NMAP

Basic scan, options, scripts and hacking

Loi Liang Yang

Certified Information Systems Security Professional

Certified Ethical Hacker

CompTIA Security+

Banner Grabbing

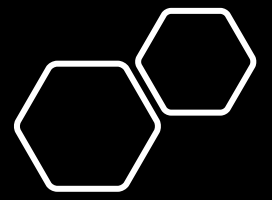
- **Banner grabbing** is a technique used to gain information about a computer system on a network and the services running on its open ports. Administrators can use this to take inventory of the systems and services on their network. However, an intruder can use banner grabbing in order to find network hosts that are running versions of applications and operating systems with known exploits.

```
loiliangyang@loiliangyang:~$ echo "" | nc -v -n -w1 192.168.1.85 21
(UNKNOWN) [192.168.1.85] 21 (ftp) open
```

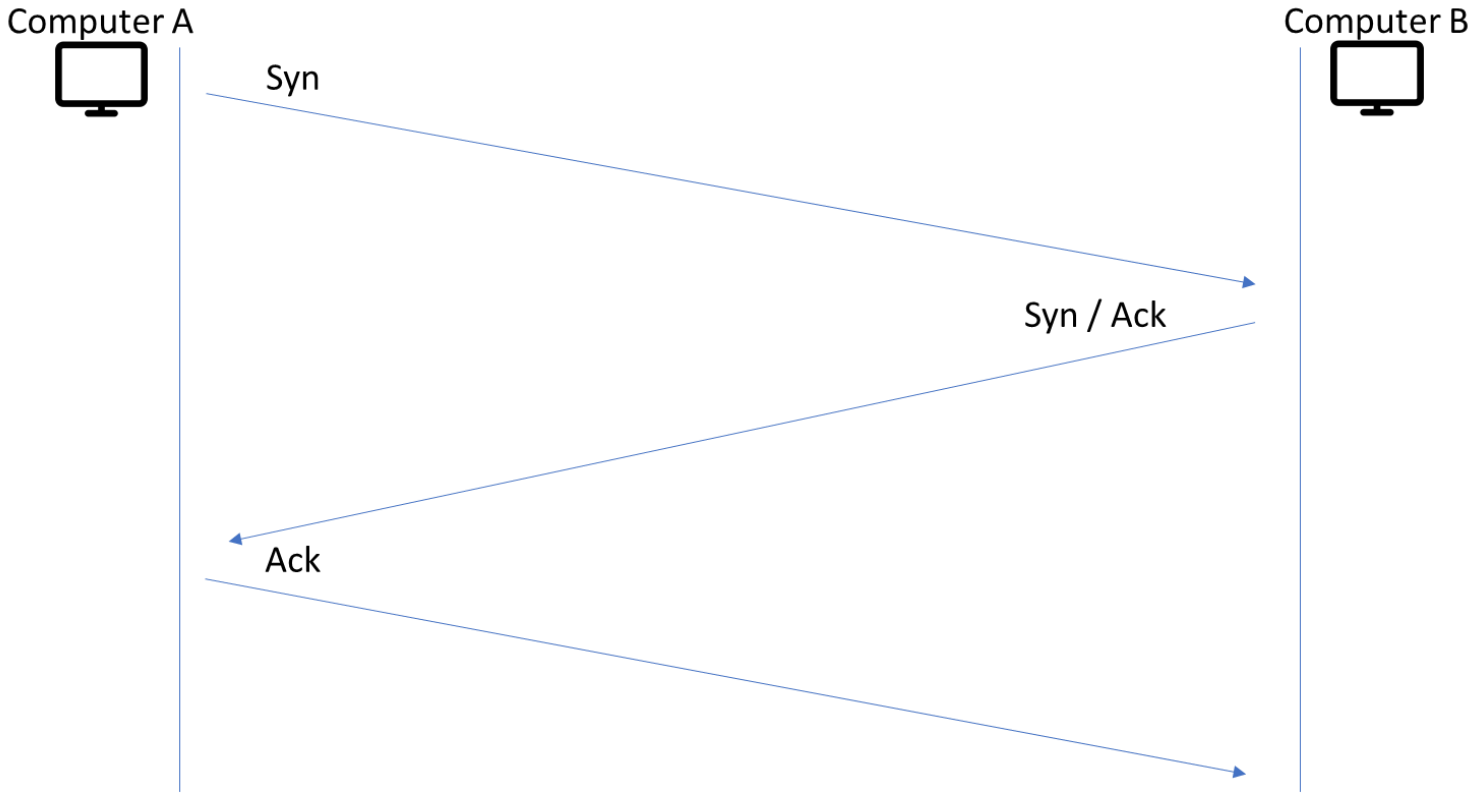
```
loiliangyang@loiliangyang:~$ echo "" | nc -v -n -w1 192.168.1.85 80
(UNKNOWN) [192.168.1.85] 80 (http) open
```

