| Nmap Full Course |

<Mina Magdy>

Linux Administration

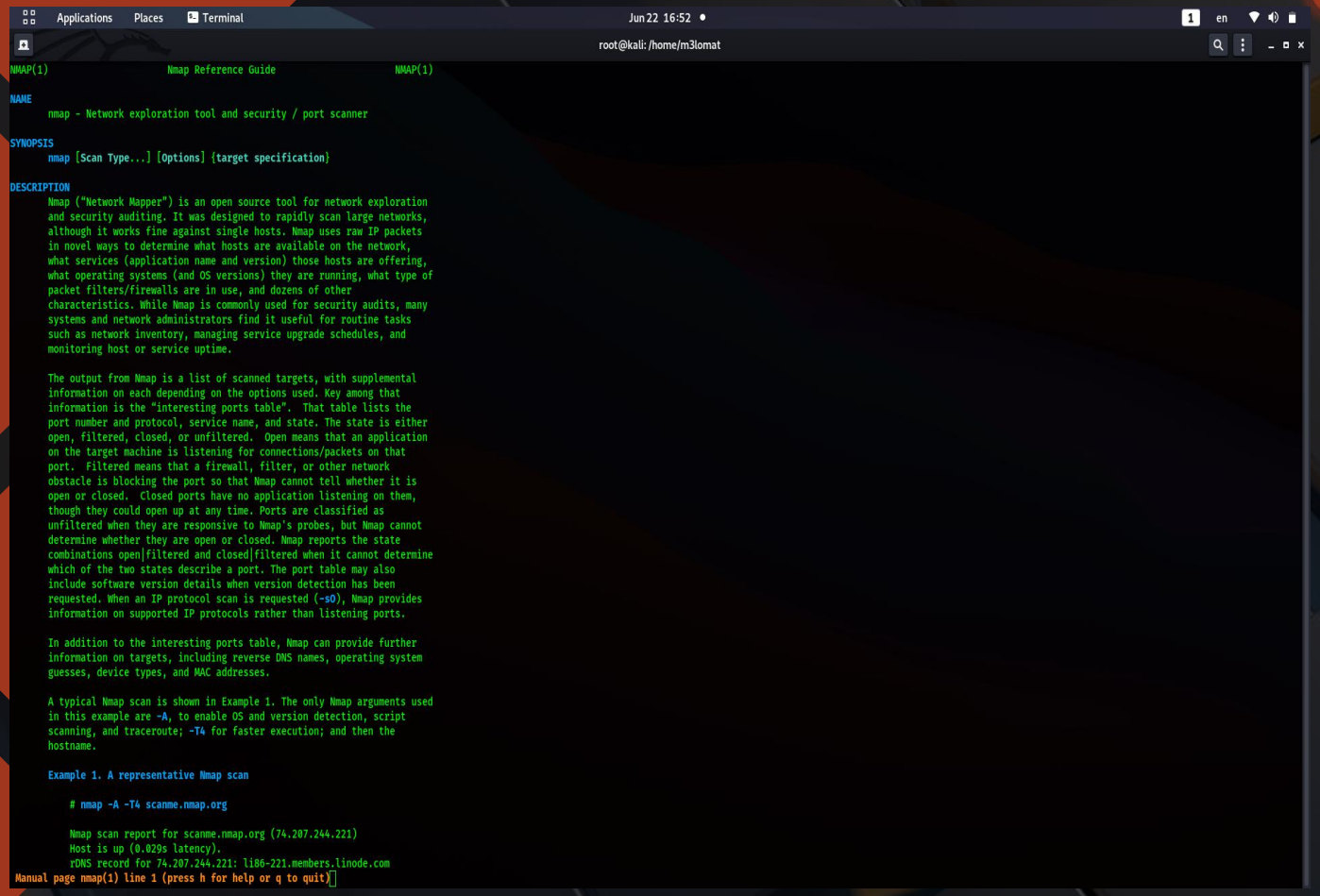
oscp,sscp,ceh,crtp

Bit Of Network Mapper History

- Created by Gordon Lyon

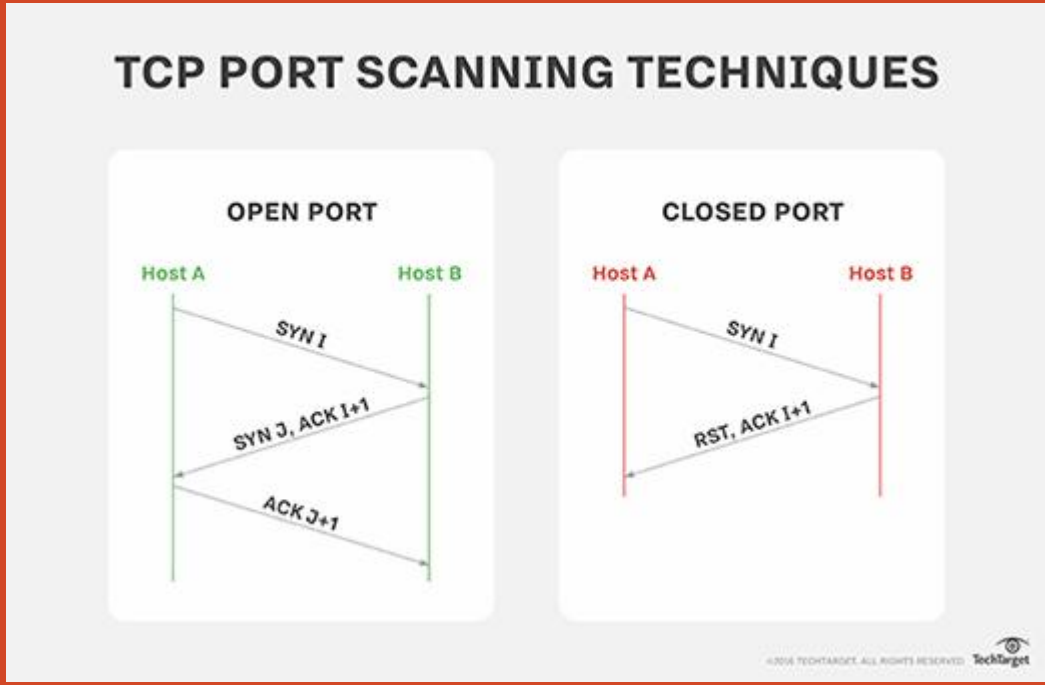
- Nmap is used to discover hosts and services on a computer network by sending packets and analyzing the responses
- Nmap (Network Mapper) is a free and open-source network scanner

Nmap Manual Options



You can Show a full survey of the network map usage options

Knowledge of tcp port scanning



1. Scanning Knowledge
   all or include (8080,443,1234)
   Wait Response of This Ports
   (Ping Scan)

2. Nmap Packet : Hello ??
   Port 80 : Hello,

   Nmap Packet : Can We Talk ?
   Port 80 : Yes we can

Nmap Basics Options To Scan

Nmap Basic Options To Scaning

Default Scaning

nmap + $ip

Ex : nmap 192.168.1.1

Ping Scaning (Default Used)

nmap -Pn $ip (Disable ping Scaning)

Ex : nmap -Pn 192.168.1.1

Fast Scaning (First Favour 100 Port)

nmap -F + $ip

Ex : nmap -F 192.168.1.1

Port Status

- OPEN
- CLOSED
- FILTERED
- UNFILTERED

Port Status

OPEN

An application is actively accepting TCP connections, UDP datagrams or SCTP associations on this port. Finding these is often the primary goal of port scanning. Security-minded people know that each open port is an

Port Status

CLOSED

A closed port is accessible (it receives and responds to Nmap probe packets), but there is no application listening on it. They can be helpful in showing that a host is up on an IP address (host discovery)

