Intrainz Project Submission

Footprinting with Nmap (Minor Project)

Introduction:

Foot printing is the process of gathering information about a target or network.

Nmap is a network exploration tool that can be used for foot printing.

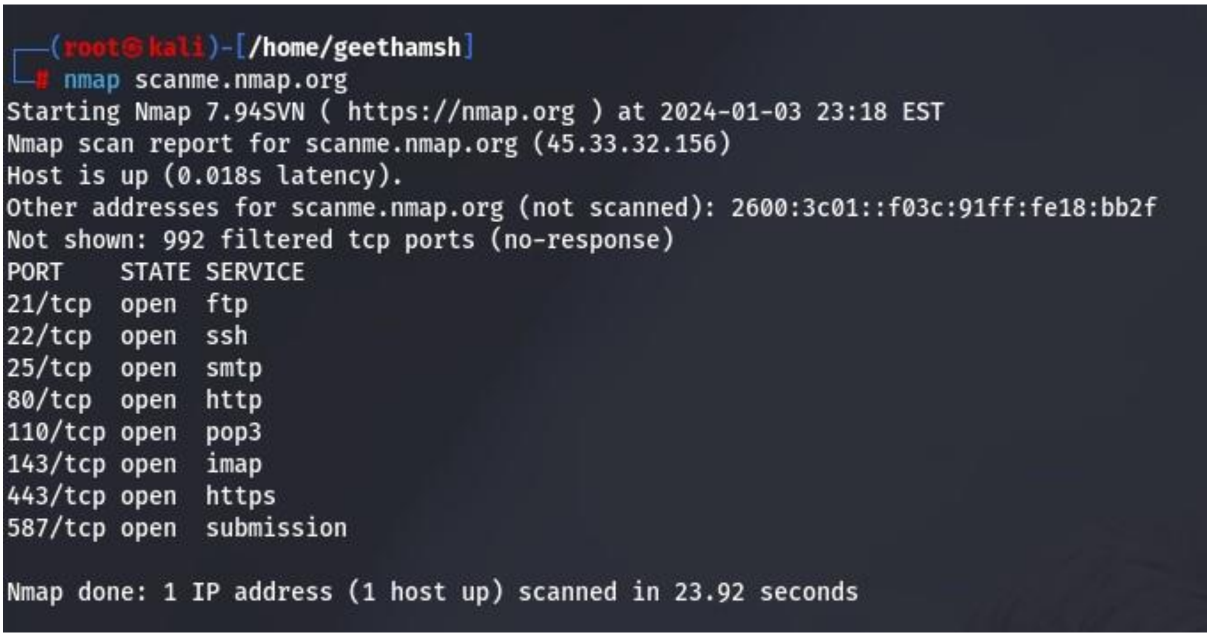
With Nmap, you can scan a target for open ports, services, operating systems, and other information.

Nmap also has many potential uses beyond foot printing, such as creating password crackers and network scanners.

BASIC NMAP SCAN:

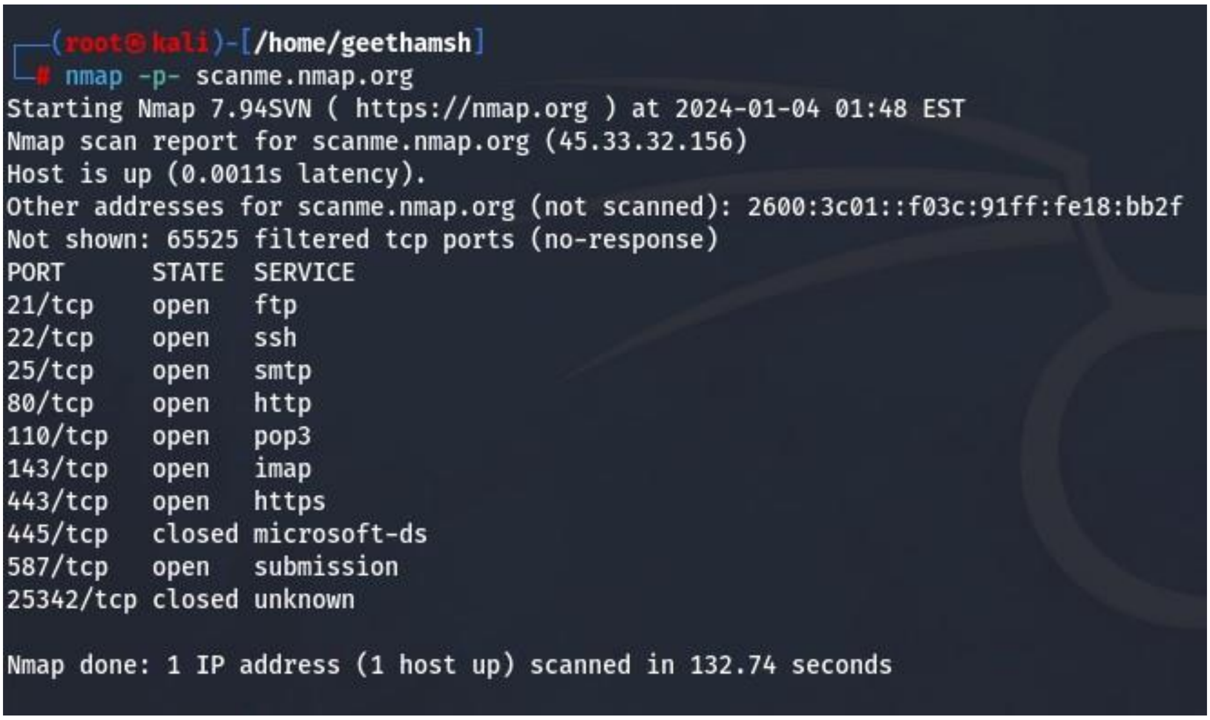
Select the target Nmap **scanme.nmap.org.**

Enter the target in the linux terminal and start scanning.



```
┌──(root㉿kali)-[/home/geethamsh]
└─# nmap scanme.nmap.org
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-03 23:18 EST
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.018s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 992 filtered tcp ports (no-response)
PORT    STATE SERVICE
21/tcp  open  ftp
22/tcp  open  ssh
25/tcp  open  smtp
80/tcp  open  http
110/tcp open  pop3
143/tcp open  imap
443/tcp open  https
587/tcp open  submission

Nmap done: 1 IP address (1 host up) scanned in 23.92 seconds
```

