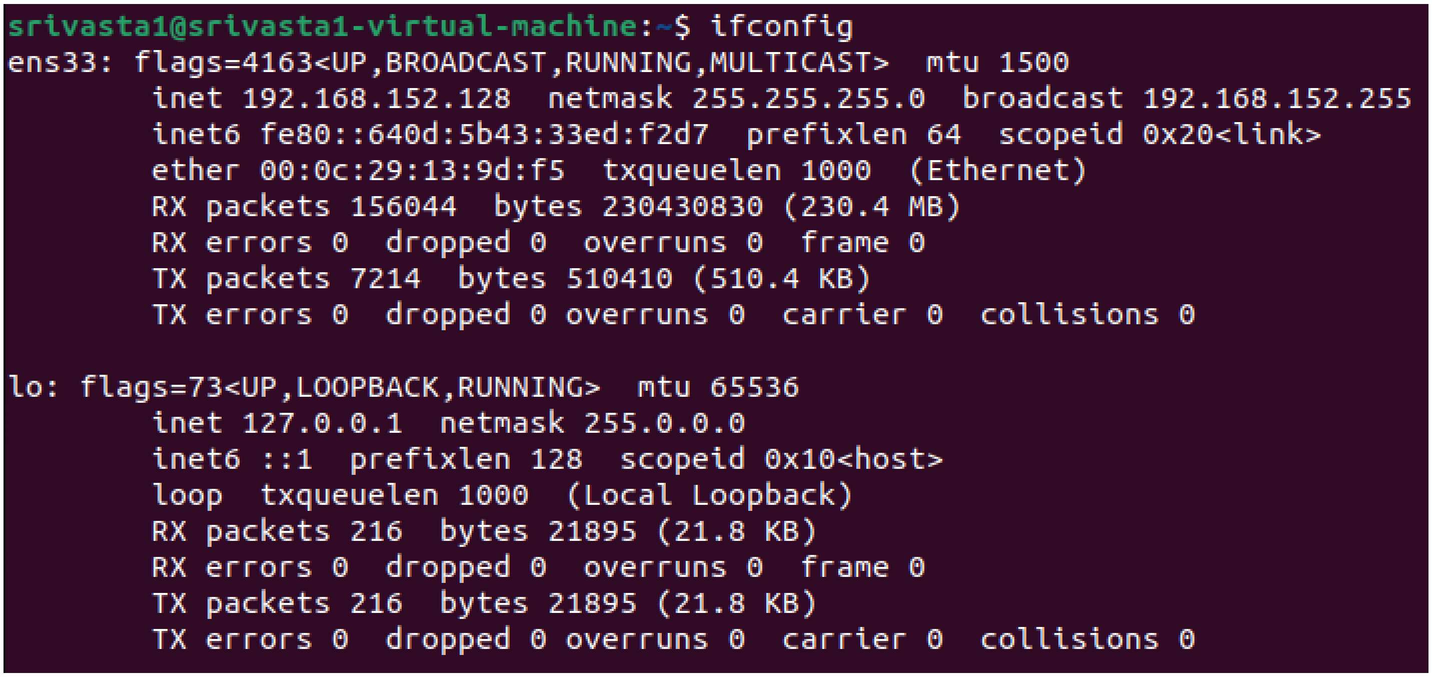
Ubuntu Exploratory Home Lab

NOTE: You will have to install some of the tools below via the command line. To install a package in ubuntu, we can use Advanced Package Tools (APT).
Use the following syntax to install a package: sudo install apt *packagename*

1. **Identify Network Interfaces and IP Addresses**

- **Command:**

```
ip a or ifconfig
```



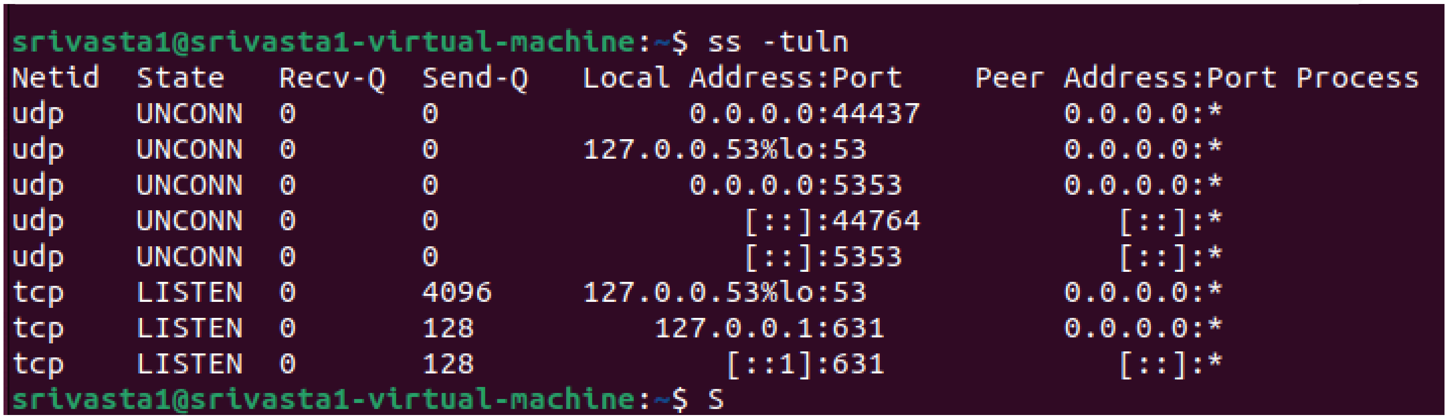
```
srivasta1@srivasta1-virtual-machine:~$ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.152.128  netmask 255.255.255.0  broadcast 192.168.152.255
        inet6 fe80::640d:5b43:33ed:f2d7  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:13:9d:f5  txqueuelen 1000  (Ethernet)
        RX packets 156044  bytes 230430830 (230.4 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 7214  bytes 510410 (510.4 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 216  bytes 21895 (21.8 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 216  bytes 21895 (21.8 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

- **Purpose:** This command displays all network interfaces and their associated IP addresses on your server. Knowing which interfaces are active and their IP addresses helps you understand your server's network configuration.
- **Tool Explanation:** ip a and ifconfig are utilities that provide detailed information about network interfaces, including their status (up or down), IP addresses, and more.
- **NOTE:** You may have to install net-tools in order to run ifconfig. To do so, run the command: sudo apt install net-tools.

2. **Check Open Ports**

- **Command:**

