EXPLORING AND AUDITING NETWORK USING NMAP

TITLE SUBMISSIONS

Submitted by

FRANCIS ALEX (18BCE2325)

ASHISH THAPA (18BCE2395)

SUMEET ROY KURIAN(18BCI0188)

SHIKHA SAH (18BCE2458)

Prepared For

ISAA – J COMPONENT DOCUMENT

Submitted To

DR LAVANYA K

Senior Professor

SCOPE

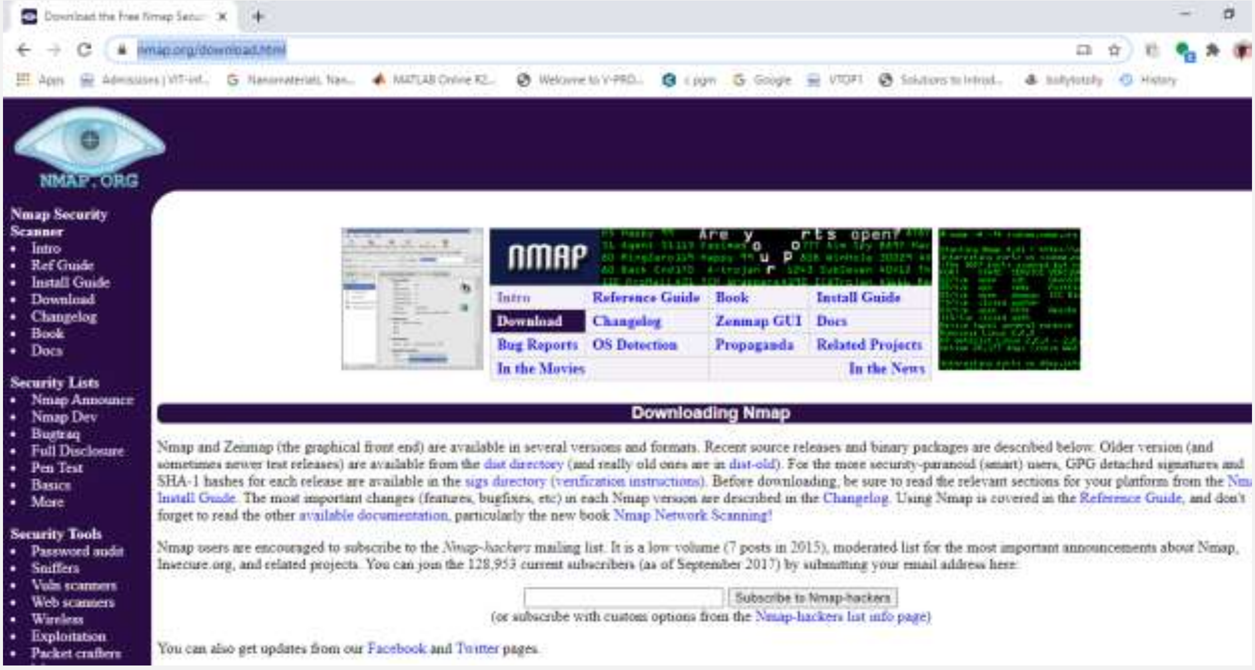
VIT®
UNIVERSITY
(Estd. u/s 3 of UGC Act 1956)
VELLORE ■ CHENNAI
www.vit.ac.in

TABLE OF CONTENTS

S/W INSTALLATION GUIDE

CASE1: FOR WORKING IN COMMAND PROMPT:

Step1: Visit Nmap.org (https://nmap.org/download.html)



Downloading Nmap

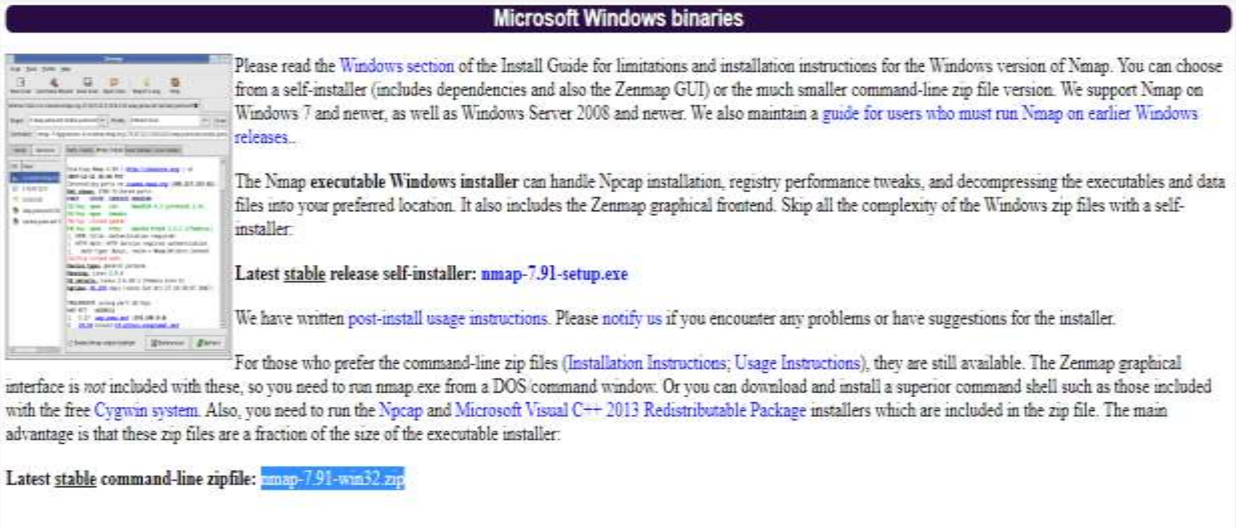
Nmap and Zenmap (the graphical front end) are available in several versions and formats. Recent source releases and binary packages are described below. Older version (and sometimes newer test releases) are available from the dist directory (and really old ones are in dist-old). For the more security-paranoid (smart) users, GPG detached signatures and SHA-1 hashes for each release are available in the sigs directory (verification instructions). Before downloading, be sure to read the relevant sections for your platform from the Nm Install Guide. The most important changes (features, bugfixes, etc) in each Nmap version are described in the Changelog. Using Nmap is covered in the Reference Guide, and don't forget to read the other available documentation, particularly the new book Nmap Network Scanning!

Nmap users are encouraged to subscribe to the *Nmap-hackers* mailing list. It is a low volume (7 posts in 2015), moderated list for the most important announcements about Nmap, Insecure.org, and related projects. You can join the 128,953 current subscribers (as of September 2017) by submitting your email address here:

(or subscribe with custom options from the Nmap-hackers list info page)

You can also get updates from our Facebook and Twitter pages.

Step2: Download zip folder given under windows tag



Microsoft Windows binaries

Please read the Windows section of the Install Guide for limitations and installation instructions for the Windows version of Nmap. You can choose from a self-installer (includes dependencies and also the Zenmap GUI) or the much smaller command-line zip file version. We support Nmap on Windows 7 and newer, as well as Windows Server 2008 and newer. We also maintain a guide for users who must run Nmap on earlier Windows releases..

The Nmap **executable Windows installer** can handle Npcap installation, registry performance tweaks, and decompressing the executables and data files into your preferred location. It also includes the Zenmap graphical frontend. Skip all the complexity of the Windows zip files with a self-installer:

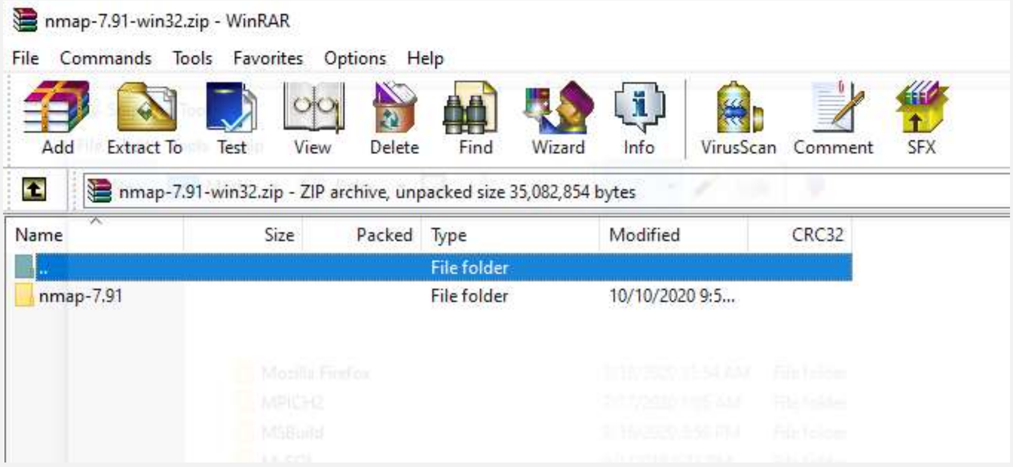
Latest stable release self-installer: nmap-7.91-setup.exe

We have written post-install usage instructions. Please notify us if you encounter any problems or have suggestions for the installer.

For those who prefer the command-line zip files (Installation Instructions; Usage Instructions), they are still available. The Zenmap graphical interface is *not* included with these, so you need to run nmap.exe from a DOS command window. Or you can download and install a superior command shell such as those included with the free Cygwin system. Also, you need to run the Npcap and Microsoft Visual C++ 2013 Redistributable Package installers which are included in the zip file. The main advantage is that these zip files are a fraction of the size of the executable installer:

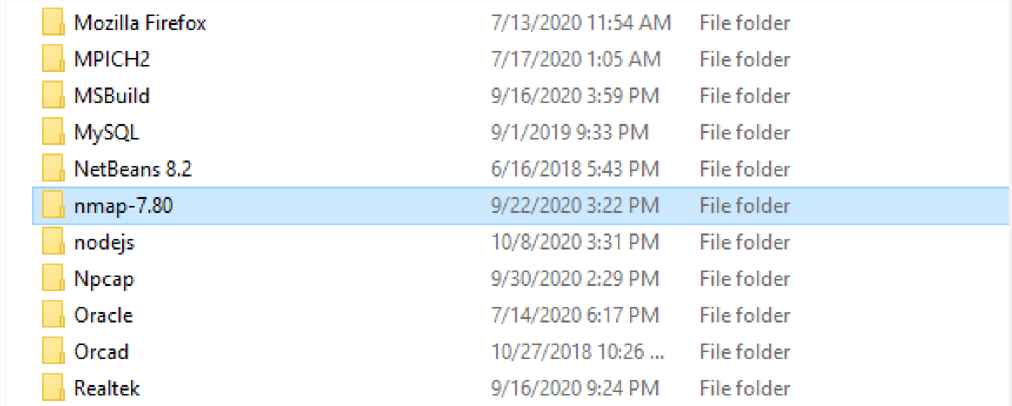
Latest stable command-line zipfile: nmap-7.91-win32.zip

Step3: Extract the Downloaded files to C drive Program Files.



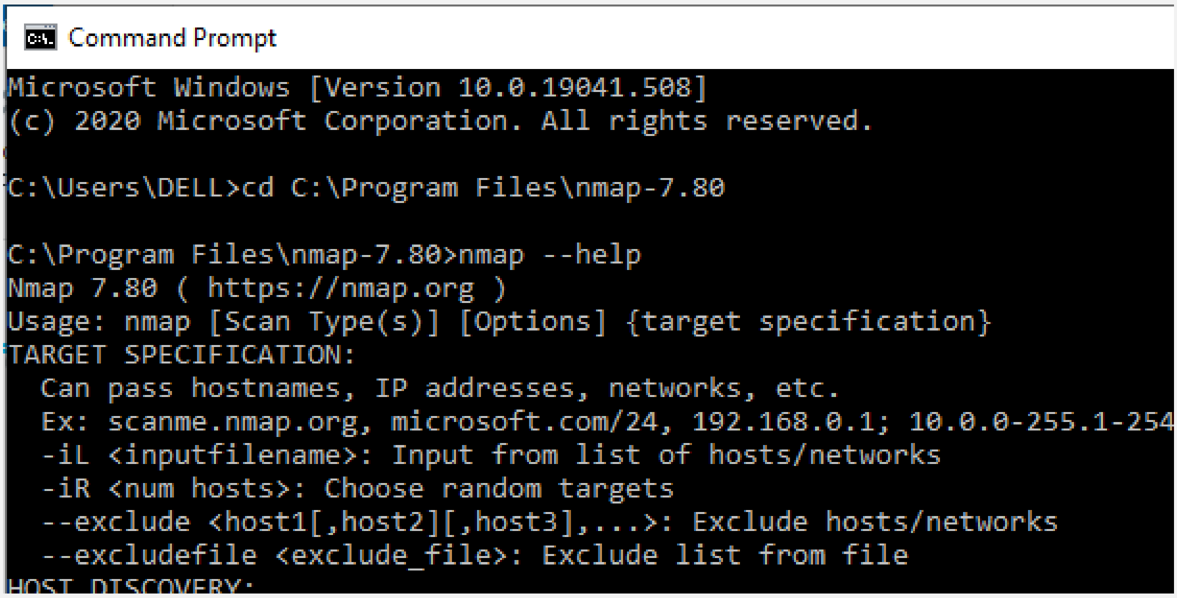
nmap-7.91-win32.zip - ZIP archive, unpacked size 35,082,854 bytes

Name	Size	Packed	Type	Modified	CRC32
..			File folder		
nmap-7.91			File folder	10/10/2020 9:5...	