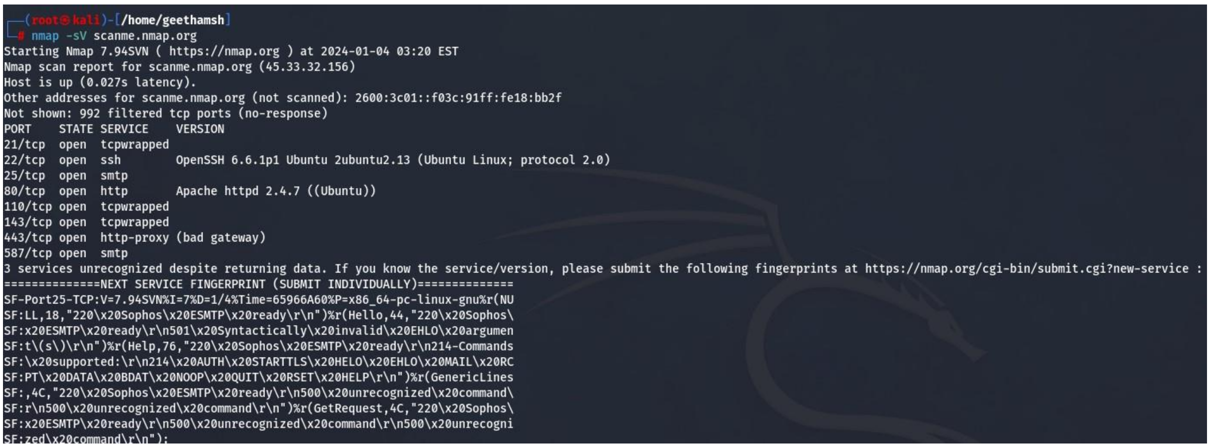
INITIAL NMAP SCAN:



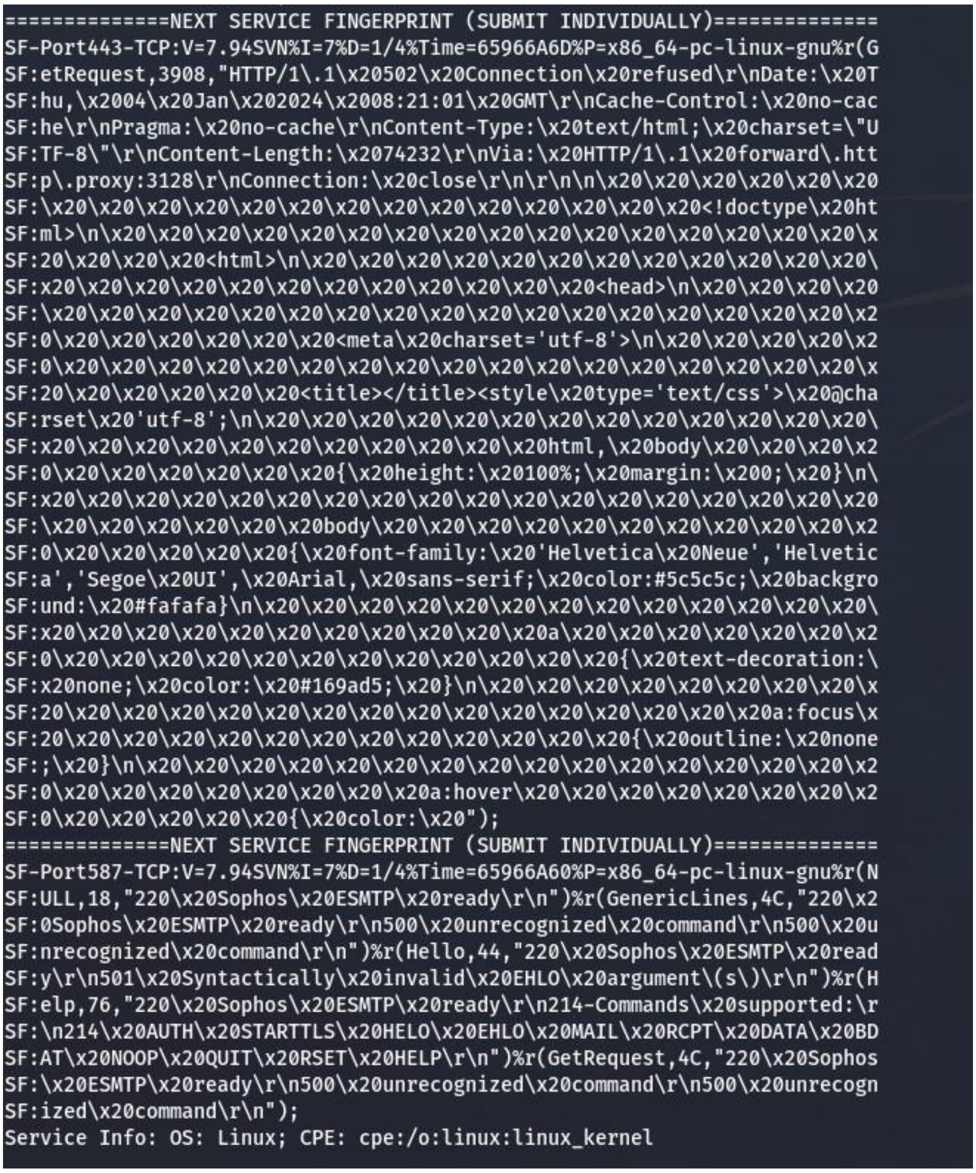
```
┌──(root㉿kali)-[/home/geethamsh]
└─# nmap -p- scanme.nmap.org
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-04 01:48 EST
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.0011s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 65525 filtered tcp ports (no-response)
PORT      STATE  SERVICE
21/tcp    open   ftp
22/tcp    open   ssh
25/tcp    open   smtp
80/tcp    open   http
110/tcp   open   pop3
143/tcp   open   imap
443/tcp   open   https
445/tcp   closed microsoft-ds
587/tcp   open   submission
25342/tcp closed unknown

Nmap done: 1 IP address (1 host up) scanned in 132.74 seconds
```

DETAILED VERSION DETECTION SCAN:

