Linux Forensics Cheatsheet

System and OS information

OS release information:
Location: /etc/os-release
Can be read using cat, vim or any text editor or viewer

User accounts information:
Location: /etc/passwd
Can be read using cat, vim or any text editor or viewer

User group information:
Location: /etc/group
Can be read using cat, vim or any text editor or viewer

Sudoers list:
Location: /etc/sudoers
Can be read using cat, vim or any text editor or viewer.
Needs sudo or root permissions to access

Login information:
Location: /var/log/wtmp
Can be read using last utility

Authentication logs:
Location: /var/log/auth.log
Can be read using cat, vim or any text editor or viewer.
Use grep for better filtering.
Might also have auth.log1, auth.log2 etc as log files that have been rotated.

System configuration

Hostname:
Location: /etc/hostname
Can be read using cat, vim or any text editor or viewer

Timezone information:
Location: /etc/timezone
Can be read using cat, vim or any text editor or viewer

Network Interfaces:
Location: /etc/network/interfaces
Can be read using cat, vim or any text editor or viewer

Command: ip address show
The above command is suitable only for live analysis

Open network connections:
Command: netstat –natp
The above command is suitable only for live analysis

Running processes:
Command: ps aux
The above command is suitable only for live analysis

DNS information:
Location: /etc/hosts for hostname resolutions
Can be read using cat, vim or any text editor or viewer

Location: /etc/resolv.conf for information about DNS servers
Can be read using cat, vim or any text editor or viewer

Persistence mechanism

Cron jobs:
Location: /etc/crontab
Can be read using cat, vim or any text editor or viewer

Services:
Location: /etc/init.d/
Registered services are present in this directory

Bash shell startup:
Location: /home/<user>/.bashrc for each user

Locations: /etc/bash.bashrc and /etc/profile for system wide settings. Can be read using cat, vim or any text editor or viewer

Evidence of execution

Authentication logs:
Location: /var/log/auth.log* |grep -i COMMAND;
the grep can be used to filter the results. Can be read using cat, vim or any text editor or viewer

Bash history:
Location: /home/<user>/.bash_history
Can be read using cat, vim or any text editor or viewer

Vim history:
Location: /home/<user>/.viminfo
Can be read using cat, vim or any text editor or viewer

Log files

Syslogs:
Location: /var/log/syslog
Can be read using cat, vim or any text editor or viewer.
Use grep or similar utility to filter results as per requirement

Authentication logs:
Location: /var/log/auth.log
Can be read using cat, vim or any text editor or viewer.
Use grep or similar utility to filter results as per requirement

Third-party logs:
Location: /var/log
Logs for each third-party application can be found in their specific directories in this location

To learn more about Linux Forensics click here: https://tryhackme.com/room/linuxforensics