Applied!

Data & Network Security

Behnam Amiri

ans.dailysec.ir

aNetSec.github.io

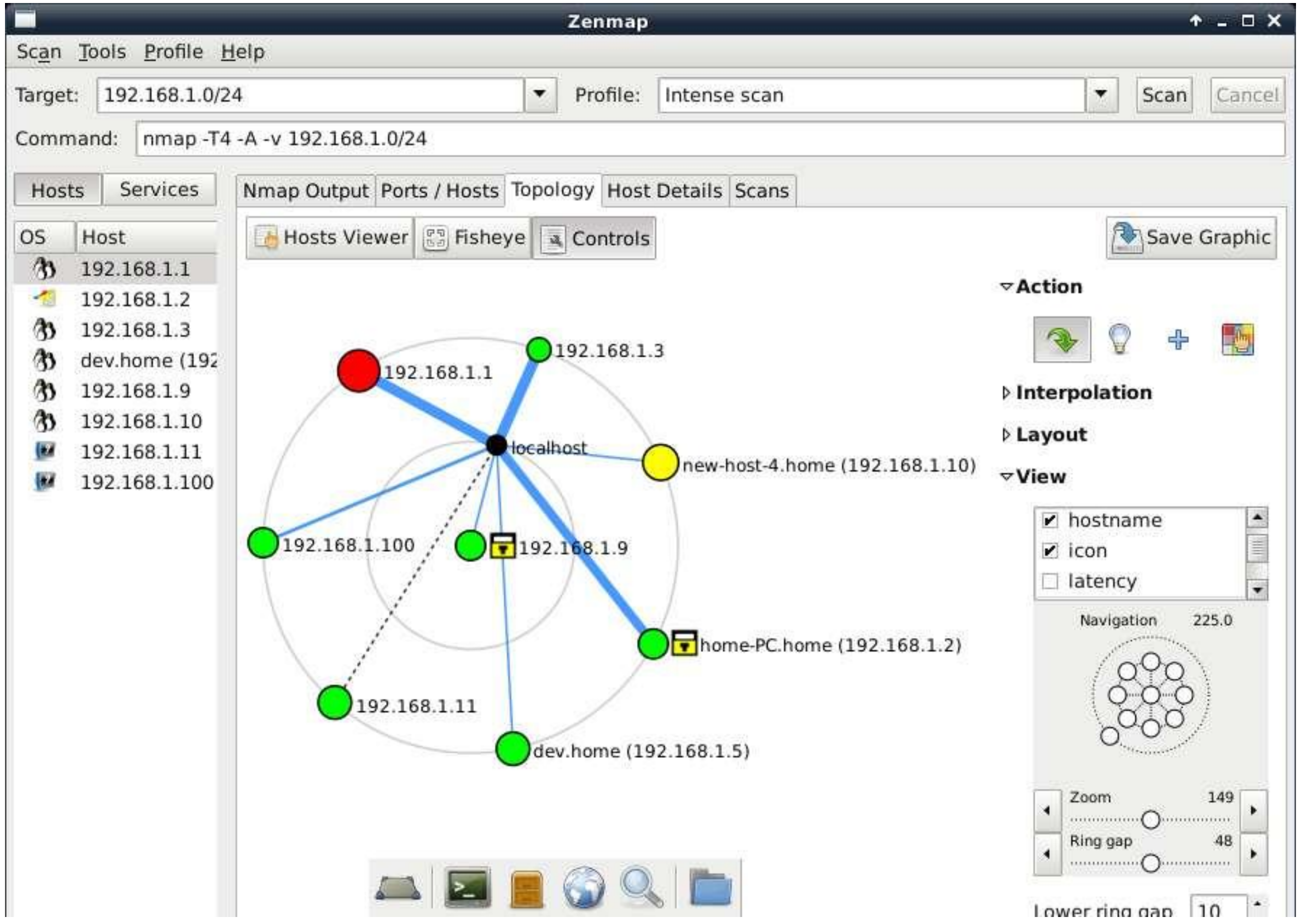
Spring 2025

Scan

Scan

- Scanning a network and its ports is a common practice in network administration and security assessments.
- It helps identify active devices, open ports, and potential vulnerabilities.
- There is 2 type of scanning
  - Host Scan: Find live hosts in network.
  - Port Scan: Find open ports on live hosts.