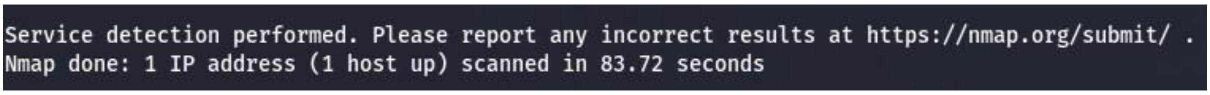
Obtain detailed information about the versions of services running on open ports. Identify potential vulnerabilities associated with specific service versions. Version Detection is used with the -sV command, and it allows the user to collect information about the port. This can include the version number, the service type, the operating system, the hostname, etc.



```
┌──(root㉿kali)-[/home/geethamsh]
└─# nmap -sV scanme.nmap.org
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-04 03:20 EST
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.027s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 992 filtered tcp ports (no-response)
PORT    STATE SERVICE    VERSION
21/tcp  open  tcpwrapped
22/tcp  open  ssh        OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
25/tcp  open  smtp
80/tcp  open  http       Apache httpd 2.4.7 ((Ubuntu))
110/tcp open  tcpwrapped
143/tcp open  tcpwrapped
443/tcp open  http-proxy (bad gateway)
587/tcp open  smtp
3 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprints at https://nmap.org/cgi-bin/submit.cgi?new-service :
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port25-TCP:V=7.94SVN%I=7%D=1/4%Time=65966A60%P=x86_64-pc-linux-gnu%r(NU
SF:LL,18,"220\x20Sophos\x20ESMTP\x20ready\r\n")%r(Hello,44,"220\x20Sophos\
SF:x20ESMTP\x20ready\r\n501\x20Syntactically\x20invalid\x20EHLO\x20argumen
SF:t\(s\)\r\n")%r(Help,76,"220\x20Sophos\x20ESMTP\x20ready\r\n214-Commands
SF:\x20supported:\r\n214\x20AUTH\x20STARTTLS\x20HELO\x20EHLO\x20MAIL\x20RC
SF:PT\x20DATA\x20BDAT\x20NOOP\x20QUIT\x20RSET\x20HELP\r\n")%r(GenericLines
SF:,4C,"220\x20Sophos\x20ESMTP\x20ready\r\n500\x20unrecognized\x20command\
SF:r\n500\x20unrecognized\x20command\r\n")%r(GetRequest,4C,"220\x20Sophos\
SF:x20ESMTP\x20ready\r\n500\x20unrecognized\x20command\r\n500\x20unrecogni
SF:zed\x20command\r\n");
```



```
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port443-TCP:V=7.94SVN%I=7%D=1/4%Time=65966A6D%P=x86_64-pc-linux-gnu%r(G
SF:etRequest,3908,"HTTP/1\.1\x20502\x20Connection\x20refused\r\nDate:\x20T
SF:hu,\x2004\x20Jan\x202024\x2008:21:01\x20GMT\r\nCache-Control:\x20no-cac
SF:he\r\nPragma:\x20no-cache\r\nContent-Type:\x20text/html;\x20charset=\"U
SF:TF-8\"\r\nContent-Length:\x2074232\r\nVia:\x20HTTP/1\.1\x20forward\.htt
SF:p\.proxy:3128\r\nConnection:\x20close\r\n\r\n\n\x20\x20\x20\x20\x20\x20
SF:\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20<!doctype\x20ht
SF:ml>\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x
SF:20\x20\x20\x20<html>\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\
SF:x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20<head>\n\x20\x20\x20\x20
SF:\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x2
SF:0\x20\x20\x20\x20\x20\x20<meta\x20charset='utf-8'>\n\x20\x20\x20\x20\x2
SF:0\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x
SF:20\x20\x20\x20\x20\x20<title></title><style\x20type='text/css'>\x20@cha
SF:rset\x20'utf-8';\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\
SF:x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20html,\x20body\x20\x20\x20\x2
SF:0\x20\x20\x20\x20\x20\x20{\x20height:\x20100%;\x20margin:\x200;\x20}\n\
SF:x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20
SF:\x20\x20\x20\x20\x20\x20body\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x2
SF:0\x20\x20\x20\x20\x20{\x20font-family:\x20'Helvetica\x20Neue','Helvetic
SF:a','Segoe\x20UI',\x20Arial,\x20sans-serif;\x20color:#5c5c5c;\x20backgro
SF:und:\x20#fafafa}\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\
SF:x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20a\x20\x20\x20\x20\x20\x20\x2
SF:0\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20{\x20text-decoration:\
SF:x20none;\x20color:\x20#169ad5;\x20}\n\x20\x20\x20\x20\x20\x20\x20\x20\x
SF:20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20a:focus\x
SF:20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20{\x20outline:\x20none
SF:;\x20}\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x2
SF:0\x20\x20\x20\x20\x20\x20\x20\x20a:hover\x20\x20\x20\x20\x20\x20\x20\x2
SF:0\x20\x20\x20\x20\x20{\x20color:\x20");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port587-TCP:V=7.94SVN%I=7%D=1/4%Time=65966A60%P=x86_64-pc-linux-gnu%r(N
SF:ULL,18,"220\x20Sophos\x20ESMTP\x20ready\r\n")%r(GenericLines,4C,"220\x2
SF:0Sophos\x20ESMTP\x20ready\r\n500\x20unrecognized\x20command\r\n500\x20u
SF:nrecognized\x20command\r\n")%r(Hello,44,"220\x20Sophos\x20ESMTP\x20read
SF:y\r\n501\x20Syntactically\x20invalid\x20EHLO\x20argument\(s\)\r\n")%r(H
SF:elp,76,"220\x20Sophos\x20ESMTP\x20ready\r\n214-Commands\x20supported:\r
SF:\n214\x20AUTH\x20STARTTLS\x20HELO\x20EHLO\x20MAIL\x20RCPT\x20DATA\x20BD
SF:AT\x20NOOP\x20QUIT\x20RSET\x20HELP\r\n")%r(GetRequest,4C,"220\x20Sophos
SF:\x20ESMTP\x20ready\r\n500\x20unrecognized\x20command\r\n500\x20unrecogn
SF:ized\x20command\r\n");
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

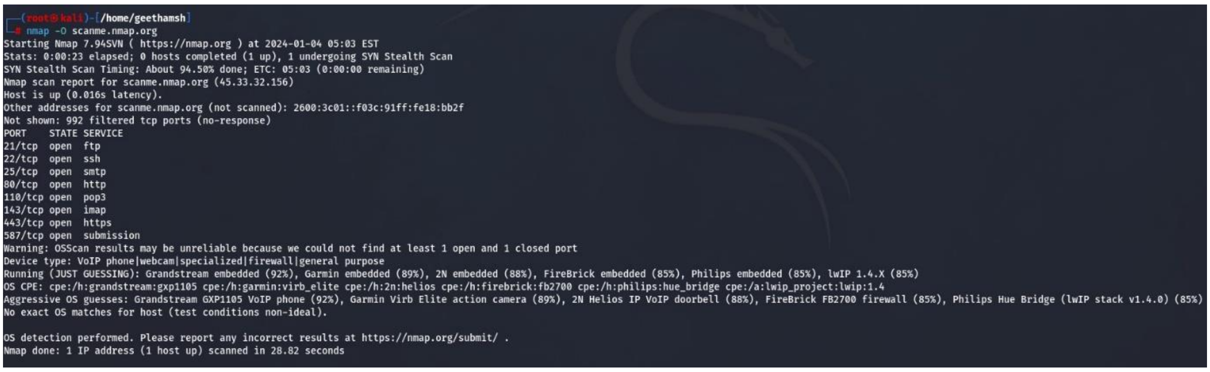


