Practices: Use cryptographic hash functions (e.g., SHA-1) to verify data integrity.

Availability

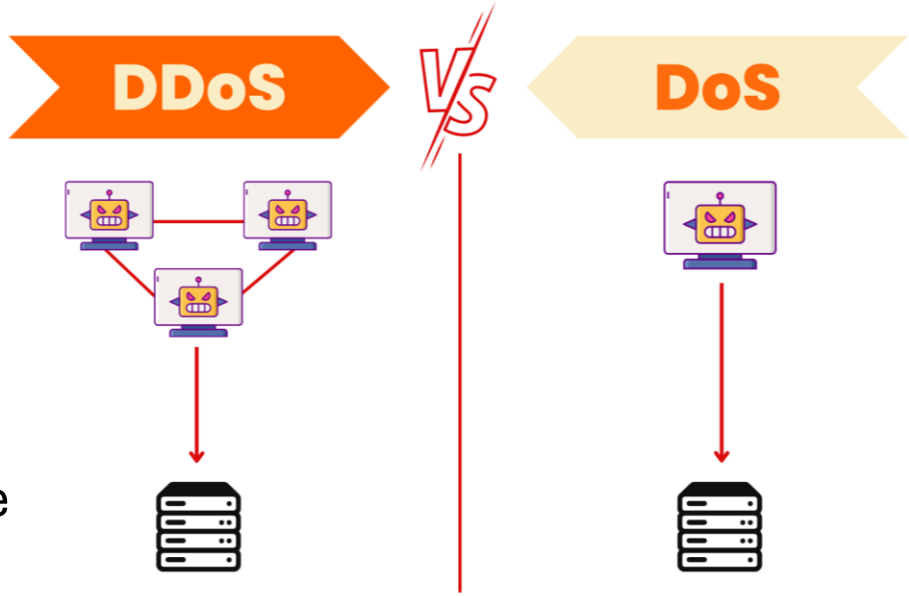
- Ensuring data and network resources are accessible to authorized users when needed
- ensures access when needed
- System's hardware and software components function correctly and can handle both anticipated and unexpected loads.
- Example: denial-of-service (DoS) or distributed denial-of-service (DDoS) attacks
- Best Practices: Use load balancers and IP blocking

DoS Attack

- Denial of Service (DoS) attack
- a malicious attempt to disrupt the normal functioning of a targeted server, service, or network by overwhelming it with a fake flood of traffic or requests.
- The goal of a DoS attack is to make the targeted system unavailable to users
- Types of DoS Attacks:
  - UDP Flood
  - ICMP Flood
  - TCP Syn Flood

DoS vs DDoS

- A DoS attack is launched from a single source
- The attacker sends a flood of requests to consuming resources (like bandwidth, memory, or CPU), which can lead to service disruption.
- A DDoS attack involves multiple compromised systems that coordinate to flood a target with traffic



Compare

Component	University	Military	Banking
Confidentiality	Reveal students grades or personal info e.g., Ali grade in Network exam	Reveal military information e.g., Number of soldiers	Reveal bank customers account information e.g., Ali has 100$
Importance	**Medium**	**Critical**	**High**

Compare

Component	University	Military	Banking
Integrity	Ensuring that academic records e.g., Ali grade in Network exam from 15 to 18	Change the number of soldiers (no reveal) e.g., from 10K to 15K soldiers	Change account balance. e.g., Change Ali account balance from 100$ to 1000$
Importance	**Critical**	**Medium**	**High**

Compare

Component	University	Military	Banking
Availability	university websites are not accessible to students	Military info system not working	Online payment not working
Importance	**High**	**Medium**	**Critical**

NVD

- National Vulnerability Database
- https://nvd.nist.gov
- It is a comprehensive repository of information related to known cybersecurity vulnerabilities.
- Managed by the National Institute of Standards and Technology (NIST) in the United States
- Provides a standardized way to identify and categorize vulnerabilities in software and hardware products.

Security Policies

- Security policies are formalized rules and guidelines that govern how an organization manages and protects its information assets
- Example: Network Security Policy
  - All network devices must be configured with strong passwords
  - Strong password has 8-25 character and number, sign & Uppercase letters

Security Policies

Security Standards

- Security standards are formalized guidelines and best practices designed to ensure the protection of information and information systems.
- These standards help organizations establish, implement, and maintain effective security measures to safeguard sensitive data and mitigate risks.
- Example: ISO 27001 (ISMS)