Troubleshooting and Tool Report

[Pelumi Johnson]

Network Problem Selected

When we first arrived and established our connection to the internet, we noticed inbound connection requests. What tool can we use to determine if any adversary is reaching into our systems through a particular port or protocol?

Troubleshooting Steps

- **Identify the Problem**

Review alerts and confirm that inbound connection attempts are occurring. Verify affected hosts and gather details on source IPs and ports involved.

- **Establish a Theory of Probable Cause**

Determine whether the inbound requests may be due to misconfigured services, legitimate remote access, or hostile scanning activity.

- **Test the Theory**

Use a port and protocol visibility tool, such as **netstat**, to check active connections, listening services, and unidentified traffic.

- **Establish a Plan of Action**

If hostile traffic is confirmed, plan to block suspicious IPs, disable unneeded services, tighten firewall rules, or isolate affected hosts.

- **Implement the Solution**

Apply firewall filtering, reconfigure services, or shut down questionable ports. Validate using netstat to confirm changes.

- **Verify Full System Functionality**

Ensure mission-critical services remain operational, confirm no further abnormal inbound traffic is seen, and validate overall connectivity.

- **Document Findings**

Record all observed activity, actions taken, tools used, and any recurring patterns for future reference and incident response.

Tool and Description

The recommended tool for this problem is **netstat**, a built-in Windows and Linux utility that displays active network connections, listening ports, associated protocols, process IDs, and foreign addresses. Netstat provides real-time insight into which ports are open, which services are active, and whether unfamiliar external systems are attempting to connect. This makes it ideal for detecting early stages of an intrusion or reconnaissance attempt.

Tool Operational Use Case

Netstat can be used any time the team needs to investigate suspicious inbound traffic, evaluate open ports, or validate network services. In the future, it will help quickly confirm whether adversaries are scanning for vulnerabilities, whether unauthorized services are running internally, or whether a compromised host is communicating externally. It also assists in audits, policy compliance checks, and routine security monitoring.

Tool Functionality

- **netstat -a**

Displays all active connections and all listening ports.

- **netstat -n**

Shows addresses numerically, making it easier to spot foreign IPs.

- **netstat -o**

Displays the process ID (PID) associated with each connection, helping identify suspicious programs.

- **netstat -an**

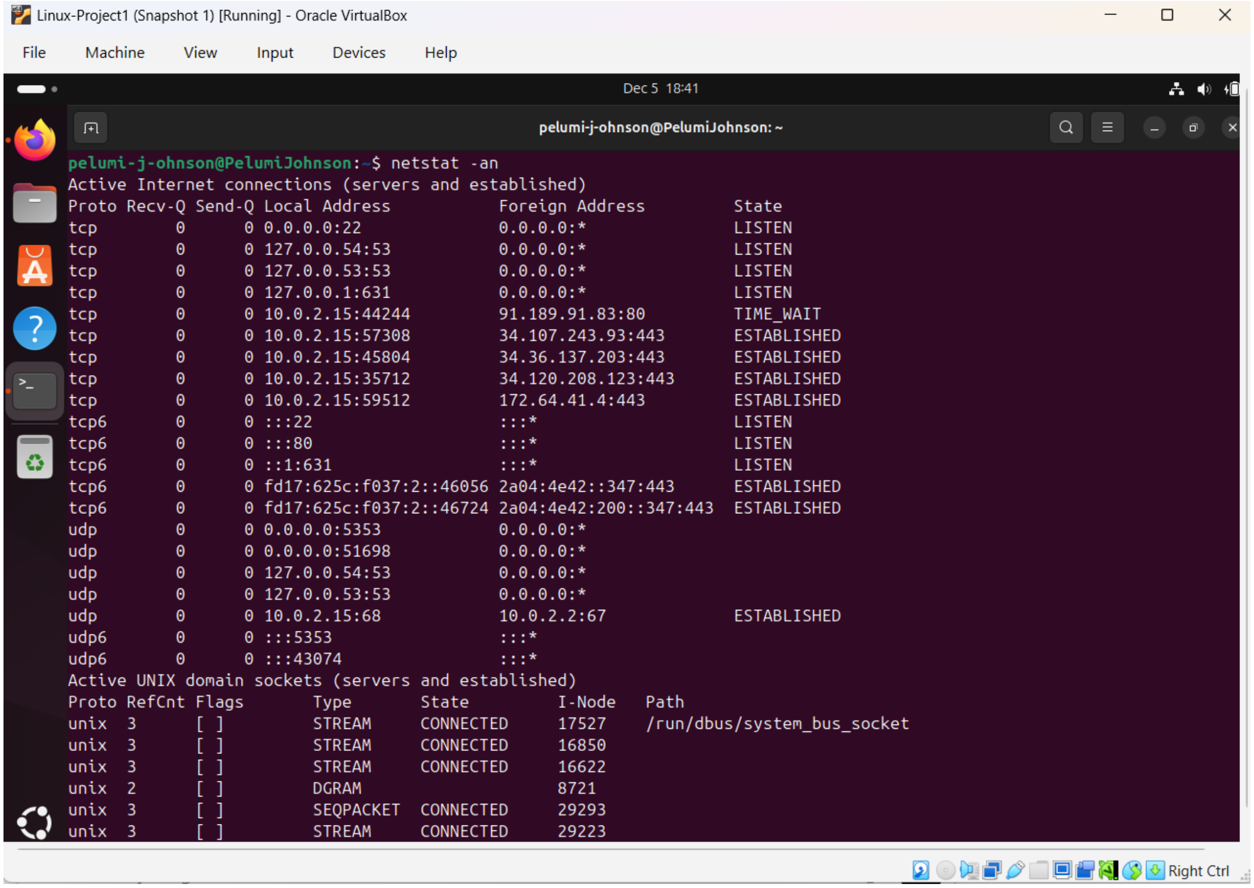
Combines both views for a complete, fast scan of current activity.