```
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 83.72 seconds
```

OS DETECTION NETWORK SCAN:

Nmap OS detection is a quick and powerful way to determine what operating system a remote device is running**.**

The following command is used for scanning the OS detection network scanning.



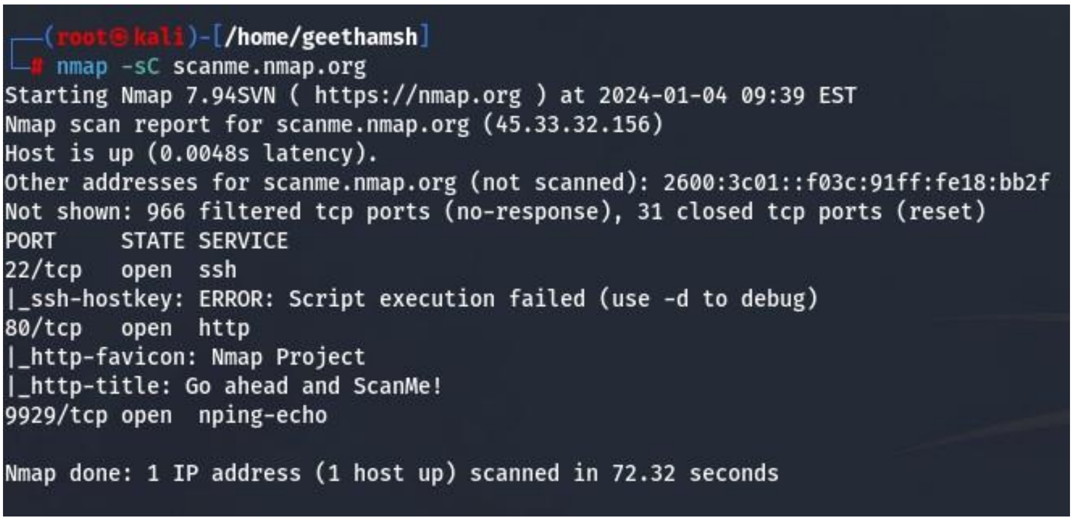
```
┌──(root㉿kali)-[/home/geethamsh]
└─# nmap -O scanme.nmap.org
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-04 05:03 EST
Stats: 0:00:23 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 94.50% done; ETC: 05:03 (0:00:00 remaining)
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.016s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 992 filtered tcp ports (no-response)
PORT    STATE SERVICE
21/tcp  open  ftp
22/tcp  open  ssh
25/tcp  open  smtp
80/tcp  open  http
110/tcp open  pop3
143/tcp open  imap
443/tcp open  https
587/tcp open  submission
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: VoIP phone|webcam|specialized|firewall|general purpose
Running (JUST GUESSING): Grandstream embedded (92%), Garmin embedded (89%), 2N embedded (88%), FireBrick embedded (85%), Philips embedded (85%), lwIP 1.4.X (85%)
OS CPE: cpe:/h:grandstream:gxp1105 cpe:/h:garmin:virb_elite cpe:/h:2n:helios cpe:/h:firebrick:fb2700 cpe:/h:philips:hue_bridge cpe:/a:lwip_project:lwip:1.4
Aggressive OS guesses: Grandstream GXP1105 VoIP phone (92%), Garmin Virb Elite action camera (89%), 2N Helios IP VoIP doorbell (88%), FireBrick FB2700 firewall (85%), Philips Hue Bridge (lwIP stack v1.4.0) (85%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 28.82 seconds
```

SCRIPT SCANNING:

Script scanning is a technique used in Nmap to execute predefined scripts against target systems to gather various types of information.

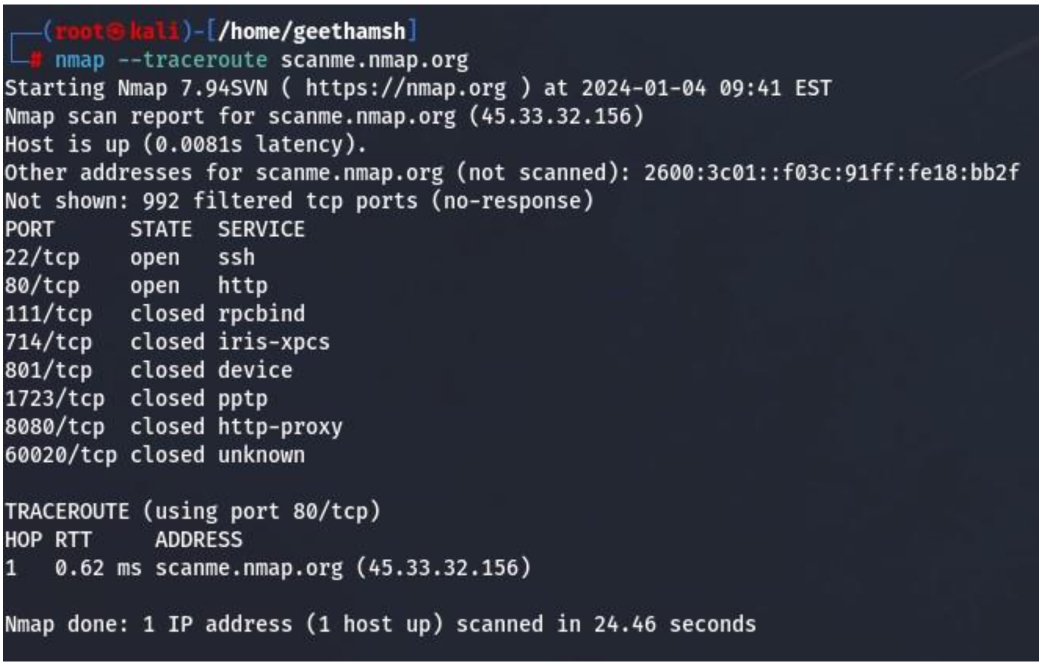
These scripts are written in the Lua programming language and are designed to probe specific services, operating systems, and applications.

Nmap script scanning can help identify vulnerabilities, misconfigurations, and potential security risks in target systems.



```
┌──(root㉿kali)-[/home/geethamsh]
└─# nmap -sC scanme.nmap.org
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-04 09:39 EST
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.0048s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 966 filtered tcp ports (no-response), 31 closed tcp ports (reset)
PORT     STATE SERVICE
22/tcp   open  ssh
|_ssh-hostkey: ERROR: Script execution failed (use -d to debug)
80/tcp   open  http
|_http-favicon: Nmap Project
|_http-title: Go ahead and ScanMe!
9929/tcp open  nping-echo