Mozilla Firefox	7/13/2020 11:54 AM	File folder
MPICH2	7/17/2020 1:05 AM	File folder
MSBuild	9/16/2020 3:59 PM	File folder
MySQL	9/1/2019 9:33 PM	File folder
NetBeans 8.2	6/16/2018 5:43 PM	File folder
nmap-7.80	9/22/2020 3:22 PM	File folder
nodejs	10/8/2020 3:31 PM	File folder
Npcap	9/30/2020 2:29 PM	File folder
Oracle	7/14/2020 6:17 PM	File folder
Orcad	10/27/2018 10:26 ...	File folder
Realtek	9/16/2020 9:24 PM	File folder

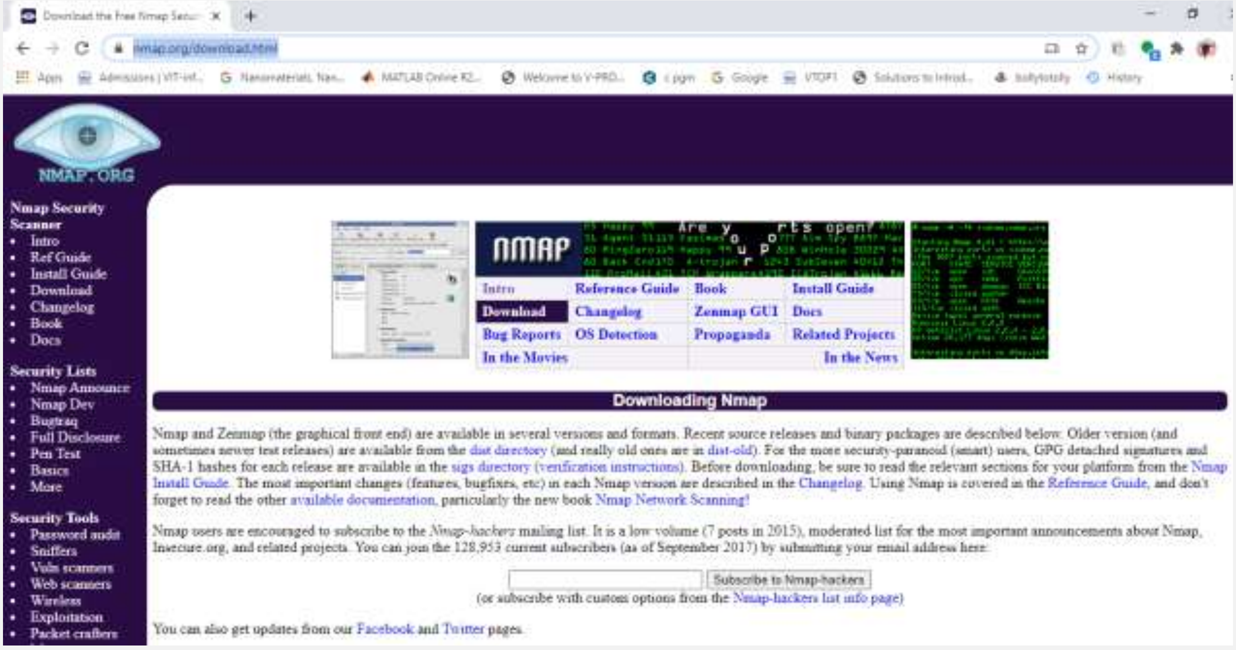
Step4: Open command prompt and change directory using cd file location



```
Microsoft Windows [Version 10.0.19041.508]
(c) 2020 Microsoft Corporation. All rights reserved.

C:\Users\DELL>cd C:\Program Files\nmap-7.80

C:\Program Files\nmap-7.80>nmap --help
Nmap 7.80 ( 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:
```

CASE2: FOR WORKING IN ZENMAP GUI:

Step1: Visit Nmap.org (https://nmap.org/download.html)



Download the Free Nmap Secur ×

nmap.org/download.html

Apps Admissions | VIT-Inf... Nanomaterials, Nan... MATLAB Online R2... Welcome to V-PRO... c pgm Google VTOP1 Solutions to Introd... bollytotally History

NMAP.ORG

Nmap Security Scanner
- Intro
- Ref Guide
- Install Guide
- Download
- Changelog
- Book
- Docs

Security Lists
- Nmap Announce
- Nmap Dev
- Bugtraq
- Full Disclosure
- Pen Test
- Basics
- More

Security Tools
- Password audit
- Sniffers
- Vuln scanners
- Web scanners
- Wireless
- Exploitation
- Packet crafters

NMAP

Intro	Reference Guide	Book	Install Guide
Download	Changelog	Zenmap GUI	Docs
Bug Reports	OS Detection	Propaganda	Related Projects
In the Movies			In the News

Downloading Nmap

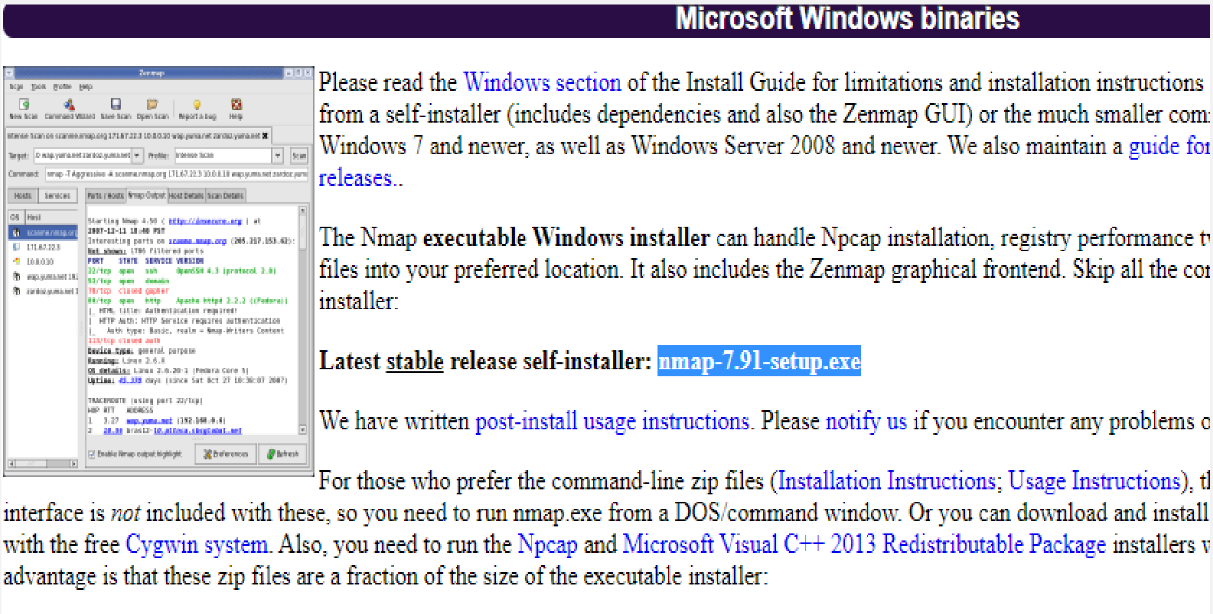
Nmap and Zenmap (the graphical front end) are available in several versions and formats. Recent source releases and binary packages are described below. Older version (and sometimes newer test releases) are available from the dist directory (and really old ones are in dist-old). For the more security-paranoid (smart) users, GPG detached signatures and SHA-1 hashes for each release are available in the sigs directory (verification instructions). Before downloading, be sure to read the relevant sections for your platform from the Nmap Install Guide. The most important changes (features, bugfixes, etc) in each Nmap version are described in the Changelog. Using Nmap is covered in the Reference Guide, and don't forget to read the other available documentation, particularly the new book Nmap Network Scanning!

Nmap users are encouraged to subscribe to the *Nmap-hackers* mailing list. It is a low volume (7 posts in 2015), moderated list for the most important announcements about Nmap, Insecure.org, and related projects. You can join the 128,953 current subscribers (as of September 2017) by submitting your email address here:

Subscribe to Nmap-hackers
(or subscribe with custom options from the Nmap-hackers list info page)

You can also get updates from our Facebook and Twitter pages.

Step2: Click the set up (exe files) for downloading the zenmap



Microsoft Windows binaries

Please read the Windows section of the Install Guide for limitations and installation instructions from a self-installer (includes dependencies and also the Zenmap GUI) or the much smaller com Windows 7 and newer, as well as Windows Server 2008 and newer. We also maintain a guide for releases..

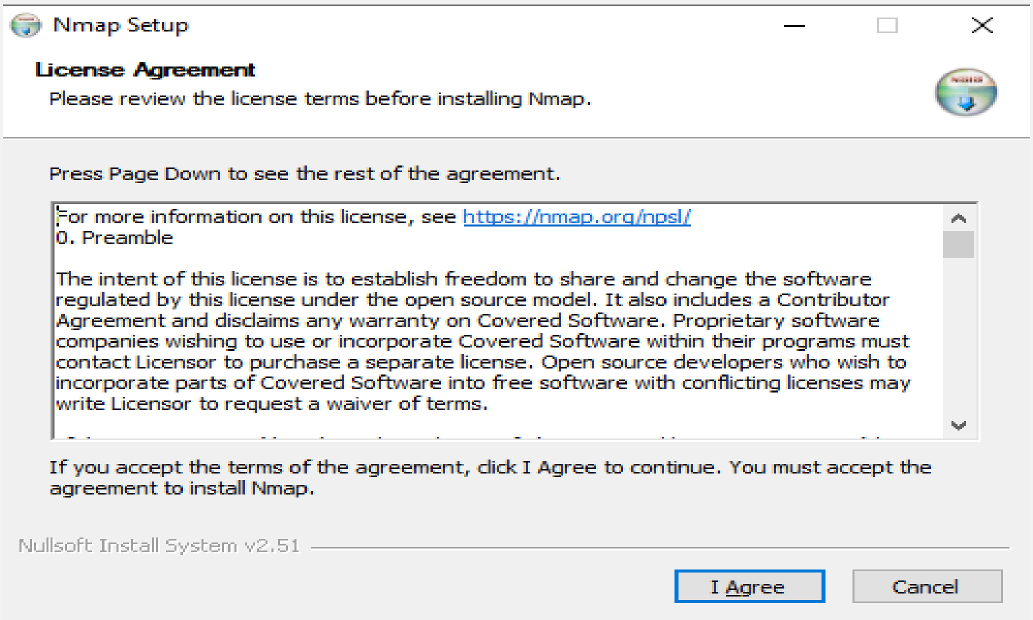
The Nmap **executable Windows installer** can handle Npcap installation, registry performance t files into your preferred location. It also includes the Zenmap graphical frontend. Skip all the co installer:

Latest stable release self-installer: nmap-7.91-setup.exe

We have written post-install usage instructions. Please notify us if you encounter any problems o

For those who prefer the command-line zip files (Installation Instructions; Usage Instructions), t interface is *not* included with these, so you need to run nmap.exe from a DOS/command window. Or you can download and install with the free Cygwin system. Also, you need to run the Npcap and Microsoft Visual C++ 2013 Redistributable Package installers v advantage is that these zip files are a fraction of the size of the executable installer:

Step3: Follow the next steps to complete the zenmap



License Agreement

Please review the license terms before installing Nmap.

Press Page Down to see the rest of the agreement.

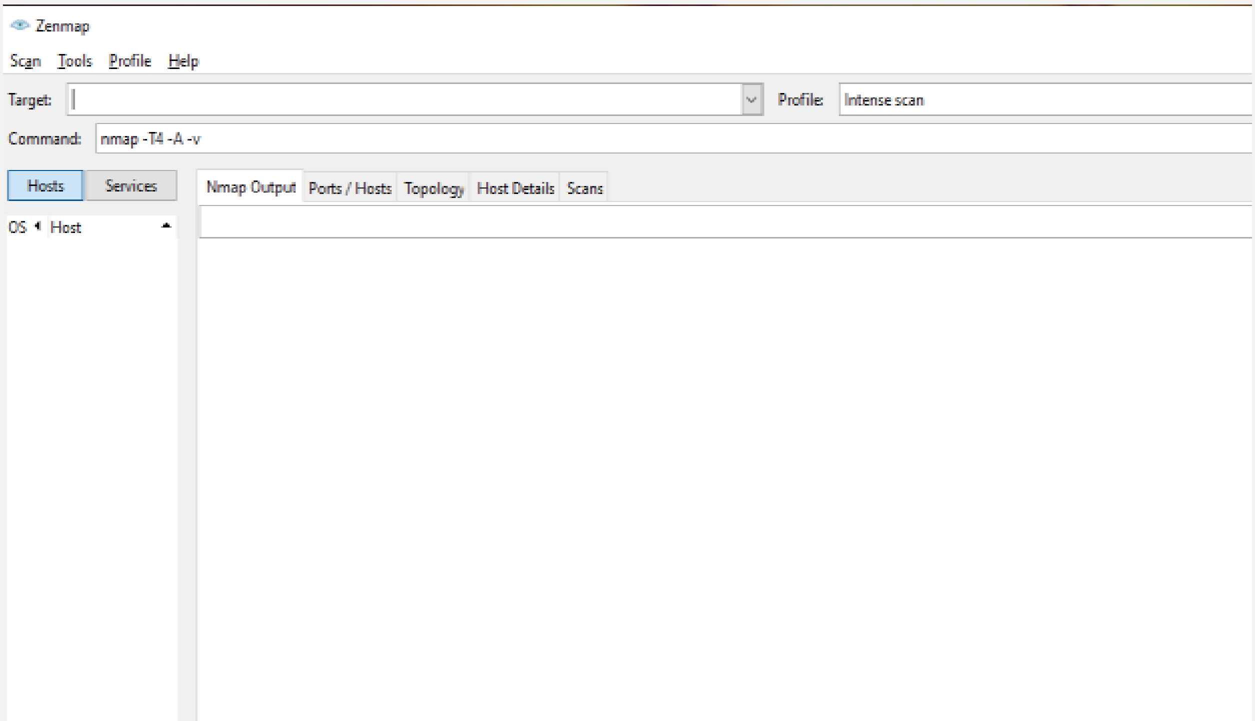
For more information on this license, see https://nmap.org/npsl/
0. Preamble

The intent of this license is to establish freedom to share and change the software regulated by this license under the open source model. It also includes a Contributor Agreement and disclaims any warranty on Covered Software. Proprietary software companies wishing to use or incorporate Covered Software within their programs must contact Licensor to purchase a separate license. Open source developers who wish to incorporate parts of Covered Software into free software with conflicting licenses may write Licensor to request a waiver of terms.

