5. Linux Endpoint Security

I. Linux Network Analysis

`netstat`

Find IP addresses that have made a connection

```
sudo netstat -t -n
```

- `-t` : Show TCP Connections
- `-n` : Don't resolve DNS

```
sudo netstat -tnp
```

- `-p` : Show Processes

`ss`

```
sudo ss -tnp
```

Use Filters to limit output:

- `src`
- `dst`
- `sport == 4444`
- `dport`

II. Linux Process Analysis

`ps`

Gets a snapshot of active processes on a machine.

- `-u <username>` : User
- `-p <PID>`
- `-A` : All processes on the system
- `-F` : Verbose Format
- `-H` : Hierarchy relationships

```
sudo ps -AFH
```

```
pstree
```

```
pstree -p -s <PID>
```

- `-p` : Show PIDs
- `-s` : Show Parent Processes
- `<PID>` : Searches for a specific PID

`top` - Dynamic continuous output of processes

- `-u <username>` : search for processes related to a specific user
- `-c` : Verbose output
- `-o` : Most Recent processes at the top

`/proc`

A virtual file system of processes. Search within this directory for the folder named after the process ID.

```
cd /proc
ls
cd <PID>
cat cmdline # Prints the cmd line that started the process
ls -al cwd #
cat environ | tr '\0' '\n' # Print environment variables
```

III. Linux Cron Jobs

Used to run tasks at regular intervals similar to Windows Task Scheduler

```
cat /etc/crontab # System wide cron jobs
ls -al /etc | grep cron # Find all cron files in /etc
ls -al /etc/cron.daily/ # look at the cron.daily directory
```

Look for references to scripts or binaries that look suspicious or unrecognized.