Nmap done: 1 IP address (1 host up) scanned in 72.32 seconds
```

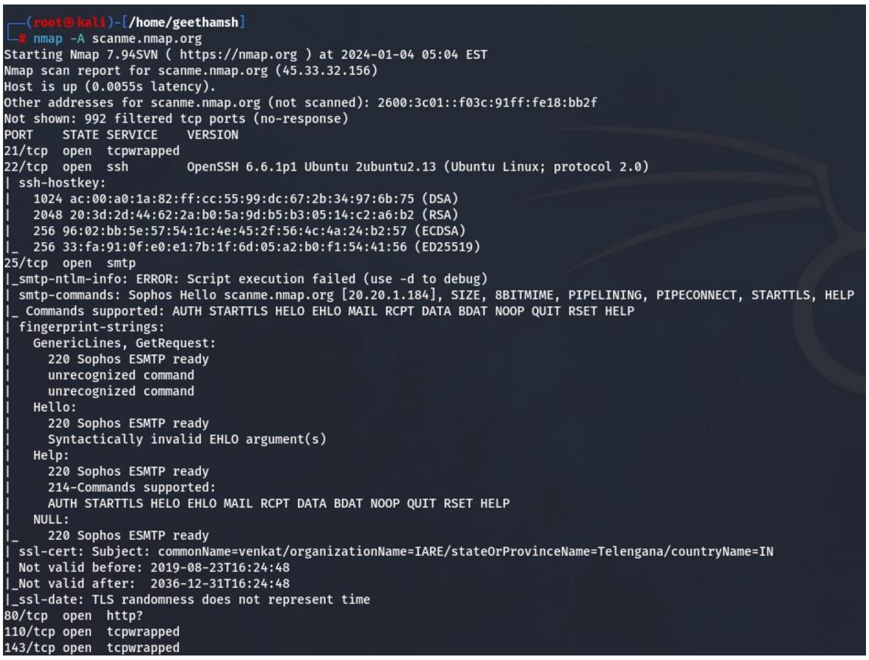
TRACEROUTE SCAN:



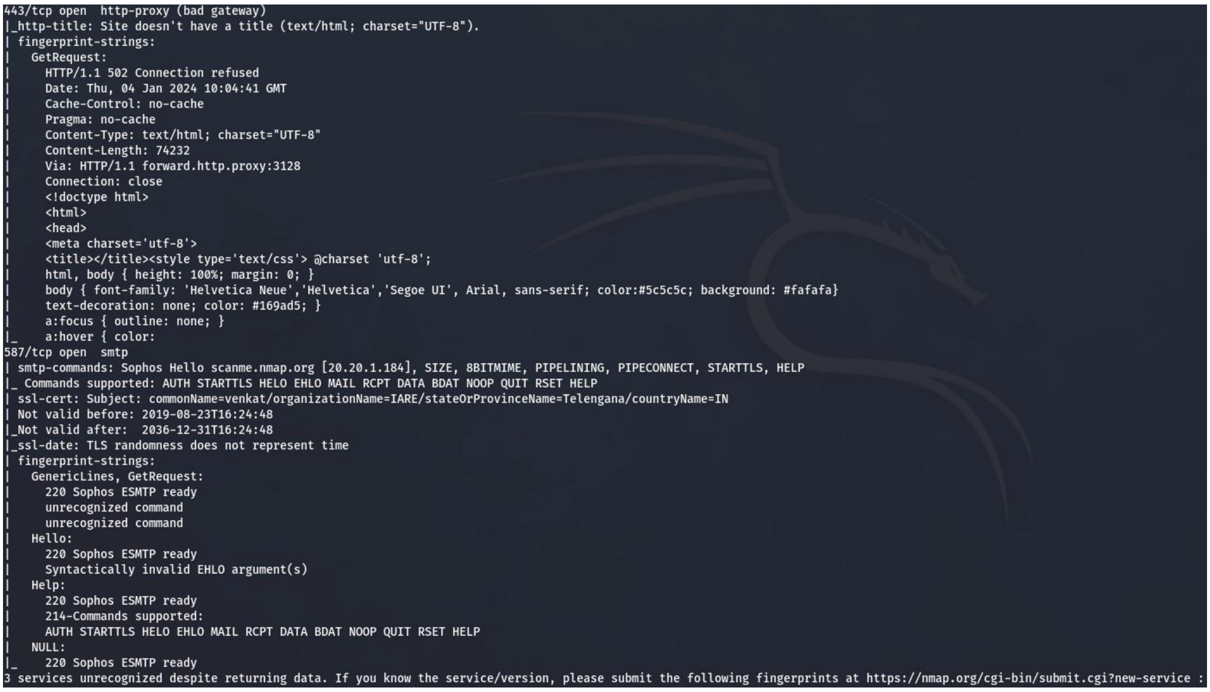
```
┌──(root㉿kali)-[/home/geethamsh]
└─# nmap --traceroute scanme.nmap.org
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-04 09:41 EST
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.0081s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 992 filtered tcp ports (no-response)
PORT      STATE  SERVICE
22/tcp    open   ssh
80/tcp    open   http
111/tcp   closed rpcbind
714/tcp   closed iris-xpcs
801/tcp   closed device
1723/tcp  closed pptp
8080/tcp  closed http-proxy
60020/tcp closed unknown

TRACEROUTE (using port 80/tcp)
HOP RTT     ADDRESS
1   0.62 ms scanme.nmap.org (45.33.32.156)

