Lab 4 – Network Mapping

Shrutika Joshi

University of Maryland Baltimore County

Presented To – Ian Coston

Date – 30th SEP 2023

Introduction

In this lab, get familiar with network scanning techniques using Nmap.

Pre-Lab

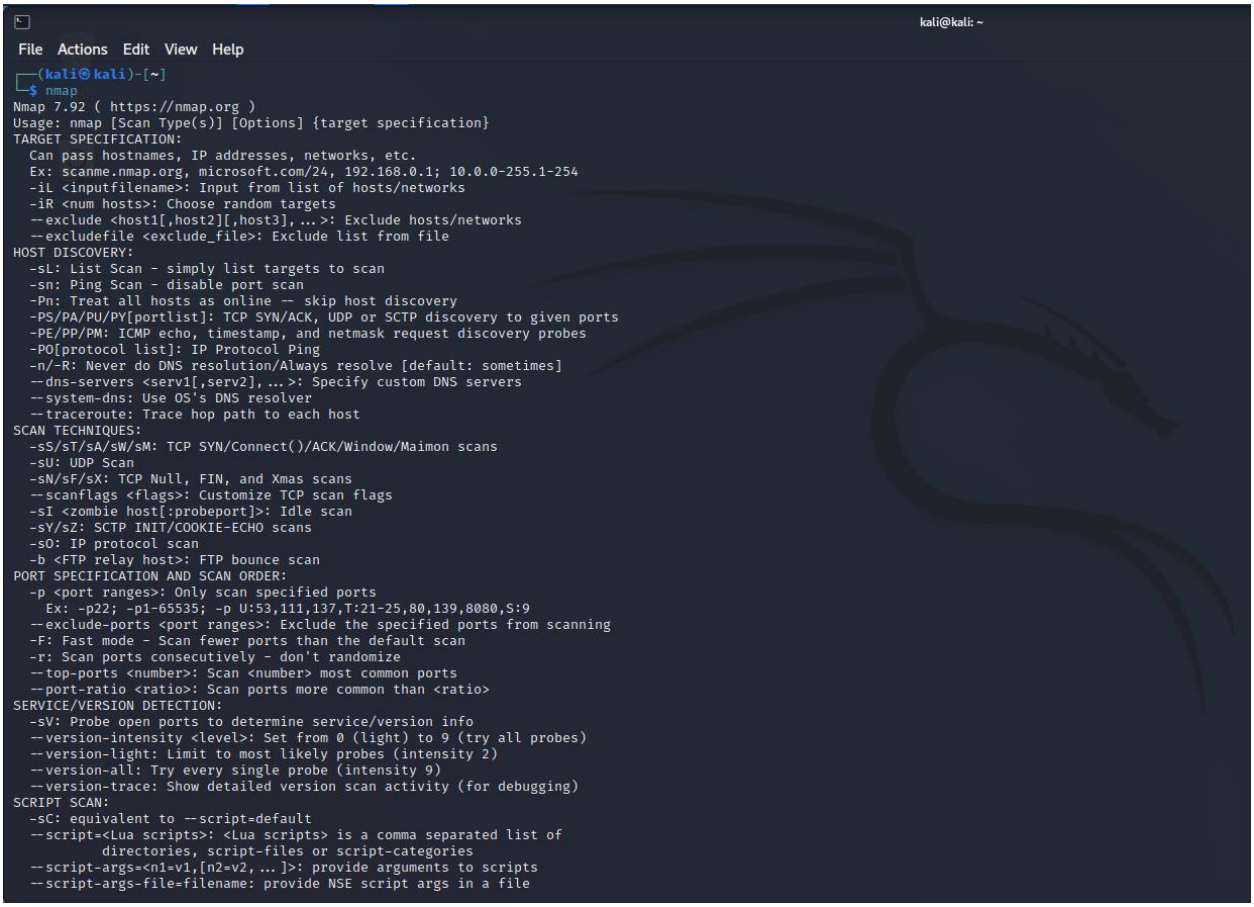
For this lab, you will require Kali Linux and Windows machines,