Scan results



Target: 192.168.1.0/24

Profile: Intense scan

Command: nmap -T4 -A -v 192.168.1.0/24

OS Host

192.168.1.1
192.168.1.2
192.168.1.3
dev.home (192
192.168.1.9
192.168.1.10
192.168.1.11
192.168.1.100

☑ hostname
☑ icon
□ latency

Navigation 225.0

Zoom 149

Ring gap 48

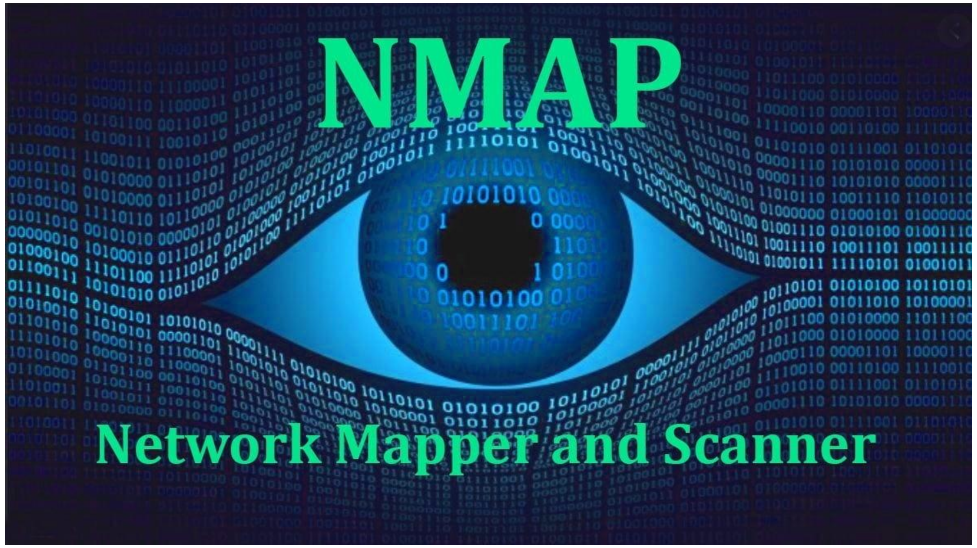
Lower ring gap 10

Scan tools

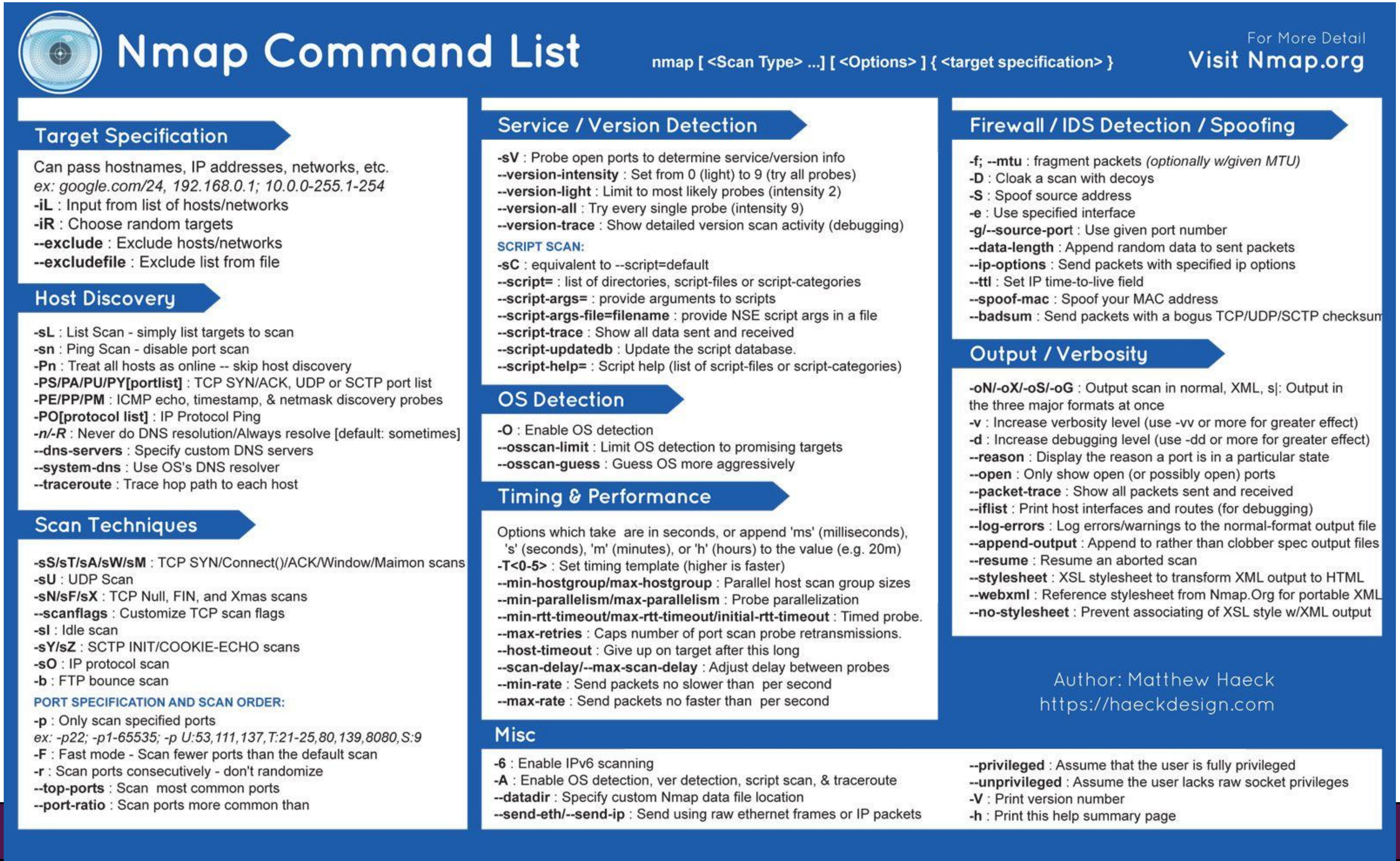
- Scanner: is a tool used to discover devices, services, and vulnerabilities on a network.
- popular scanners
  - Nmap
  - Zenmap
  - Zmap
  - OpenVAS
  - masscan
  - Nessus
  - Metasploit
  - ….