Port Status

FILTERED

Nmap cannot determine whether the port is open because packet filtering prevents its probes from reaching the port. The filtering could be from a dedicated firewall device, router rules, or host-based firewall

Port Status

UNFILTERED

The unfiltered state means that a port is accessible, but Nmap is unable to determine whether it is open or closed. Only the ACK scan, which is used to map firewall rulesets, classifies ports into this

Nmap Advanced Options To Scaning

Nmap Advanced Options To Scaning

Aggressive Scan

Nmap -A + $ip

Ex : nmap -A + 192.168.1.1

Oprating System

Nmap -O + $ip

Ex : nmap -O + 192.168.1.1

Vesrpose Mode

Nmap -v + $ip

Ex : nmap -v + 192.168.1.1

Udp Port Scan

Nmap -sU + $ip

Ex : nmap -sU 192.168.1.1

Nmap Advanced Options To Scaning

Time Of Port Scaning

nmap -T1,2,3,4 + $ip

Ex : nmap -T4 192.168.1.1

Port Service Scaning

nmap -Ss + $ip

Ex : nmap -Ss 192.168.1.1

Port Version Scaning

nmap -Sv + $ip

Ex : nmap -sV 192.168.1.1

Checking Big list of targets

nmap -iL $ip list

Ex : nmap -iL targets.txt

Nmap Advanced Options To Scaning

Skip Host Discover

nmap -Pn + $ip

Ex : nmap -Pn 192.168.1.1

nmap --disable-arp-ping 192.168.1.1

Treat All Hhosts as Online

nmap -sn + $ip

EX : nmap -sn 192.168.1.1

No Dns Reslution

nmap -n + $ip

Ex : nmap -n test.com

Scan Under Discovering Mode

nmap -D $ip1,$ip2 -A $ip3

Ex : nmap -D 172.217.171.206,102.132.97.35 -A nmap.org

Nmap Advanced Scripts To Scaning