Nmap done: 1 IP address (1 host up) scanned in 24.46 seconds
```

AGGRESSIVE SCAN:

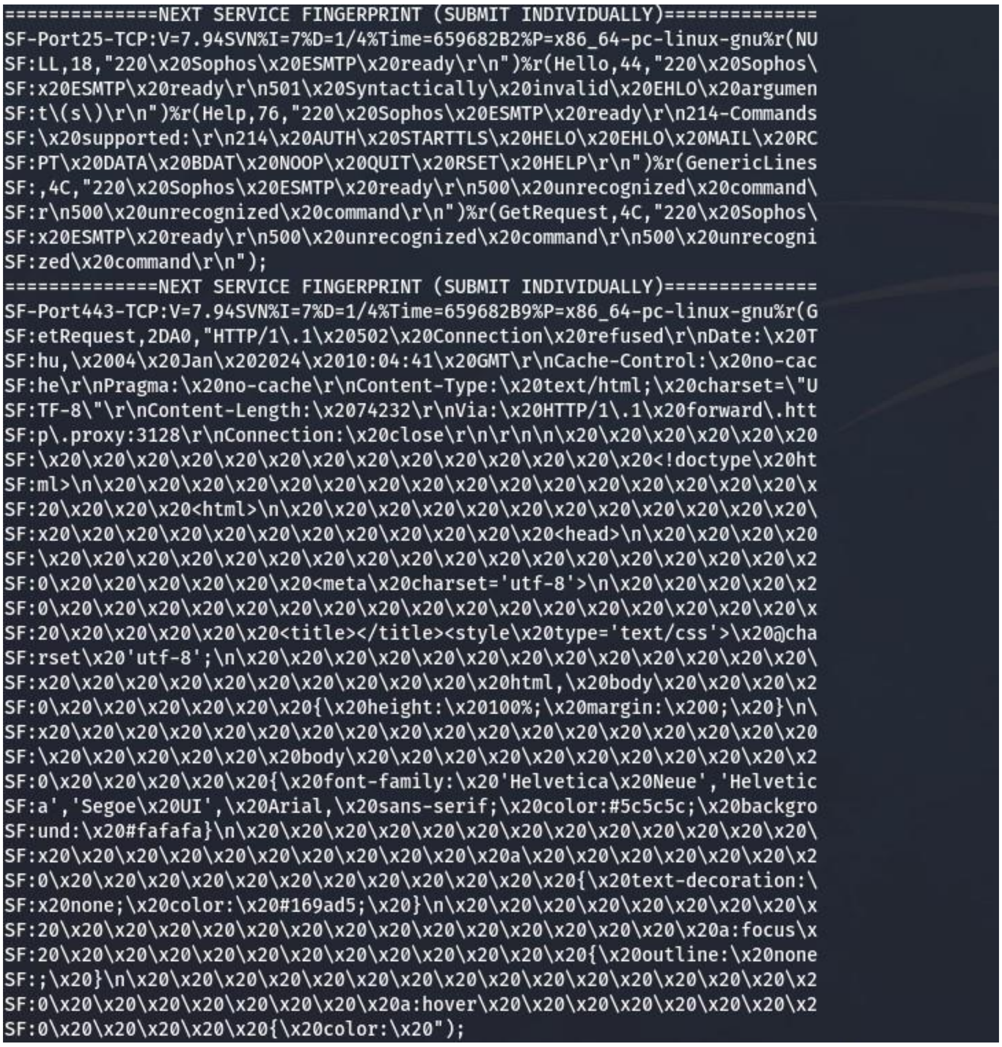
Aggressive mode enables OS detection (-O), version detection (-sV), script scanning (-sC), and traceroute (--traceroute). This mode sends a lot more probes, and it is more likely to be detected, but provides a lot of valuable host information. This scan mode can provide more detailed information about the systems and services installed on the target system, but it also requires more time and resources to run.



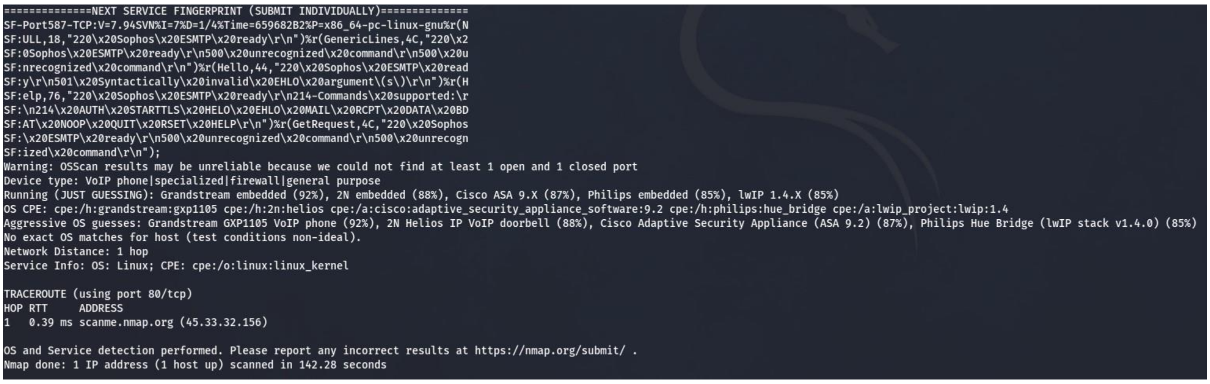
```
┌──(root㉿kali)-[/home/geethamsh]
└─# nmap -A scanme.nmap.org
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-04 05:04 EST
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.0055s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 992 filtered tcp ports (no-response)
PORT    STATE SERVICE    VERSION
21/tcp  open  tcpwrapped
22/tcp  open  ssh        OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 ac:00:a0:1a:82:ff:cc:55:99:dc:67:2b:34:97:6b:75 (DSA)
|   2048 20:3d:2d:44:62:2a:b0:5a:9d:b5:b3:05:14:c2:a6:b2 (RSA)
|   256 96:02:bb:5e:57:54:1c:4e:45:2f:56:4c:4a:24:b2:57 (ECDSA)
|_  256 33:fa:91:0f:e0:e1:7b:1f:6d:05:a2:b0:f1:54:41:56 (ED25519)
25/tcp  open  smtp
|_smtp-ntlm-info: ERROR: Script execution failed (use -d to debug)
| smtp-commands: Sophos Hello scanme.nmap.org [20.20.1.184], SIZE, 8BITMIME, PIPELINING, PIPECONNECT, STARTTLS, HELP
|_ Commands supported: AUTH STARTTLS HELO EHLO MAIL RCPT DATA BDAT NOOP QUIT RSET HELP
| fingerprint-strings:
|   GenericLines, GetRequest:
|     220 Sophos ESMTP ready
|     unrecognized command
|     unrecognized command
|   Hello:
|     220 Sophos ESMTP ready
|     Syntactically invalid EHLO argument(s)
|   Help:
|     220 Sophos ESMTP ready
|     214-Commands supported:
|     AUTH STARTTLS HELO EHLO MAIL RCPT DATA BDAT NOOP QUIT RSET HELP
|   NULL:
|_    220 Sophos ESMTP ready
| ssl-cert: Subject: commonName=venkat/organizationName=IARE/stateOrProvinceName=Telengana/countryName=IN
| Not valid before: 2019-08-23T16:24:48
|_Not valid after:  2036-12-31T16:24:48
|_ssl-date: TLS randomness does not represent time
80/tcp  open  http?
110/tcp open  tcpwrapped
143/tcp open  tcpwrapped
```



