

| Nmap Full Course |

<Mina Magdy>

Linux Administration

oscp,sscp,ceh,crtip

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

```
Applications  Places  Terminal  Jun22 16:52  1 en  WiFi  Speaker  Battery
root@kali: /home/m3lomat

NMAP(1)  Nmap Reference Guide  NMAP(1)

NAME
nmap - Network exploration tool and security / port scanner

SYNOPSIS
nmap [Scan Type...] [Options] {target specification}

DESCRIPTION
Nmap ("Network Mapper") is an open source tool for network exploration
and security auditing. It was designed to rapidly scan large networks,
although it works fine against single hosts. Nmap uses raw IP packets
in novel ways to determine what hosts are available on the network,
what services (application name and version) those hosts are offering,
what operating systems (and OS versions) they are running, what type of
packet filters/firewalls are in use, and dozens of other
characteristics. While Nmap is commonly used for security audits, many
systems and network administrators find it useful for routine tasks
such as network inventory, managing service upgrade schedules, and
monitoring host or service uptime.

The output from Nmap is a list of scanned targets, with supplemental
information on each depending on the options used. Key among that
information is the "interesting ports table". That table lists the
port number and protocol, service name, and state. The state is either
open, filtered, closed, or unfiltered. Open means that an application
on the target machine is listening for connections/packets on that
port. Filtered means that a firewall, filter, or other network
obstacle is blocking the port so that Nmap cannot tell whether it is
open or closed. Closed ports have no application listening on them,
though they could open up at any time. Ports are classified as
unfiltered when they are responsive to Nmap's probes, but Nmap cannot
determine whether they are open or closed. Nmap reports the state
combinations open|filtered and closed|filtered when it cannot determine
which of the two states describe a port. The port table may also
include software version details when version detection has been
requested. When an IP protocol scan is requested (-s0), Nmap provides
information on supported IP protocols rather than listening ports.

In addition to the interesting ports table, Nmap can provide further
information on targets, including reverse DNS names, operating system
guesses, device types, and MAC addresses.

A typical Nmap scan is shown in Example 1. The only Nmap arguments used
in this example are -A, to enable OS and version detection, script
scanning, and traceroute; -T4 for faster execution; and then the
hostname.

Example 1. A representative Nmap scan

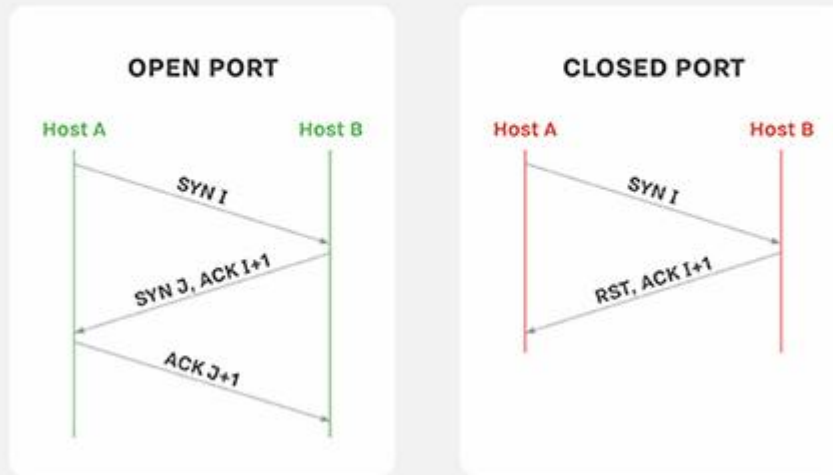
# nmap -A -T4 scanme.nmap.org

Nmap scan report for scanme.nmap.org (74.207.244.221)
Host is up (0.029s latency).
rDNS record for 74.207.244.221: 1186-221.members.linode.com
Manual page nmap(1) line 1 (press h for help or q to quit)
```

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

Knowledge of tcp port scanning

TCP PORT SCANNING TECHNIQUES



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 Scanning

Default Scanning

`nmap + $ip`

Ex : `nmap 192.168.1.1`

Ping Scanning (Default Used)

`nmap -Pn $ip` (Disable ping Scanning)