Directory

cd /usr/share/nmap/scripts/

USE : ls Command

To show nmap scripts

Nmap Advanced Scripts Explain

Nmap Scripts Use

nmap --script=SCRIPT + $ ip

Ex : nmap --script=vuln 192.168.1.1

Nmap Scripts Revarse Use

nmap + $ ip --script=SCRIPT.nse

Ex : nmap 192.168.1.1 --script=vulners.nse

Explain Nmap Scripts

VULNERS,VUL,CVE,INFO,ENUM

Nmap Save Result Scan

Save on Txt File

nmap + $ip >> NAME.txt

nmap + 192.168.1.1 >> m3lomat.txt

Save To Xml File

nmap + $ip -oX

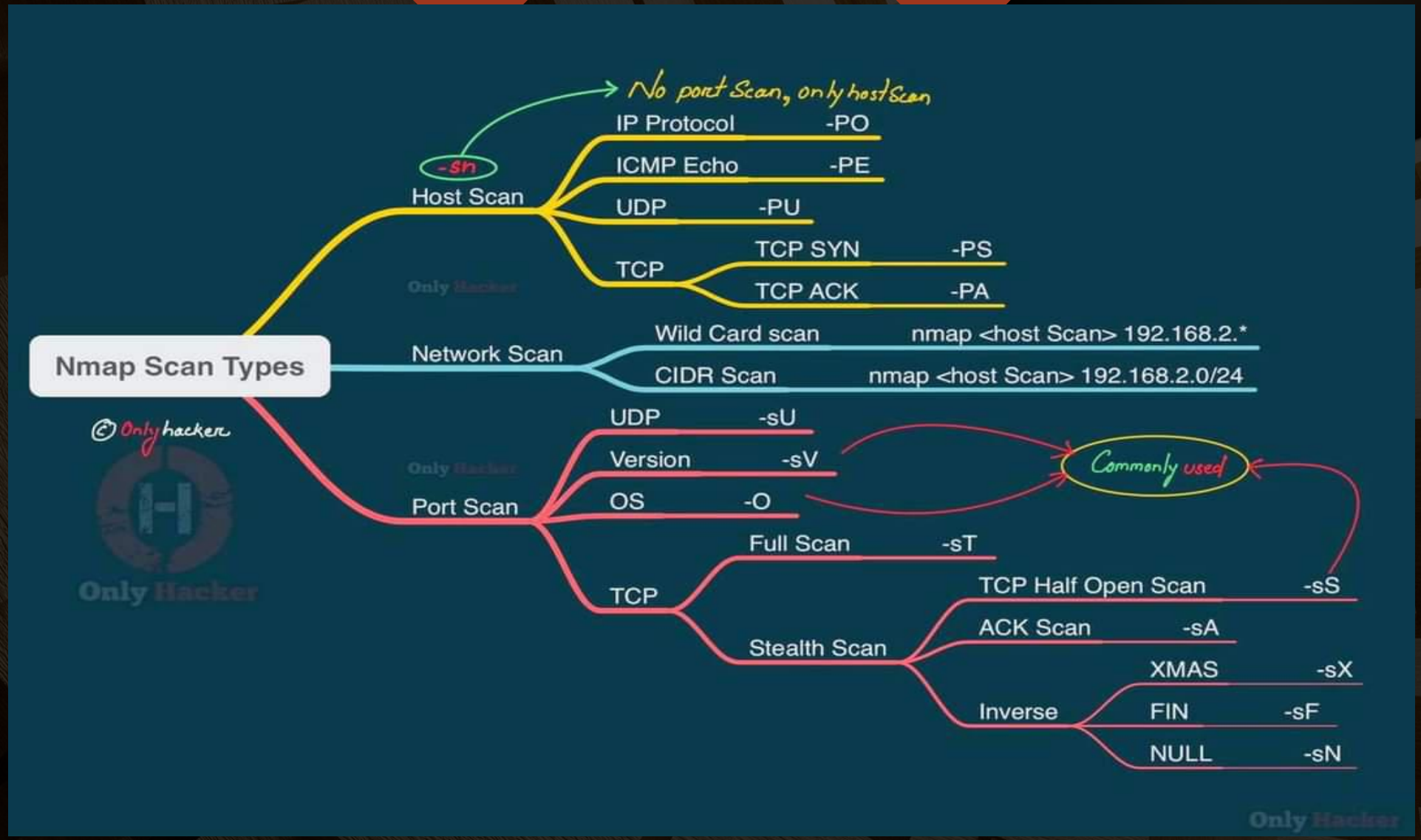
nmap 192.168.1.1 -oX m3lomat

Save To Some File Formats >> NAME.format

nmap + $ip >> NAME.fileformat

nmap + 192.168.1.1 >> m3lomat.html,xml,txt

Nmap Advanced Options To Scaning



| Final Result |

- Part 1 >> Bit Of Nmap History
- Part 2 >> Nmap Basics Options To Scan
- Part 3 >> Port Status
- Part 4 >> Nmap Advanced Options To Scan
- Part 5 >> Nmap Advanced Scripts To Scan
- Part 6 >> Nmap Advanced Scripts Explain
- Part 7 >> Nmap Save Result Scan

ASKING TIME ??

You can Ask Me ON ?

- Facebook : https://www.facebook.com/m3lomatthephone
- My YouTube Chanel : https://www.youtube.com/c/m3lomatthephone
- M3lomat the phone 2 : https://www.youtube.com/channel/UCixopZbFBzdYKk2qsZLsRCA
- M3lomat Electric : https://www.youtube.com/channel/UCGnXhX2E_MaGYOY8kyOowbQ
- Instagram : https://instagram.com/mena.m.rushdy?igshid=1xg5sxvjtek7i
- LinkedIn : https://www.linkedin.com/in/mina-magdy-38362b1b6/
- Facebook Group : https://www.facebook.com/groups/391033085092937