If you accept the terms of the agreement, click I Agree to continue. You must accept the agreement to install Nmap.

Nullsoft Install System v2.51

Step4: Type Zenmap in search bar and click the icon



Target:

Profile: Intense scan

Command: nmap -T4 -A -v

SERIES OF FEATURES EXECUTED.

1) BASIC SCANS

i) SCANNING USING DNS

While entering the command DNS is converted to IP address and then scan is performed.

ii) SCANNING MULTIPLE SITES

While entering the command DNS is converted to IP address and then scan is performed for multiple sites

iii) SCANNING A GIVEN RANGE OF IP ADDRESS.

Sequentially each IP address is scanned and overall result is displayed.

2) VARIOUS TYPES OF SCANS

i) TCP SYN SCAN

TCP SYN scan is a most popular and default scan in Nmap because it perform quickly compare to other scan types and it is also less likely to block from firewalls. Another reason is that when it comes to states open, closed and filtered, TCP SYN scan gives a clear definition. Main concept behind this scan is TCP three way handshake. TCP SYN scan required raw-packet privileges that needs root access

ii) TCP ACK SCAN

This scan is different than the others, in that it never determines open (or even open| filtered) ports. It is used to map out firewall rulesets, determining whether they are stateful or not and which ports are filtered.

ACK scan is enabled by specifying the -sA option. Its probe packet has only the ACK flag set (unless you use --scanflags). When scanning unfiltered systems, open and closed ports will both return a RST packet. Nmap then labels them as unfiltered, meaning that they are reachable by the ACK packet, but whether they are open or closed is undetermined. Ports that don't respond, or send certain ICMP error messages back, are labeled filtered.

iii) UDP SCAN

UDP scan works by sending a UDP packet to every targeted port. For some common ports such as 53 and 161, a protocol-specific payload is sent to increase response rate, but for most ports the packet is empty unless the --data, --data-string, or --data-length options are specified. If an ICMP port unreachable error (type 3, code 3) is returned, the port is closed. Other ICMP unreachable errors (type 3, codes 0, 1, 2, 9, 10, or 13) mark the port as filtered. Occasionally, a service will respond with a UDP packet, proving that it is open. If no response is received after retransmissions, the port is classified as open|filtered. This means that the port could be open, or

iv) TCP WINDOW SCAN

Window scan is exactly the same as ACK scan except that it exploits an implementation detail of certain systems to differentiate open ports from closed ones, rather than always printing unfiltered when a RST is returned. It does this by examining the TCP Window value of the RST packets returned

v) TCP MAIMON SCAN

The scan does not open the port, it tests if the port is open or not.This is useful for enumeration, it can not only help enumerate that the target host may be a BSD derived system, but that the port that is being targeted is open, which you can tell by the absence of a reply.

vi) AGGRESSIVE SCANNING/ADVANCED SCANNING

Nmap has an aggressive mode that enables OS detection, version detection, script scanning, and traceroute. You can use the -A argument to perform an aggressive scan. Aggressive scans provide far better information than regular scans.

3) HOST DISCOVERY

i) LISTING OUT THE TARGETS

This is just to identify which all targets

ii) PORT SCAN

Does any of the above scan mentioned.

iii) HOST DISCOVERY WITHOUT PORT SCAN

This is to check is a host is accepting responses or not. This helps hackers to differentiate between active and inactive ports.

4) FIREWALL DETECTION

A firewall is a network security device which, based on a set of security rules, monitors incoming and outgoing network traffic and permits or blocks data packets. In order to block malicious traffic such as viruses and hackers, its purpose is to create a firewall between your internal network and incoming traffic from external sources (such as the internet). Nmap has a simplified recognition feature for firewall filtering that can be used to recognize port filtering based on ACK probe responses. To evaluate the filtering status, this feature may be used to assess a single port or multiple ports in sequence. You would need to have a remote system that runs network services to use Nmap to perform firewall identification. In addition, you will need to incorporate some kind of mechanism for filtering. This can be achieved with an individual firewall system or with Windows firewall host-based filtering. You should be able to change the results of scans by modifying the filtering settings on the firewall system.

5) SQL INJECTION

SQL injection is a code injection technique that might destroy our database. It usually occurs when we ask users

for input like their username and passwords. The exploiter tries to input some queries through the field to modify/change the database. Similarly, URL containing queries can also be modified to perform a SQL injection

With the help of NMAP we can scan our website for possible SQL injections so that we can make our site better prepared from sql attacks. NMAP first finds URLs containing queries of the website. It then proceeds to combine crafted SQL commands with susceptible URLs in order to obtain errors. The errors are then analysed to see if the URL is vulnerable to attack or not.

http-sql-injection is the command used in nmap for sql injection

6) VULNERABILITY SCANNING

A vulnerability is a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source. While Nmap isn't a comprehensive vulnerability scanner, NSE(Nmap Scripting Engine) scripts like vulners,vulscan etc can be used to perform vulnerability checks on websites/web servers.

The Nmap vulners NSE script works by getting the CPE (Common Platform Enumeration or standard name) of software on each port on the targeted IP and then makes a request to ‘vulners.com’ to get known vulnerabilities for the CPEs, vulnerabilities are then displayed in order of descending CVSS score along with a link to the ‘vulners.com’ page for the vulnerability. An attacker can then use these vulnerabilities to exploit a web application.

Nmap vulscan NSE script performs a similar operation but uses a local database for vulnerabilities as compared to vulners which gets vulnerabilities from ‘vulners.com’. One advantage of ‘vulscan’ is that it allow for user to provide their own vulnerability database but ‘vulners’ may provide more up to date information.

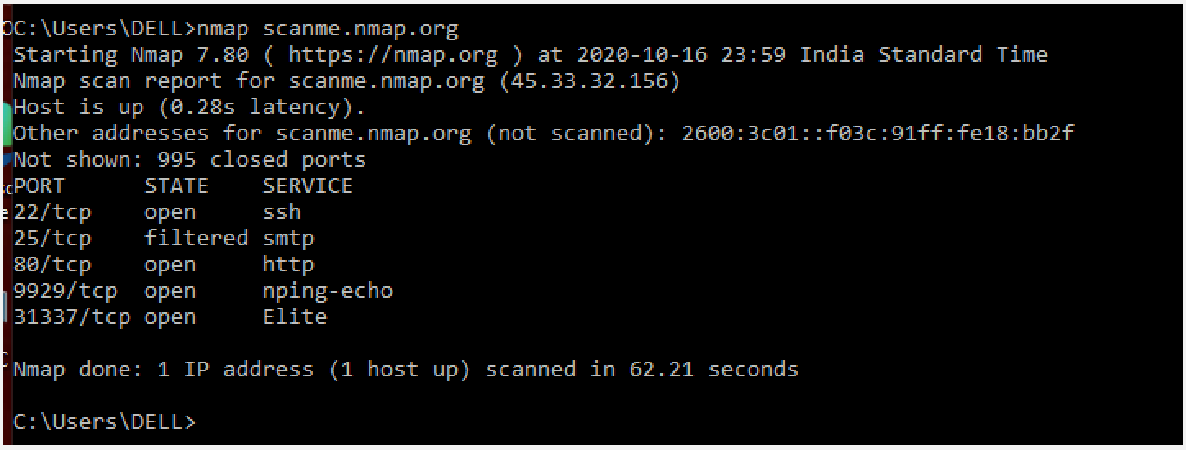
CODING

CASE 1: USING COMMAND PROMPT

1) BASIC SCANS

i) SCANNING USING DNS

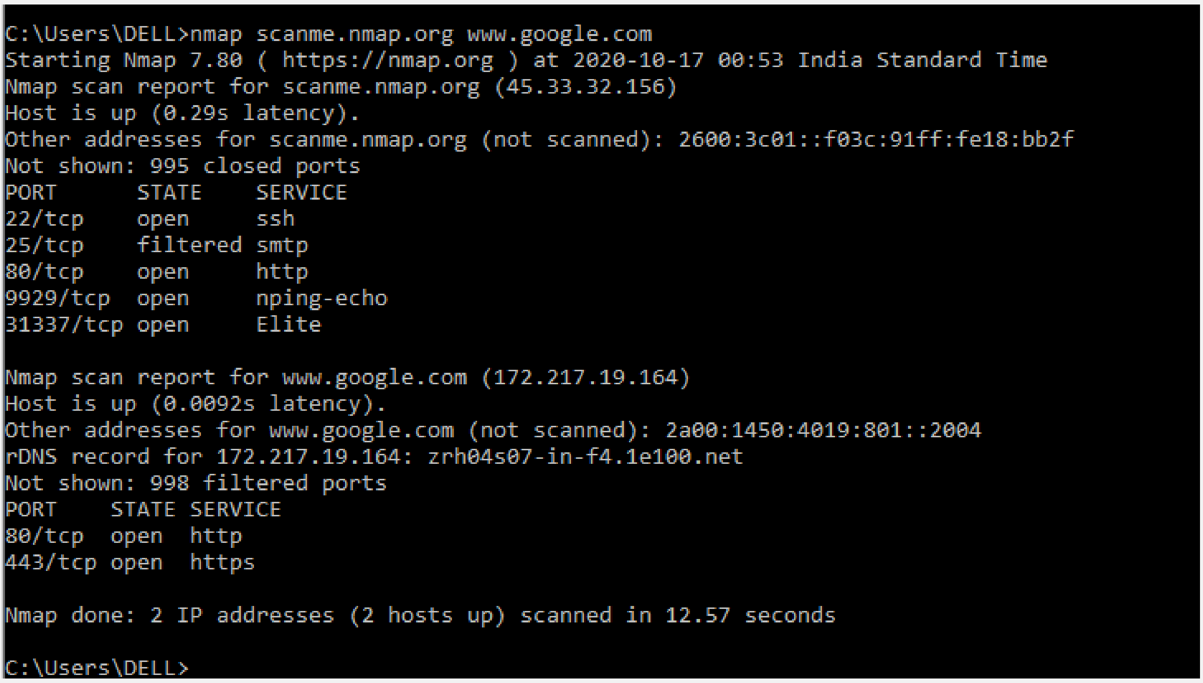
Command: nmap scanme.nmap.org



```
C:\Users\DELL>nmap scanme.nmap.org
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-16 23:59 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.28s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 995 closed ports
PORT      STATE    SERVICE
22/tcp    open     ssh
25/tcp    filtered smtp
80/tcp    open     http
9929/tcp  open     nping-echo
31337/tcp open     Elite

Nmap done: 1 IP address (1 host up) scanned in 62.21 seconds

C:\Users\DELL>
```