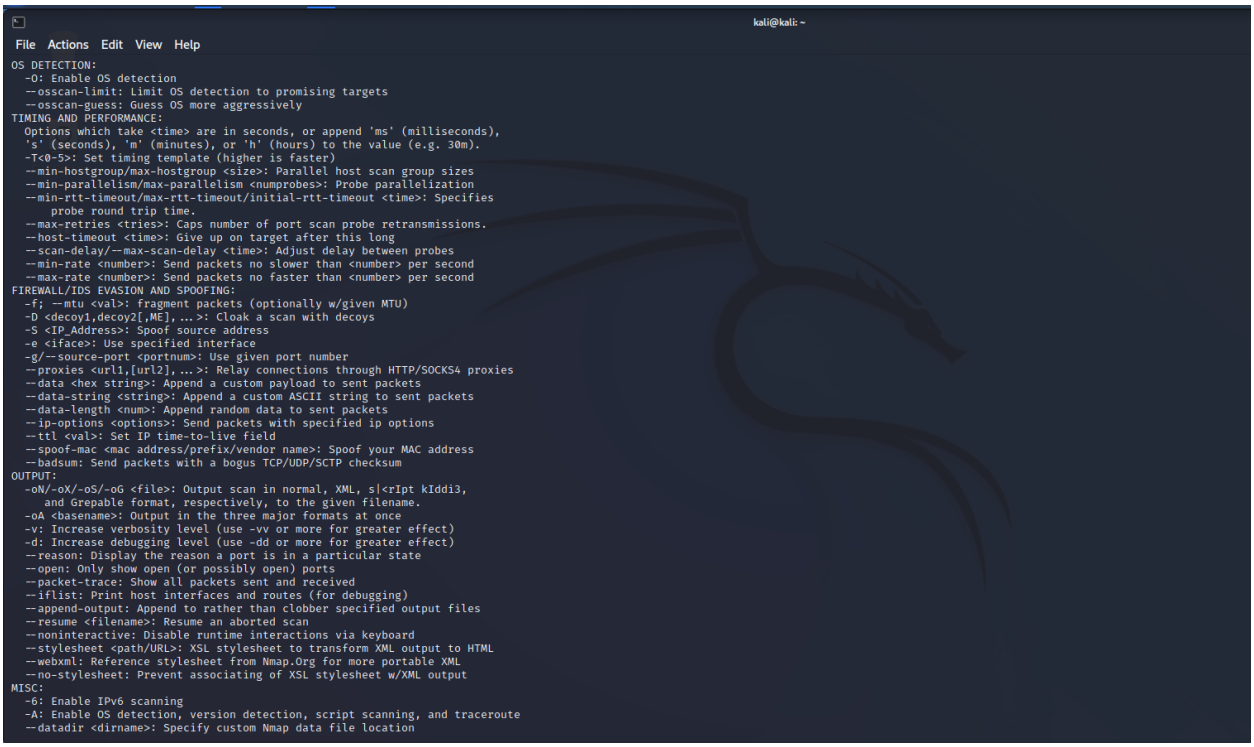
Practical

1. NMAP

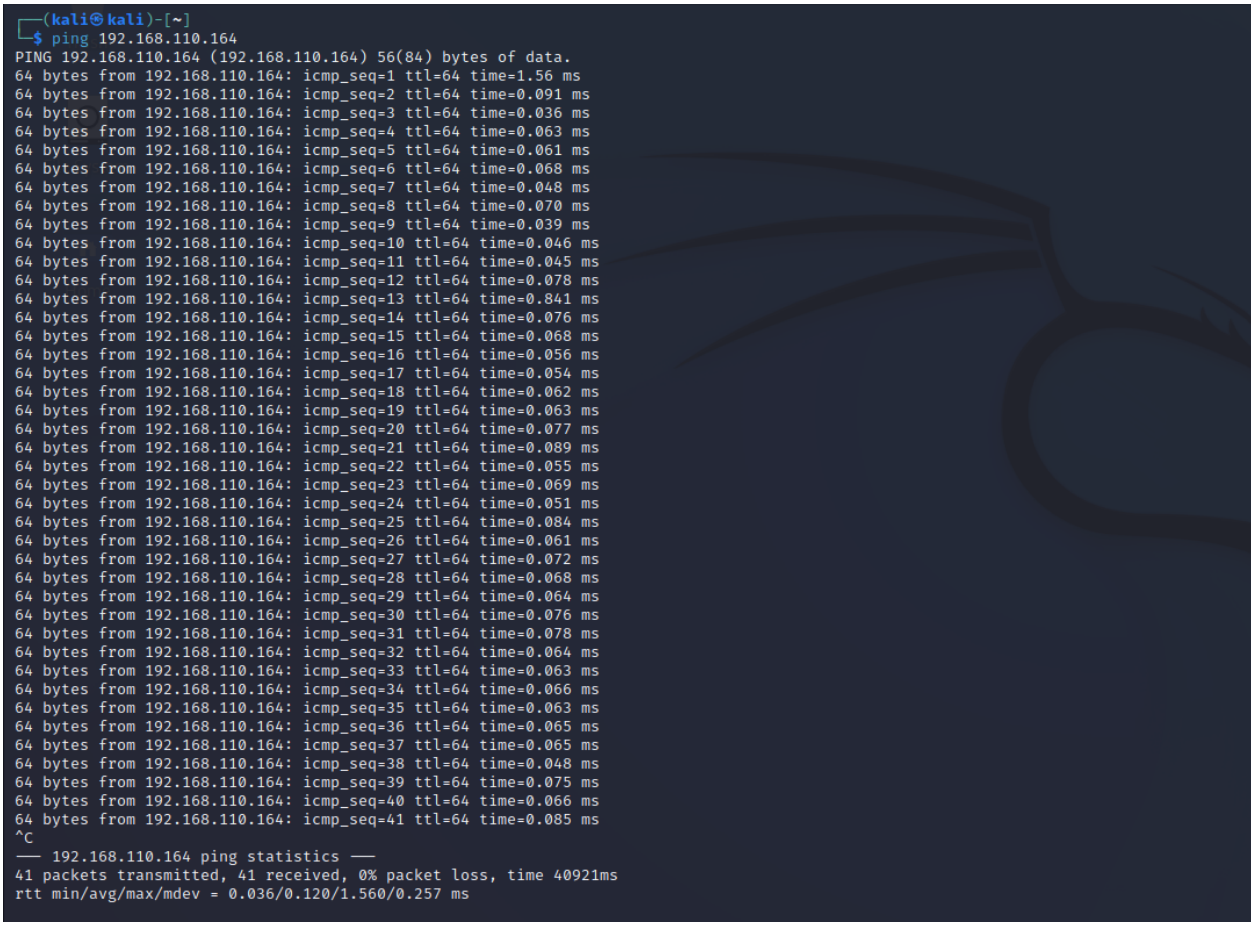
Open a linux terminal. Simply type “nmap” and take note of the syntax and available options

Perform a simple ping scan of your Kali VM (via localhost address or IP address) and note


kali@kali: ~
File Actions Edit View Help
┌──(kali㉿kali)-[~]
└─$ nmap
Nmap 7.92 (https://nmap.org)
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
Can pass hostnames, IP addresses, networks, etc.
Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
-iL <inputfilename>: Input from list of hosts/networks
-iR <num hosts>: Choose random targets
--exclude <host1[,host2][,host3],...>: Exclude hosts/networks
--excludefile <exclude_file>: 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 discovery to given ports
-PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
-PO[protocol list]: IP Protocol Ping
-n/-R: Never do DNS resolution/Always resolve [default: sometimes]
--dns-servers <serv1[,serv2],...>: 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 <flags>: Customize TCP scan flags
-sI <zombie host[:probeport]>: Idle scan
-sY/sZ: SCTP INIT/COOKIE-ECHO scans
-sO: IP protocol scan
-b <FTP relay host>: FTP bounce scan
PORT SPECIFICATION AND SCAN ORDER:
-p <port ranges>: Only scan specified ports
Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080,S:9
--exclude-ports <port ranges>: Exclude the specified ports from scanning
-F: Fast mode - Scan fewer ports than the default scan
-r: Scan ports consecutively - don't randomize
--top-ports <number>: Scan <number> most common ports
--port-ratio <ratio>: Scan ports more common than <ratio>
SERVICE/VERSION DETECTION:
-sV: Probe open ports to determine service/version info
--version-intensity <level>: 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 (for debugging)
SCRIPT SCAN:
-sC: equivalent to --script=default
--script=<Lua scripts>: <Lua scripts> is a comma separated list of
directories, script-files or script-categories
--script-args=<n1=v1,[n2=v2,...]>: provide arguments to scripts
--script-args-file=filename: provide NSE script args in a file