Ex : `nmap -Pn 192.168.1.1`

Fast Scanning (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 Scanning

Nmap Advanced Options To Scanning

Aggressive Scan

Nmap -A + \$ip

Ex : nmap -A + 192.168.1.1

Operating System

Nmap -O + \$ip

Ex : nmap -O + 192.168.1.1

Verbose 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 Scanning

Time Of Port Scanning

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

Ex : `nmap -T4 192.168.1.1`

Port Service Scanning

`nmap -Ss + $ip`

Ex : `nmap -Ss 192.168.1.1`

Port Version Scanning

`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 Scanning

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 Scanning

Directory

cd /usr/share/nmap/scripts/

USE : ls Command

To show nmap scripts

```
Applications  Places  Terminal  Jul 4 20:18
m3lomat@kali: /usr/share/nmap/scripts

(m3lomat@kali)-[/usr/share/nmap/scripts]
$ ls
acarsd-info.nse dns-random-srcport.nse http-hp-ilo-info.nse ip-geolocation-ipinfodb.nse ntp-info.nse smtp-enum-users.nse
address-info.nse dns-random-txid.nse http-huawei-hg5xx-vuln.nse ip-geolocation-map-bing.nse ntp-monlist.nse smtp-ntlm-info.nse
afp-brute.nse dns-recursion.nse http-icloud-findmyiphone.nse ip-geolocation-map-google.nse omp2-brute.nse smtp-open-relay.nse
afp-ls.nse dns-service-discovery.nse http-icloud-sendmsg.nse ip-geolocation-map-kml.nse omp2-enum-targets.nse smtp-strangeport.nse
afp-path-vuln.nse dns-srv-enum.nse http-iis-short-name-brute.nse ip-geolocation-maxmind.nse omron-info.nse smtp-vuln-cve2010-4344.nse
afp-serverinfo.nse dns-update.nse http-iis-webdav-vuln.nse ip-https-discover.nse openlookup-info.nse smtp-vuln-cve2011-1720.nse
afp-showmount.nse dns-zeustracker.nse http-internal-ip-disclosure.nse ip-https-discover.nse openvas-otp-brute.nse smtp-vuln-cve2011-1764.nse
ajp-auth.nse dns-zone-transfer.nse http-joomla-brute.nse ipidseq.nse openwebnet-discovery.nse sniffer-detect.nse
ajp-brute.nse docker-version.nse http-jsoup-brute.nse ipmi-brute.nse oracle-brute.nse snmp-brute.nse
ajp-headers.nse dockercon-brute.nse http-litespeed-sourcecode-download.nse ipmi-cipher-zero.nse oracle-brute-stealth.nse snmp-hh3c-logins.nse
ajp-methods.nse domcon-cmd.nse http-ls.nse ipmi-version.nse oracle-enum-users.nse snmp-info.nse
ajp-request.nse domino-enum-users.nse http-majordomo2-dir-traversal.nse ipmi-multicast-mld-list.nse oracle-sid-brute.nse snmp-interfaces.nse
allseeingeye-info.nse dpap-brute.nse http-malware-host.nse ipv6-multicast-mld-list.nse oracle-tns-version.nse snmp-ios-config.nse
amqp-info.nse drda-brute.nse http-mcnp.nse ipv6-node-info.nse ovs-agent-version.nse snmp-netstat.nse
asn-query.nse drda-info.nse http-methods.nse ipv6-ra-flood.nse p2p-conficker.nse snmp-processes.nse
auth-owners.nse duplicates.nse http-mobileversion-checker.nse irc-botnet-channels.nse path-mtu.nse snmp-sysdescr.nse
auth-spoof.nse eap-info.nse http-nip-info.nse irc-brute.nse pcapwhere-brute.nse snmp-win32-services.nse
backorifice-brute.nse epmd-info.nse http-open-proxy.nse irc-info.nse pcwpx-info.nse snmp-win32-shares.nse
backorifice-info.nse eppc-enum-processes.nse http-open-redirect.nse irc-sasl-brute.nse pgsql-brute.nse snmp-win32-software.nse
bacnet-info.nse fcrdns.nse http-passwd.nse irc-unrealircd-backdoor.nse pjl-ready-message.nse snmp-win32-users.nse
banner.nse finger.nse http-phpmymadmin-dir-traversal.nse iscsi-brute.nse pop3-brute.nse socks-auth-info.nse
bitcoin-getaddr.nse fingerprint-strings.nse http-phpself-xss.nse iscsi-info.nse pop3-capabilities.nse socks-brute.nse
bitcoin-info.nse firewall.nse http-php-version.nse iscsi-info.nse pop3-ntlm-info.nse socks-open-proxy.nse