Message	Description
Syn	Initiate and establish a connection. Synchronize sequence numbers between devices.
ACK	Confirms to the other computer that it has received the SYN packet.
SYN-ACK	SYN message from local device and ACK of the earlier packet.
FIN	Terminate a connection.

TCP message types

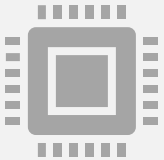


3-way Handshake



Terms

TCP – Transmission Control Protocol



UDP – User Datagram Protocol

Socket - <ip address>:<port number>

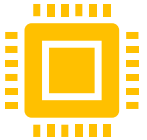
What is NMAP?

Network exploration tool and security / port scanner

Scan Types

Sweep – Send a series of ICMP ping to find hosts

Trace – Use tools like traceroute and/or tracert to map network



Port Scanning – Checking for open TCP or UDP ports

Fingerprinting – Determine operating system

Version Scanning – Finding versions of services and protocols

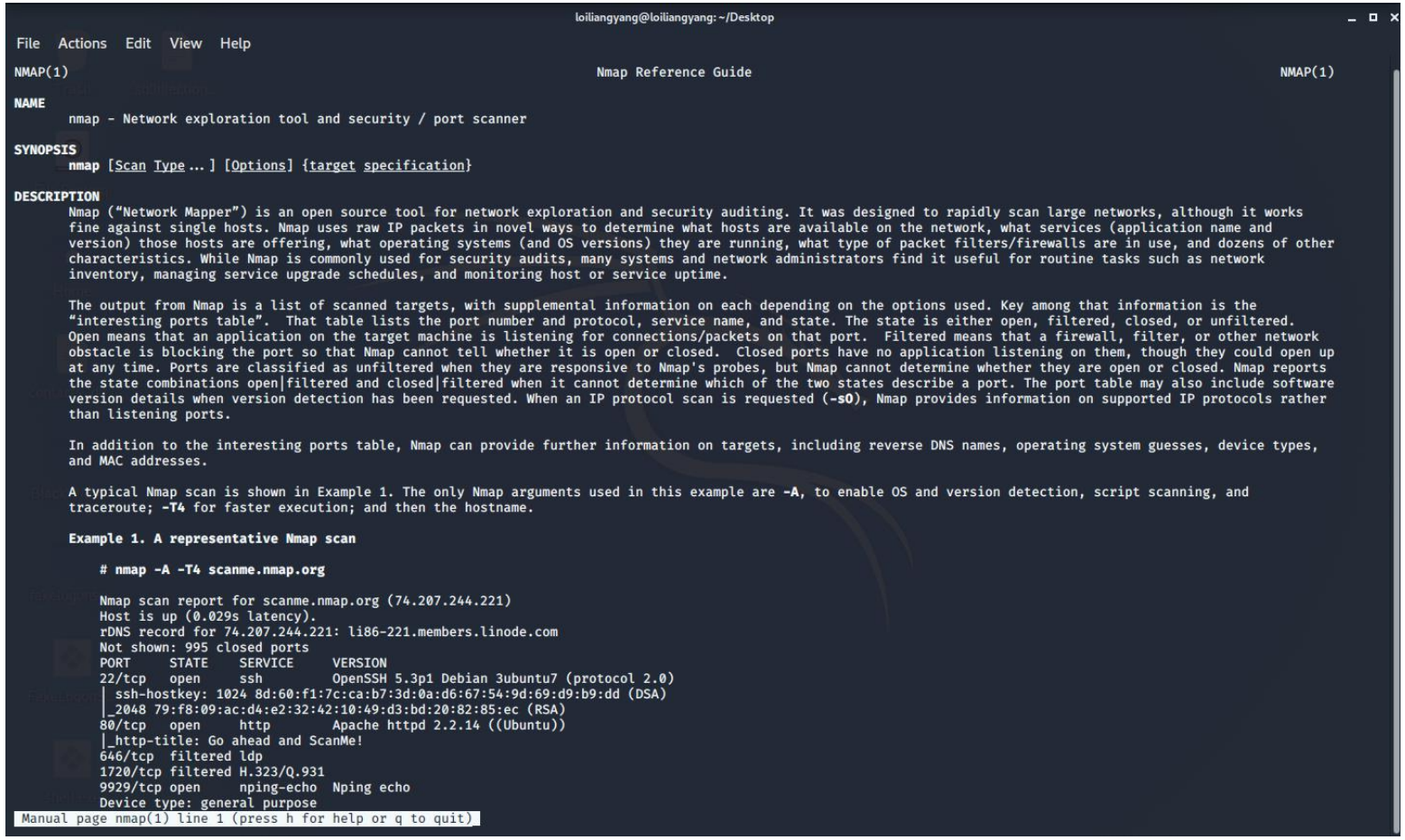
Vulnerability Scanning

NMAP Port Scan Result

Port State	Description
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 avenue for attack. Attackers and pen-testers want to exploit the open ports, while administrators try to close or protect them with firewalls without thwarting legitimate users. Open ports are also interesting for non-security scans because they show services available for use on the network.
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, or ping scanning), and as part of OS detection. Because closed ports are reachable, it may be worth scanning later in case some open. Administrators may want to consider blocking such ports with a firewall. Then they would appear in the filtered state, discussed next.
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 software. These ports frustrate attackers because they provide so little information. Sometimes they respond with ICMP error messages such as type 3 code 13 (destination unreachable: communication administratively prohibited), but filters that simply drop probes without responding are far more common. This forces Nmap to retry several times just in case the probe was dropped due to network congestion rather than filtering. This slows down the scan dramatically.
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 state. Scanning unfiltered ports with other scan types such as Window scan, SYN scan, or FIN scan, may help resolve whether the port is open.
Open|Filtered	Nmap places ports in this state when it is unable to determine whether a port is open or filtered. This occurs for scan types in which open ports give no response. The lack of response could also mean that a packet filter dropped the probe or any response it elicited. So Nmap does not know for sure whether the port is open or being filtered. The UDP, IP protocol, FIN, NULL, and Xmas scans classify ports this way.
Closed|Filtered	This state is used when Nmap is unable to determine whether a port is closed or filtered. It is only used for the IP ID idle scan.

https://wiki.onap.org/display/DW/Nmap

NMAP Manual Page



Scan Options - TARGET SPECIFICATION

- TARGET SPECIFICATION:
- Can pass hostnames, IP addresses, networks, etc.
- Ex: scanme.nmap.org, 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