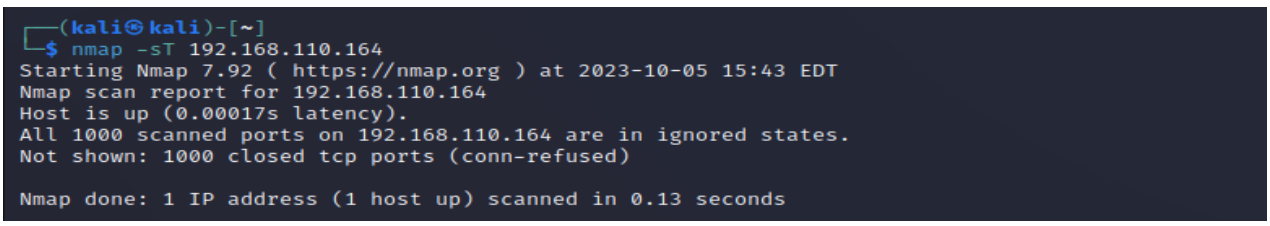

kali@kali: ~
File Actions Edit View Help
OS DETECTION:
-O: Enable OS detection
--osscan-limit: Limit OS detection to promising targets
--osscan-guess: Guess OS more aggressively
TIMING AND PERFORMANCE:
Options which take <time> are in seconds, or append 'ms' (milliseconds),
's' (seconds), 'm' (minutes), or 'h' (hours) to the value (e.g. 30m).
-T<0-5>: Set timing template (higher is faster)
--min-hostgroup/max-hostgroup <size>: Parallel host scan group sizes
--min-parallelism/max-parallelism <numprobes>: Probe parallelization
--min-rtt-timeout/max-rtt-timeout/initial-rtt-timeout <time>: Specifies
probe round trip time.
--max-retries <tries>: Caps number of port scan probe retransmissions.
--host-timeout <time>: Give up on target after this long
--scan-delay/--max-scan-delay <time>: Adjust delay between probes
--min-rate <number>: Send packets no slower than <number> per second
--max-rate <number>: Send packets no faster than <number> per second
FIREWALL/IDS EVASION AND SPOOFING:
-f; --mtu <val>: fragment packets (optionally w/given MTU)
-D <decoy1,decoy2[,ME],...>: Cloak a scan with decoys
-S <IP_Address>: Spoof source address
-e <iface>: Use specified interface
-g/--source-port <portnum>: Use given port number
--proxies <url1,[url2],...>: Relay connections through HTTP/SOCKS4 proxies
--data <hex string>: Append a custom payload to sent packets
--data-string <string>: Append a custom ASCII string to sent packets
--data-length <num>: Append random data to sent packets
--ip-options <options>: Send packets with specified ip options
--ttl <val>: Set IP time-to-live field
--spoof-mac <mac address/prefix/vendor name>: Spoof your MAC address
--badsum: Send packets with a bogus TCP/UDP/SCTP checksum
OUTPUT:
-oN/-oX/-oS/-oG <file>: Output scan in normal, XML, s|<rIpt kIdd3,
and Grepable format, respectively, to the given filename.
-oA <basename>: 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)
--append-output: Append to rather than clobber specified output files
--resume <filename>: Resume an aborted scan
--noninteractive: Disable runtime interactions via keyboard
--stylesheet <path/URL>: XSL stylesheet to transform XML output to HTML
--webxml: Reference stylesheet from Nmap.Org for more portable XML
--no-stylesheet: Prevent associating of XSL stylesheet w/XML output
MISC:
-6: Enable IPv6 scanning
-A: Enable OS detection, version detection, script scanning, and traceroute
--datadir <dirname>: Specify custom Nmap data file location

Perform a simple ping scan of your Kali VM (via localhost address or IP address) and note what information you get back.



Perform a TCP Connect scan of your Kali VM (via localhost address or IP address) and note what information you get back.

- To perform a TCP connect scan use flag –sT



Perform a TCP Connect scan with version identification of your Kali VM (via localhost address or IP address) and note what information do you get back?

- To perform a TCP connect scan use flag –sT and –sV for version identification

```
┌──(kali㉿kali)-[~]
└─$ nmap -sT -sV 192.168.110.164
Starting Nmap 7.92 ( https://nmap.org ) at 2023-10-05 15:46 EDT
Nmap scan report for 192.168.110.164
Host is up (0.00022s latency).
All 1000 scanned ports on 192.168.110.164 are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.82 seconds
```

Perform an Aggressive TCP Connect scan across the entire virtual network range and note the results.

- To perform an aggresive TCP connect scan use flag –sT and –A enable aggressive scan and select entire subnet range to scan.

```
kali@kali: ~
File  Actions  Edit  View  Help

┌──(kali㉿kali)-[~]
└─$ nmap -sT -A 192.168.110.164/24
Starting Nmap 7.92 ( https://nmap.org ) at 2023-10-05 15:54 EDT
Nmap scan report for 192.168.110.2
Host is up (0.00019s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
53/tcp open  domain  (unknown banner: [SECURED])
| dns-nsid:
|   NSID: alex-cns20 (616c65782d636e733230)
|   id.server: alex-cns20
|_  bind.version: [SECURED]
| fingerprint-strings:
|   DNSVersionBindReqTCP:
|     version
|     bind
|_    [SECURED]
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port53-TCP:V=7.92%I=7%D=10/5%Time=651F14A2%P=x86_64-pc-linux-gnu%r(DNSV
SF:ersionBindReqTCP,36,"\x004\0\x06\x81\x80\0\x01\0\x01\0\0\0\0\x07version
SF:\x04bind\0\0\x10\0\x03\xc0\x0c\0\x10\0\x03\0\0\0\0\n\t\[SECURED\]");

Nmap scan report for 192.168.110.163
Host is up (0.00028s latency).
Not shown: 987 closed tcp ports (conn-refused)
PORT      STATE SERVICE            VERSION
135/tcp   open  msrpc              Microsoft Windows RPC
139/tcp   open  netbios-ssn        Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds       Windows 7 Enterprise 7600 microsoft-ds (workgroup: WORKGROUP)
554/tcp   open  rtsp?
2869/tcp  open  http               Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
3389/tcp  open  ssl/ms-wbt-server?
|_ssl-date: 2023-10-05T19:57:59+00:00; 0s from scanner time.
| ssl-cert: Subject: commonName=WIN-1O5VFTJ7ISE
| Not valid before: 2023-09-06T18:52:16
|_Not valid after:  2024-03-07T18:52:16
10243/tcp open  http               Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
49152/tcp open  msrpc              Microsoft Windows RPC
49153/tcp open  msrpc              Microsoft Windows RPC
49154/tcp open  msrpc              Microsoft Windows RPC
49155/tcp open  msrpc              Microsoft Windows RPC
49156/tcp open  msrpc              Microsoft Windows RPC
49157/tcp open  msrpc              Microsoft Windows RPC
Service Info: Host: WIN-1O5VFTJ7ISE; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb-security-mode:
|   account_used: guest
```


