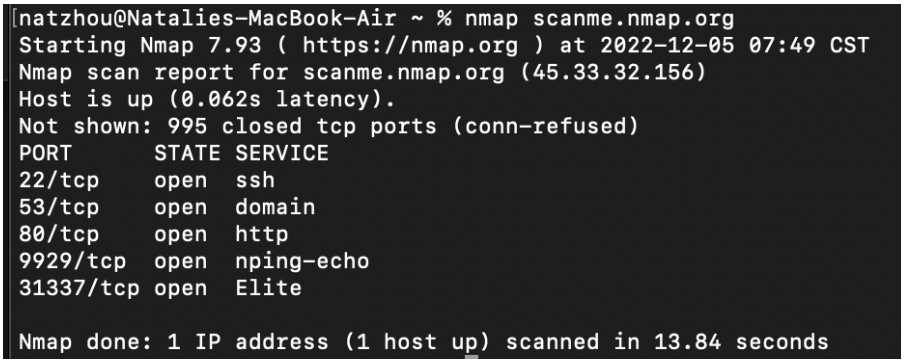
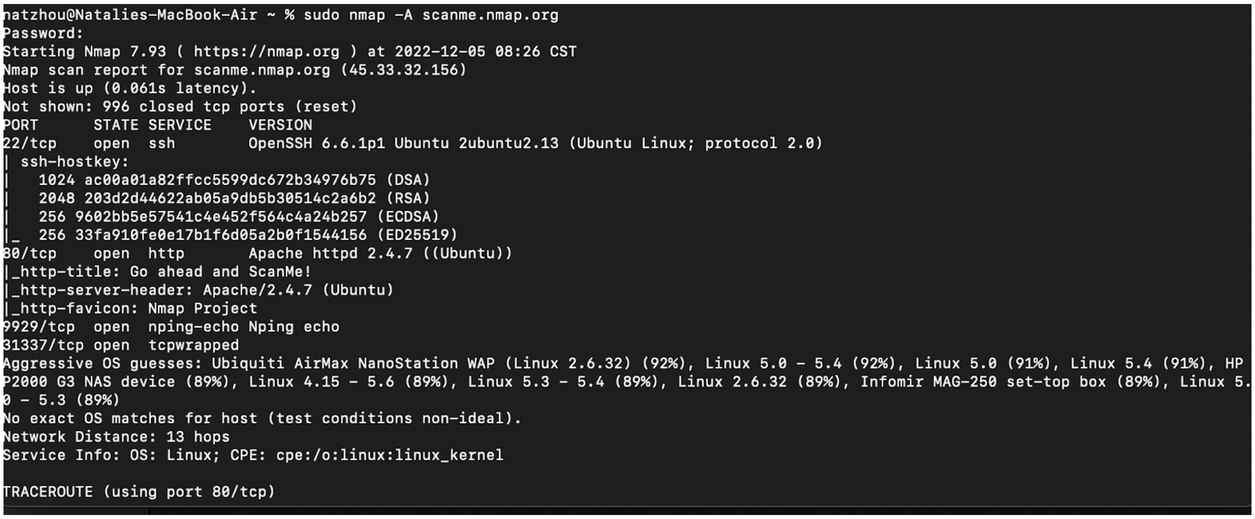
scanme.nmap.org



```
natzhou@Natalies-MacBook-Air ~ % nmap scanme.nmap.org
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-05 07:49 CST
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.062s latency).
Not shown: 995 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    open  ssh
53/tcp    open  domain
80/tcp    open  http
9929/tcp  open  nping-echo
31337/tcp open  Elite

Nmap done: 1 IP address (1 host up) scanned in 13.84 seconds
```