- **netstat -b** *(Windows)*

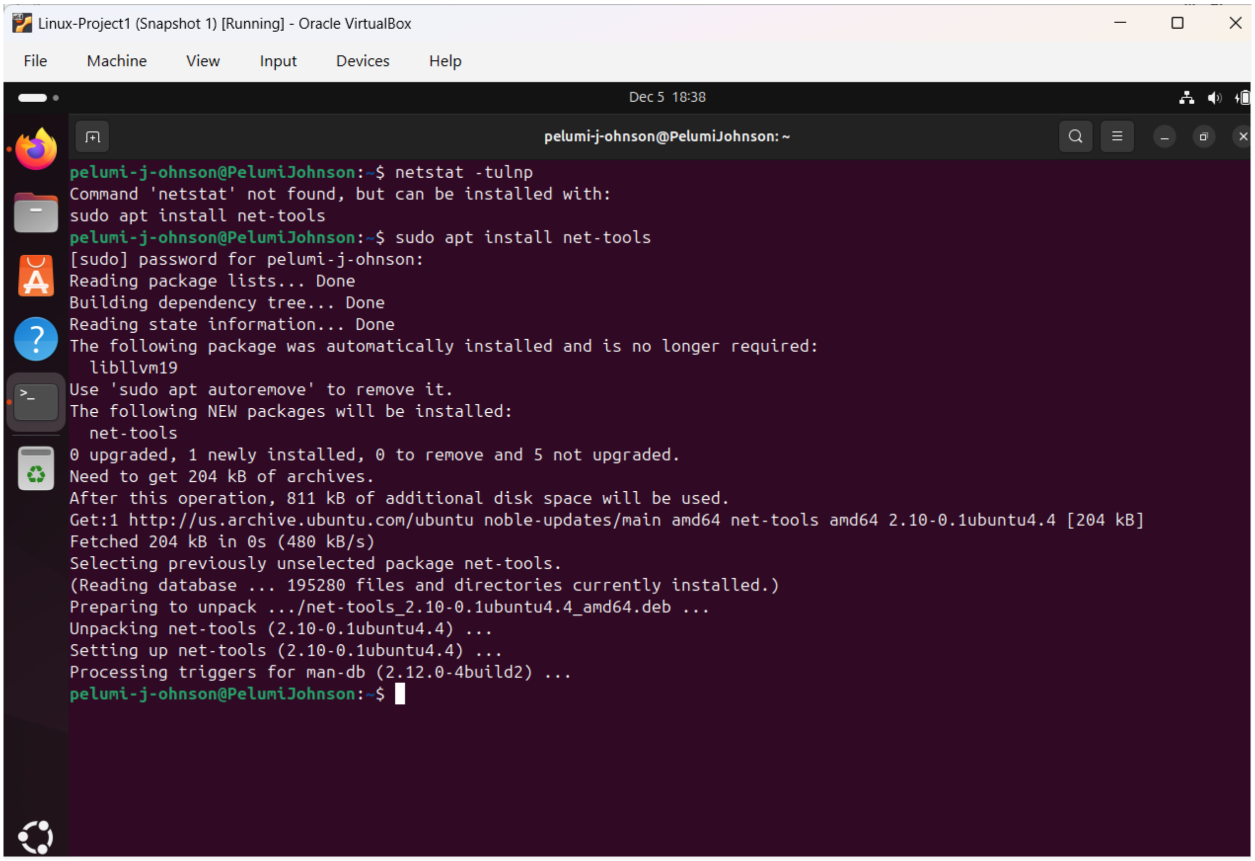
Shows which executable created each connection.

- **netstat -r**

Displays routing tables, useful for verifying correct pathing during connection attempts.