nmap

- Free & Open source
- Reliable
- Cross platform
- Popular
- https://nmap.org



Nmap commands



Nmap Command List

nmap [<Scan Type> ...] [<Options>] { <target specification> }

For More Detail
Visit Nmap.org

Target Specification

Can pass hostnames, IP addresses, networks, etc.
ex: google.com/24, 192.168.0.1; 10.0.0-255.1-254
-iL : Input from list of hosts/networks
-iR : Choose random targets
--exclude : Exclude hosts/networks
--excludefile : Exclude list from file

Host Discovery

-sL : List Scan - simply list targets to scan
-sn : Ping Scan - disable port scan
-Pn : Treat all hosts as online -- skip host discovery
-PS/PA/PU/PY[portlist] : TCP SYN/ACK, UDP or SCTP port list
-PE/PP/PM : ICMP echo, timestamp, & netmask discovery probes
-PO[protocol list] : IP Protocol Ping
-n/-R : Never do DNS resolution/Always resolve [default: sometimes]
--dns-servers : Specify custom DNS servers
--system-dns : Use OS's DNS resolver
--traceroute : Trace hop path to each host

Scan Techniques

-sS/sT/sA/sW/sM : TCP SYN/Connect()/ACK/Window/Maimon scans
-sU : UDP Scan
-sN/sF/sX : TCP Null, FIN, and Xmas scans
--scanflags : Customize TCP scan flags
-sI : Idle scan
-sY/sZ : SCTP INIT/COOKIE-ECHO scans
-sO : IP protocol scan
-b : FTP bounce scan

PORT SPECIFICATION AND SCAN ORDER:

-p : Only scan specified ports
ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080,S:9
-F : Fast mode - Scan fewer ports than the default scan
-r : Scan ports consecutively - don't randomize
--top-ports : Scan most common ports
--port-ratio : Scan ports more common than

Service / Version Detection

-sV : Probe open ports to determine service/version info
--version-intensity : Set from 0 (light) to 9 (try all probes)
--version-light : Limit to most likely probes (intensity 2)
--version-all : Try every single probe (intensity 9)
--version-trace : Show detailed version scan activity (debugging)

SCRIPT SCAN:

-sC : equivalent to --script=default
--script= : list of directories, script-files or script-categories
--script-args= : provide arguments to scripts
--script-args-file=filename : provide NSE script args in a file
--script-trace : Show all data sent and received
--script-updatedb : Update the script database.
--script-help= : Script help (list of script-files or script-categories)

OS Detection

-O : Enable OS detection
--osscan-limit : Limit OS detection to promising targets
--osscan-guess : Guess OS more aggressively

Timing & Performance

Options which take are in seconds, or append 'ms' (milliseconds), 's' (seconds), 'm' (minutes), or 'h' (hours) to the value (e.g. 20m)
-T<0-5> : Set timing template (higher is faster)
--min-hostgroup/max-hostgroup : Parallel host scan group sizes
--min-parallelism/max-parallelism : Probe parallelization
--min-rtt-timeout/max-rtt-timeout/initial-rtt-timeout : Timed probe.
--max-retries : Caps number of port scan probe retransmissions.
--host-timeout : Give up on target after this long
--scan-delay/--max-scan-delay : Adjust delay between probes
--min-rate : Send packets no slower than per second
--max-rate : Send packets no faster than per second

Firewall / IDS Detection / Spoofing

-f; --mtu : fragment packets *(optionally w/given MTU)*
-D : Cloak a scan with decoys
-S : Spoof source address
-e : Use specified interface
-g/--source-port : Use given port number
--data-length : Append random data to sent packets
--ip-options : Send packets with specified ip options
--ttl : Set IP time-to-live field
--spoof-mac : Spoof your MAC address
--badsum : Send packets with a bogus TCP/UDP/SCTP checksum

Output / Verbosity

-oN/-oX/-oS/-oG : Output scan in normal, XML, s|: Output in the three major formats at once
-v : Increase verbosity level (use -vv or more for greater effect)
-d : Increase debugging level (use -dd or more for greater effect)
--reason : Display the reason a port is in a particular state
--open : Only show open (or possibly open) ports
--packet-trace : Show all packets sent and received
--iflist : Print host interfaces and routes (for debugging)
--log-errors : Log errors/warnings to the normal-format output file
--append-output : Append to rather than clobber spec output files
--resume : Resume an aborted scan
--stylesheet : XSL stylesheet to transform XML output to HTML
--webxml : Reference stylesheet from Nmap.Org for portable XML
--no-stylesheet : Prevent associating of XSL style w/XML output