```
sudo netstat -tuln or ss -tuln
```



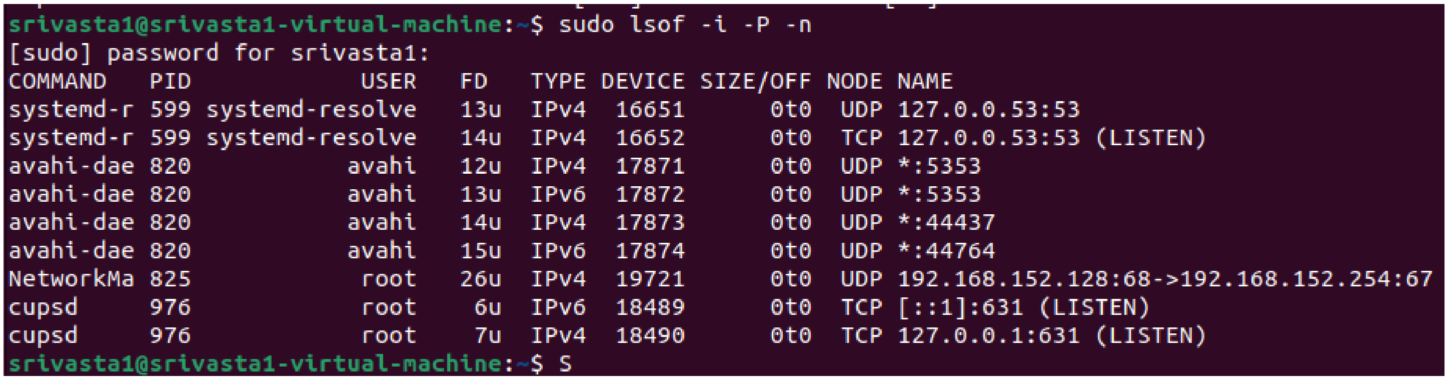
```
srivasta1@srivasta1-virtual-machine:~$ ss -tuln
Netid  State   Recv-Q  Send-Q   Local Address:Port    Peer Address:Port Process
udp    UNCONN  0       0              0.0.0.0:44437        0.0.0.0:*
udp    UNCONN  0       0        127.0.0.53%lo:53           0.0.0.0:*
udp    UNCONN  0       0              0.0.0.0:5353         0.0.0.0:*
udp    UNCONN  0       0                 [::]:44764           [::]:*
udp    UNCONN  0       0                 [::]:5353            [::]:*
tcp    LISTEN  0       4096     127.0.0.53%lo:53           0.0.0.0:*
tcp    LISTEN  0       128          127.0.0.1:631          0.0.0.0:*
tcp    LISTEN  0       128              [::1]:631             [::]:*
srivasta1@srivasta1-virtual-machine:~$ S
```

- **Purpose:** Lists all open ports on the server along with the services listening on them. This helps you identify unnecessary open ports that could be potential entry points for attackers.
- **Tool Explanation:** netstat and ss show network connections, routing tables, interface statistics, masquerade connections, and multicast memberships. The -tuln options restrict the output to show only TCP (t) and UDP (u) ports in listening (l) state without resolving names (n).

3. Analyze Network Connections

- **Command:**