ii) SCANNING MULTIPLE SITES TOGETHER

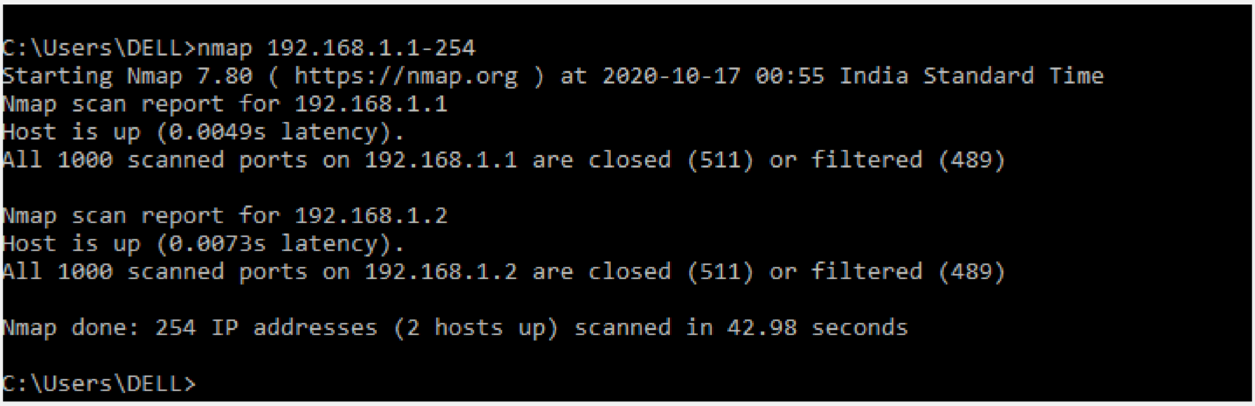
Command: nmap scanme.nmap.org www.google.com



```
C:\Users\DELL>nmap scanme.nmap.org www.google.com
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-17 00:53 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.29s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 995 closed ports
PORT      STATE    SERVICE
22/tcp    open     ssh
25/tcp    filtered smtp
80/tcp    open     http
9929/tcp  open     nping-echo
31337/tcp open     Elite

Nmap scan report for www.google.com (172.217.19.164)
Host is up (0.0092s latency).
Other addresses for www.google.com (not scanned): 2a00:1450:4019:801::2004
rDNS record for 172.217.19.164: zrh04s07-in-f4.1e100.net
Not shown: 998 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 2 IP addresses (2 hosts up) scanned in 12.57 seconds

C:\Users\DELL>
```

iii) SCANNING USING IP ADDRESS FOR A GIVEN RANGE

Command: nmap 192.168.1.1-254

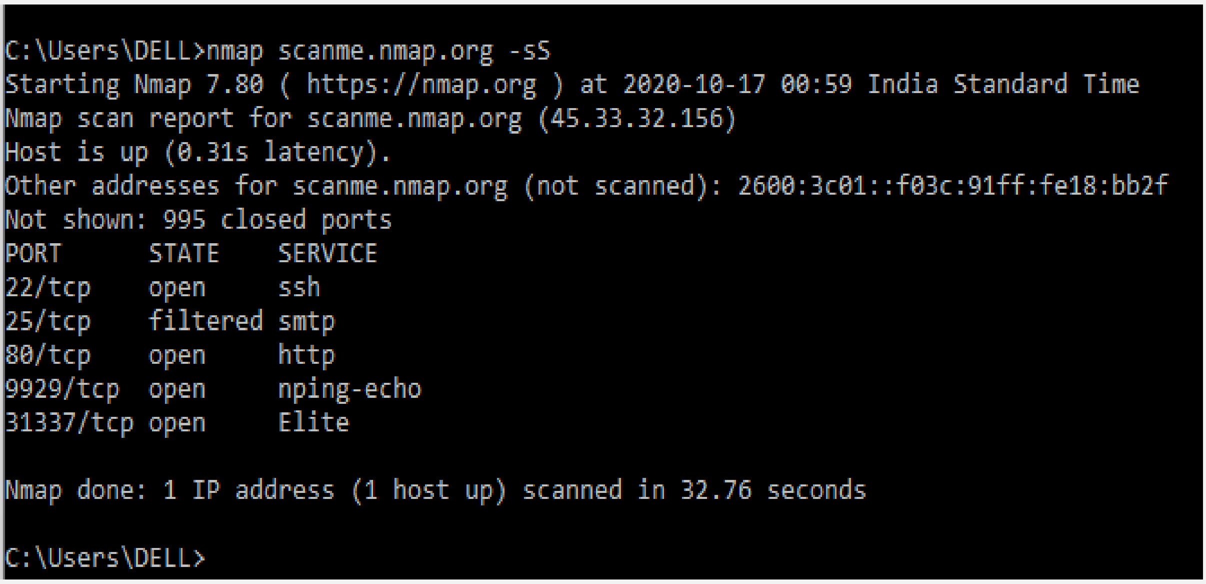


```
C:\Users\DELL>nmap 192.168.1.1-254
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-17 00:55 India Standard Time
Nmap scan report for 192.168.1.1
Host is up (0.0049s latency).
All 1000 scanned ports on 192.168.1.1 are closed (511) or filtered (489)

Nmap scan report for 192.168.1.2
Host is up (0.0073s latency).
All 1000 scanned ports on 192.168.1.2 are closed (511) or filtered (489)

Nmap done: 254 IP addresses (2 hosts up) scanned in 42.98 seconds

C:\Users\DELL>
```

2) VARIOUS TYPES OF SCANS

i) TCP SYN SCAN

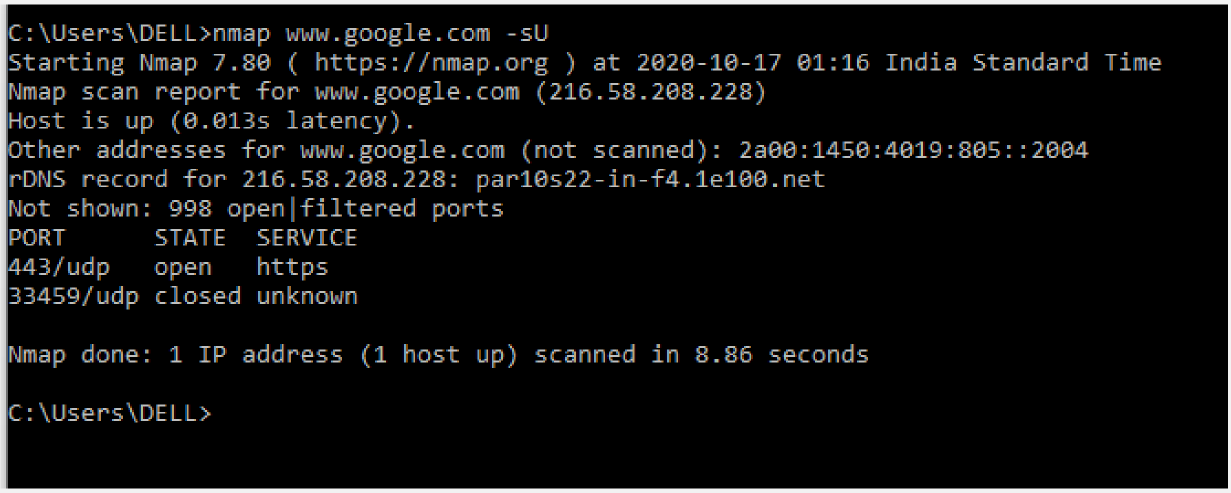
Command: nmap scanme.nmap.org -sS



```
C:\Users\DELL>nmap scanme.nmap.org -sS
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-17 00:59 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.31s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 995 closed ports
PORT      STATE    SERVICE
22/tcp    open     ssh
25/tcp    filtered smtp
80/tcp    open     http
9929/tcp  open     nping-echo
31337/tcp open     Elite

Nmap done: 1 IP address (1 host up) scanned in 32.76 seconds

C:\Users\DELL>
```

ii) UDP SCAN

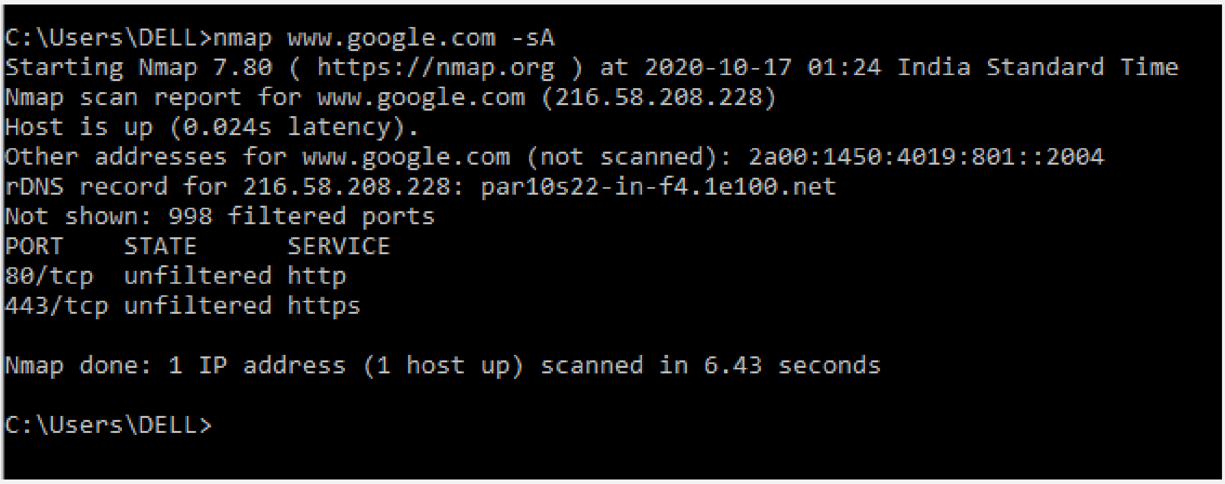
Command: nmap scanme.nmap.org –sU



```
C:\Users\DELL>nmap www.google.com -sU
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-17 01:16 India Standard Time
Nmap scan report for www.google.com (216.58.208.228)
Host is up (0.013s latency).
Other addresses for www.google.com (not scanned): 2a00:1450:4019:805::2004
rDNS record for 216.58.208.228: par10s22-in-f4.1e100.net
Not shown: 998 open|filtered ports
PORT      STATE  SERVICE
443/udp   open   https
33459/udp closed unknown

Nmap done: 1 IP address (1 host up) scanned in 8.86 seconds

C:\Users\DELL>
```

iii) TCP ACK SCAN

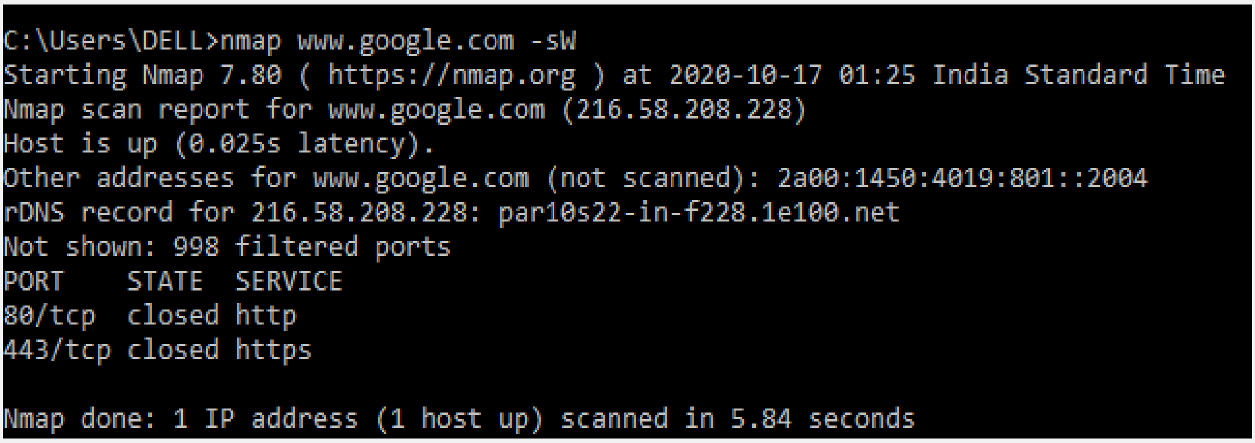
Command: nmap www.google.com –sA



```
C:\Users\DELL>nmap www.google.com -sA
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-17 01:24 India Standard Time
Nmap scan report for www.google.com (216.58.208.228)
Host is up (0.024s latency).
Other addresses for www.google.com (not scanned): 2a00:1450:4019:801::2004
rDNS record for 216.58.208.228: par10s22-in-f4.1e100.net
Not shown: 998 filtered ports
PORT    STATE      SERVICE
80/tcp  unfiltered http
443/tcp unfiltered https

Nmap done: 1 IP address (1 host up) scanned in 6.43 seconds

C:\Users\DELL>
```

iv) TCP WINDOW SCAN

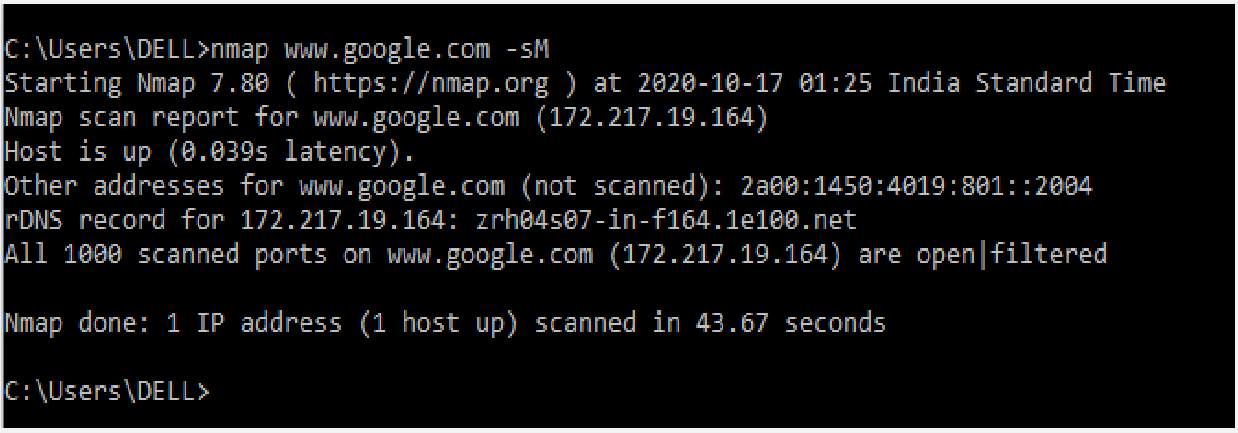
Command: nmap www.google.com –sW



```
C:\Users\DELL>nmap www.google.com -sW
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-17 01:25 India Standard Time
Nmap scan report for www.google.com (216.58.208.228)
Host is up (0.025s latency).
Other addresses for www.google.com (not scanned): 2a00:1450:4019:801::2004
rDNS record for 216.58.208.228: par10s22-in-f228.1e100.net
Not shown: 998 filtered ports
PORT    STATE  SERVICE
80/tcp  closed http
443/tcp closed https

Nmap done: 1 IP address (1 host up) scanned in 5.84 seconds
```