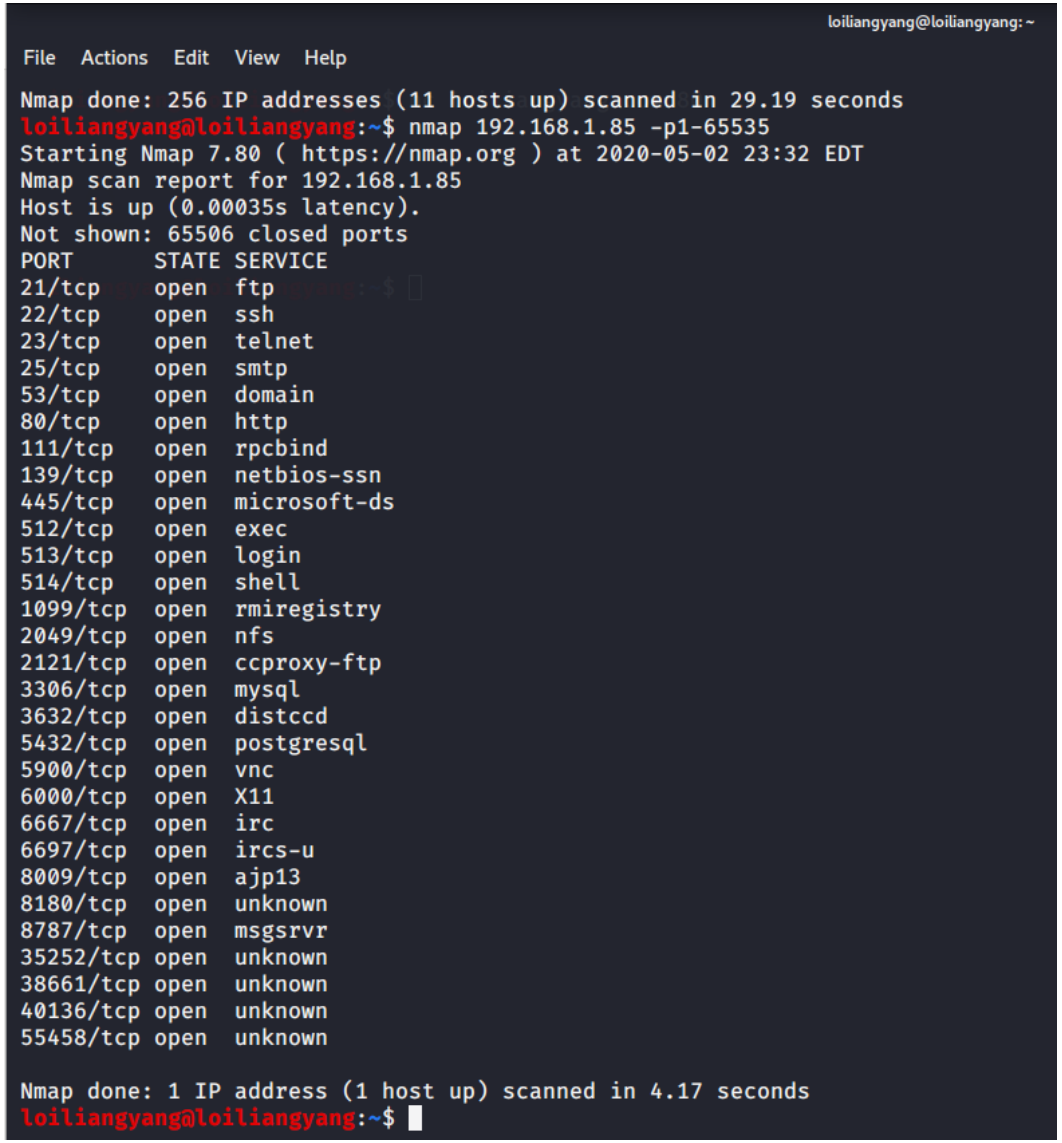
Scan Options – HOST DISCOVERY

- 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

```
loiliangyang@loiliangyang:~$ nmap -sn 192.168.1.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-02 23:04 EDT
Nmap scan report for 192.168.1.65
Host is up (0.014s latency).
Nmap scan report for 192.168.1.66
Host is up (0.0053s latency).
Nmap scan report for 192.168.1.72
Host is up (0.40s latency).
Nmap scan report for 192.168.1.75
Host is up (0.38s latency).
Nmap scan report for 192.168.1.76
Host is up (0.27s latency).
Nmap scan report for 192.168.1.82
Host is up (0.0073s latency).
Nmap scan report for 192.168.1.83
Host is up (0.17s latency).
Nmap scan report for 192.168.1.85
Host is up (0.0071s latency).
Nmap scan report for 192.168.1.87
Host is up (0.0070s latency).
Nmap scan report for 192.168.1.91
Host is up (0.0069s latency).
Nmap scan report for 192.168.1.254
Host is up (0.086s latency).
Nmap done: 256 IP addresses (11 hosts up) scanned in 29.19 seconds
loiliangyang@loiliangyang:~$
```