```
sudo lsof -i -P -n
```



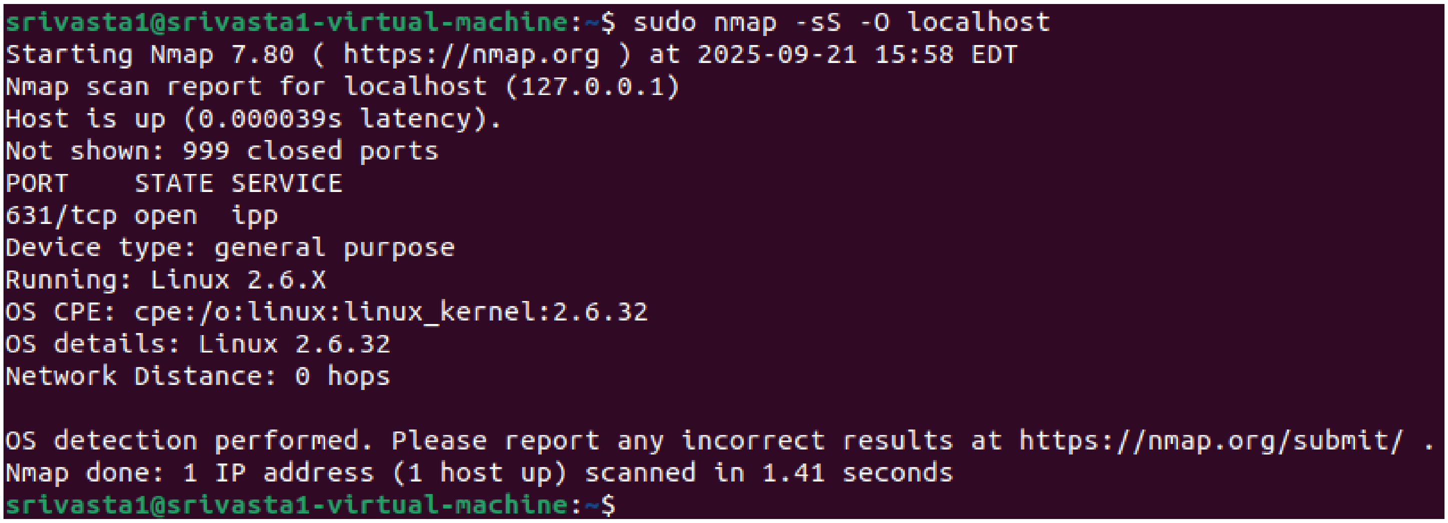
```
srivasta1@srivasta1-virtual-machine:~$ sudo lsof -i -P -n
[sudo] password for srivasta1:
COMMAND    PID            USER   FD   TYPE DEVICE SIZE/OFF NODE NAME
systemd-r 599 systemd-resolve   13u  IPv4  16651      0t0  UDP 127.0.0.53:53
systemd-r 599 systemd-resolve   14u  IPv4  16652      0t0  TCP 127.0.0.53:53 (LISTEN)
avahi-dae 820           avahi   12u  IPv4  17871      0t0  UDP *:5353
avahi-dae 820           avahi   13u  IPv6  17872      0t0  UDP *:5353
avahi-dae 820           avahi   14u  IPv4  17873      0t0  UDP *:44437
avahi-dae 820           avahi   15u  IPv6  17874      0t0  UDP *:44764
NetworkMa 825            root   26u  IPv4  19721      0t0  UDP 192.168.152.128:68->192.168.152.254:67
cupsd     976            root    6u  IPv6  18489      0t0  TCP [::1]:631 (LISTEN)
cupsd     976            root    7u  IPv4  18490      0t0  TCP 127.0.0.1:631 (LISTEN)
srivasta1@srivasta1-virtual-machine:~$ S
```

- **Purpose:** Lists all open network connections, which can help you identify unexpected or unauthorized connections to your server.
- **Tool Explanation:** lsof stands for 'list open files'. With the -i flag, it lists all network files, including their associated processes. The -P and -n flags prevent the resolution of port numbers and IP addresses, making the output easier to read and faster to generate.

4. **Perform Network Scanning with Nmap**

- **Command:**