kali@kali: ~
File Actions Edit View Help
Host script results:
| smb-security-mode:
| account_used: guest
| authentication_level: user
| challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
|_clock-skew: mean: 1h00m00s, deviation: 2h00m01s, median: 0s
| smb-os-discovery:
| OS: Windows 7 Enterprise 7600 (Windows 7 Enterprise 6.1)
| OS CPE: cpe:/o:microsoft:windows_7::-
| Computer name: WIN-1O5VFTJ7ISE
| NetBIOS computer name: WIN-1O5VFTJ7ISE\x00
| Workgroup: WORKGROUP\x00
|_ System time: 2023-10-05T15:56:56-04:00
|_nbstat: NetBIOS name: WIN-1O5VFTJ7ISE, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:98:65:fd (VMware)
| smb2-time:
| date: 2023-10-05T19:56:56
|_ start_date: 2023-10-02T14:42:26
| smb2-security-mode:
| 2.1:
|_ Message signing enabled but not required
Nmap scan report for 192.168.110.164
Host is up (0.000047s latency).
All 1000 scanned ports on 192.168.110.164 are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)
Nmap scan report for 192.168.110.165
Host is up (0.00026s latency).
Not shown: 992 closed tcp ports (conn-refused)
PORT STATE SERVICE VERSION
21/tcp open ftp Microsoft ftpd
| ftp-syst:
| SYST: Windows_NT
| STAT:
| Microsoft FTP Service status:
| Connected to 192.168.110.164
| Logged in as IEUser@
| TYPE: ASCII, FORM: Nonprint; STRUcture: File; transfer MODE: STREAM
| No data connection
|_End of status.
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
25/tcp open smtp Microsoft ESMTP 6.0.2600.2180
| smtp-commands: win-xp Hello [192.168.110.164], SIZE 2097152, PIPELINING, DSN, ENHANCEDSTATUSCODES, 8bitmime, BINARYMIME, CHUNKING, VRFY, OK
|_ This server supports the following commands: HELO EHLO STARTTLS RCPT DATA RSET MAIL QUIT HELP AUTH BDAT VRFY
80/tcp open http Microsoft IIS httpd 5.1
| http-webdav-scan:
| Allowed Methods: OPTIONS, TRACE, GET, HEAD, COPY, PROPFIND, SEARCH, LOCK, UNLOCK
| Server Type: Microsoft-IIS/5.1
| Server Date: Thu, 05 Oct 2023 19:56:56 GMT


kali@kali: ~
File Actions Edit View Help
| Allowed Methods: OPTIONS, TRACE, GET, HEAD, COPY, PROPFIND, SEARCH, LOCK, UNLOCK
| Server Type: Microsoft-IIS/5.1
| Server Date: Thu, 05 Oct 2023 19:56:56 GMT
| WebDAV type: Unknown
|_ Public Options: OPTIONS, TRACE, GET, HEAD, DELETE, PUT, POST, COPY, MOVE, MKCOL, PROPFIND, PROPPATCH, LOCK, UNLOCK, SEARCH
| http-methods:
|_ Potentially risky methods: TRACE COPY PROPFIND SEARCH LOCK UNLOCK DELETE PUT MOVE MKCOL PROPPATCH
| http-title:
| title: \x0D
|_\x0D
|_http-server-header: Microsoft-IIS/5.1
135/tcp open msrpc Microsoft Windows RPC
139/tcp open netbios-ssn Microsoft Windows netbios-ssn
443/tcp open https?
445/tcp open microsoft-ds Windows XP microsoft-ds
1025/tcp open msrpc Microsoft Windows RPC
Service Info: Host: win-xp; OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp
Host script results:
|_smb2-time: Protocol negotiation failed (SMB2)
| ms-sql-info:
| Windows server name: WIN-XP
| 192.168.110.165\SQLEXPRESS:
| Instance name: SQLEXPRESS
| Version:
| name: Microsoft SQL Server 2005 RTM
| Product: Microsoft SQL Server 2005
| Service pack level: RTM
| TCP port: 1433
|_ Clustered: false
|_clock-skew: mean: 2h00m00s, deviation: 2h49m43s, median: 0s
| smb-security-mode:
| account_used: guest
| authentication_level: user
| challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
| smb-os-discovery:
| OS: Windows XP (Windows 2000 LAN Manager)
| OS CPE: cpe:/o:microsoft:windows_xp::-
| Computer name: win-xp
| NetBIOS computer name: WIN-XP\x00
| Workgroup: WORKGROUP\x00
|_ System time: 2023-10-05T15:56:55-04:00
|_nbstat: NetBIOS name: WIN-XP, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:90:64:48 (VMware)
Post-scan script results:
| clock-skew:
| 1h00m00s:
| 192.168.110.163
|_ 192.168.110.165
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Perform a Paranoid TCP SYN scan against a specific target.

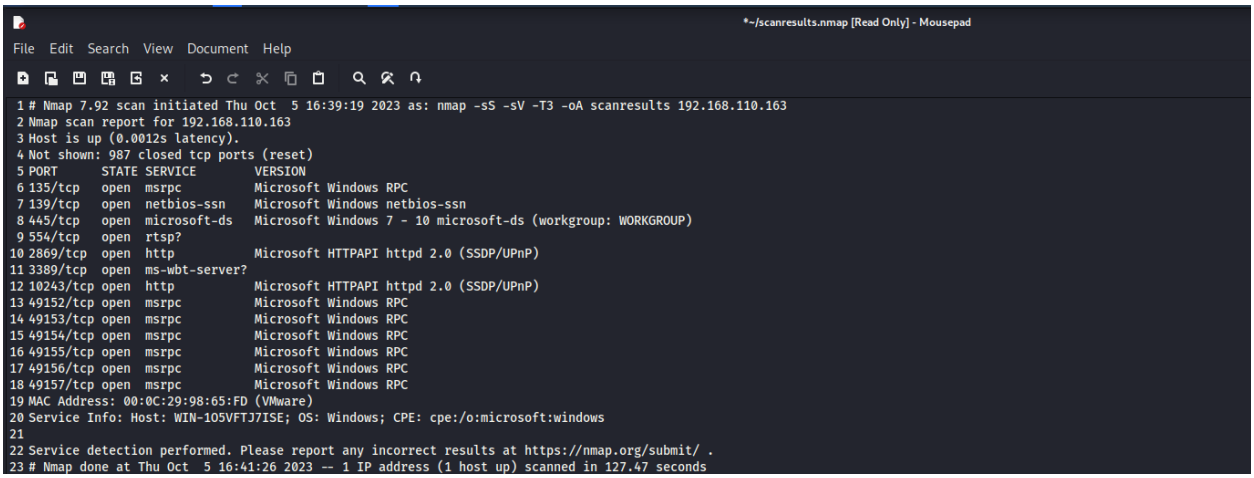
- To perform paranoid TCP SYN scan use flag –sS and –T0 for selecting paranoid scan. This makes the scan slower having longer delays between packets to avoid detection by IDS or IPS or any security devices.