iv) TCP MAIMON SCAN

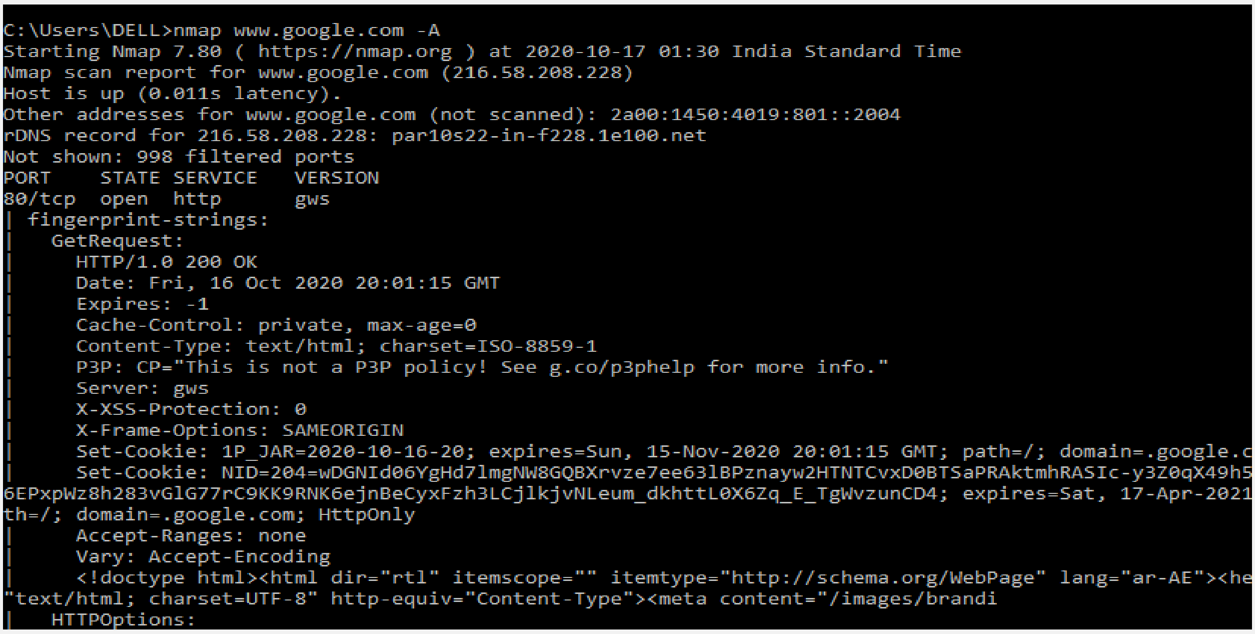
Command: nmap www.google.com –sM



```
C:\Users\DELL>nmap www.google.com -sM
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-17 01:25 India Standard Time
Nmap scan report for www.google.com (172.217.19.164)
Host is up (0.039s latency).
Other addresses for www.google.com (not scanned): 2a00:1450:4019:801::2004
rDNS record for 172.217.19.164: zrh04s07-in-f164.1e100.net
All 1000 scanned ports on www.google.com (172.217.19.164) are open|filtered

Nmap done: 1 IP address (1 host up) scanned in 43.67 seconds

C:\Users\DELL>
```

v) ADVANCED SCANNING/ AGGRESSIVE SCANNING

Command: nmap www.google.com –A

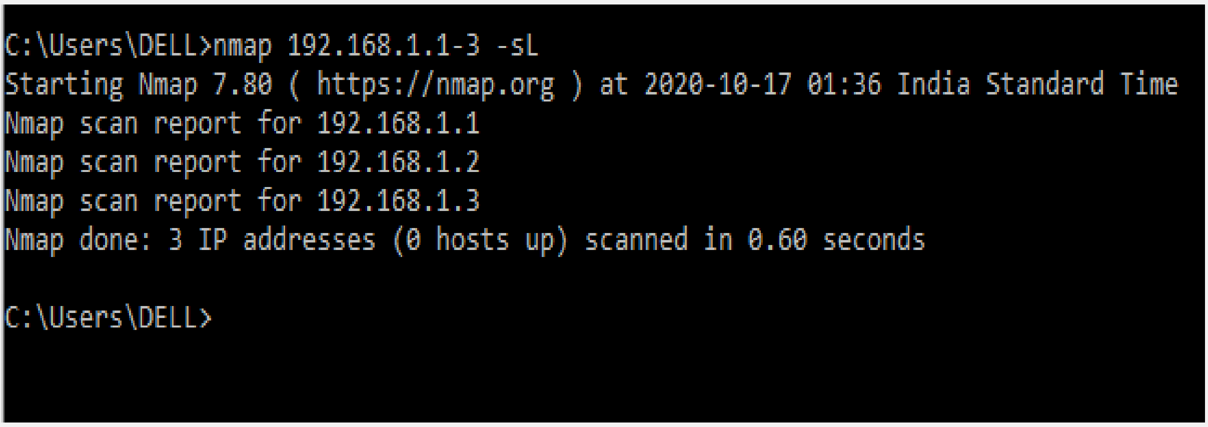


```
C:\Users\DELL>nmap www.google.com -A
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-17 01:30 India Standard Time
Nmap scan report for www.google.com (216.58.208.228)
Host is up (0.011s latency).
Other addresses for www.google.com (not scanned): 2a00:1450:4019:801::2004
rDNS record for 216.58.208.228: par10s22-in-f228.1e100.net
Not shown: 998 filtered ports
PORT    STATE SERVICE   VERSION
80/tcp  open  http      gws
| fingerprint-strings:
|   GetRequest:
|     HTTP/1.0 200 OK
|     Date: Fri, 16 Oct 2020 20:01:15 GMT
|     Expires: -1
|     Cache-Control: private, max-age=0
|     Content-Type: text/html; charset=ISO-8859-1
|     P3P: CP="This is not a P3P policy! See g.co/p3phelp for more info."
|     Server: gws
|     X-XSS-Protection: 0
|     X-Frame-Options: SAMEORIGIN
|     Set-Cookie: 1P_JAR=2020-10-16-20; expires=Sun, 15-Nov-2020 20:01:15 GMT; path=/; domain=.google.c
|     Set-Cookie: NID=204=wDGNId06YgHd7lmgNW8GQBXrvze7ee63lBPznayw2HTNTCvxD0BTSaPRAktmhRASIc-y3Z0qX49h5
6EPxpWz8h283vGlG77rC9KK9RNK6ejnBeCyxFzh3LCjlkjvNLeum_dkhttL0X6Zq_E_TgWvzunCD4; expires=Sat, 17-Apr-2021
th=/; domain=.google.com; HttpOnly
|     Accept-Ranges: none
|     Vary: Accept-Encoding
|     <!doctype html><html dir="rtl" itemscope="" itemtype="http://schema.org/WebPage" lang="ar-AE"><he
"text/html; charset=UTF-8" http-equiv="Content-Type"><meta content="/images/brandi
|   HTTPOptions:
```

3) HOST DISCOVERY

i) LISTING THE TARGETS

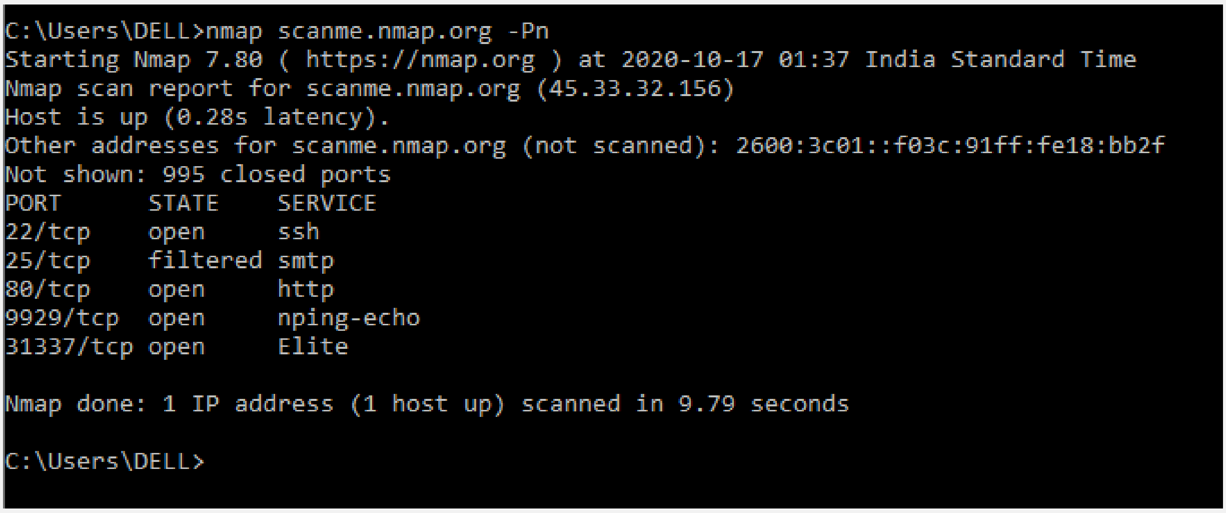
Command: nmap 192.168.1.1-3 –sL



```
C:\Users\DELL>nmap 192.168.1.1-3 -sL
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-17 01:36 India Standard Time
Nmap scan report for 192.168.1.1
Nmap scan report for 192.168.1.2
Nmap scan report for 192.168.1.3
Nmap done: 3 IP addresses (0 hosts up) scanned in 0.60 seconds

C:\Users\DELL>
```

ii) DOING PORT SCAN

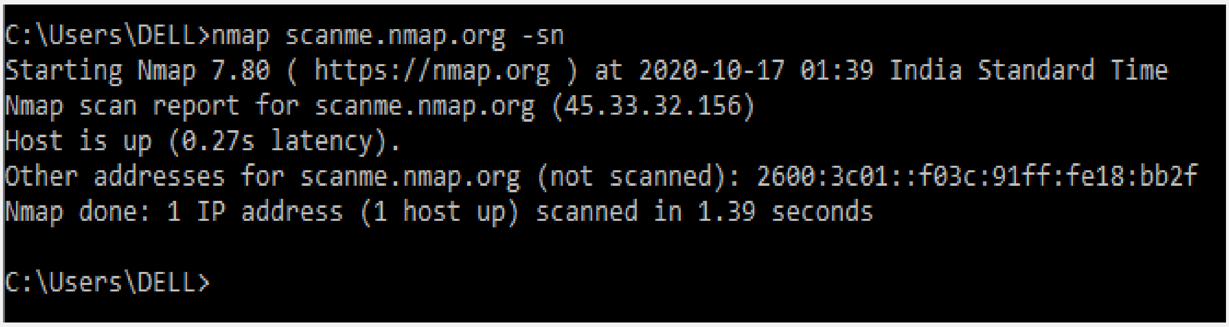
Command: nmap scanme.nmap.org –Pn



```
C:\Users\DELL>nmap scanme.nmap.org -Pn
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-17 01:37 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.28s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 995 closed ports
PORT      STATE    SERVICE
22/tcp    open     ssh
25/tcp    filtered smtp
80/tcp    open     http
9929/tcp  open     nping-echo
31337/tcp open     Elite

Nmap done: 1 IP address (1 host up) scanned in 9.79 seconds

C:\Users\DELL>
```

iii) HOST SCAN WITHOUT PORT SCAN

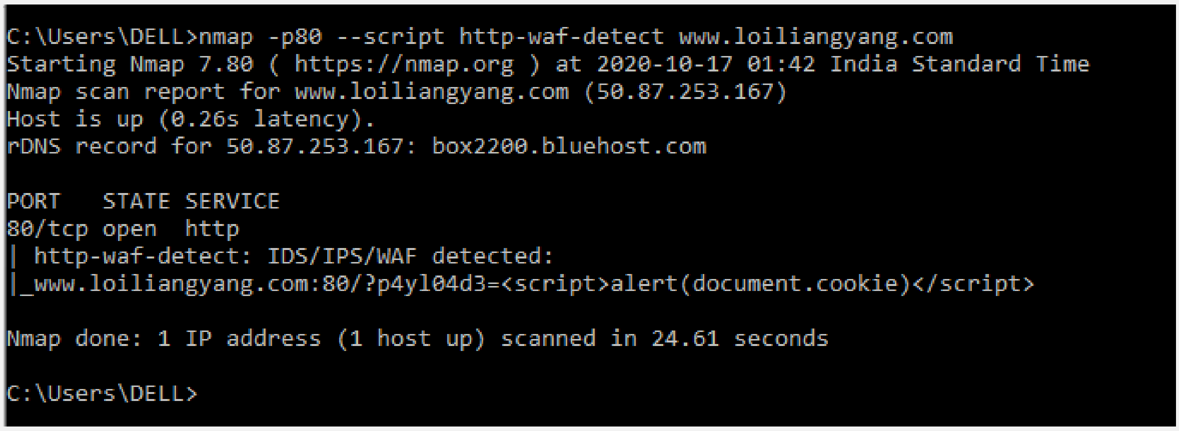
Command: nmap scanme.nmap.org –sn



```
C:\Users\DELL>nmap scanme.nmap.org -sn
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-17 01:39 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.27s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Nmap done: 1 IP address (1 host up) scanned in 1.39 seconds

C:\Users\DELL>
```