```
sudo nmap -sS -O localhost
```



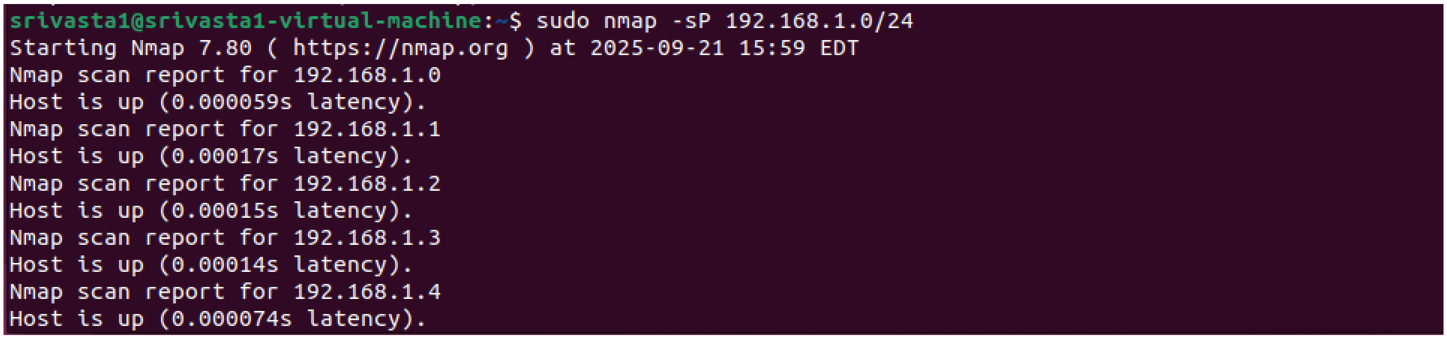
```
srivasta1@srivasta1-virtual-machine:~$ sudo nmap -sS -O localhost
Starting Nmap 7.80 ( https://nmap.org ) at 2025-09-21 15:58 EDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000039s latency).
Not shown: 999 closed ports
PORT    STATE SERVICE
631/tcp open  ipp
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6.32
OS details: Linux 2.6.32
Network Distance: 0 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.41 seconds
srivasta1@srivasta1-virtual-machine:~$
```

- **Purpose:** Scans your server to identify open ports, running services, and the operating system. This can help you discover services that are unintentionally exposed.
- **Tool Explanation:** Nmap (Network Mapper) is a powerful network scanning tool used to discover hosts and services on a network. The -sS option performs a stealth TCP SYN scan, and -O attempts to determine the operating system of the target.
- **NOTE:** You will have to install Nmap. To do so, run: sudo apt install nmap Nmap can be a little slow on the VM, so some of the commands may take a bit to complete. Be patient!

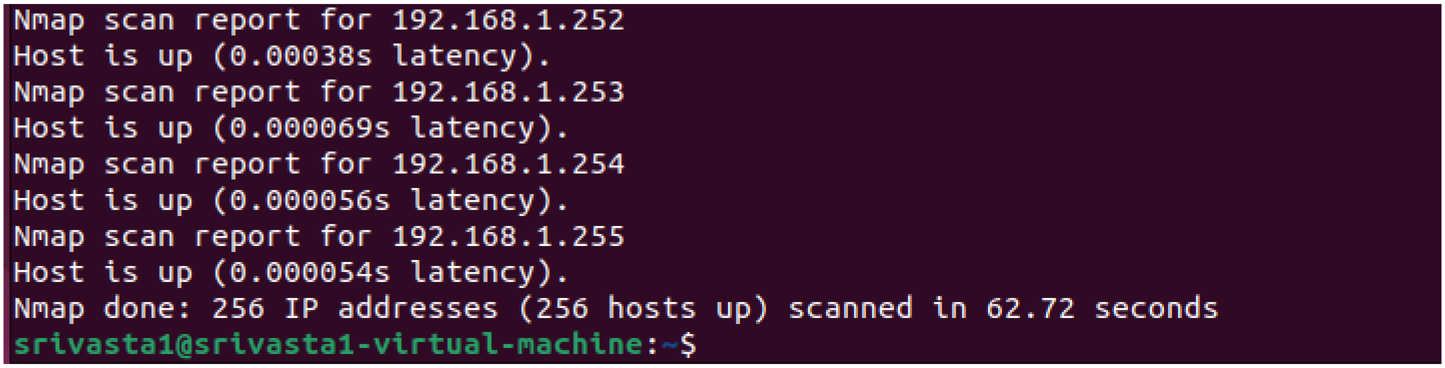
5. **Check for Open Ports on the Server's Network**

- **Command:**

```
sudo nmap -sP 192.168.1.0/24
```



```
srivasta1@srivasta1-virtual-machine:~$ sudo nmap -sP 192.168.1.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2025-09-21 15:59 EDT
Nmap scan report for 192.168.1.0
Host is up (0.000059s latency).
Nmap scan report for 192.168.1.1
Host is up (0.00017s latency).
Nmap scan report for 192.168.1.2
Host is up (0.00015s latency).
Nmap scan report for 192.168.1.3
Host is up (0.00014s latency).
Nmap scan report for 192.168.1.4
Host is up (0.000074s latency).
```



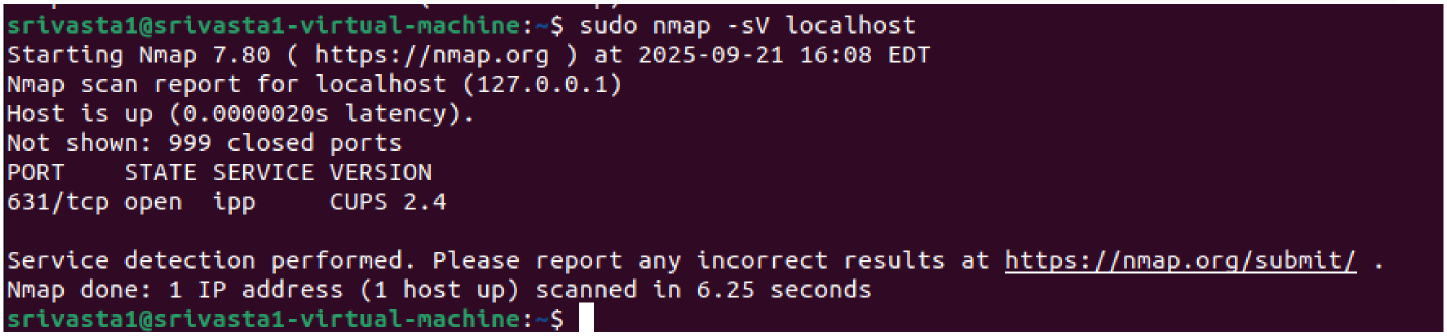
```
Nmap scan report for 192.168.1.252
Host is up (0.00038s latency).
Nmap scan report for 192.168.1.253
Host is up (0.000069s latency).
Nmap scan report for 192.168.1.254
Host is up (0.000056s latency).
Nmap scan report for 192.168.1.255
Host is up (0.000054s latency).
Nmap done: 256 IP addresses (256 hosts up) scanned in 62.72 seconds
srivasta1@srivasta1-virtual-machine:~$
```

- **Purpose:** Identifies all live hosts on your local network. This helps you understand the devices present in your network and ensures there are no unauthorized devices connected.
- **Tool Explanation:** The -sP option in Nmap is a Ping Scan, which discovers which hosts on a network are up without performing a port scan.

6. **Check for Services and Versions**

- **Command:**