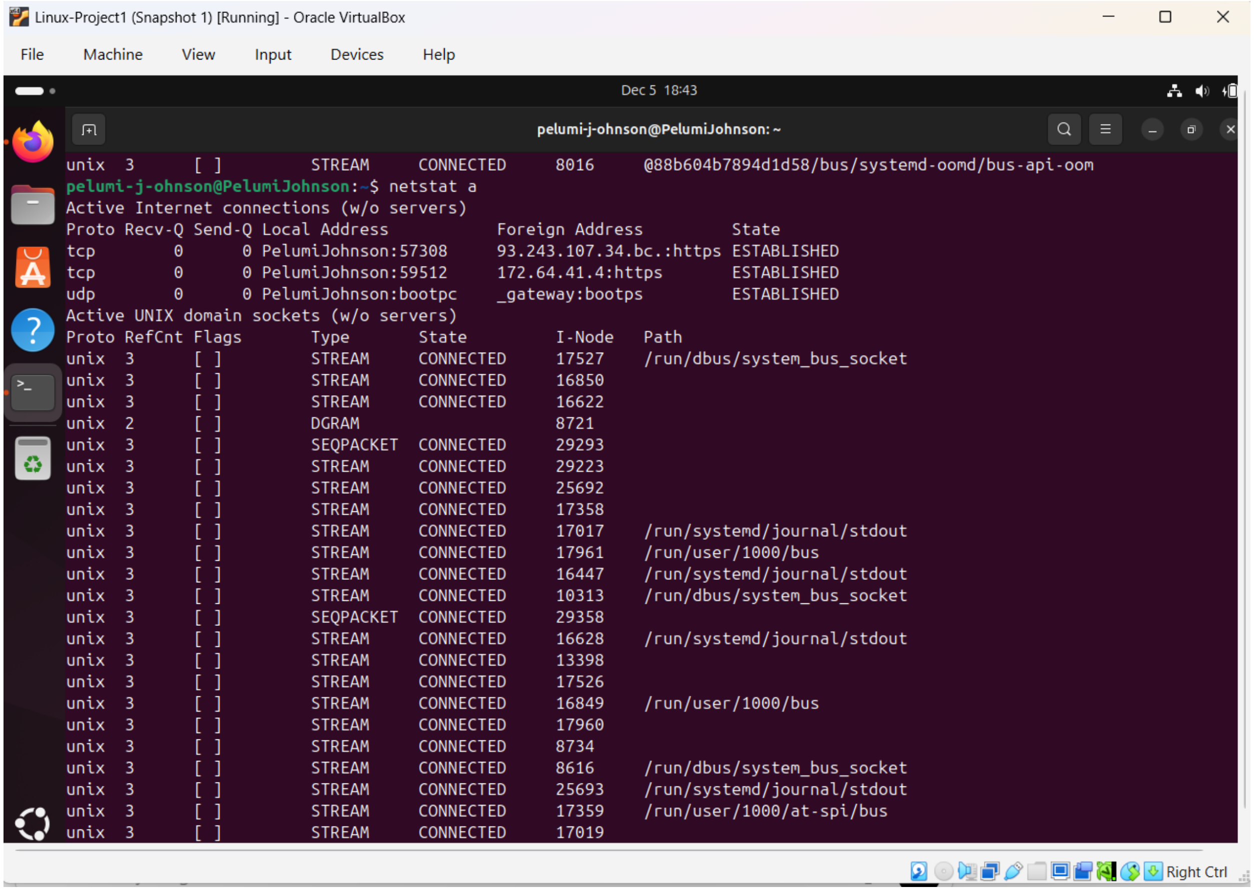

Linux-Project1 (Snapshot 1) [Running] - Oracle VirtualBox
File
Machine
View
Input
Devices
Help
Dec 5 18:41
pelumi-j-ohnson@PelumiJohnson: ~
Right Ctrl

```
pelumi-j-ohnson@PelumiJohnson:~$ netstat -an
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.54:53           0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN
tcp        0      0 10.0.2.15:44244         91.189.91.83:80         TIME_WAIT
tcp        0      0 10.0.2.15:57308         34.107.243.93:443       ESTABLISHED
tcp        0      0 10.0.2.15:45804         34.36.137.203:443       ESTABLISHED
tcp        0      0 10.0.2.15:35712         34.120.208.123:443      ESTABLISHED
tcp        0      0 10.0.2.15:59512         172.64.41.4:443         ESTABLISHED
tcp6       0      0 :::22                   :::*                    LISTEN
tcp6       0      0 :::80                   :::*                    LISTEN
tcp6       0      0 ::1:631                 :::*                    LISTEN
tcp6       0      0 fd17:625c:f037:2::46056 2a04:4e42::347:443      ESTABLISHED
tcp6       0      0 fd17:625c:f037:2::46724 2a04:4e42:200::347:443  ESTABLISHED
udp        0      0 0.0.0.0:5353            0.0.0.0:*
udp        0      0 0.0.0.0:51698           0.0.0.0:*
udp        0      0 127.0.0.54:53           0.0.0.0:*
udp        0      0 127.0.0.53:53           0.0.0.0:*
udp        0      0 10.0.2.15:68            10.0.2.2:67             ESTABLISHED
udp6       0      0 :::5353                 :::*
udp6       0      0 :::43074                :::*
Active UNIX domain sockets (servers and established)
Proto RefCnt Flags       Type       State         I-Node   Path
unix  3      [ ]         STREAM     CONNECTED     17527    /run/dbus/system_bus_socket
unix  3      [ ]         STREAM     CONNECTED     16850
unix  3      [ ]         STREAM     CONNECTED     16622
unix  2      [ ]         DGRAM                    8721
unix  3      [ ]         SEQPACKET  CONNECTED     29293
unix  3      [ ]         STREAM     CONNECTED     29223
```