4) WEB APPLICATION FIREWALL DETECTION

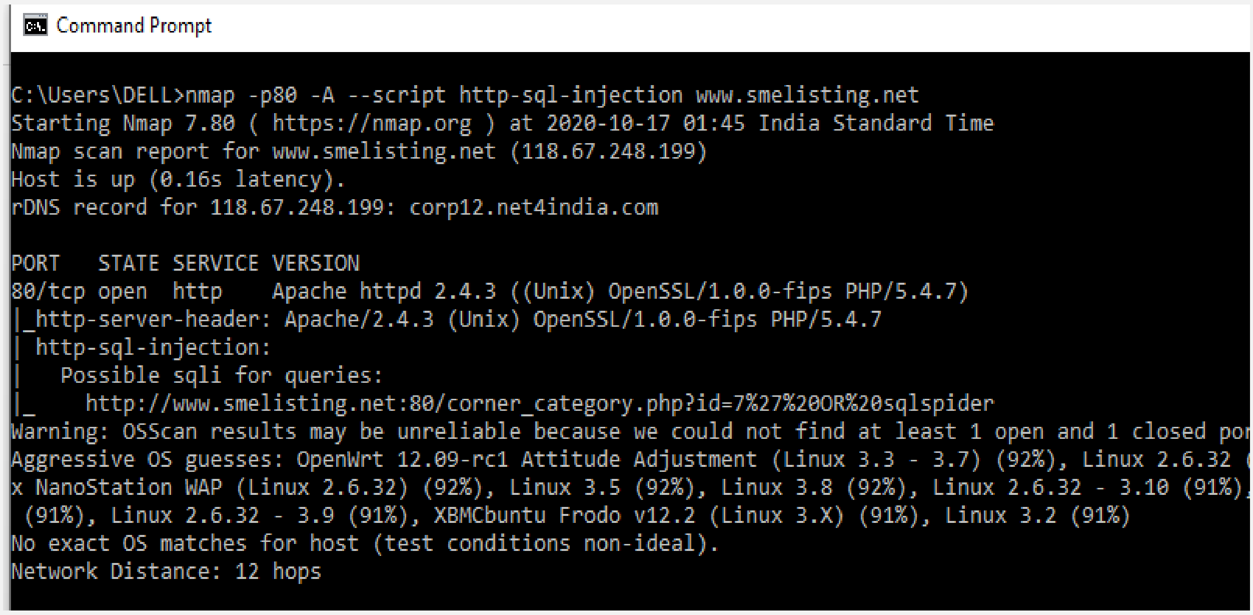
Command: nmap -p80 --script http-waf-detect www.loiliangyang.com



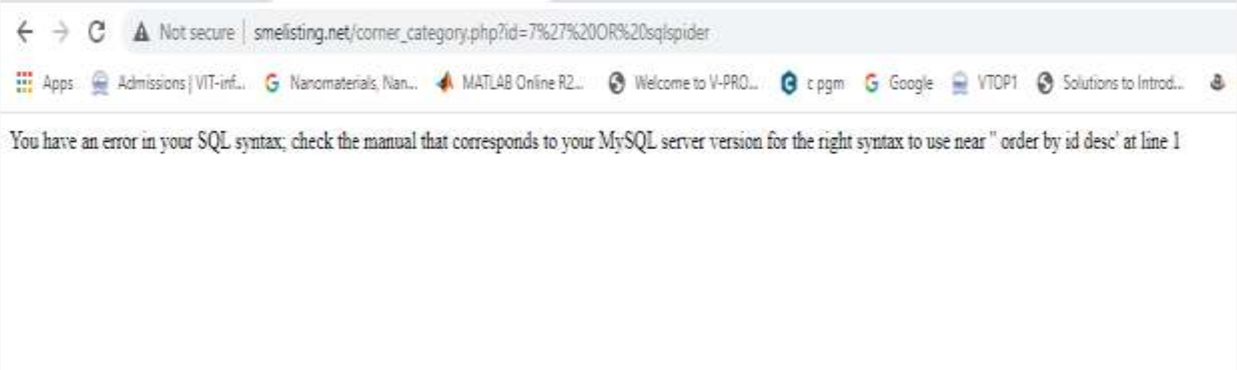
```
C:\Users\DELL>nmap -p80 --script http-waf-detect www.loiliangyang.com
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-17 01:42 India Standard Time
Nmap scan report for www.loiliangyang.com (50.87.253.167)
Host is up (0.26s latency).
rDNS record for 50.87.253.167: box2200.bluehost.com

PORT   STATE SERVICE
80/tcp open  http
| http-waf-detect: IDS/IPS/WAF detected:
|_www.loiliangyang.com:80/?p4yl04d3=<script>alert(document.cookie)</script>

Nmap done: 1 IP address (1 host up) scanned in 24.61 seconds

C:\Users\DELL>
```

5) SQL INJECTION ATTACK ON WEBSITE

Command: nmap -p80 -A --script http-sql-injection www.smelisting.net



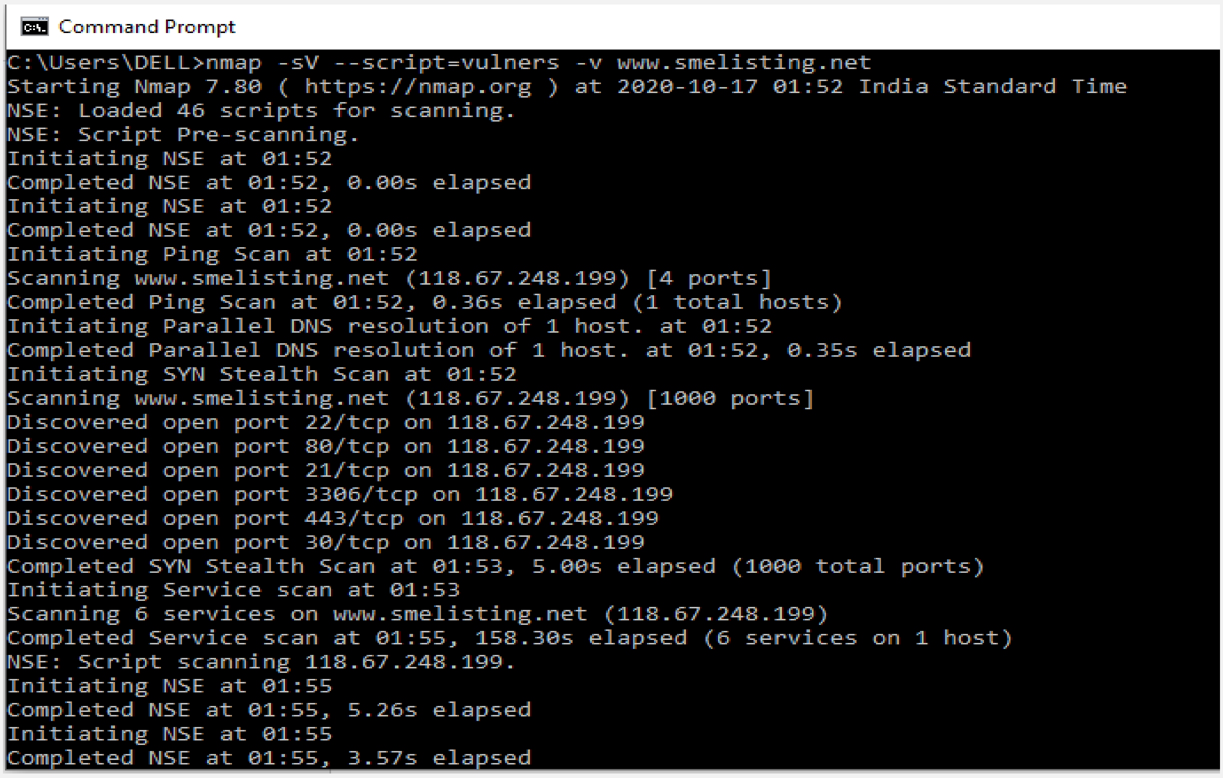
```
C:\Users\DELL>nmap -p80 -A --script http-sql-injection www.smelisting.net
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-17 01:45 India Standard Time
Nmap scan report for www.smelisting.net (118.67.248.199)
Host is up (0.16s latency).
rDNS record for 118.67.248.199: corp12.net4india.com

PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.3 ((Unix) OpenSSL/1.0.0-fips PHP/5.4.7)
|_http-server-header: Apache/2.4.3 (Unix) OpenSSL/1.0.0-fips PHP/5.4.7
| http-sql-injection:
|   Possible sqli for queries:
|_    http://www.smelisting.net:80/corner_category.php?id=7%27%20OR%20sqlspider
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed por
Aggressive OS guesses: OpenWrt 12.09-rc1 Attitude Adjustment (Linux 3.3 - 3.7) (92%), Linux 2.6.32 (
x NanoStation WAP (Linux 2.6.32) (92%), Linux 3.5 (92%), Linux 3.8 (92%), Linux 2.6.32 - 3.10 (91%),
 (91%), Linux 2.6.32 - 3.9 (91%), XBMCbuntu Frodo v12.2 (Linux 3.X) (91%), Linux 3.2 (91%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 12 hops
```



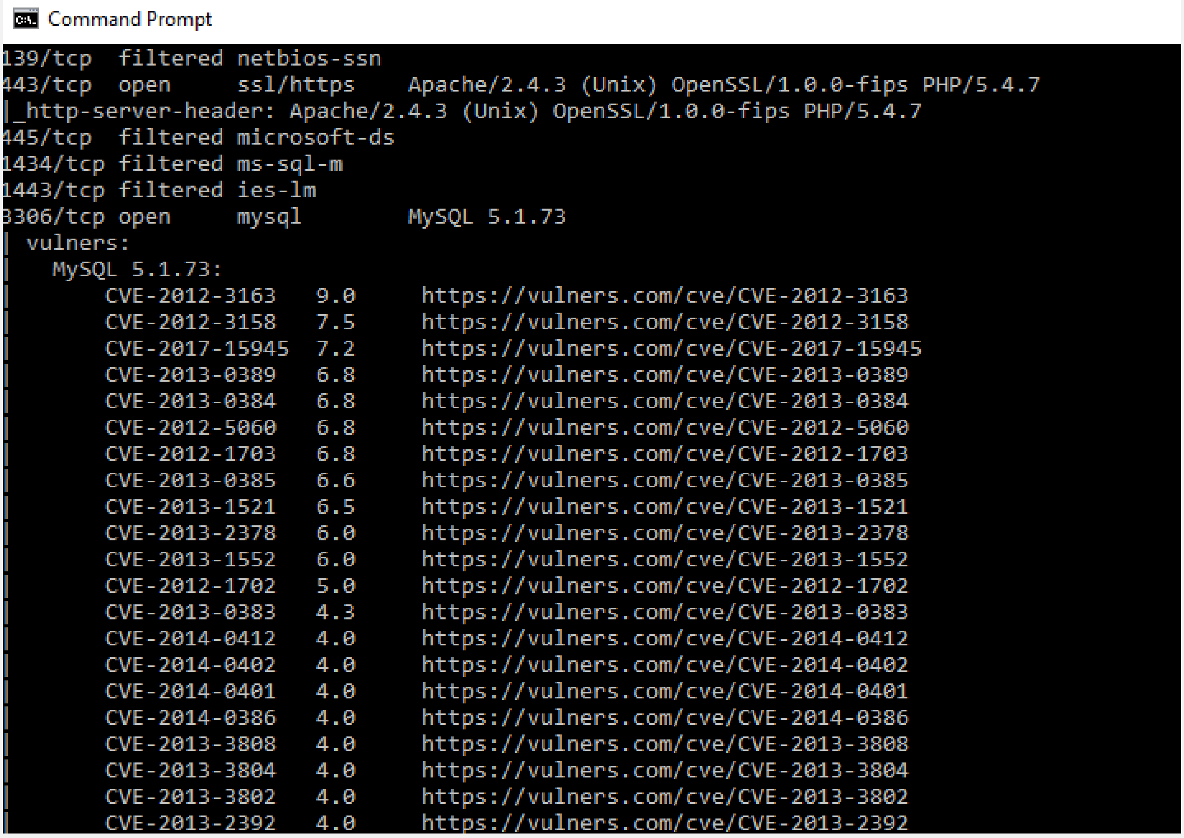
You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '' order by id desc' at line 1

