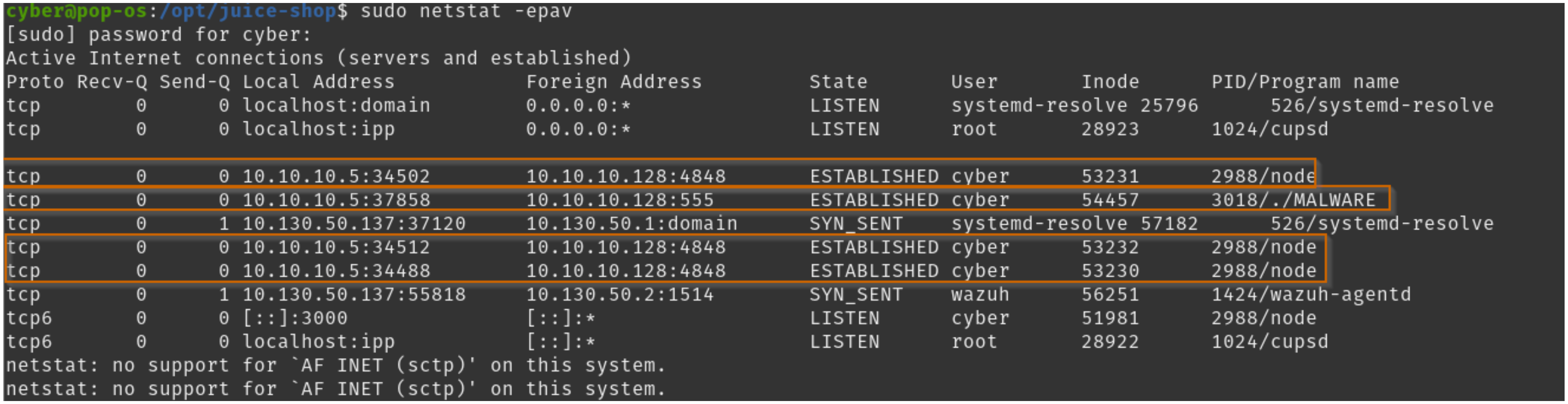
Linux Hunting

Linux

Due to Nix* being mostly CLI based. We will focus our efforts on BASH One-Liners. If you are comfortable with other languages feel free to modify the script to your liking. This section will focus on BASH/SH/ZSH

Using netstat to view listening, established or pending sockets

netstat -epav
e: display other/more information
p: display PID/Program name for sockets
v: be Verbose



```
cyber@pop-os:/opt/juice-shop$ sudo netstat -epav
[sudo] password for cyber:
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       User       Inode      PID/Program name
tcp        0      0 localhost:domain        0.0.0.0:*               LISTEN      systemd-resolve 25796      526/systemd-resolve
tcp        0      0 localhost:ipp           0.0.0.0:*               LISTEN      root       28923      1024/cupsd

tcp        0      0 10.10.10.5:34502        10.10.10.128:4848       ESTABLISHED cyber      53231      2988/node
tcp        0      0 10.10.10.5:37858        10.10.10.128:555        ESTABLISHED cyber      54457      3018/./MALWARE
tcp        0      1 10.130.50.137:37120     10.130.50.1:domain      SYN_SENT    systemd-resolve 57182      526/systemd-resolve
tcp        0      0 10.10.10.5:34512        10.10.10.128:4848       ESTABLISHED cyber      53232      2988/node
tcp        0      0 10.10.10.5:34488        10.10.10.128:4848       ESTABLISHED cyber      53230      2988/node
tcp        0      1 10.130.50.137:55818     10.130.50.2:1514        SYN_SENT    wazuh      56251      1424/wazuh-agentd
tcp6       0      0 [::]:3000               [::]:*                  LISTEN      cyber      51981      2988/node
tcp6       0      0 localhost:ipp           [::]:*                  LISTEN      root       28922      1024/cupsd
netstat: no support for `AF INET (sctp)' on this system.
netstat: no support for `AF INET (sctp)' on this system.
```

Find odd processes running on Linux and the corresponding command

- `ps -aef --forest`

After finding the malicious PID
Use `cd /proc/ODD_PID_Found`
Then `ls -la | grep cwd`
This will output what the PID is doing, whether its a RevShell, or attacker actively modifying files

Kill process to prevent hacker from maintaining access.

- `kill ODD_PID_Found`
- or `pkill ODD_PID_Found`

Check users on Linux Box

- `cat /etc/passwd | grep 'bash\|sh'`

Checking for IP addresses in `/var/log` directory
NOTE this will check all files, and list all IPs found within the Logs
`grep -E -o "([0-9]{1,3}\.){3}[0-9]{1,3}:" -R /var/log/*`
or
`grep -E -o "([0-9]{1,3}\.){3}[0-9]{1,3}:" SomeLog.txt`
or
`cat log.log | grep 'KNOWN-IP'`

Check CrobJobs for Odd Jobs

`cat /etc/crontab`
OR
`find /var/spool/cron/crontabs/ -type f -mtime -1`
The objective is to look for oddities. Not everything in cronjobs are bad. CronJobs are used for persistence. Do your research

Check firewall rules

- `iptables -L -n`

- `ufw status verbose`
- `ufw app list`

Check for Private SSH keys on Linux

- `find / -name "id_*" -type f 2>/dev/null | grep -E "^/.*ssh/.*$"`