bitcoinrpc-info.nse firewall-bypass.nse http-proxy-brute.nse jdwmp-exec.nse pptp-version.nse ssh2-enum-algos.nse
bittorrent-discovery.nse flume-master-info.nse http-put.nse jdwmp-info.nse puppet-naivesigning.nse ssh-auth-methods.nse
bjnp-discover.nse fox-info.nse http-qnap-nas-info.nse jdwmp-inject.nse qconn-exec.nse ssh-brute.nse
broadcast-ataoe-discover.nse freelancer-info.nse http-referer-checker.nse jdwmp-version.nse qscan.nse ssh-hostkey.nse
broadcast-avahi-dos.nse ftp-anon.nse http-rfi-spider.nse knx-gateway-discover.nse quake1-info.nse ssh-publickey-acceptance.nse
broadcast-bjnp-discover.nse ftp-bounce.nse http-robtxt-reverse-ip.nse knx-gateway-info.nse quake3-info.nse ssh-run.nse
broadcast-dhcp6-discover.nse ftp-brute.nse http-robtxt-shared-n5.nse krb5-enum-users.nse quake3-master-getservers.nse sshv1.nse
broadcast-dhcp-discover.nse ftp-libopie.nse http-sap-netweaver-leak.nse ldap-brute.nse rdp-enum-encryption.nse ssl-ccs-injection.nse
broadcast-dns-service-discovery.nse ftp-proftpd-backdoor.nse http-security-headers.nse ldap-rootdse.nse rdp-ntlm-info.nse ssl-cert-intaddr.nse
broadcast-dropbox-listener.nse ftp-syst.nse http-shellshock.nse ldap-search.nse rdp-vuln-ms12-020.nse ssl-cert.nse
broadcast-eigrp-discovery.nse ftp-vstftpd-backdoor.nse http-slowloris-check.nse ldap-vuln-ms12-020.nse realvnc-auth-bypass.nse ssl-date.nse
broadcast-hid-discovery.nse ganglia-info.nse http-sql-injection.nse lexmark-config.nse redis-brute.nse ssl-dh-params.nse
broadcast-igmp-discovery.nse giop-info.nse https-redirect.nse lmnrr-resolve.nse redis-info.nse ssl-enum-ciphers.nse
broadcast-jenkins-discover.nse gopher-ls.nse http-svn-enum.nse lmnrr-resolve.nse resolveall.nse ssl-heartbleed.nse
broadcast-listener.nse gopher-ls.nse http-title.nse lmnrr-resolve.nse reverse-index.nse ssl-known-key.nse
broadcast-ms-sql-discover.nse gopher-ls.nse http-tplink-dir-traversal.nse lu-enum.nse rexec-brute.nse ssl-poodle.nse
broadcast-netbios-master-browser.nse gopher-ls.nse http-trace.nse maxdb-info.nse rfc868-time.nse sslv2-drown.nse
broadcast-networker-discover.nse gopher-ls.nse http-traceroute.nse mcafee-epo-agent.nse memcached-info.nse riak-http-info.nse sslv2.nse
broadcast-novell-locate.nse gopher-ls.nse http-trane-info.nse memcached-brute.nse rlogin-brute.nse sstp-discover.nse
broadcast-ospf2-discover.nse gopher-ls.nse http-trane-info.nse metasploit-info.nse rmi-dumpregistry.nse stun-info.nse
broadcast-pc-anywhere.nse gopher-ls.nse http-trane-info.nse metasploit-msgrpc-brute.nse rmi-vuln-classloader.nse stuxnet-detect.nse
broadcast-pc-duo.nse gopher-ls.nse http-trane-info.nse metasploit-xmlrpc-brute.nse rpcap-brute.nse supermicro-ipmi-conf.nse
broadcast-pim-discovery.nse gopher-ls.nse http-trane-info.nse mikrotik-routeros-brute.nse rpcap-info.nse svn-brute.nse
broadcast-ping.nse gopher-ls.nse http-trane-info.nse mmouse-brute.nse mmouse-exec.nse rpcinfo.nse targets-asn.nse
broadcast-pppoe-discover.nse gopher-ls.nse http-trane-info.nse modbus-discover.nse mongodbr-brute.nse rsync-brute.nse targets-ipv6-map4to6.nse
broadcast-rip-discover.nse gopher-ls.nse http-trane-info.nse mongodbr-databases.nse mongodbr-brute.nse rsync-list-modules.nse targets-ipv6-multicast-echo.nse
broadcast-ripng-discover.nse gopher-ls.nse http-trane-info.nse mongodbr-info.nse mqtt-subscribe.nse rtsp-methods.nse targets-ipv6-multicast-invalid-dst.nse
broadcast-sonicwall-discover.nse gopher-ls.nse http-trane-info.nse mrtinfo.nse rtsp-url-brute.nse targets-ipv6-multicast-mld.nse
broadcast-sybase-asa-discover.nse gopher-ls.nse http-trane-info.nse mrtinfo.nse targets-ipv6-multicast-slaac.nse
```