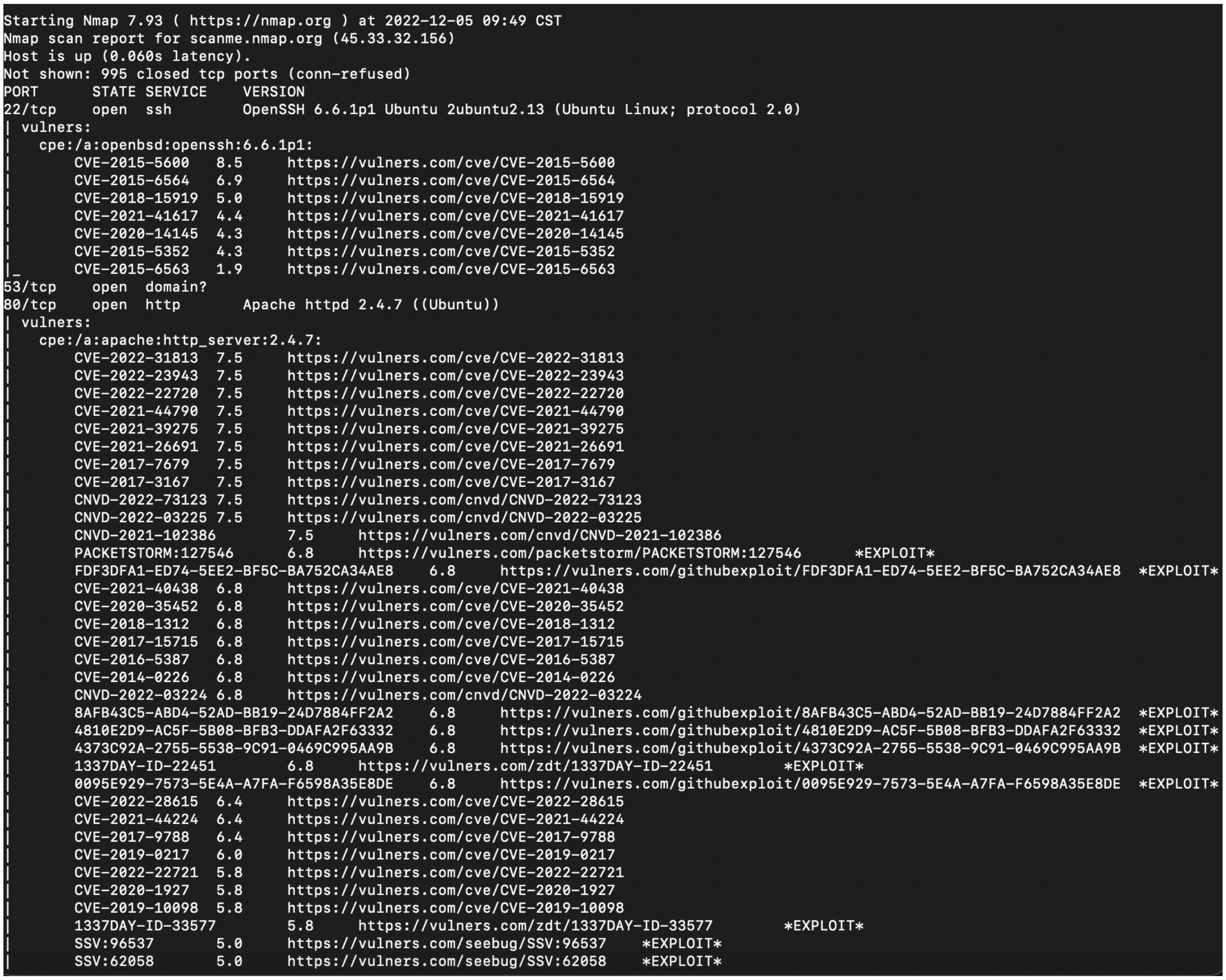
```
natzhou@Natalies-MacBook-Air ~ % sudo nmap -A scanme.nmap.org
Password:
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-05 08:26 CST
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.061s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE    VERSION
22/tcp    open  ssh        OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 ac00a01a82ffcc5599dc672b34976b75 (DSA)
|   2048 203d2d44622ab05a9db5b30514c2a6b2 (RSA)
|   256 9602bb5e57541c4e452f564c4a24b257 (ECDSA)
|_  256 33fa910fe0e17b1f6d05a2b0f1544156 (ED25519)
80/tcp    open  http       Apache httpd 2.4.7 ((Ubuntu))
|_http-title: Go ahead and ScanMe!
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-favicon: Nmap Project
9929/tcp  open  nping-echo Nping echo
31337/tcp open  tcpwrapped
Aggressive OS guesses: Ubiquiti AirMax NanoStation WAP (Linux 2.6.32) (92%), Linux 5.0 - 5.4 (92%), Linux 5.0 (91%), Linux 5.4 (91%), HP
P2000 G3 NAS device (89%), Linux 4.15 - 5.6 (89%), Linux 5.3 - 5.4 (89%), Linux 2.6.32 (89%), Infomir MAG-250 set-top box (89%), Linux 5.
0 - 5.3 (89%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 13 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 80/tcp)
```