```
sudo nmap -sV localhost
```



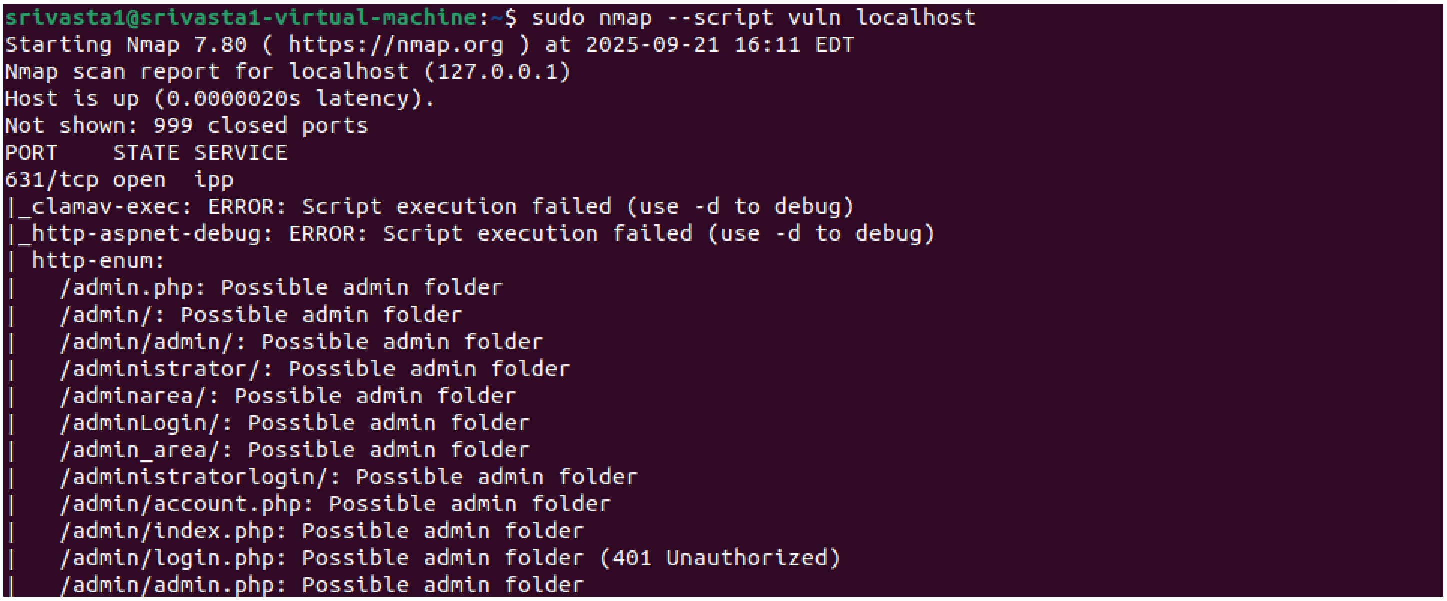
```
srivasta1@srivasta1-virtual-machine:~$ sudo nmap -sV localhost
Starting Nmap 7.80 ( https://nmap.org ) at 2025-09-21 16:08 EDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0000020s latency).
Not shown: 999 closed ports
PORT    STATE SERVICE VERSION
631/tcp open  ipp     CUPS 2.4