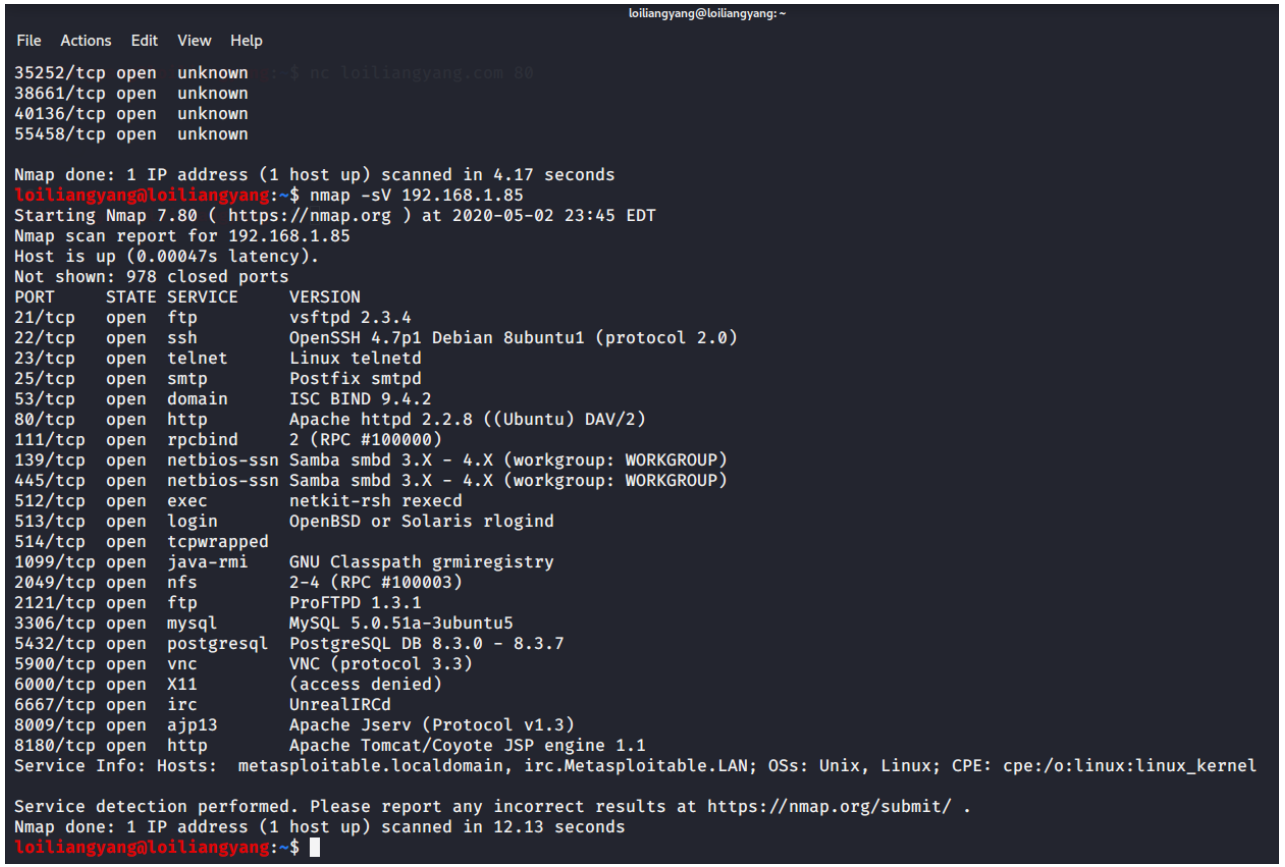
Scan Options – SCAN TECHNIQUES

- 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



SCAN OPTIONS – PORT SPECIFICATION AND SCAN ORDER

- 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
- -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>

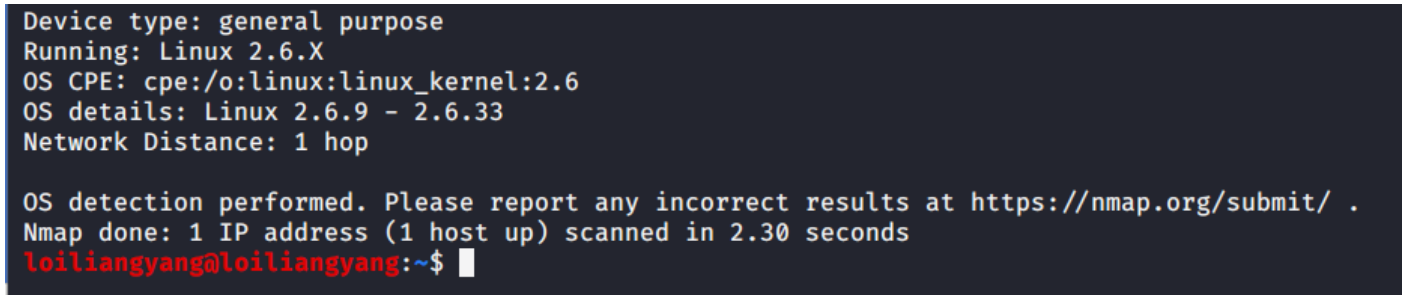


SCAN OPTIONS – SERVICE/VERSION DETECTION

- 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)

SCAN OPTIONS – SCRIPT SCAN

- 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-trace: Show all data sent and received
- --script-updatedb: Update the script database.