Open ports:

- Port 22/tcp is running ssh service and the OpenSSH software
- Port 53/tcp is running service “domain”
- Port 80/tcp is running HTTP service and the Apache httpd application
- Port 9929/tcp is running the Nping service with echo mode
- Port 331337/tcp is running a service called Elite

Using nmap’s OS detection, the OS being used is most likely Linux.

Vulnerability scan:



```
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-05 09:49 CST
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.060s latency).
Not shown: 995 closed tcp ports (conn-refused)
PORT      STATE SERVICE    VERSION
22/tcp    open  ssh        OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
| vulners:
|   cpe:/a:openbsd:openssh:6.6.1p1:
|       CVE-2015-5600   8.5     https://vulners.com/cve/CVE-2015-5600
|       CVE-2015-6564   6.9     https://vulners.com/cve/CVE-2015-6564
|       CVE-2018-15919  5.0     https://vulners.com/cve/CVE-2018-15919
|       CVE-2021-41617  4.4     https://vulners.com/cve/CVE-2021-41617
|       CVE-2020-14145  4.3     https://vulners.com/cve/CVE-2020-14145
|       CVE-2015-5352   4.3     https://vulners.com/cve/CVE-2015-5352
|_      CVE-2015-6563   1.9     https://vulners.com/cve/CVE-2015-6563
53/tcp    open  domain?
80/tcp    open  http       Apache httpd 2.4.7 ((Ubuntu))
| vulners:
|   cpe:/a:apache:http_server:2.4.7:
|       CVE-2022-31813  7.5     https://vulners.com/cve/CVE-2022-31813
|       CVE-2022-23943  7.5     https://vulners.com/cve/CVE-2022-23943
|       CVE-2022-22720  7.5     https://vulners.com/cve/CVE-2022-22720
|       CVE-2021-44790  7.5     https://vulners.com/cve/CVE-2021-44790
|       CVE-2021-39275  7.5     https://vulners.com/cve/CVE-2021-39275
|       CVE-2021-26691  7.5     https://vulners.com/cve/CVE-2021-26691
|       CVE-2017-7679   7.5     https://vulners.com/cve/CVE-2017-7679
|       CVE-2017-3167   7.5     https://vulners.com/cve/CVE-2017-3167
|       CNVD-2022-73123 7.5     https://vulners.com/cnvd/CNVD-2022-73123
|       CNVD-2022-03225 7.5     https://vulners.com/cnvd/CNVD-2022-03225
|       CNVD-2021-102386        7.5     https://vulners.com/cnvd/CNVD-2021-102386
|       PACKETSTORM:127546      6.8     https://vulners.com/packetstorm/PACKETSTORM:127546      *EXPLOIT*
|       FDF3DFA1-ED74-5EE2-BF5C-BA752CA34AE8    6.8     https://vulners.com/githubexploit/FDF3DFA1-ED74-5EE2-BF5C-BA752CA34AE8  *EXPLOIT*
|       CVE-2021-40438  6.8     https://vulners.com/cve/CVE-2021-40438
|       CVE-2020-35452  6.8     https://vulners.com/cve/CVE-2020-35452
|       CVE-2018-1312   6.8     https://vulners.com/cve/CVE-2018-1312
|       CVE-2017-15715  6.8     https://vulners.com/cve/CVE-2017-15715
|       CVE-2016-5387   6.8     https://vulners.com/cve/CVE-2016-5387
|       CVE-2014-0226   6.8     https://vulners.com/cve/CVE-2014-0226