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.25 seconds
srivasta1@srivasta1-virtual-machine:~$
```

- **Purpose:** Scans for open ports and attempts to determine the service and version running on each port. This helps identify outdated or vulnerable software that might need updating.
- **Tool Explanation:** The -sV option in Nmap enables version detection, providing detailed information about the services running on open ports.

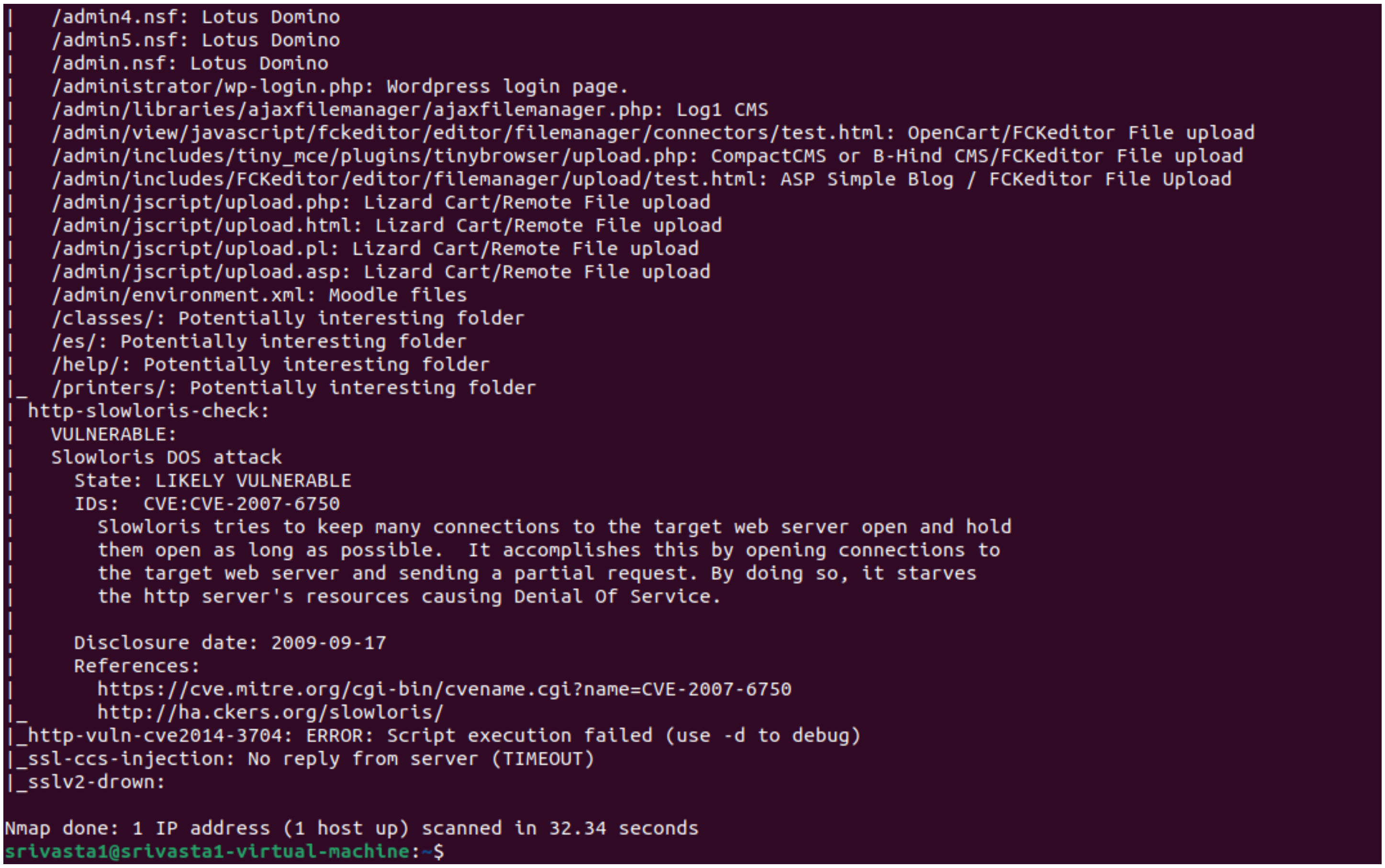
7. **Identify Potential Vulnerabilities**

- **Command:**

```
sudo nmap --script vuln localhost
```



```
srivasta1@srivasta1-virtual-machine:~$ sudo nmap --script vuln localhost
Starting Nmap 7.80 ( https://nmap.org ) at 2025-09-21 16:11 EDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0000020s latency).
Not shown: 999 closed ports
PORT    STATE SERVICE
631/tcp open  ipp
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
|_http-aspnet-debug: ERROR: Script execution failed (use -d to debug)
| http-enum:
|   /admin.php: Possible admin folder
|   /admin/: Possible admin folder
|   /admin/admin/: Possible admin folder
|   /administrator/: Possible admin folder
|   /adminarea/: Possible admin folder
|   /adminLogin/: Possible admin folder
|   /admin_area/: Possible admin folder
|   /administratorlogin/: Possible admin folder
|   /admin/account.php: Possible admin folder
|   /admin/index.php: Possible admin folder
|   /admin/login.php: Possible admin folder (401 Unauthorized)
|   /admin/admin.php: Possible admin folder
```



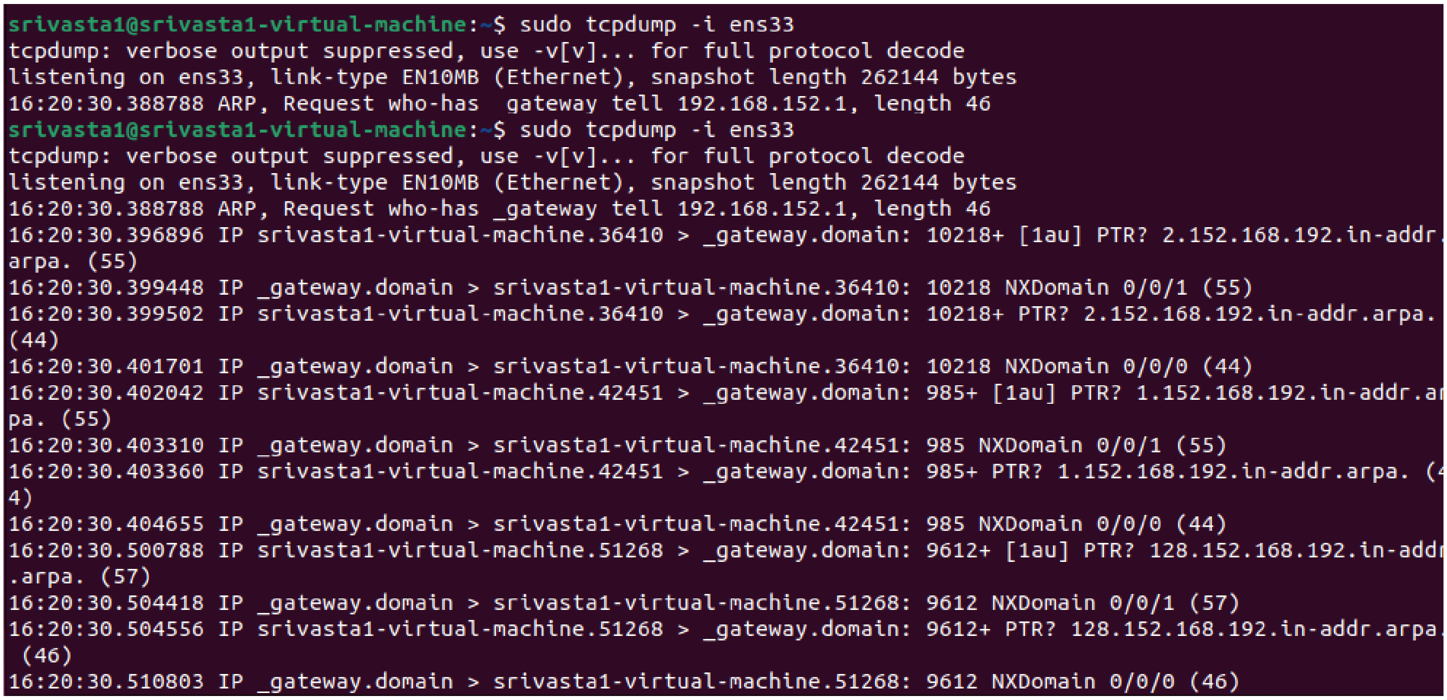
```
|   /admin4.nsf: Lotus Domino
|   /admin5.nsf: Lotus Domino