Nmap Advanced Scripts Explain

Nmap Scripts Use

`nmap --script=SCRIPT + $ ip`

Ex : `nmap --script=vuln 192.168.1.1`

Nmap Scripts Reverse 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
```

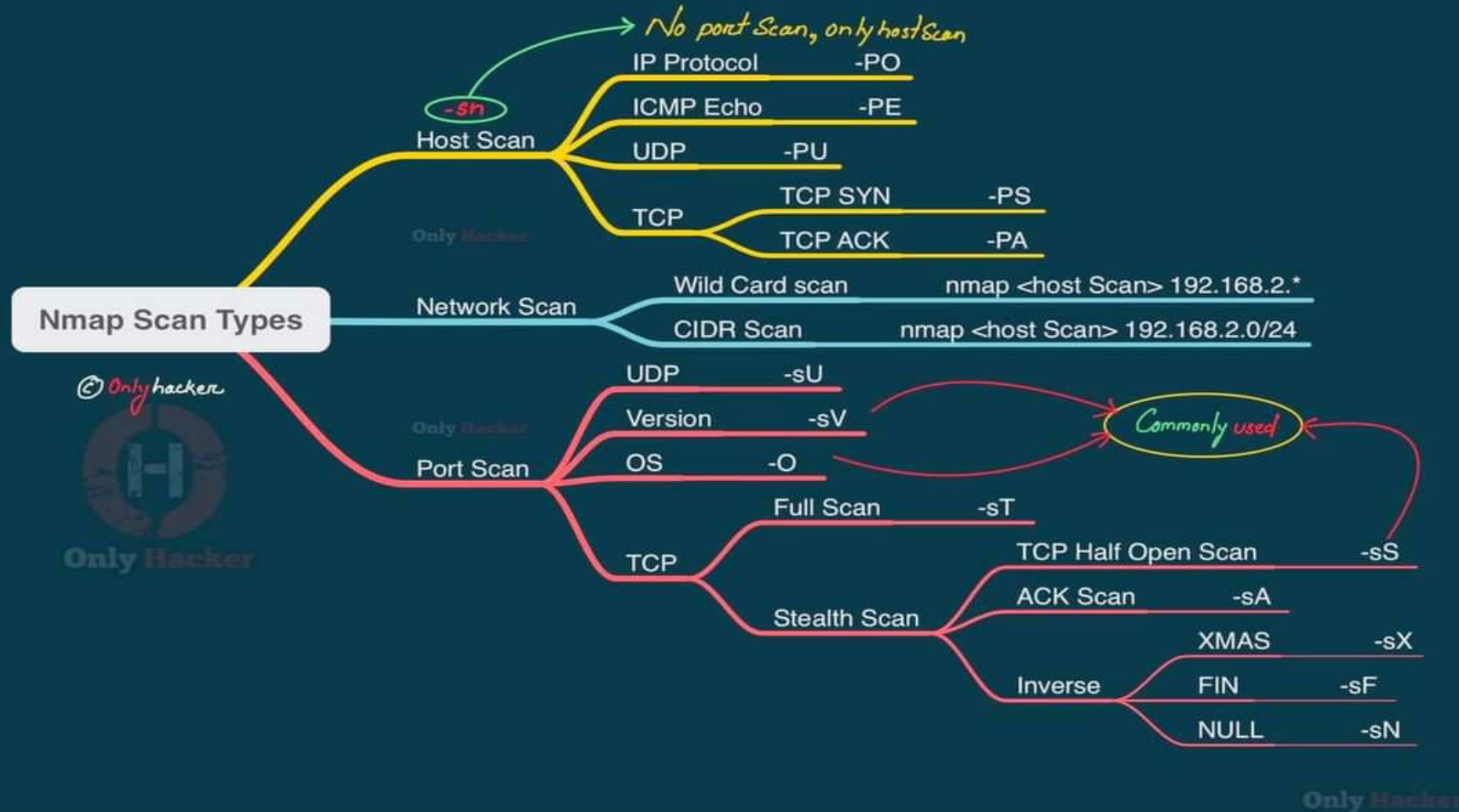
```
nmap 192.168.1.1 -oX m3lomat
```

Save To Some File Formats >> NAME.format

```
nmap + $ip >> NAME.fileformat
```

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


Nmap Advanced Options To Scanning



| 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>