|       CNVD-2022-03224 6.8     https://vulners.com/cnvd/CNVD-2022-03224
|       8AFB43C5-ABD4-52AD-BB19-24D7884FF2A2    6.8     https://vulners.com/githubexploit/8AFB43C5-ABD4-52AD-BB19-24D7884FF2A2  *EXPLOIT*
|       4810E2D9-AC5F-5B08-BFB3-DDAFA2F63332    6.8     https://vulners.com/githubexploit/4810E2D9-AC5F-5B08-BFB3-DDAFA2F63332  *EXPLOIT*
|       4373C92A-2755-5538-9C91-0469C995AA9B    6.8     https://vulners.com/githubexploit/4373C92A-2755-5538-9C91-0469C995AA9B  *EXPLOIT*
|       1337DAY-ID-22451        6.8     https://vulners.com/zdt/1337DAY-ID-22451        *EXPLOIT*
|       0095E929-7573-5E4A-A7FA-F6598A35E8DE    6.8     https://vulners.com/githubexploit/0095E929-7573-5E4A-A7FA-F6598A35E8DE  *EXPLOIT*
|       CVE-2022-28615  6.4     https://vulners.com/cve/CVE-2022-28615
|       CVE-2021-44224  6.4     https://vulners.com/cve/CVE-2021-44224
|       CVE-2017-9788   6.4     https://vulners.com/cve/CVE-2017-9788
|       CVE-2019-0217   6.0     https://vulners.com/cve/CVE-2019-0217
|       CVE-2022-22721  5.8     https://vulners.com/cve/CVE-2022-22721
|       CVE-2020-1927   5.8     https://vulners.com/cve/CVE-2020-1927
|       CVE-2019-10098  5.8     https://vulners.com/cve/CVE-2019-10098
|       1337DAY-ID-33577        5.8     https://vulners.com/zdt/1337DAY-ID-33577        *EXPLOIT*
|       SSV:96537       5.0     https://vulners.com/seebug/SSV:96537    *EXPLOIT*
|       SSV:62058       5.0     https://vulners.com/seebug/SSV:62058    *EXPLOIT*
```

When using Nmap-vulners to scan scanme.nmap.org for vulnerabilities, I found the following significant vulnerabilities (ones with the highest severity ratings) for two open ports:

- 22/tcp has several OpenSSH related vulnerabilities.
    - CVE-2015-5600: A function in OpenSSH does not properly restrict the processing of keyboard-interactive devices within a single connection, which makes it easier for remote attackers to conduct brute-force attacks
    - CVE-2015-656: Cross-site scripting (XSS) vulnerability in the login page in Cisco Network Analysis Module (NAM) allows remote attackers to inject arbitrary web script or HTML
    - CVE-2021-41617: SSHD allows privilege escalation because supplemental groups are not initialized as expected
- 80/tcp has several Apache HTTP server vulnerabilities, including:
    - CVE-2022-31813: Apache HTTP Server 2.4.53 and earlier may not send the X-Forwarded-* headers to the origin server- may be used to bypass IP based authentication on the origin server/application.
    - CVE-2022-23943: Write vulnerability in mod_sed of Apache HTTP Server allows an attacker to overwrite heap memory with possibly attacker provided data

- CVE-2022-22720: Apache HTTP Server 2.4.52 and earlier fails to close inbound connection when errors are encountered, exposing the server to HTTP Request Smuggling