```
443/tcp open  http-proxy (bad gateway)
|_http-title: Site doesn't have a title (text/html; charset="UTF-8").
| fingerprint-strings:
|   GetRequest:
|     HTTP/1.1 502 Connection refused
|     Date: Thu, 04 Jan 2024 10:04:41 GMT
|     Cache-Control: no-cache
|     Pragma: no-cache
|     Content-Type: text/html; charset="UTF-8"
|     Content-Length: 74232
|     Via: HTTP/1.1 forward.http.proxy:3128
|     Connection: close
|     <!doctype html>
|     <html>
|     <head>
|     <meta charset='utf-8'>
|     <title></title><style type='text/css'> @charset 'utf-8';
|     html, body { height: 100%; margin: 0; }
|     body { font-family: 'Helvetica Neue','Helvetica','Segoe UI', Arial, sans-serif; color:#5c5c5c; background: #fafafa}
|     text-decoration: none; color: #169ad5; }
|     a:focus { outline: none; }
|_    a:hover { color:
587/tcp open  smtp
| smtp-commands: Sophos Hello scanme.nmap.org [20.20.1.184], SIZE, 8BITMIME, PIPELINING, PIPECONNECT, STARTTLS, HELP
|_ Commands supported: AUTH STARTTLS HELO EHLO MAIL RCPT DATA BDAT NOOP QUIT RSET HELP
| ssl-cert: Subject: commonName=venkat/organizationName=IARE/stateOrProvinceName=Telengana/countryName=IN
| Not valid before: 2019-08-23T16:24:48
|_Not valid after:  2036-12-31T16:24:48
|_ssl-date: TLS randomness does not represent time
| fingerprint-strings:
|   GenericLines, GetRequest:
|     220 Sophos ESMTP ready
|     unrecognized command
|     unrecognized command
|   Hello:
|     220 Sophos ESMTP ready
|     Syntactically invalid EHLO argument(s)
|   Help:
|     220 Sophos ESMTP ready
|     214-Commands supported:
|     AUTH STARTTLS HELO EHLO MAIL RCPT DATA BDAT NOOP QUIT RSET HELP
|   NULL:
|_    220 Sophos ESMTP ready
3 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprints at https://nmap.org/cgi-bin/submit.cgi?new-service :
```



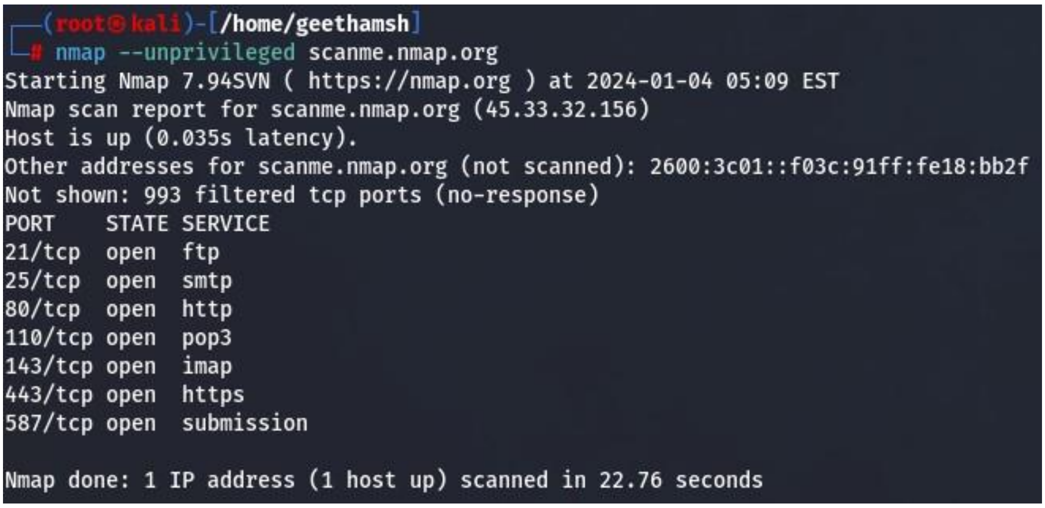
```
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port25-TCP:V=7.94SVN%I=7%D=1/4%Time=659682B2%P=x86_64-pc-linux-gnu%r(NU
SF:LL,18,"220\x20Sophos\x20ESMTP\x20ready\r\n")%r(Hello,44,"220\x20Sophos\
SF:x20ESMTP\x20ready\r\n501\x20Syntactically\x20invalid\x20EHLO\x20argumen
SF:t\(s\)\r\n")%r(Help,76,"220\x20Sophos\x20ESMTP\x20ready\r\n214-Commands
SF:\x20supported:\r\n214\x20AUTH\x20STARTTLS\x20HELO\x20EHLO\x20MAIL\x20RC
SF:PT\x20DATA\x20BDAT\x20NOOP\x20QUIT\x20RSET\x20HELP\r\n")%r(GenericLines
SF:,4C,"220\x20Sophos\x20ESMTP\x20ready\r\n500\x20unrecognized\x20command\
SF:r\n500\x20unrecognized\x20command\r\n")%r(GetRequest,4C,"220\x20Sophos\
SF:x20ESMTP\x20ready\r\n500\x20unrecognized\x20command\r\n500\x20unrecogni
SF:zed\x20command\r\n");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port443-TCP:V=7.94SVN%I=7%D=1/4%Time=659682B9%P=x86_64-pc-linux-gnu%r(G
SF:etRequest,2DA0,"HTTP/1\.1\x20502\x20Connection\x20refused\r\nDate:\x20T
SF:hu,\x2004\x20Jan\x202024\x2010:04:41\x20GMT\r\nCache-Control:\x20no-cac
SF:he\r\nPragma:\x20no-cache\r\nContent-Type:\x20text/html;\x20charset=\"U
SF:TF-8\"\r\nContent-Length:\x2074232\r\nVia:\x20HTTP/1\.1\x20forward\.htt
SF:p\.proxy:3128\r\nConnection:\x20close\r\n\r\n\n\x20\x20\x20\x20\x20\x20
SF:\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20<!doctype\x20ht
SF:ml>\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x
SF:20\x20\x20\x20<html>\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\
SF:x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20<head>\n\x20\x20\x20\x20
SF:\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x2
SF:0\x20\x20\x20\x20\x20\x20<meta\x20charset='utf-8'>\n\x20\x20\x20\x20\x2
SF:0\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x
SF:20\x20\x20\x20\x20\x20<title></title><style\x20type='text/css'>\x20@cha
SF:rset\x20'utf-8';\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\
SF:x20\x20\x20\x20\x20\x20\x20\x20\x20\x20html,\x20body\x20\x20\x20\x2
SF:0\x20\x20\x20\x20\x20\x20{\x20height:\x20100%;\x20margin:\x200;\x20}\n\
SF:x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20
SF:\x20\x20\x20\x20\x20\x20body\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x2
SF:0\x20\x20\x20\x20\x20{\x20font-family:\x20'Helvetica\x20Neue','Helvetic
SF:a','Segoe\x20UI',\x20Arial,\x20sans-serif;\x20color:#5c5c5c;\x20backgro
SF:und:\x20#fafafa}\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\
SF:x20\x20\x20\x20\x20\x20\x20\x20\x20\x20a\x20\x20\x20\x20\x20\x20\x2
SF:0\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20{\x20text-decoration:\
SF:x20none;\x20color:\x20#169ad5;\x20}\n\x20\x20\x20\x20\x20\x20\x20\x20\x
SF:20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20a:focus\x
SF:20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20{\x20outline:\x20none
SF:;\x20}\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x2
SF:0\x20\x20\x20\x20\x20\x20\x20a:hover\x20\x20\x20\x20\x20\x20\x20\x2
SF:0\x20\x20\x20\x20\x20{\x20color:\x20");
```



```
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port587-TCP:V=7.94SVN%I=7%D=1/4%Time=659682B2%P=x86_64-pc-linux-gnu%r(N
SF:ULL,18,"220\x20Sophos\x20ESMTP\x20ready\r\n")%r(GenericLines,4C,"220\x2
SF:0Sophos\x20ESMTP\x20ready\r\n500\x20unrecognized\x20command\r\n500\x20u
SF:nrecognized\x20command\r\n")%r(Hello,44,"220\x20Sophos\x20ESMTP\x20read
SF:y\r\n501\x20Syntactically\x20invalid\x20EHLO\x20argument\(s\)\r\n")%r(H
SF:elp,76,"220\x20Sophos\x20ESMTP\x20ready\r\n214-Commands\x20supported:\r
SF:\n214\x20AUTH\x20STARTTLS\x20HELO\x20EHLO\x20MAIL\x20RCPT\x20DATA\x20BD
SF:AT\x20NOOP\x20QUIT\x20RSET\x20HELP\r\n")%r(GetRequest,4C,"220\x20Sophos
SF:\x20ESMTP\x20ready\r\n500\x20unrecognized\x20command\r\n500\x20unrecogn
SF:ized\x20command\r\n");
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: VoIP phone|specialized|firewall|general purpose
Running (JUST GUESSING): Grandstream embedded (92%), 2N embedded (88%), Cisco ASA 9.X (87%), Philips embedded (85%), lwIP 1.4.X (85%)
OS CPE: cpe:/h:grandstream:gxp1105 cpe:/h:2n:helios cpe:/a:cisco:adaptive_security_appliance_software:9.2 cpe:/h:philips:hue_bridge cpe:/a:lwip_project:lwip:1.4
Aggressive OS guesses: Grandstream GXP1105 VoIP phone (92%), 2N Helios IP VoIP doorbell (88%), Cisco Adaptive Security Appliance (ASA 9.2) (87%), Philips Hue Bridge (lwIP stack v1.4.0) (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 80/tcp)
HOP RTT     ADDRESS
1   0.39 ms scanme.nmap.org (45.33.32.156)