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS -T0 192.168.110.163
[sudo] password for kali:
Starting Nmap 7.92 ( https://nmap.org ) at 2023-10-05 16:17 EDT
```

Perform a Normal TCP SYN scan with version identification on a specific target and output to a file

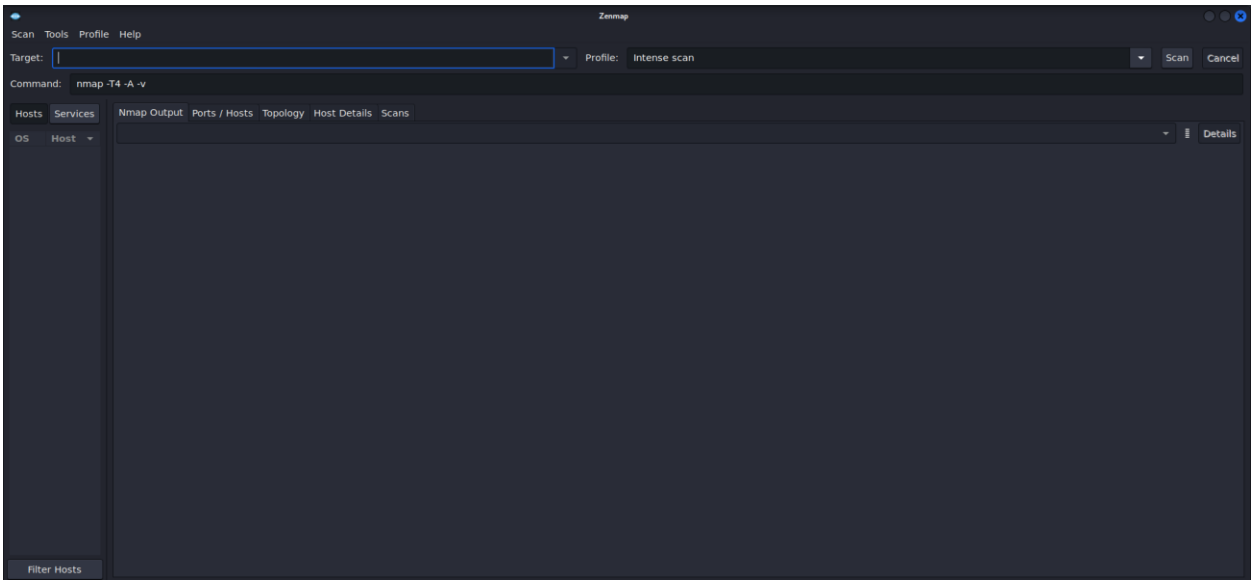
- To perform a normal TCP scan with version identification use flag –sS and –sV. Use -T3 to set the scan speed to normal. –oA scanresult_filename use to output result into file. Three files gets created using this flag –
    - a plain text file (scanresult _filename.nmap),
    - an XML file (scanresult_filename.xml), and a grepable file
    - (scanresult_filename.gnmap)

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS -sV -T3 -oA scanresults 192.168.110.163
[sudo] password for kali:
Starting Nmap 7.92 ( https://nmap.org ) at 2023-10-05 16:39 EDT
Nmap scan report for 192.168.110.163
Host is up (0.0012s latency).
Not shown: 987 closed tcp ports (reset)
PORT      STATE SERVICE       VERSION
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds  Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
554/tcp   open  rtsp?
2869/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
3389/tcp  open  ms-wbt-server?
10243/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49152/tcp open  msrpc         Microsoft Windows RPC
49153/tcp open  msrpc         Microsoft Windows RPC
49154/tcp open  msrpc         Microsoft Windows RPC
49155/tcp open  msrpc         Microsoft Windows RPC
49156/tcp open  msrpc         Microsoft Windows RPC
49157/tcp open  msrpc         Microsoft Windows RPC
MAC Address: 00:0C:29:98:65:FD (VMware)
Service Info: Host: WIN-1O5VFTJ7ISE; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 127.47 seconds

┌──(kali㉿kali)-[~]
└─$ ls
armitage-tmp  Desktop  Documents  Downloads  Music  Pictures  Public  scanresults.gnmap  scanresults.nmap  scanresults.xml  Templates  Videos
```



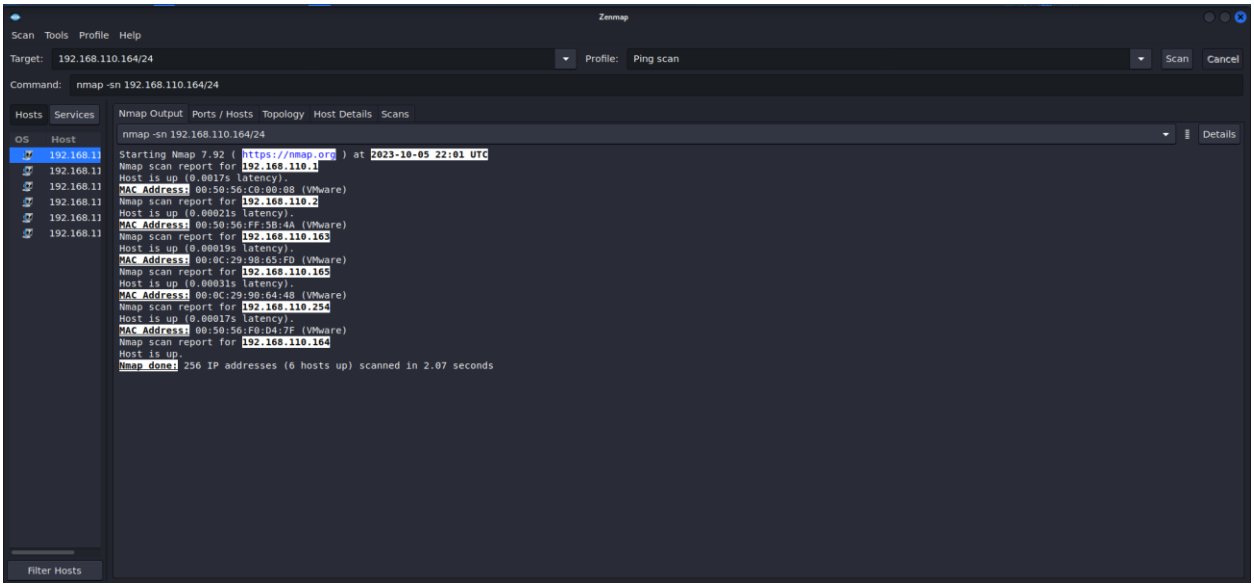
2. Zenmap

Open ZenMap and in the target window, type in the network address of the virtual network on your system.