SCAN OPTIONS – OS DETECTION

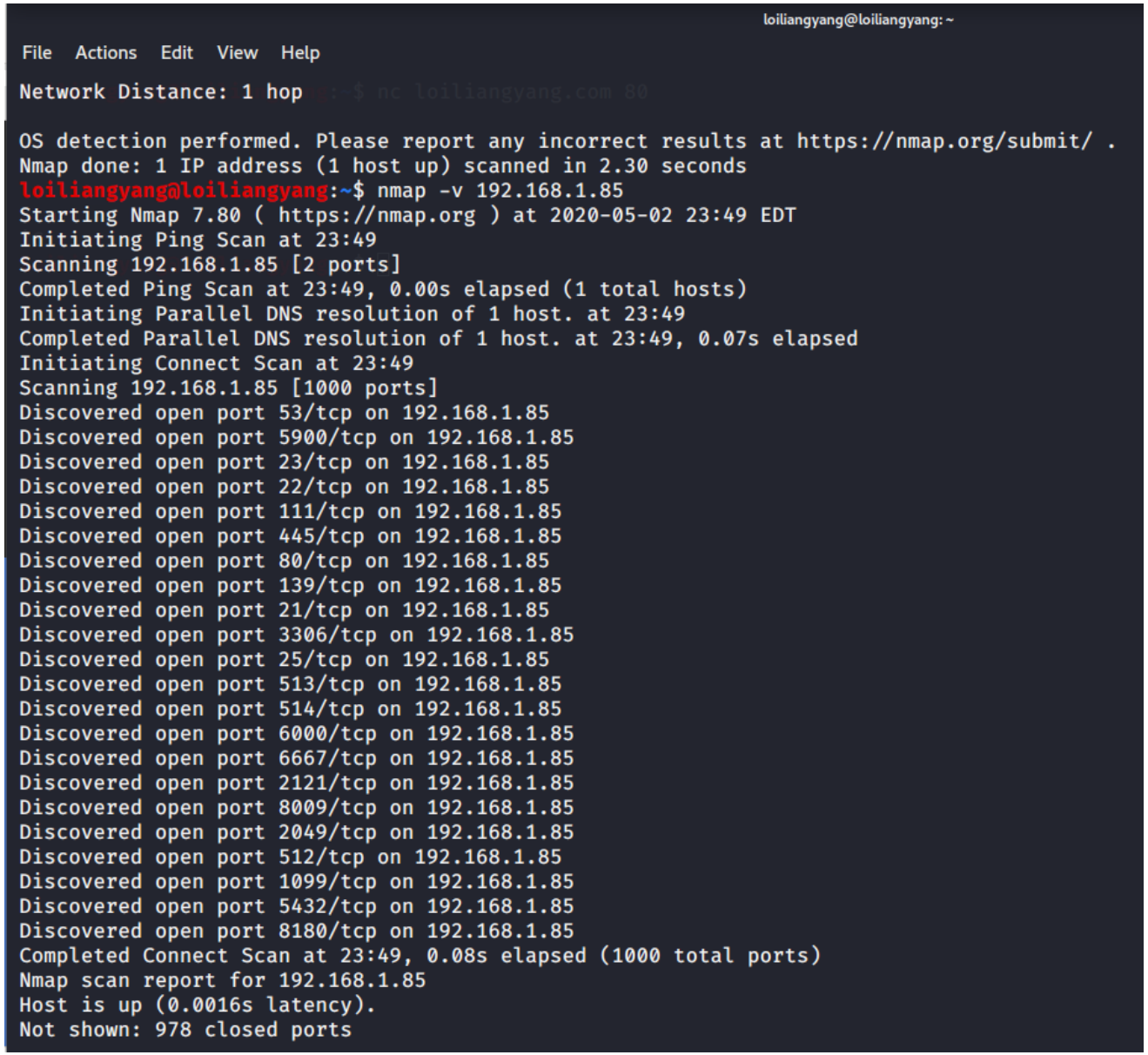
- OS DETECTION:
- -O: Enable OS detection
- --osscan-limit: Limit OS detection to promising targets
- --osscan-guess: Guess OS more aggressively