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 142.28 seconds
```

FIREWALL EVASION TECHNIQUE SCAN:

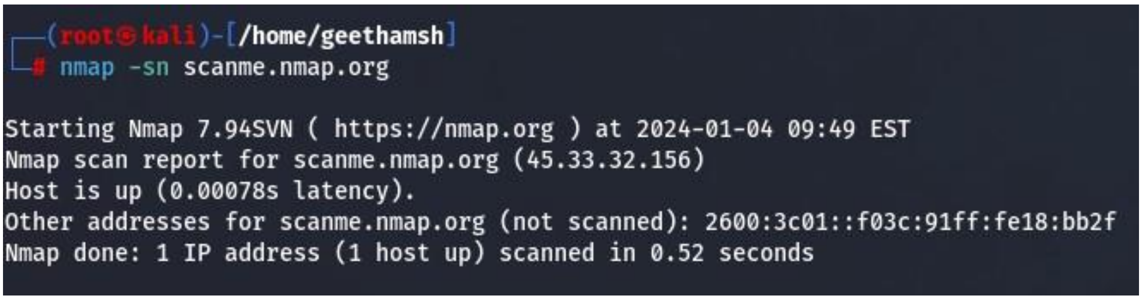
Test for firewall evasion techniques by running the scan with unprivileged mode. Identify if any ports are being filtered or if the firewall is actively blocking scans.



```
┌──(root㉿kali)-[/home/geethamsh]
└─# nmap --unprivileged scanme.nmap.org
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-04 05:09 EST
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.035s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 993 filtered tcp ports (no-response)
PORT    STATE SERVICE
21/tcp  open  ftp
25/tcp  open  smtp
80/tcp  open  http
110/tcp open  pop3
143/tcp open  imap
443/tcp open  https
587/tcp open  submission

Nmap done: 1 IP address (1 host up) scanned in 22.76 seconds
```

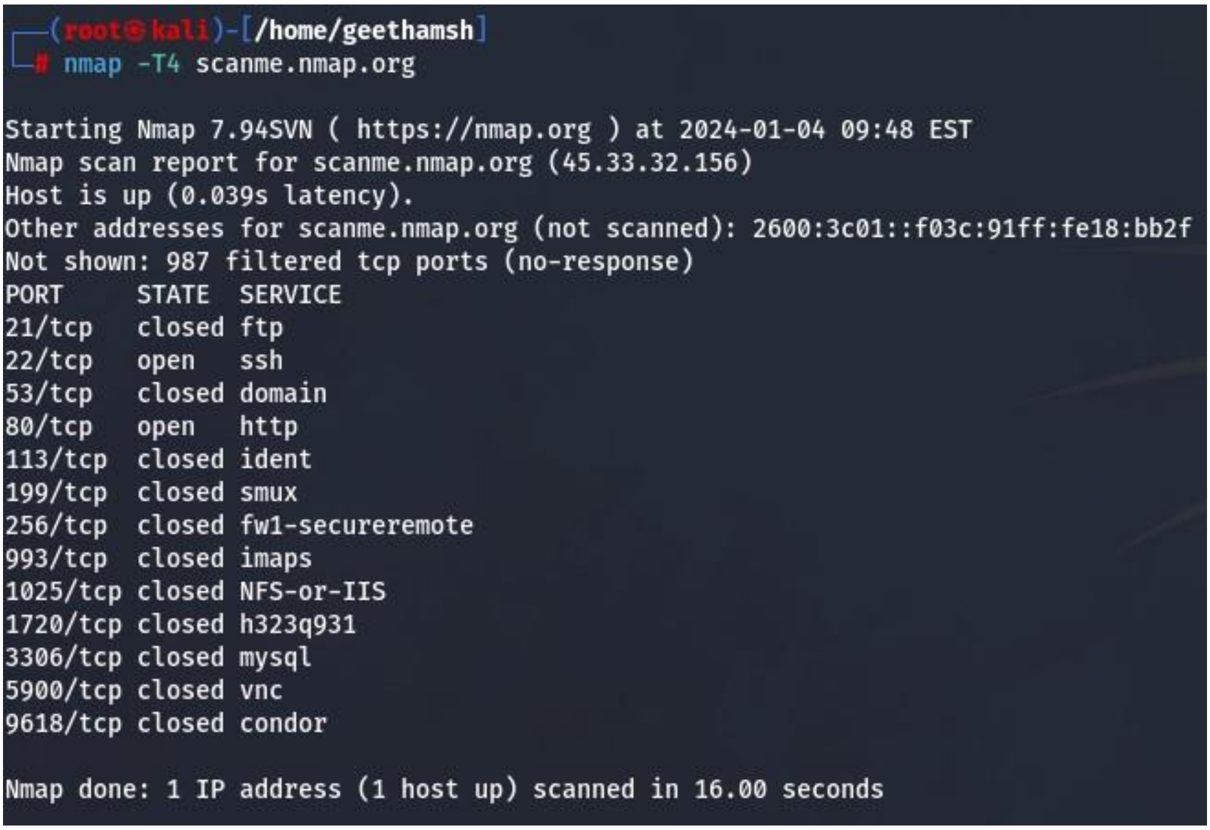
NETWORK TOPOLOGY SCAN:

ping scan and identify live hosts on the network



```
┌──(root㉿kali)-[/home/geethamsh]
└─# nmap -sn scanme.nmap.org

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-04 09:49 EST
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.00078s 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 0.52 seconds
```

AGGRESSIVE TIMING SCAN:



```
┌──(root㉿kali)-[/home/geethamsh]
└─# nmap -T4 scanme.nmap.org

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-04 09:48 EST
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.039s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 987 filtered tcp ports (no-response)
PORT     STATE  SERVICE
21/tcp   closed ftp
22/tcp   open   ssh
53/tcp   closed domain
80/tcp   open   http
113/tcp  closed ident
199/tcp  closed smux
256/tcp  closed fw1-secureremote
993/tcp  closed imaps
1025/tcp closed NFS-or-IIS
1720/tcp closed h323q931
3306/tcp closed mysql
5900/tcp closed vnc
9618/tcp closed condor

Nmap done: 1 IP address (1 host up) scanned in 16.00 seconds
```

CONCLUSION:

The Nmap scans on scanme.nmap.org revealed valuable insights into the target system's network configuration and services. Key findings include a range of open ports, identification of services running on those ports, and an attempt to fingerprint the operating system. The target system, being a deliberately vulnerable server, provided a safe environment for testing various scanning techniques. Open Ports: Multiple open ports were identified, showcasing a variety of services potentially running on the system. Port numbers and associated services were documented for reference. Service Versions: Detailed version detection uncovered specific software versions associated with running services. Potential vulnerabilities associated with specific versions were highlighted for further analysis. Operating System Fingerprinting: The OS detection attempt provided insights into the underlying infrastructure, aiding in the understanding of the target environment. Firewall Evasion Techniques: The scan, conducted in unprivileged mode, tested for potential evasion of firewall restrictions. No significant issues were encountered, suggesting a relatively permissive network configuration.