In the Profile drop-down, select Ping scan. Note the “Command” shown. Press the “Scan” button. Take note of the results

Command - nmap -sn 192.168.110.164/24



Perform a slow comprehensive scan on a select target. As with the Ping scan, note the "Command" shown. Take note of the results and the time it takes to get them

Command - nmap -sS -sU -T4 -A -v -PE -PP -PS80,443 -PA3389 -PU40125 -PY -g 53 --script "default or (discovery and safe)" 192.168.110.164/24

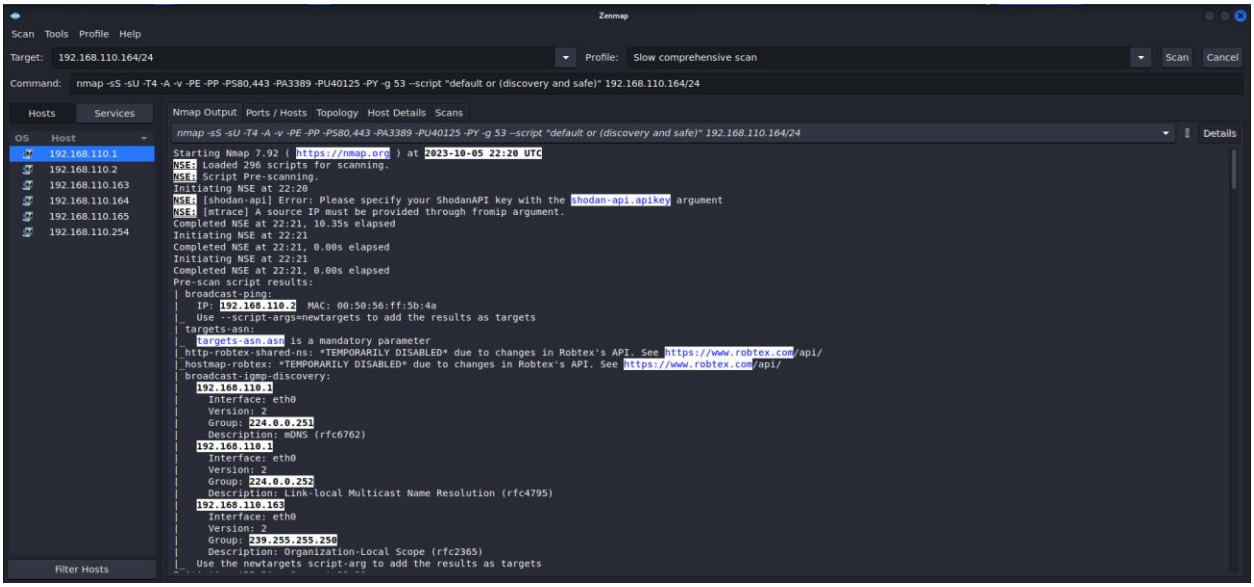
-sU is used for UDP scan

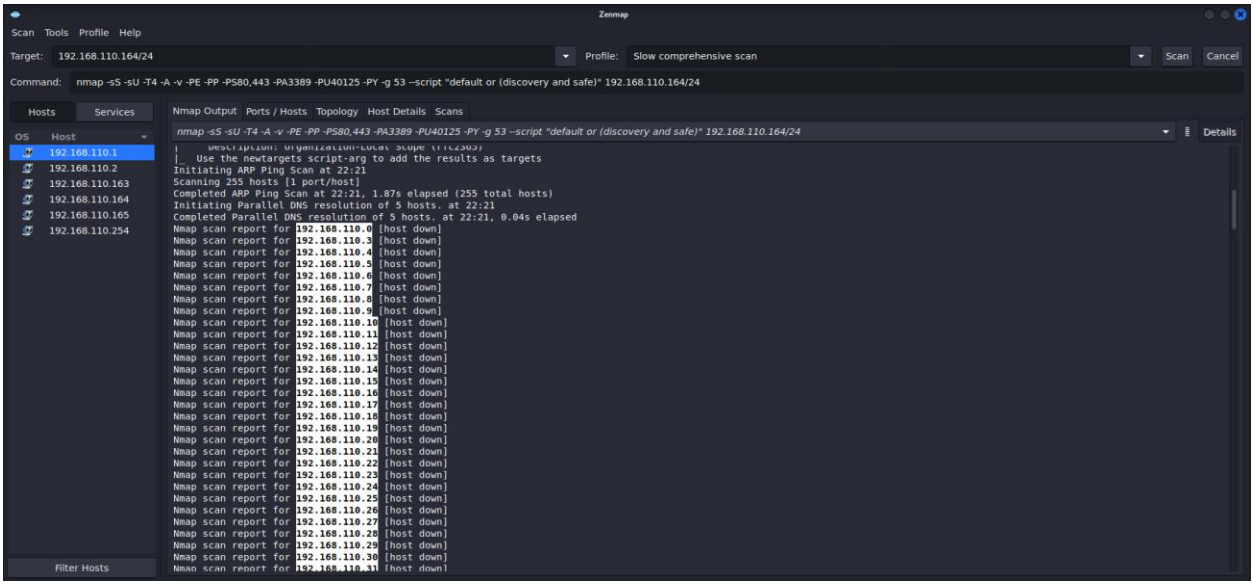
- T4 sets the timing template to an aggressive scan

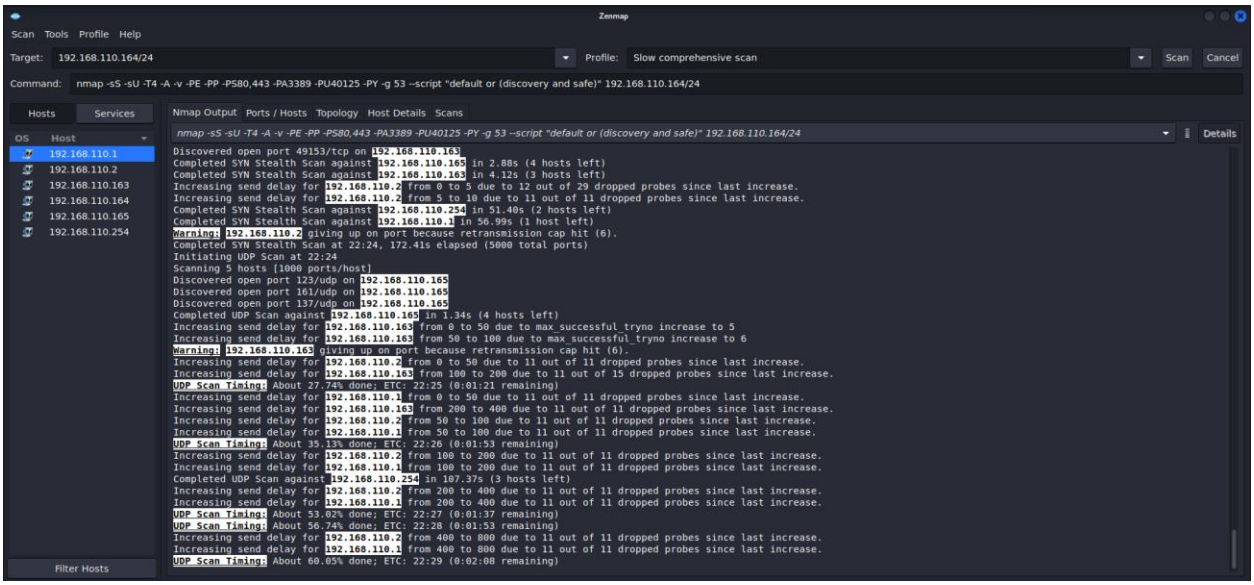
-PE -PP -PS80,443 -PA3389 -PU40125 –PY is controls how how nmap send packets to check if host is up or not.