6) VULNERABILITY SCANNING

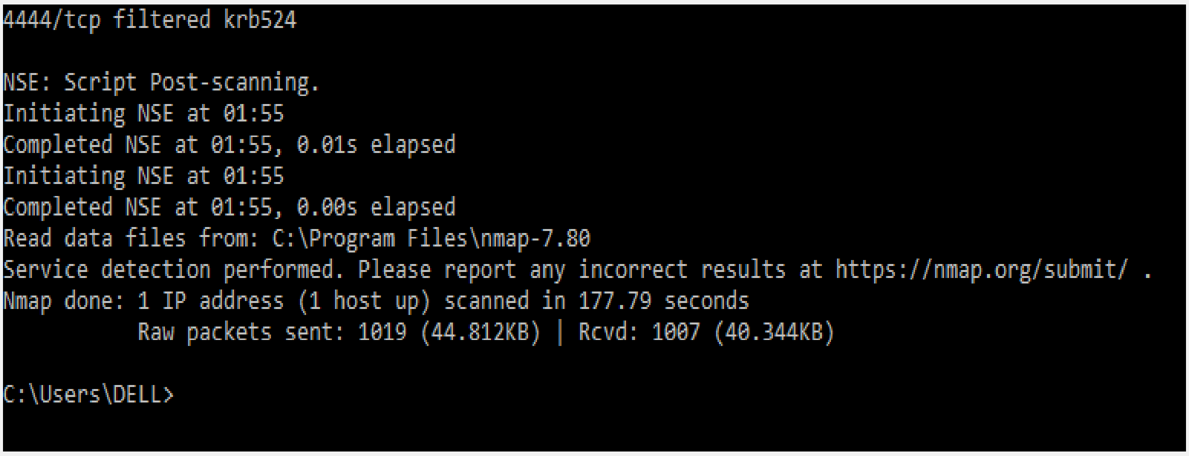
Command: nmap -sV --script=vulners -v www.smelisting.net



```
C:\Users\DELL>nmap -sV --script=vulners -v www.smelisting.net
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-17 01:52 India Standard Time
NSE: Loaded 46 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 01:52
Completed NSE at 01:52, 0.00s elapsed
Initiating NSE at 01:52
Completed NSE at 01:52, 0.00s elapsed
Initiating Ping Scan at 01:52
Scanning www.smelisting.net (118.67.248.199) [4 ports]
Completed Ping Scan at 01:52, 0.36s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 01:52
Completed Parallel DNS resolution of 1 host. at 01:52, 0.35s elapsed
Initiating SYN Stealth Scan at 01:52
Scanning www.smelisting.net (118.67.248.199) [1000 ports]
Discovered open port 22/tcp on 118.67.248.199
Discovered open port 80/tcp on 118.67.248.199
Discovered open port 21/tcp on 118.67.248.199
Discovered open port 3306/tcp on 118.67.248.199
Discovered open port 443/tcp on 118.67.248.199
Discovered open port 30/tcp on 118.67.248.199
Completed SYN Stealth Scan at 01:53, 5.00s elapsed (1000 total ports)
Initiating Service scan at 01:53
Scanning 6 services on www.smelisting.net (118.67.248.199)
Completed Service scan at 01:55, 158.30s elapsed (6 services on 1 host)
NSE: Script scanning 118.67.248.199.
Initiating NSE at 01:55
Completed NSE at 01:55, 5.26s elapsed
Initiating NSE at 01:55
Completed NSE at 01:55, 3.57s elapsed
```



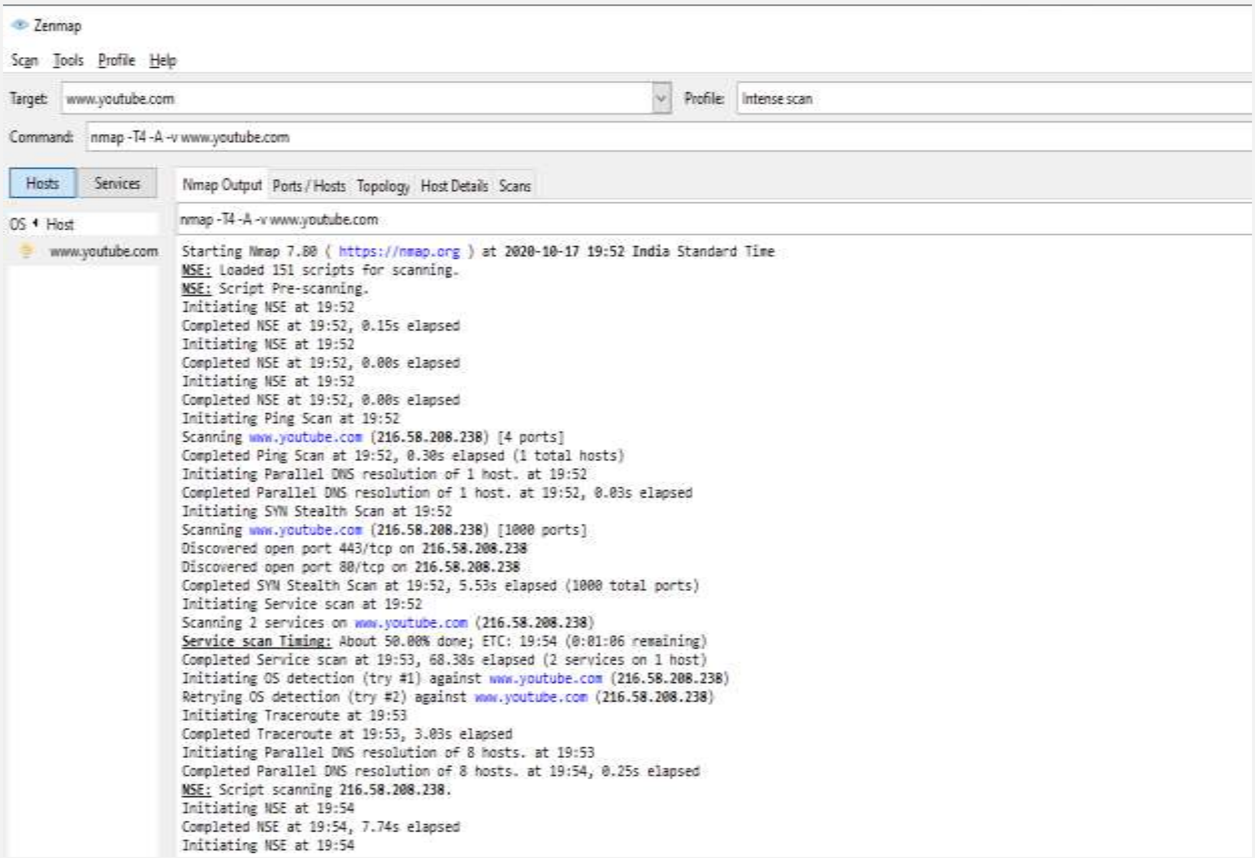
```
139/tcp  filtered netbios-ssn
443/tcp  open     ssl/https    Apache/2.4.3 (Unix) OpenSSL/1.0.0-fips PHP/5.4.7
|_http-server-header: Apache/2.4.3 (Unix) OpenSSL/1.0.0-fips PHP/5.4.7
445/tcp  filtered microsoft-ds
1434/tcp filtered ms-sql-m
1443/tcp filtered ies-lm
3306/tcp open     mysql        MySQL 5.1.73
| vulners:
|   MySQL 5.1.73:
|       CVE-2012-3163   9.0     https://vulners.com/cve/CVE-2012-3163
|       CVE-2012-3158   7.5     https://vulners.com/cve/CVE-2012-3158
|       CVE-2017-15945  7.2     https://vulners.com/cve/CVE-2017-15945
|       CVE-2013-0389   6.8     https://vulners.com/cve/CVE-2013-0389
|       CVE-2013-0384   6.8     https://vulners.com/cve/CVE-2013-0384
|       CVE-2012-5060   6.8     https://vulners.com/cve/CVE-2012-5060
|       CVE-2012-1703   6.8     https://vulners.com/cve/CVE-2012-1703
|       CVE-2013-0385   6.6     https://vulners.com/cve/CVE-2013-0385
|       CVE-2013-1521   6.5     https://vulners.com/cve/CVE-2013-1521
|       CVE-2013-2378   6.0     https://vulners.com/cve/CVE-2013-2378
|       CVE-2013-1552   6.0     https://vulners.com/cve/CVE-2013-1552
|       CVE-2012-1702   5.0     https://vulners.com/cve/CVE-2012-1702
|       CVE-2013-0383   4.3     https://vulners.com/cve/CVE-2013-0383
|       CVE-2014-0412   4.0     https://vulners.com/cve/CVE-2014-0412
|       CVE-2014-0402   4.0     https://vulners.com/cve/CVE-2014-0402
|       CVE-2014-0401   4.0     https://vulners.com/cve/CVE-2014-0401
|       CVE-2014-0386   4.0     https://vulners.com/cve/CVE-2014-0386
|       CVE-2013-3808   4.0     https://vulners.com/cve/CVE-2013-3808
|       CVE-2013-3804   4.0     https://vulners.com/cve/CVE-2013-3804
|       CVE-2013-3802   4.0     https://vulners.com/cve/CVE-2013-3802
|       CVE-2013-2392   4.0     https://vulners.com/cve/CVE-2013-2392
```



```
4444/tcp filtered krb524

NSE: Script Post-scanning.
Initiating NSE at 01:55
Completed NSE at 01:55, 0.01s elapsed
Initiating NSE at 01:55
Completed NSE at 01:55, 0.00s elapsed
Read data files from: C:\Program Files\nmap-7.80
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 177.79 seconds
           Raw packets sent: 1019 (44.812KB) | Rcvd: 1007 (40.344KB)

C:\Users\DELL>
```

CASE 2: USING ZENMAP

Doing an intense scan and obtaining the results.