Author: Matthew Haeck
https://haeckdesign.com

Misc

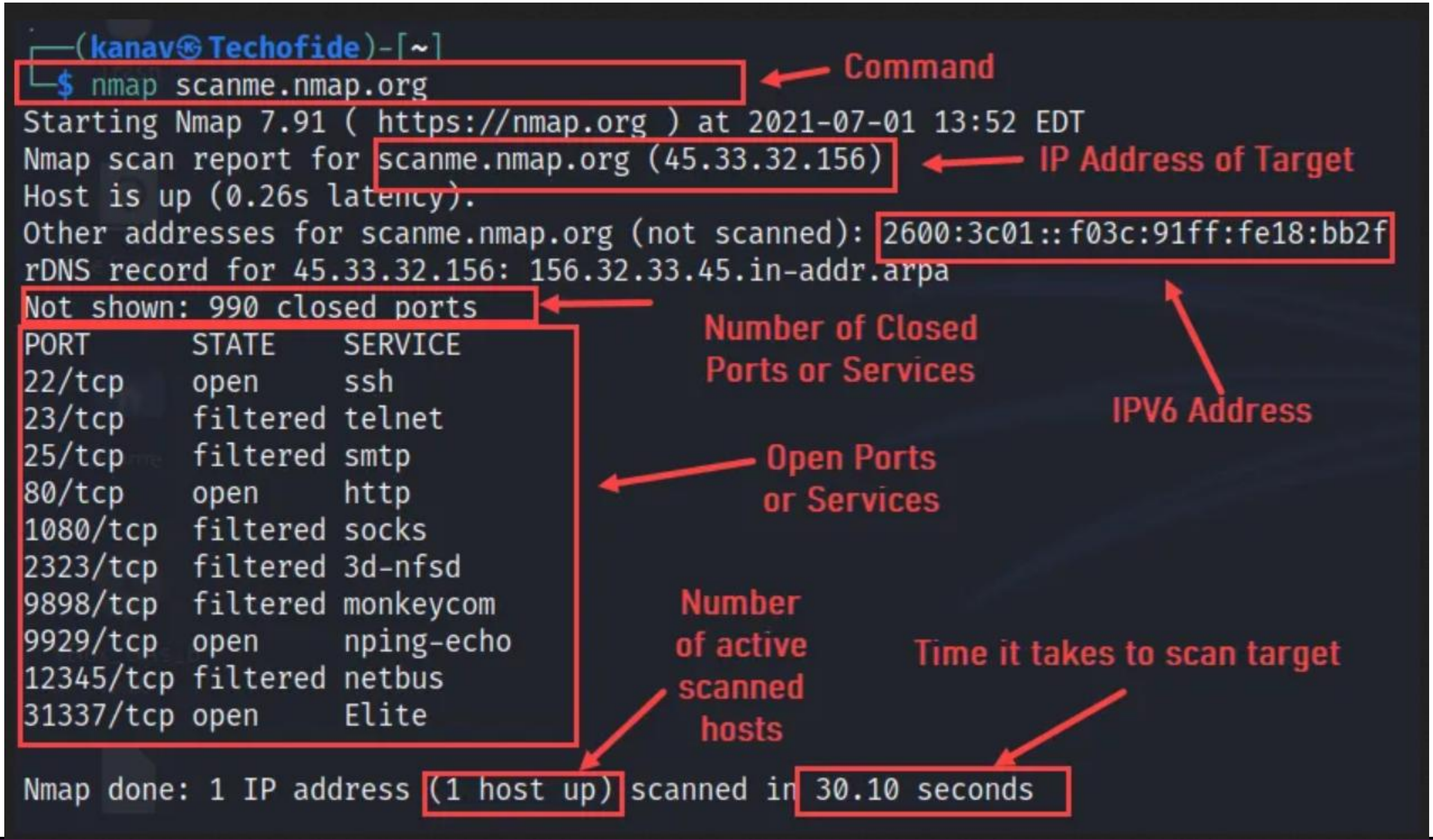
-6 : Enable IPv6 scanning
-A : Enable OS detection, ver detection, script scan, & traceroute
--datadir : Specify custom Nmap data file location
--send-eth/--send-ip : Send using raw ethernet frames or IP packets
--privileged : Assume that the user is fully privileged
--unprivileged : Assume the user lacks raw socket privileges
-V : Print version number
-h : Print this help summary page

Basic NMAP Commands

- Ping scan (Host Discovery)
  - The following command is used to perform a ping scan on a target system or network.
  - nmap -sn <target IPs>
- TCP Scan
  - The following command is used to perform a basic TCP scan on the specified target using the Nmap tool.
  - nmap <target IPs>
- Version Detection
  - The following command is used to perform a version detection scan on the specified target system(s).
  - nmap -sV <target>
- More at: https://www.geeksforgeeks.org/top-30-basic-nmap-commands-for-beginners/