-g 53 specifies a source port

--script enables Nmap script engine.

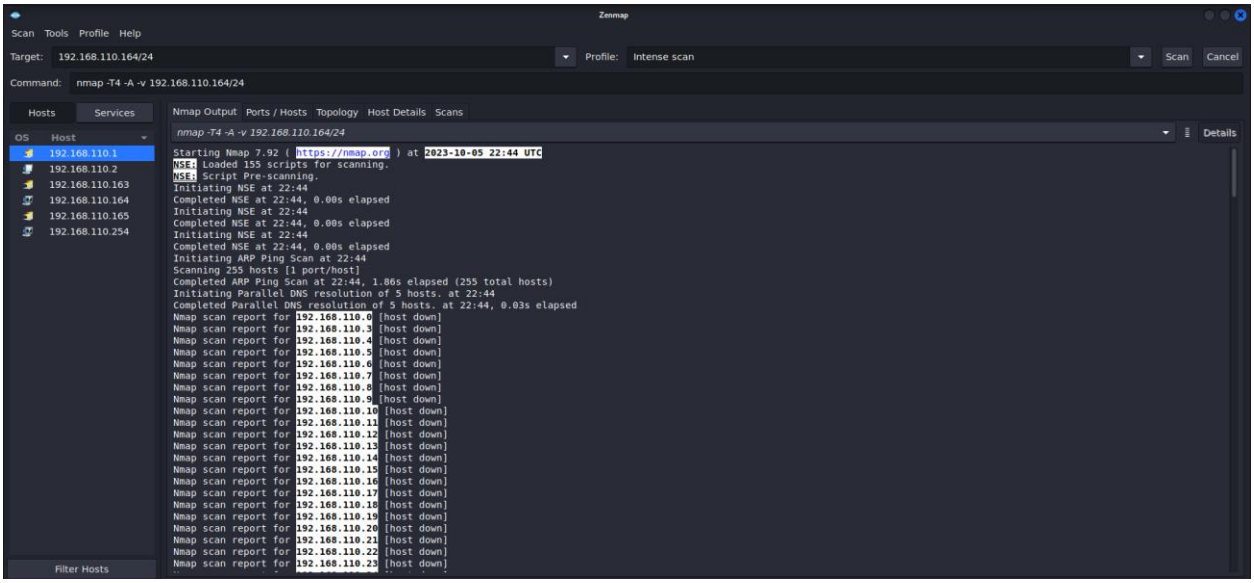

Zenmap
Scan Tools Profile Help
Target: 192.168.110.164/24
Profile: Slow comprehensive scan
Scan Cancel
Command: nmap -sS -sU -T4 -A -v -PE -PP -PS80,443 -PA3389 -PU40125 -PY -g 53 --script "default or (discovery and safe)" 192.168.110.164/24
Hosts Services
OS Host
192.168.110.1
192.168.110.2
192.168.110.163
192.168.110.164
192.168.110.165
192.168.110.254
Filter Hosts
Nmap Output Ports / Hosts Topology Host Details Scans
nmap -sS -sU -T4 -A -v -PE -PP -PS80,443 -PA3389 -PU40125 -PY -g 53 --script "default or (discovery and safe)" 192.168.110.164/24
Details
Starting Nmap 7.92 (https://nmap.org) at 2023-10-05 22:20 UTC
NSE: Loaded 296 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 22:20
NSE: [shodan-api] Error: Please specify your ShodanAPI key with the shodan-api.apikey argument
NSE: [mtrace] A source IP must be provided through fromip argument.
Completed NSE at 22:21, 10.35s elapsed
Initiating NSE at 22:21
Completed NSE at 22:21, 0.00s elapsed
Initiating NSE at 22:21
Completed NSE at 22:21, 0.00s elapsed
Pre-scan script results:
| broadcast-ping:
| IP: 192.168.110.2 MAC: 00:50:56:ff:5b:4a
|_ Use --script-args=newtargets to add the results as targets
| targets-asn:
|_ targets-asn.asn is a mandatory parameter
|_http-robtex-shared-ns: *TEMPORARILY DISABLED* due to changes in Robtex's API. See https://www.robtex.com/api/
|_hostmap-robtex: *TEMPORARILY DISABLED* due to changes in Robtex's API. See https://www.robtex.com/api/
| broadcast-igmp-discovery:
| 192.168.110.1
| Interface: eth0
| Version: 2
| Group: 224.0.0.251
| Description: mDNS (rfc6762)
| 192.168.110.1
| Interface: eth0
| Version: 2
| Group: 224.0.0.252
| Description: Link-local Multicast Name Resolution (rfc4795)
| 192.168.110.163
| Interface: eth0
| Version: 2
| Group: 239.255.255.250
| Description: Organization-Local Scope (rfc2365)
|_ Use the newtargets script-arg to add the results as targets