Scan Options – TIMING AND PERFORMANCE

- 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

Scan Options – FIREWALL/IDS EVASION AND SPOOFING

- 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
- --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



SCAN OPTIONS - OUTPUT

- OUTPUT:
- -oN/-oX/-oS/-oG <file>: Output scan in normal, XML, s|<rIpt kIddi3,
- 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)
- --log-errors: Log errors/warnings to the normal-format output file
- --append-output: Append to rather than clobber specified output files
- --resume <filename>: Resume an aborted scan
- --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

SCAN OPTIONS - MISC

- MISC:
- -6: Enable IPv6 scanning
- -A: Enable OS detection, version detection, script scanning, and traceroute
- --datadir <dirname>: 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.

NMAP Scripting Engine (NSE)

- The Nmap Scripting Engine (NSE) is one of Nmap's most powerful and flexible features. It allows users to write (and share) simple scripts (using the Lua programming language) to automate a wide variety of networking tasks. Those scripts are executed in parallel with the speed and efficiency you expect from Nmap. Users can rely on the growing and diverse set of scripts distributed with Nmap, or write their own to meet custom needs.

Script Categories

- Auth
- Broadcast
- Brute
- Default
- Discovery
- Dos
- Exploit
- External
- Fuzzer
- Intrusive
- Malware
- Safe
- Version
- Vuln

```
loiliangyang@loiliangyang:/usr/share/nmap/scripts$ ls -l | grep vuln
-rw-r--r-- 1 root root  7001 Nov 26 04:21 afp-path-vuln.nse
-rw-r--r-- 1 root root  5923 Nov 26 04:21 ftp-vuln-cve2010-4221.nse
-rw-r--r-- 1 root root  6973 Nov 26 04:21 http-huawei-hg5xx-vuln.nse
-rw-r--r-- 1 root root  7921 Nov 26 04:21 http-iis-webdav-vuln.nse
-rw-r--r-- 1 root root  4111 Nov 26 04:21 http-vmware-path-vuln.nse
-rw-r--r-- 1 root root  3273 Nov 26 04:21 http-vuln-cve2006-3392.nse
-rw-r--r-- 1 root root  6610 Nov 26 04:21 http-vuln-cve2009-3960.nse
-rw-r--r-- 1 root root  2957 Nov 26 04:21 http-vuln-cve2010-0738.nse
-rw-r--r-- 1 root root  5607 Nov 26 04:21 http-vuln-cve2010-2861.nse
-rw-r--r-- 1 root root  4527 Nov 26 04:21 http-vuln-cve2011-3192.nse
-rw-r--r-- 1 root root  5851 Nov 26 04:21 http-vuln-cve2011-3368.nse
-rw-r--r-- 1 root root  4403 Nov 26 04:21 http-vuln-cve2012-1823.nse
-rw-r--r-- 1 root root  4831 Nov 26 04:21 http-vuln-cve2013-0156.nse
-rw-r--r-- 1 root root  2853 Nov 26 04:21 http-vuln-cve2013-6786.nse
-rw-r--r-- 1 root root  5009 Nov 26 04:21 http-vuln-cve2013-7091.nse
-rw-r--r-- 1 root root  2945 Nov 26 04:21 http-vuln-cve2014-2126.nse
-rw-r--r-- 1 root root  3334 Nov 26 04:21 http-vuln-cve2014-2127.nse
-rw-r--r-- 1 root root  3193 Nov 26 04:21 http-vuln-cve2014-2128.nse
-rw-r--r-- 1 root root  2979 Nov 26 04:21 http-vuln-cve2014-2129.nse
-rw-r--r-- 1 root root 14018 Nov 26 04:21 http-vuln-cve2014-3704.nse
-rw-r--r-- 1 root root  4523 Nov 26 04:21 http-vuln-cve2014-8877.nse
-rw-r--r-- 1 root root  7774 Nov 26 04:21 http-vuln-cve2015-1427.nse
-rw-r--r-- 1 root root  3443 Nov 26 04:21 http-vuln-cve2015-1635.nse
-rw-r--r-- 1 root root  4372 Nov 26 04:21 http-vuln-cve2017-1001000.nse
-rw-r--r-- 1 root root  2594 Nov 26 04:21 http-vuln-cve2017-5638.nse
-rw-r--r-- 1 root root  5480 Nov 26 04:21 http-vuln-cve2017-5689.nse
-rw-r--r-- 1 root root  5187 Nov 26 04:21 http-vuln-cve2017-8917.nse
-rw-r--r-- 1 root root  2699 Nov 26 04:21 http-vuln-misfortune-cookie.nse
-rw-r--r-- 1 root root  4225 Nov 26 04:21 http-vuln-wnr1000-creds.nse
-rw-r--r-- 1 root root  6977 Nov 26 04:21 mysql-vuln-cve2012-2122.nse
-rw-r--r-- 1 root root  8904 Nov 26 04:21 rdp-vuln-ms12-020.nse
-rw-r--r-- 1 root root  4011 Nov 26 04:21 rmi-vuln-classloader.nse
-rw-r--r-- 1 root root  6528 Nov 26 04:21 rsa-vuln-roca.nse
-rw-r--r-- 1 root root  4148 Nov 26 04:21 samba-vuln-cve-2012-1182.nse
-rw-r--r-- 1 root root  5238 Nov 26 04:21 smb2-vuln-uptime.nse
-rw-r--r-- 1 root root  7524 Nov 26 04:21 smb-vuln-conficker.nse
-rw-r--r-- 1 root root  6402 Nov 26 04:21 smb-vuln-cve2009-3103.nse
```