Nmap results

- Sample results



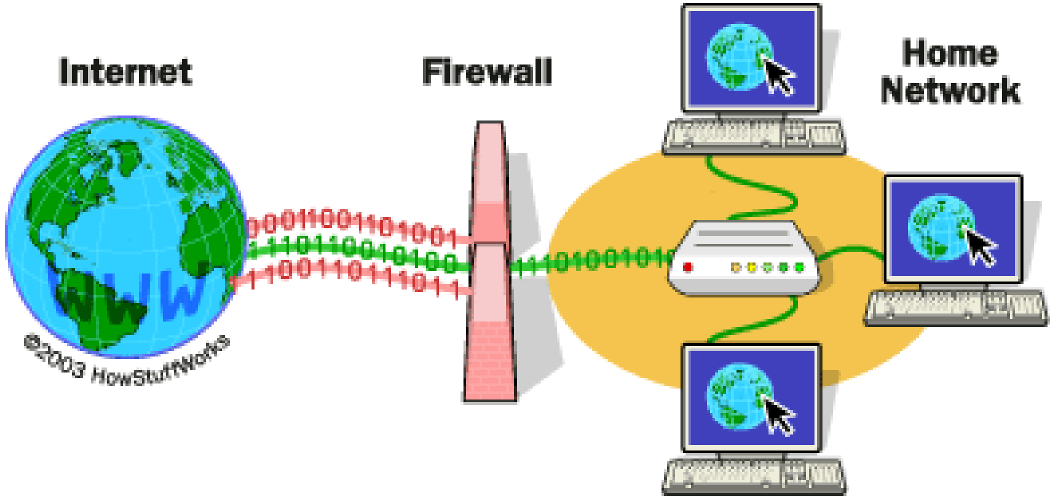
```
┌──(kanav㉿Techofide)-[~]
└─$ nmap scanme.nmap.org
Starting Nmap 7.91 ( https://nmap.org ) at 2021-07-01 13:52 EDT
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.26s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
rDNS record for 45.33.32.156: 156.32.33.45.in-addr.arpa
Not shown: 990 closed ports
PORT      STATE    SERVICE
22/tcp    open     ssh
23/tcp    filtered telnet
25/tcp    filtered smtp
80/tcp    open     http
1080/tcp  filtered socks
2323/tcp  filtered 3d-nfsd
9898/tcp  filtered monkeycom
9929/tcp  open     nping-echo
12345/tcp filtered netbus
31337/tcp open     Elite

Nmap done: 1 IP address (1 host up) scanned in 30.10 seconds
```

Command
IP Address of Target
Number of Closed Ports or Services
IPV6 Address
Open Ports or Services
Number of active scanned hosts
Time it takes to scan target

Firewall

Firewall

- A firewall is a network security device or software that monitors and controls incoming and outgoing network traffic based on predetermined security rules.
- Firewall just blocks port and IP.
- Firewall can’t understand payload.