Linux-Project1 (Snapshot 1) [Running] - Oracle VirtualBox
File
Machine
View
Input
Devices
Help
Dec 5 18:38
pelumi-j-ohnson@PelumiJohnson: ~

```
pelumi-j-ohnson@PelumiJohnson:~$ netstat -tulnp
Command 'netstat' not found, but can be installed with:
sudo apt install net-tools
pelumi-j-ohnson@PelumiJohnson:~$ sudo apt install net-tools
[sudo] password for pelumi-j-ohnson:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following package was automatically installed and is no longer required:
  libllvm19
Use 'sudo apt autoremove' to remove it.
The following NEW packages will be installed:
  net-tools
0 upgraded, 1 newly installed, 0 to remove and 5 not upgraded.
Need to get 204 kB of archives.
After this operation, 811 kB of additional disk space will be used.
Get:1 http://us.archive.ubuntu.com/ubuntu noble-updates/main amd64 net-tools amd64 2.10-0.1ubuntu4.4 [204 kB]
Fetched 204 kB in 0s (480 kB/s)
Selecting previously unselected package net-tools.
(Reading database ... 195280 files and directories currently installed.)
Preparing to unpack .../net-tools_2.10-0.1ubuntu4.4_amd64.deb ...
Unpacking net-tools (2.10-0.1ubuntu4.4) ...
Setting up net-tools (2.10-0.1ubuntu4.4) ...
Processing triggers for man-db (2.12.0-4build2) ...
pelumi-j-ohnson@PelumiJohnson:~$
```


Linux-Project1 (Snapshot 1) [Running] - Oracle VirtualBox
File
Machine
View
Input
Devices
Help
Dec 5 18:43
pelumi-j-ohnson@PelumiJohnson: ~
Right Ctrl

```
unix  3      [ ]         STREAM     CONNECTED     8016     @88b604b7894d1d58/bus/systemd-oomd/bus-api-oom
pelumi-j-ohnson@PelumiJohnson:~$ netstat a
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 PelumiJohnson:57308     93.243.107.34.bc.:https ESTABLISHED
tcp        0      0 PelumiJohnson:59512     172.64.41.4:https       ESTABLISHED
udp        0      0 PelumiJohnson:bootpc    _gateway:bootps         ESTABLISHED
Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags       Type       State         I-Node   Path
unix  3      [ ]         STREAM     CONNECTED     17527    /run/dbus/system_bus_socket
unix  3      [ ]         STREAM     CONNECTED     16850
unix  3      [ ]         STREAM     CONNECTED     16622
unix  2      [ ]         DGRAM                    8721
unix  3      [ ]         SEQPACKET  CONNECTED     29293
unix  3      [ ]         STREAM     CONNECTED     29223
unix  3      [ ]         STREAM     CONNECTED     25692
unix  3      [ ]         STREAM     CONNECTED     17358
unix  3      [ ]         STREAM     CONNECTED     17017    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     17961    /run/user/1000/bus
unix  3      [ ]         STREAM     CONNECTED     16447    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     10313    /run/dbus/system_bus_socket
unix  3      [ ]         SEQPACKET  CONNECTED     29358
unix  3      [ ]         STREAM     CONNECTED     16628    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     13398
unix  3      [ ]         STREAM     CONNECTED     17526
unix  3      [ ]         STREAM     CONNECTED     16849    /run/user/1000/bus
unix  3      [ ]         STREAM     CONNECTED     17960
unix  3      [ ]         STREAM     CONNECTED     8734
unix  3      [ ]         STREAM     CONNECTED     8616     /run/dbus/system_bus_socket
unix  3      [ ]         STREAM     CONNECTED     25693    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     17359    /run/user/1000/at-spi/bus
unix  3      [ ]         STREAM     CONNECTED     17019
```