NMAP Vulnerability Scan

```
loiliangyang@loiliangyang:/usr/share/nmap/scripts$ nmap -sV --script=vulners 192.168.1.85
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-03 00:26 EDT
Nmap scan report for 192.168.1.85
Host is up (0.00030s latency).
Not shown: 978 closed ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| vulners:
|   cpe:/a:openbsd:openssh:4.7p1:
|       CVE-2010-4478   7.5     https://vulners.com/cve/CVE-2010-4478
|       CVE-2017-15906  5.0     https://vulners.com/cve/CVE-2017-15906
|       CVE-2016-10708  5.0     https://vulners.com/cve/CVE-2016-10708
|       CVE-2010-4755   4.0     https://vulners.com/cve/CVE-2010-4755
|_      CVE-2008-5161   2.6     https://vulners.com/cve/CVE-2008-5161
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
| vulners:
|   cpe:/a:isc:bind:9.4.2:
|       CVE-2012-1667   8.5     https://vulners.com/cve/CVE-2012-1667
|       CVE-2014-8500   7.8     https://vulners.com/cve/CVE-2014-8500
|       CVE-2012-5166   7.8     https://vulners.com/cve/CVE-2012-5166
|       CVE-2012-4244   7.8     https://vulners.com/cve/CVE-2012-4244
|       CVE-2012-3817   7.8     https://vulners.com/cve/CVE-2012-3817
|       CVE-2008-4163   7.8     https://vulners.com/cve/CVE-2008-4163
|       CVE-2010-0382   7.6     https://vulners.com/cve/CVE-2010-0382
|       CVE-2017-3141   7.2     https://vulners.com/cve/CVE-2017-3141
|       CVE-2015-8461   7.1     https://vulners.com/cve/CVE-2015-8461
|       CVE-2015-8704   6.8     https://vulners.com/cve/CVE-2015-8704
|       CVE-2009-0025   6.8     https://vulners.com/cve/CVE-2009-0025
|       CVE-2015-8705   6.6     https://vulners.com/cve/CVE-2015-8705
|       CVE-2010-3614   6.4     https://vulners.com/cve/CVE-2010-3614
|       CVE-2017-3145   5.0     https://vulners.com/cve/CVE-2017-3145
|       CVE-2016-9444   5.0     https://vulners.com/cve/CVE-2016-9444
|       CVE-2016-9131   5.0     https://vulners.com/cve/CVE-2016-9131
|       CVE-2016-8864   5.0     https://vulners.com/cve/CVE-2016-8864
|       CVE-2016-2848   5.0     https://vulners.com/cve/CVE-2016-2848
```

References

- https://linux.die.net/man/1/nmap
- https://nmap.org/
- https://wiki.onap.org/display/DW/Nmap

Hacking with NMAP?