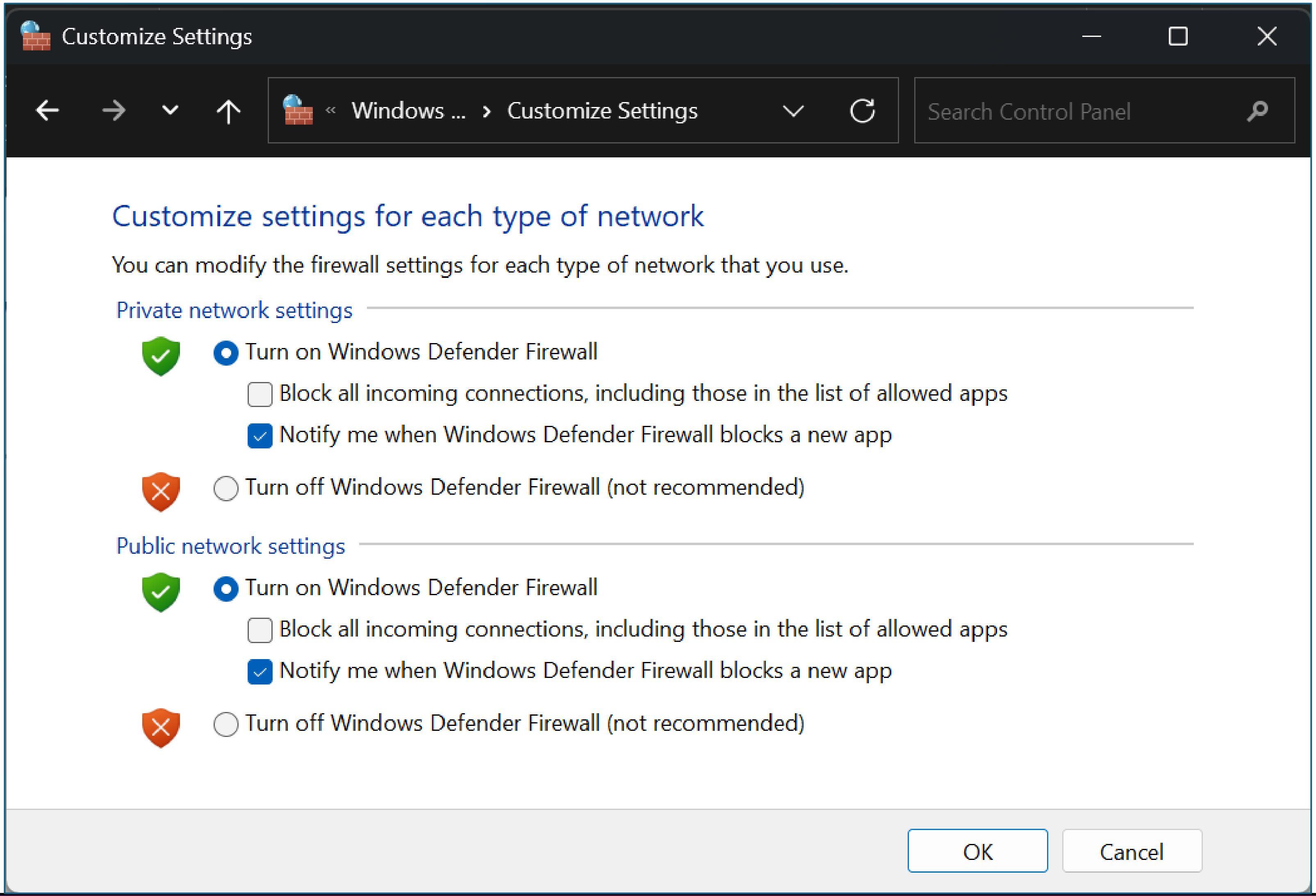
©2003 HowStuffWorks

Firewall Types

- **Network Firewall**
- Is a security device or software that monitors and controls incoming and outgoing network traffic for an entire network.
- It is typically deployed at the perimeter of a network, acting as a barrier between the internal network and external networks.
- Examples: pfSense, cisco ASA, FortiGate, ...
- **Host based Firewall**
- Is a security software application that runs on an individual device (host) to monitor and control incoming and outgoing traffic for that specific device.
- It provides a layer of security at the endpoint level.
- examples: windows firewall, iptables, ufw, ...

Windows Firewall

- status



Customize settings for each type of network

You can modify the firewall settings for each type of network that you use.

Private network settings

● Turn on Windows Defender Firewall

□ Block all incoming connections, including those in the list of allowed apps

☑ Notify me when Windows Defender Firewall blocks a new app

○ Turn off Windows Defender Firewall (not recommended)

Public network settings

● Turn on Windows Defender Firewall

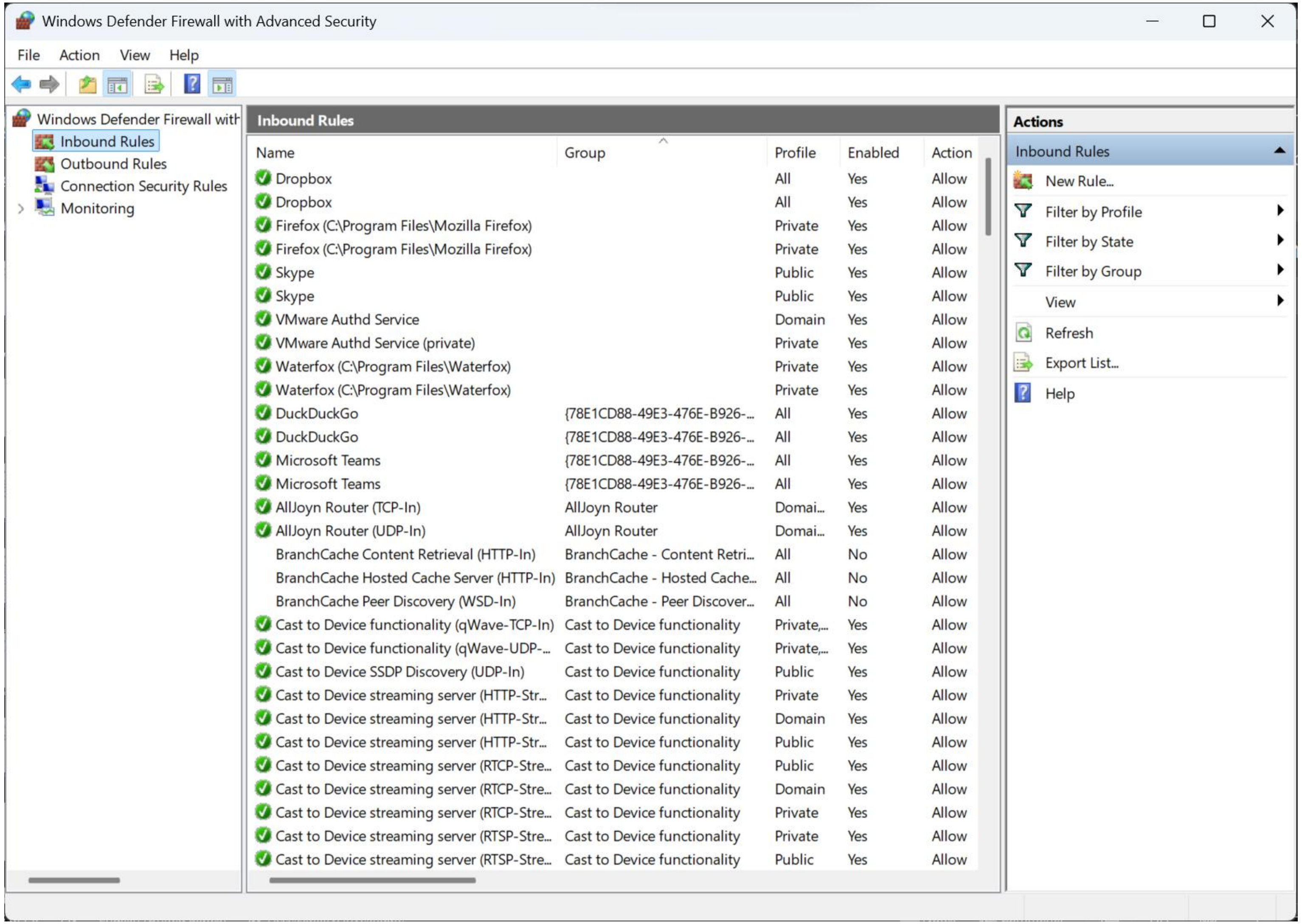
□ Block all incoming connections, including those in the list of allowed apps