|   /admin.nsf: Lotus Domino
|   /administrator/wp-login.php: Wordpress login page.
|   /admin/libraries/ajaxfilemanager/ajaxfilemanager.php: Log1 CMS
|   /admin/view/javascript/fckeditor/editor/filemanager/connectors/test.html: OpenCart/FCKeditor File upload
|   /admin/includes/tiny_mce/plugins/tinybrowser/upload.php: CompactCMS or B-Hind CMS/FCKeditor File upload
|   /admin/includes/FCKeditor/editor/filemanager/upload/test.html: ASP Simple Blog / FCKeditor File Upload
|   /admin/jscript/upload.php: Lizard Cart/Remote File upload
|   /admin/jscript/upload.html: Lizard Cart/Remote File upload
|   /admin/jscript/upload.pl: Lizard Cart/Remote File upload
|   /admin/jscript/upload.asp: Lizard Cart/Remote File upload
|   /admin/environment.xml: Moodle files
|   /classes/: Potentially interesting folder
|   /es/: Potentially interesting folder
|   /help/: Potentially interesting folder
|_  /printers/: Potentially interesting folder
| http-slowloris-check:
|   VULNERABLE:
|   Slowloris DOS attack
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2007-6750
|       Slowloris tries to keep many connections to the target web server open and hold
|       them open as long as possible.  It accomplishes this by opening connections to
|       the target web server and sending a partial request. By doing so, it starves
|       the http server's resources causing Denial Of Service.
|
|     Disclosure date: 2009-09-17
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
|_      http://ha.ckers.org/slowloris/
|_http-vuln-cve2014-3704: ERROR: Script execution failed (use -d to debug)
|_ssl-ccs-injection: No reply from server (TIMEOUT)
|_sslv2-drown:

Nmap done: 1 IP address (1 host up) scanned in 32.34 seconds
srivasta1@srivasta1-virtual-machine:~$
```

- **Purpose:** Uses Nmap's vulnerability scanning scripts to identify known vulnerabilities on the server. This step is useful for finding common security issues in installed software.
- **Tool Explanation:** Nmap has a scripting engine that allows for a wide range of scans. The --script vuln option runs scripts that check for various vulnerabilities.

8. **Inspect Network Traffic**

- **Command:**

```
sudo tcpdump -i ens33
```



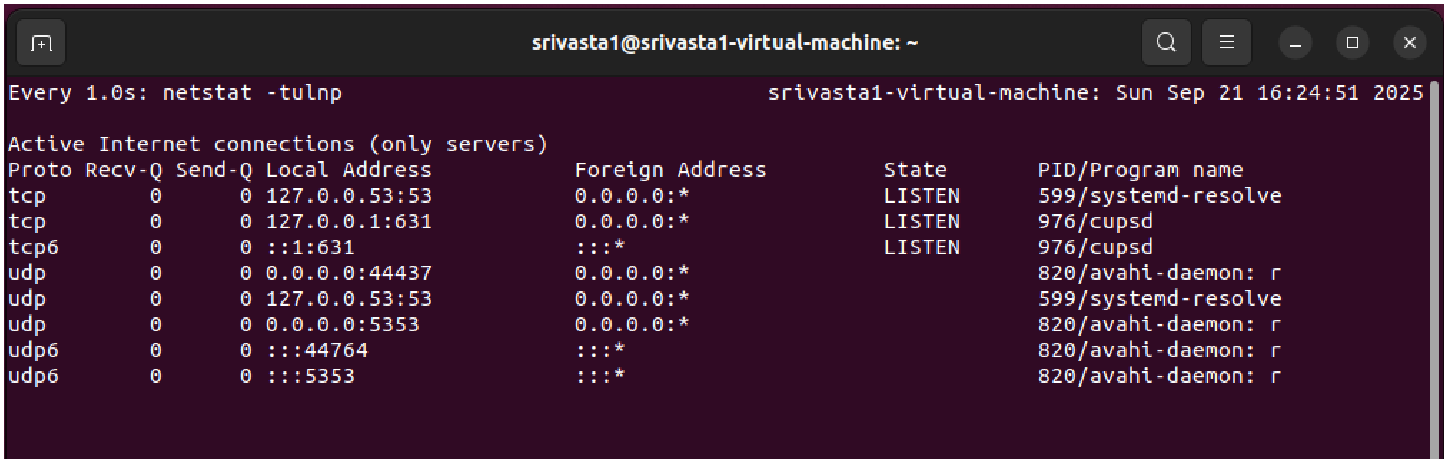
```
srivasta1@srivasta1-virtual-machine:~$ sudo tcpdump -i ens33
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on ens33, link-type EN10MB (Ethernet), snapshot length 262144 bytes
16:20:30.388788 ARP, Request who-has  gateway tell 192.168.152.1, length 46
srivasta1@srivasta1-virtual-machine:~$ sudo tcpdump -i ens33
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on ens33, link-type EN10MB (Ethernet), snapshot length 262144 bytes
16:20:30.388788 ARP, Request who-has _gateway tell 192.168.152.1, length 46
16:20:30.396896 IP srivasta1-virtual-machine.36410 > _gateway.domain: 10218+ [1au] PTR? 2.152.168.192.in-addr.
arpa. (55)
16:20:30.399448 IP _gateway.domain > srivasta1-virtual-machine.36410: 10218 NXDomain 0/0/1 (55)
16:20:30.399502 IP srivasta1-virtual-machine.36410 > _gateway.domain: 10218+ PTR? 2.152.168.192.in-addr.arpa.
(44)
16:20:30.401701 IP _gateway.domain > srivasta1-virtual-machine.36410: 10218 NXDomain 0/0/0 (44)
16:20:30.402042 IP srivasta1-virtual-machine.42451 > _gateway.domain: 985+ [1au] PTR? 1.152.168.192.in-addr.ar
pa. (55)
16:20:30.403310 IP _gateway.domain > srivasta1-virtual-machine.42451: 985 NXDomain 0/0/1 (55)
16:20:30.403360 IP srivasta1-virtual-machine.42451 > _gateway.domain: 985+ PTR? 1.152.168.192.in-addr.arpa. (4
4)
16:20:30.404655 IP _gateway.domain > srivasta1-virtual-machine.42451: 985 NXDomain 0/0/0 (44)
16:20:30.500788 IP srivasta1-virtual-machine.51268 > _gateway.domain: 9612+ [1au] PTR? 128.152.168.192.in-addr
.arpa. (57)
16:20:30.504418 IP _gateway.domain > srivasta1-virtual-machine.51268: 9612 NXDomain 0/0/1 (57)
16:20:30.504556 IP srivasta1-virtual-machine.51268 > _gateway.domain: 9612+ PTR? 128.152.168.192.in-addr.arpa.
 (46)
16:20:30.510803 IP _gateway.domain > srivasta1-virtual-machine.51268: 9612 NXDomain 0/0/0 (46)
```

- **Purpose:** Monitors network traffic on a specific interface (e.g., eth0). This is helpful to observe real-time traffic and detect suspicious activities or anomalies.
- **Tool Explanation:** tcpdump is a packet analyzer that captures and displays packet headers of network traffic passing through a specified interface.
- **NOTE:** To stop process, hit ctrl+c on your keyboard.

9. Monitor Network Connections in Real-Time

- **Command:**

```
sudo watch -n 1 netstat -tulnp
```



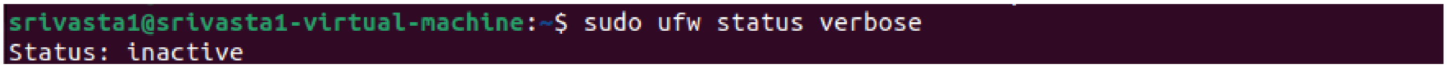
```
Every 1.0s: netstat -tulnp                         srivasta1-virtual-machine: Sun Sep 21 16:24:51 2025

Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      599/systemd-resolve
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN      976/cupsd
tcp6       0      0 ::1:631                 :::*                    LISTEN      976/cupsd
udp        0      0 0.0.0.0:44437           0.0.0.0:*                           820/avahi-daemon: r
udp        0      0 127.0.0.53:53           0.0.0.0:*                           599/systemd-resolve
udp        0      0 0.0.0.0:5353            0.0.0.0:*                           820/avahi-daemon: r
udp6       0      0 :::44764                :::*                                820/avahi-daemon: r
udp6       0      0 :::5353                 :::*                                820/avahi-daemon: r
```

- **Purpose:** Continuously monitors network connections, updating every second (-n 1). This helps in real-time observation of network activities, such as new connections or services starting.
- **Tool Explanation:** watch runs a specified command at regular intervals. In this case, it runs netstat to keep you updated about network connections in real time.
- **NOTE:** To stop process, hit ctrl+c on your keyboard.

10. Check Firewall Rules

- **Command:**

```
sudo ufw status verbose
```



```
srivasta1@srivasta1-virtual-machine:~$ sudo ufw status verbose
Status: inactive
```

- **Purpose:** Displays the current firewall rules configured on your server, showing which ports and services are allowed or blocked. This helps ensure that only necessary ports are open.
- **Tool Explanation:** ufw (Uncomplicated Firewall) is a front-end for managing iptables, designed to make it easier to configure a firewall. The status verbose option provides a detailed view of the current firewall configuration.
- **NOTE:** The machine doesn’t have a firewall setup just yet, therefore the status is inactive.