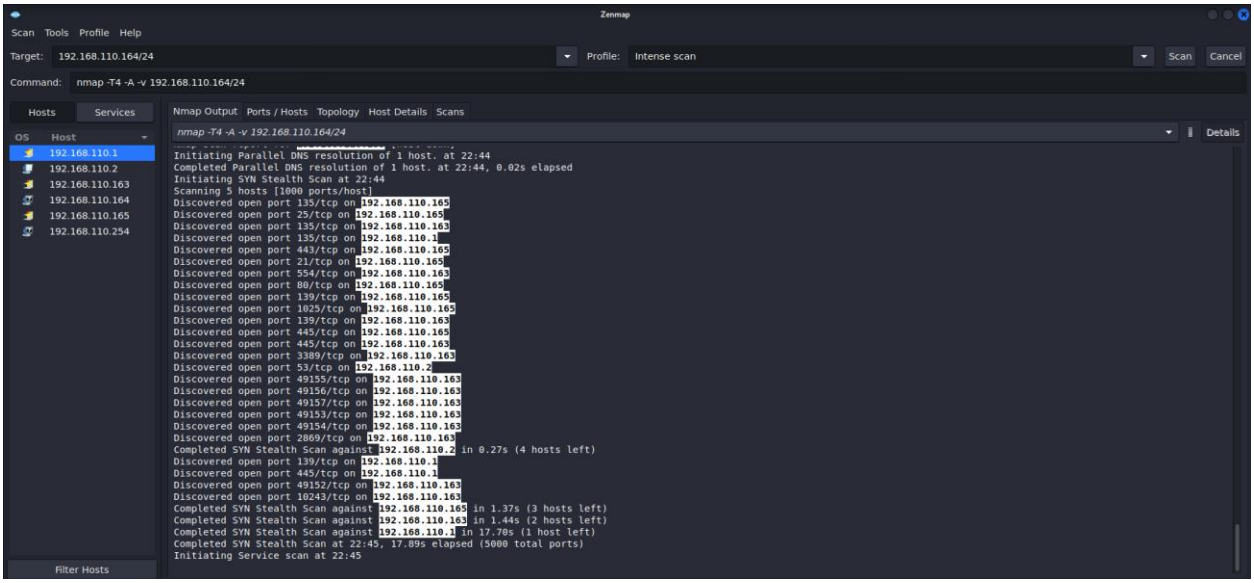

Zenmap
Scan Tools Profile Help
Target: 192.168.110.164/24
Profile: Slow comprehensive scan
Scan Cancel
Command: nmap -sS -sU -T4 -A -v -PE -PP -PS80,443 -PA3389 -PU40125 -PY -g 53 --script "default or (discovery and safe)" 192.168.110.164/24
Hosts Services
OS Host
192.168.110.1
192.168.110.2
192.168.110.163
192.168.110.164
192.168.110.165
192.168.110.254
Filter Hosts
Nmap Output Ports / Hosts Topology Host Details Scans
nmap -sS -sU -T4 -A -v -PE -PP -PS80,443 -PA3389 -PU40125 -PY -g 53 --script "default or (discovery and safe)" 192.168.110.164/24
Details
|_ Use the newtargets script-arg to add the results as targets
Initiating ARP Ping Scan at 22:21
Scanning 255 hosts [1 port/host]
Completed ARP Ping Scan at 22:21, 1.87s elapsed (255 total hosts)
Initiating Parallel DNS resolution of 5 hosts. at 22:21
Completed Parallel DNS resolution of 5 hosts. at 22:21, 0.04s elapsed
Nmap scan report for 192.168.110.0 [host down]
Nmap scan report for 192.168.110.3 [host down]
Nmap scan report for 192.168.110.4 [host down]
Nmap scan report for 192.168.110.5 [host down]
Nmap scan report for 192.168.110.6 [host down]
Nmap scan report for 192.168.110.7 [host down]
Nmap scan report for 192.168.110.8 [host down]
Nmap scan report for 192.168.110.9 [host down]
Nmap scan report for 192.168.110.10 [host down]
Nmap scan report for 192.168.110.11 [host down]
Nmap scan report for 192.168.110.12 [host down]
Nmap scan report for 192.168.110.13 [host down]
Nmap scan report for 192.168.110.14 [host down]
Nmap scan report for 192.168.110.15 [host down]
Nmap scan report for 192.168.110.16 [host down]
Nmap scan report for 192.168.110.17 [host down]
Nmap scan report for 192.168.110.18 [host down]
Nmap scan report for 192.168.110.19 [host down]
Nmap scan report for 192.168.110.20 [host down]
Nmap scan report for 192.168.110.21 [host down]
Nmap scan report for 192.168.110.22 [host down]
Nmap scan report for 192.168.110.23 [host down]
Nmap scan report for 192.168.110.24 [host down]
Nmap scan report for 192.168.110.25 [host down]
Nmap scan report for 192.168.110.26 [host down]
Nmap scan report for 192.168.110.27 [host down]
Nmap scan report for 192.168.110.28 [host down]
Nmap scan report for 192.168.110.29 [host down]
Nmap scan report for 192.168.110.30 [host down]



Perform an intense scan on the same target you selected above. As with the previous scans, note the “Command” shown. Take note of the results and the time it takes to get them

Command use - nmap -T4 -A -v 192.168.110.164/24




Zenmap
Scan Tools Profile Help
Target: 192.168.110.164/24
Profile: Intense scan
Scan
Cancel
Command: nmap -T4 -A -v 192.168.110.164/24
Hosts
Services
OS Host
192.168.110.1
192.168.110.2
192.168.110.163
192.168.110.164
192.168.110.165
192.168.110.254
Filter Hosts
Nmap Output Ports / Hosts Topology Host Details Scans
nmap -T4 -A -v 192.168.110.164/24
Details
Initiating Parallel DNS resolution of 1 host. at 22:44
Completed Parallel DNS resolution of 1 host. at 22:44, 0.02s elapsed
Initiating SYN Stealth Scan at 22:44
Scanning 5 hosts [1000 ports/host]
Discovered open port 135/tcp on 192.168.110.165
Discovered open port 25/tcp on 192.168.110.165
Discovered open port 135/tcp on 192.168.110.163
Discovered open port 135/tcp on 192.168.110.1
Discovered open port 443/tcp on 192.168.110.165
Discovered open port 21/tcp on 192.168.110.165
Discovered open port 554/tcp on 192.168.110.163
Discovered open port 80/tcp on 192.168.110.165
Discovered open port 139/tcp on 192.168.110.165
Discovered open port 1025/tcp on 192.168.110.165
Discovered open port 139/tcp on 192.168.110.163
Discovered open port 445/tcp on 192.168.110.165
Discovered open port 445/tcp on 192.168.110.163
Discovered open port 3389/tcp on 192.168.110.163
Discovered open port 53/tcp on 192.168.110.2
Discovered open port 49155/tcp on 192.168.110.163
Discovered open port 49156/tcp on 192.168.110.163
Discovered open port 49157/tcp on 192.168.110.163
Discovered open port 49153/tcp on 192.168.110.163
Discovered open port 49154/tcp on 192.168.110.163
Discovered open port 2869/tcp on 192.168.110.163
Completed SYN Stealth Scan against 192.168.110.2 in 0.27s (4 hosts left)
Discovered open port 139/tcp on 192.168.110.1
Discovered open port 445/tcp on 192.168.110.1
Discovered open port 49152/tcp on 192.168.110.163
Discovered open port 10243/tcp on 192.168.110.163
Completed SYN Stealth Scan against 192.168.110.165 in 1.37s (3 hosts left)
Completed SYN Stealth Scan against 192.168.110.163 in 1.44s (2 hosts left)
Completed SYN Stealth Scan against 192.168.110.1 in 17.70s (1 host left)
Completed SYN Stealth Scan at 22:45, 17.89s elapsed (5000 total ports)
Initiating Service scan at 22:45