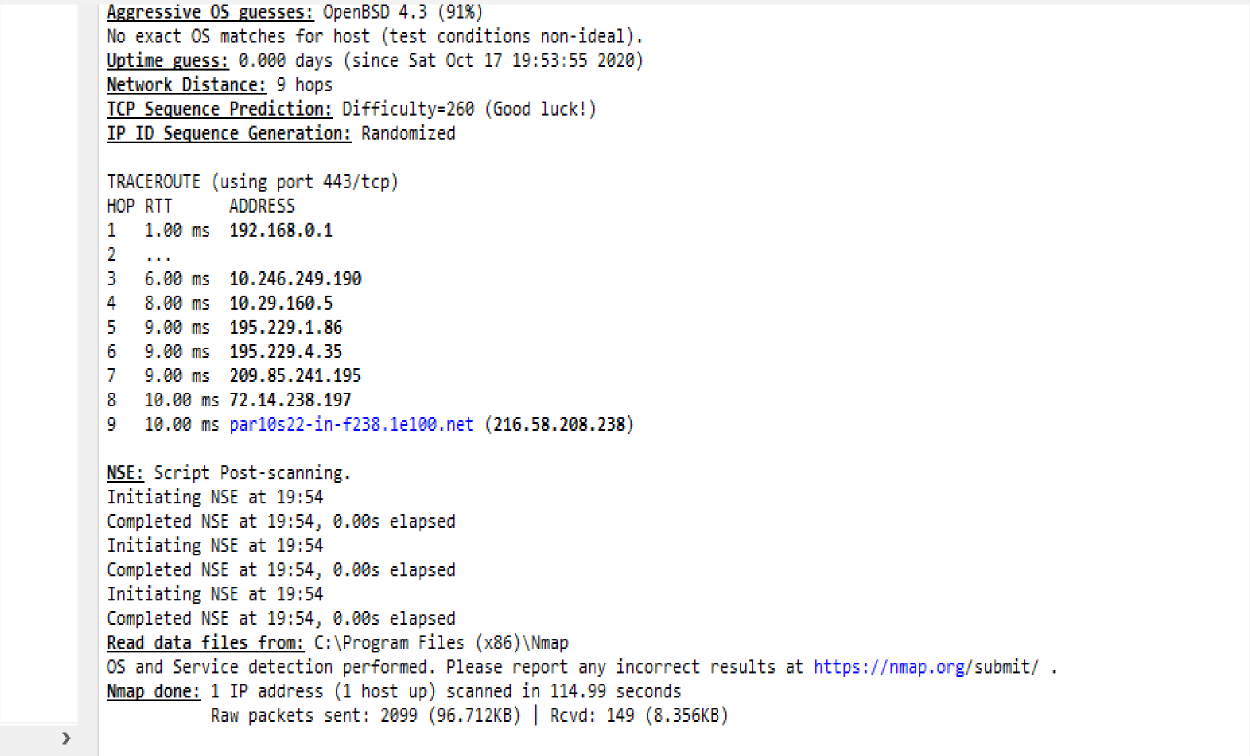


Target: www.youtube.com

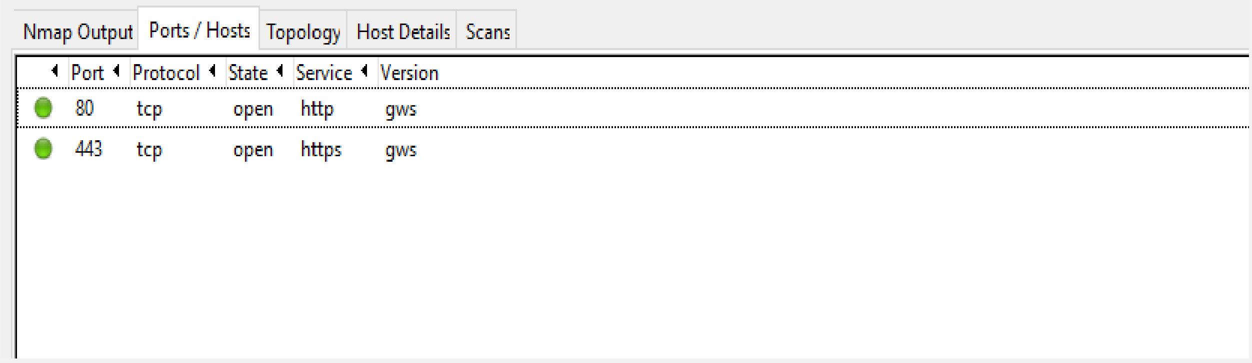
Profile: Intense scan

Command: nmap -T4 -A -v www.youtube.com

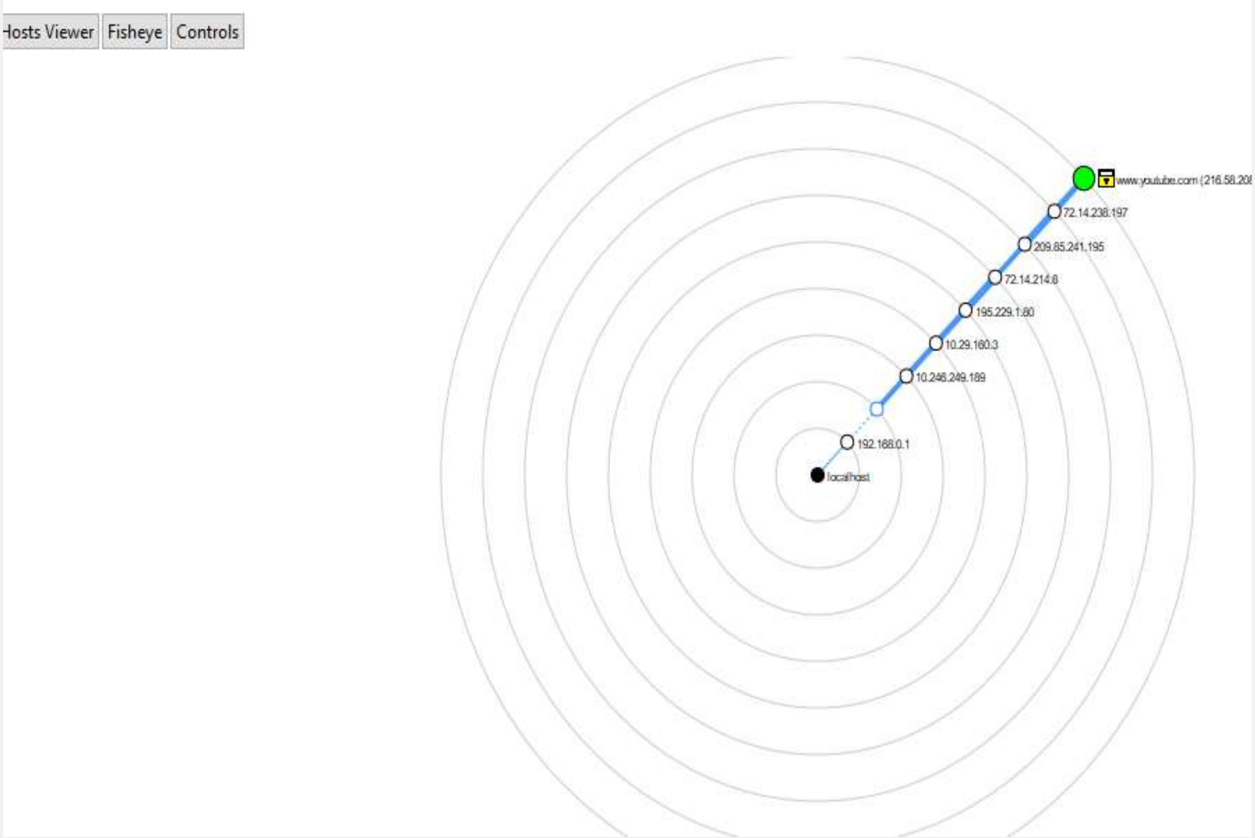
```
nmap -T4 -A -v www.youtube.com
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-17 19:52 India Standard Time
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 19:52
Completed NSE at 19:52, 0.15s elapsed
Initiating NSE at 19:52
Completed NSE at 19:52, 0.00s elapsed
Initiating NSE at 19:52
Completed NSE at 19:52, 0.00s elapsed
Initiating Ping Scan at 19:52
Scanning www.youtube.com (216.58.208.238) [4 ports]
Completed Ping Scan at 19:52, 0.30s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 19:52
Completed Parallel DNS resolution of 1 host. at 19:52, 0.03s elapsed
Initiating SYN Stealth Scan at 19:52
Scanning www.youtube.com (216.58.208.238) [1000 ports]
Discovered open port 443/tcp on 216.58.208.238
Discovered open port 80/tcp on 216.58.208.238
Completed SYN Stealth Scan at 19:52, 5.53s elapsed (1000 total ports)
Initiating Service scan at 19:52
Scanning 2 services on www.youtube.com (216.58.208.238)
Service scan Timing: About 50.00% done; ETC: 19:54 (0:01:06 remaining)
Completed Service scan at 19:53, 68.38s elapsed (2 services on 1 host)
Initiating OS detection (try #1) against www.youtube.com (216.58.208.238)
Retrying OS detection (try #2) against www.youtube.com (216.58.208.238)
Initiating Traceroute at 19:53
Completed Traceroute at 19:53, 3.03s elapsed
Initiating Parallel DNS resolution of 8 hosts. at 19:53
Completed Parallel DNS resolution of 8 hosts. at 19:54, 0.25s elapsed
NSE: Script scanning 216.58.208.238.
Initiating NSE at 19:54
Completed NSE at 19:54, 7.74s elapsed
Initiating NSE at 19:54
```

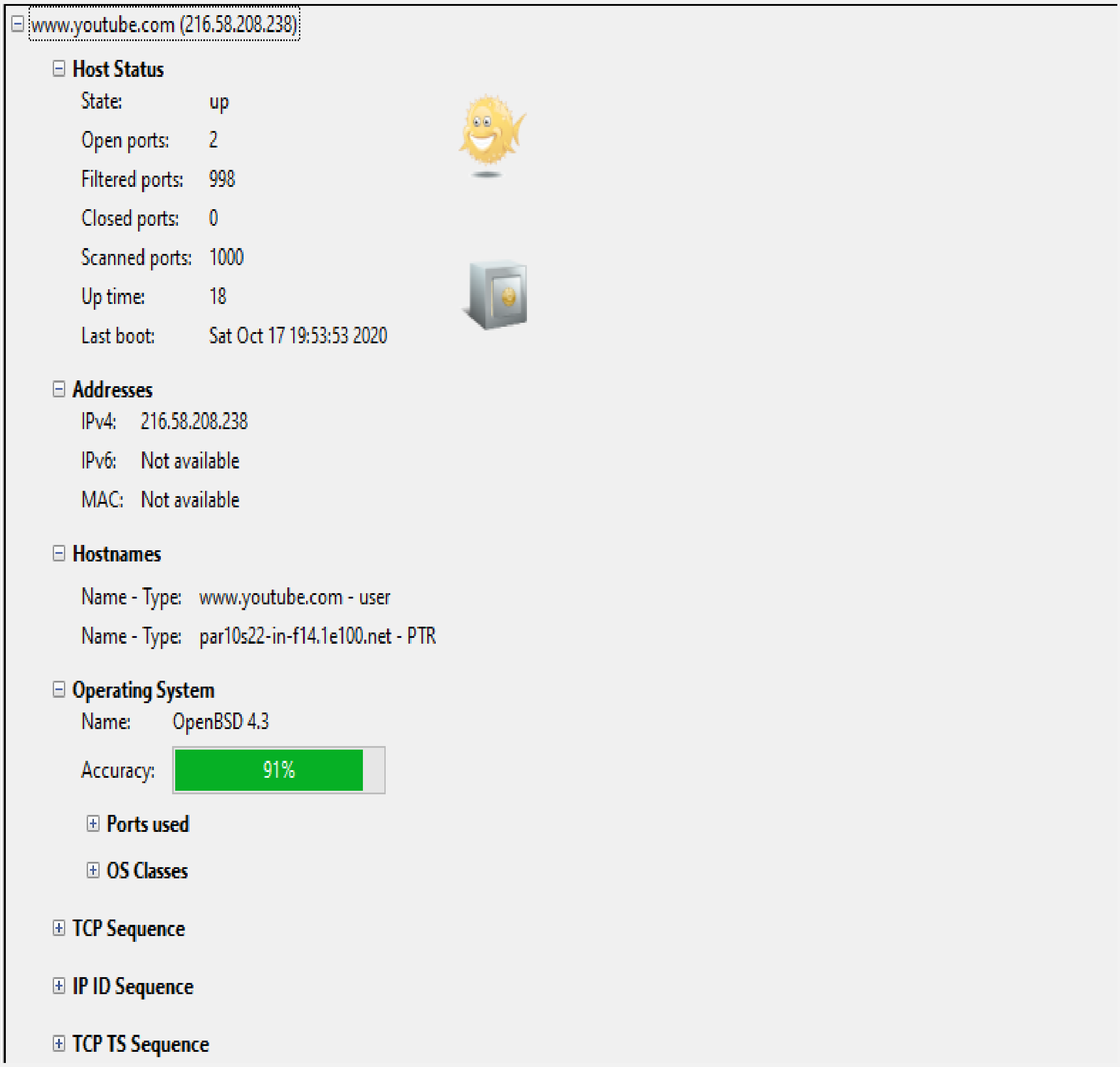


```
Aggressive OS guesses: OpenBSD 4.3 (91%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 0.000 days (since Sat Oct 17 19:53:55 2020)
Network Distance: 9 hops
TCP Sequence Prediction: Difficulty=260 (Good luck!)
IP ID Sequence Generation: Randomized

TRACEROUTE (using port 443/tcp)
HOP RTT      ADDRESS
1   1.00 ms  192.168.0.1
2   ...
3   6.00 ms  10.246.249.190
4   8.00 ms  10.29.160.5
5   9.00 ms  195.229.1.86
6   9.00 ms  195.229.4.35
7   9.00 ms  209.85.241.195
8   10.00 ms 72.14.238.197
9   10.00 ms par10s22-in-f238.1e100.net (216.58.208.238)

NSE: Script Post-scanning.
Initiating NSE at 19:54
Completed NSE at 19:54, 0.00s elapsed
Initiating NSE at 19:54
Completed NSE at 19:54, 0.00s elapsed
Initiating NSE at 19:54
Completed NSE at 19:54, 0.00s elapsed
Read data files from: C:\Program Files (x86)\Nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 114.99 seconds
           Raw packets sent: 2099 (96.712KB) | Rcvd: 149 (8.356KB)
```



	Port	Protocol	State	Service	Version
●	80	tcp	open	http	gws
●	443	tcp	open	https	gws





```
⊟ www.youtube.com (216.58.208.238)
    ⊟ Host Status
        State:           up
        Open ports:      2
        Filtered ports:  998
        Closed ports:    0
        Scanned ports:   1000
        Up time:         18
        Last boot:       Sat Oct 17 19:53:53 2020

    ⊟ Addresses
        IPv4:   216.58.208.238
        IPv6:   Not available
        MAC:    Not available

    ⊟ Hostnames
        Name - Type:   www.youtube.com - user
        Name - Type:   par10s22-in-f14.1e100.net - PTR

    ⊟ Operating System
        Name:       OpenBSD 4.3
        Accuracy:   91%

        ⊞ Ports used

        ⊞ OS Classes

    ⊞ TCP Sequence

    ⊞ IP ID Sequence

    ⊞ TCP TS Sequence
```

EXECUTION-VIDEO LINK

https://drive.google.com/drive/folders/14ZhAi1M_-U80fjSZ_dxk5ZBBtXB9A0L4?usp=sharing

REFERENCES

1) https://nmap.org/

2) https://www.stationx.net/nmap-cheat-sheet/

3)https://www.youtube.com/watch?v=aCC1O9hSzWo&ab_channel=LinuxAcademy

4)https://www.youtube.com/playlist?list=PLBf0hzazHTGOEuhPQSnq-Ej8jRyXxfYvl

5)https://www.youtube.com/watch?v=xHTXUjLod6Q&ab_channel=RuitzeCoderz

6) https://www.youtube.com/watch?v=3U1pJ-eJrAU&ab_channel=NullByte