☑ Notify me when Windows Defender Firewall blocks a new app

○ Turn off Windows Defender Firewall (not recommended)

Windows Firewall

- Advanced view



Name	Group	Profile	Enabled	Action
Dropbox		All	Yes	Allow
Dropbox		All	Yes	Allow
Firefox (C:\Program Files\Mozilla Firefox)		Private	Yes	Allow
Firefox (C:\Program Files\Mozilla Firefox)		Private	Yes	Allow
Skype		Public	Yes	Allow
Skype		Public	Yes	Allow
VMware Authd Service		Domain	Yes	Allow
VMware Authd Service (private)		Private	Yes	Allow
Waterfox (C:\Program Files\Waterfox)		Private	Yes	Allow
Waterfox (C:\Program Files\Waterfox)		Private	Yes	Allow
DuckDuckGo	{78E1CD88-49E3-476E-B926-...	All	Yes	Allow
DuckDuckGo	{78E1CD88-49E3-476E-B926-...	All	Yes	Allow
Microsoft Teams	{78E1CD88-49E3-476E-B926-...	All	Yes	Allow
Microsoft Teams	{78E1CD88-49E3-476E-B926-...	All	Yes	Allow
AllJoyn Router (TCP-In)	AllJoyn Router	Domai...	Yes	Allow
AllJoyn Router (UDP-In)	AllJoyn Router	Domai...	Yes	Allow
BranchCache Content Retrieval (HTTP-In)	BranchCache - Content Retri...	All	No	Allow
BranchCache Hosted Cache Server (HTTP-In)	BranchCache - Hosted Cache...	All	No	Allow
BranchCache Peer Discovery (WSD-In)	BranchCache - Peer Discover...	All	No	Allow
Cast to Device functionality (qWave-TCP-In)	Cast to Device functionality	Private,...	Yes	Allow
Cast to Device functionality (qWave-UDP-...	Cast to Device functionality	Private,...	Yes	Allow
Cast to Device SSDP Discovery (UDP-In)	Cast to Device functionality	Public	Yes	Allow
Cast to Device streaming server (HTTP-Str...	Cast to Device functionality	Private	Yes	Allow
Cast to Device streaming server (HTTP-Str...	Cast to Device functionality	Domain	Yes	Allow
Cast to Device streaming server (HTTP-Str...	Cast to Device functionality	Public	Yes	Allow
Cast to Device streaming server (RTCP-Stre...	Cast to Device functionality	Public	Yes	Allow
Cast to Device streaming server (RTCP-Stre...	Cast to Device functionality	Domain	Yes	Allow
Cast to Device streaming server (RTCP-Stre...	Cast to Device functionality	Private	Yes	Allow
Cast to Device streaming server (RTSP-Stre...	Cast to Device functionality	Private	Yes	Allow
Cast to Device streaming server (RTSP-Stre...	Cast to Device functionality	Public	Yes	Allow

Firewall rules

- Inbound rules for incoming traffic.
- Outbound rules for outgoing traffic.
- Rule style:
  - Src IP, des IP, Allow|Deny

Linux Firewall

- IP tables
  - is a powerful command-line utility.
  - iptables is commonly used to implement firewalls, manage network traffic, and enhance security on Linux-based systems.

  ```
  iptables -A INPUT -p tcp --dport 80 -j ACCEPT
  ```

- UFW
  - UFW (Uncomplicated Firewall)
  - is a user-friendly front-end for managing iptables firewall rules on Linux systems.
  - It is designed to simplify the process of configuring a firewall.
  - UFW is particularly popular on Ubuntu and other Debian-based distributions.

  ```
  sudo ufw allow http
  ```

Firewall limitation

- Firewall can block/unblock port and IP.
- Firewall can’t detect network attacks.

IDS/IPS

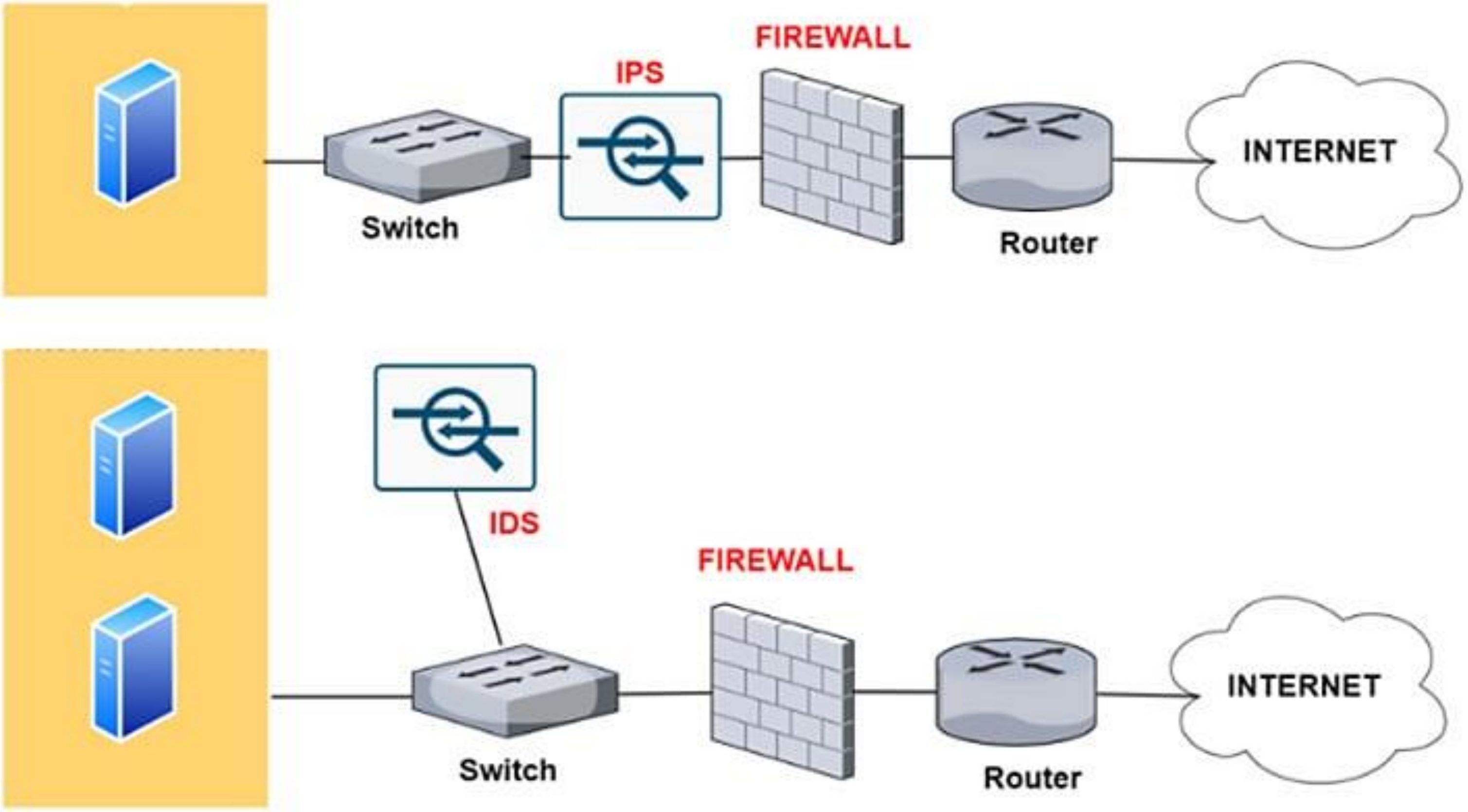
Intrusion

- Intrusion is any attack type, like:
  - Brute Force
  - Worm
  - DoS/DDoS

IDS/IPS

- **Intrusion Detection System (IDS)**
- An IDS monitors network traffic for suspicious activity and potential threats.
- It analyzes traffic patterns and alerts administrators when it detects anomalies or known attack signatures.
- **Types**:
  - **Network-based IDS (NIDS)**: Monitors network traffic for all devices on the network.
  - **Host-based IDS (HIDS)**: Monitors a single host or device for suspicious activity.
- **Intrusion Prevention System (IPS)**
- IPS not only detects potential threats but also takes action to prevent them. It can block or reject malicious traffic in real-time.
- **Functionality**: An IPS is often placed in-line with network traffic, allowing it to actively monitor and respond to threats as they occur.

Network location



IDS Evasion

- IDS can detect all attacks
  - Fragment packets
  - Overlap packets
  - …
- IDS performance is challenging topic.
- Snort & Suricata are famous IDS/IPS