**IT System Security Lab Experiment 01**

**B. Tech CSF-CSE Semester III Course: Physical Security and IT Security Code: CSSF 2109**

**Lab Objective: Learn About Logs**

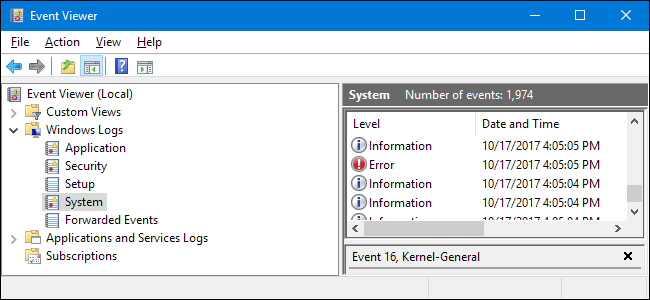
Attackers gain access to endpoint devices and can use them to penetrate the network. Hence, it is essential to collect data from endpoint logs and identify malicious or unauthorized activity.

**Tool:**

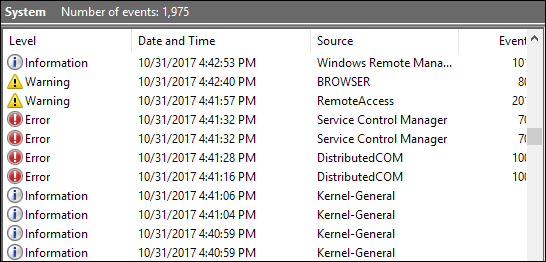
* Windows OS
* Event Viewer

**Steps to perform:**

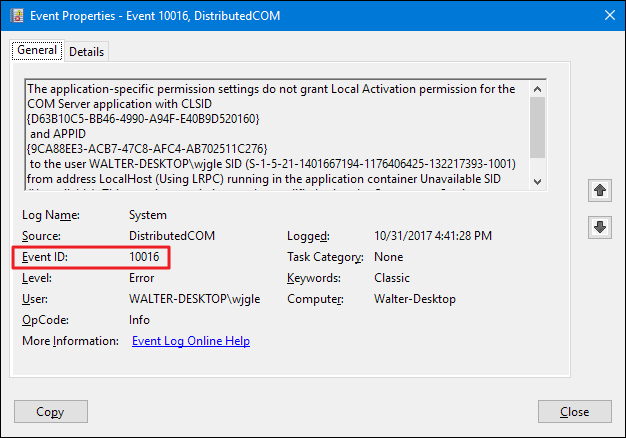
1. Start 🡪 type “Event Viewer” OR from “Control Panel” 🡪 Admin Tools 🡪 “Event Viewer”.
2. Events are placed in different categories, each of which are related to a log that Windows keeps on events regarding that category.
3. Types of Events:
   * **Application:** records events related to Windows system components 🡪 Drivers and built-in interface elements.
   * **System:** records events related to programs installed on the system.
   * **Security:** When Security logging is enabled (this is off by default in Windows), this log records events related to security, such as logon attempts and resource access.
   * **Setup**
   * **Forwarded Events:** records events written by other computers in the same network ("source computers") that have forwarded their events to the "collector computer."



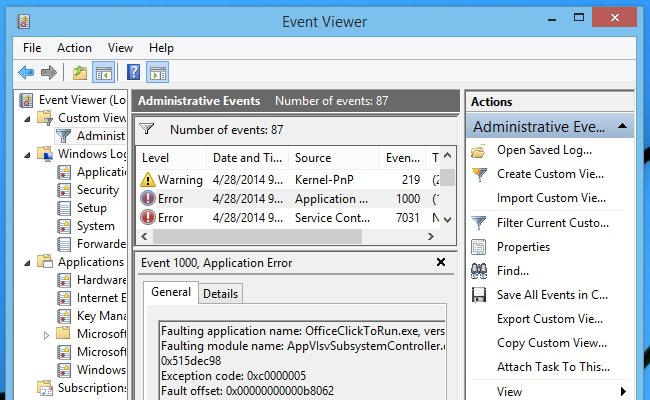
1. Types of events (Information, Warning, Error/Critical)



1. Details about each Log can be checked for details and searched online from EVENT ID



1. Check Vendor Portals (HP, Dell, Microsoft….), Search Engines (Google, Yahoo…) or CVE Details web portal (<https://www.cvedetails.com/>) for more information about the events
2. You can also Filter Events to gather only CRITICAL Logs, Save and Export the log to view on other systems OR another Log Analyzer.



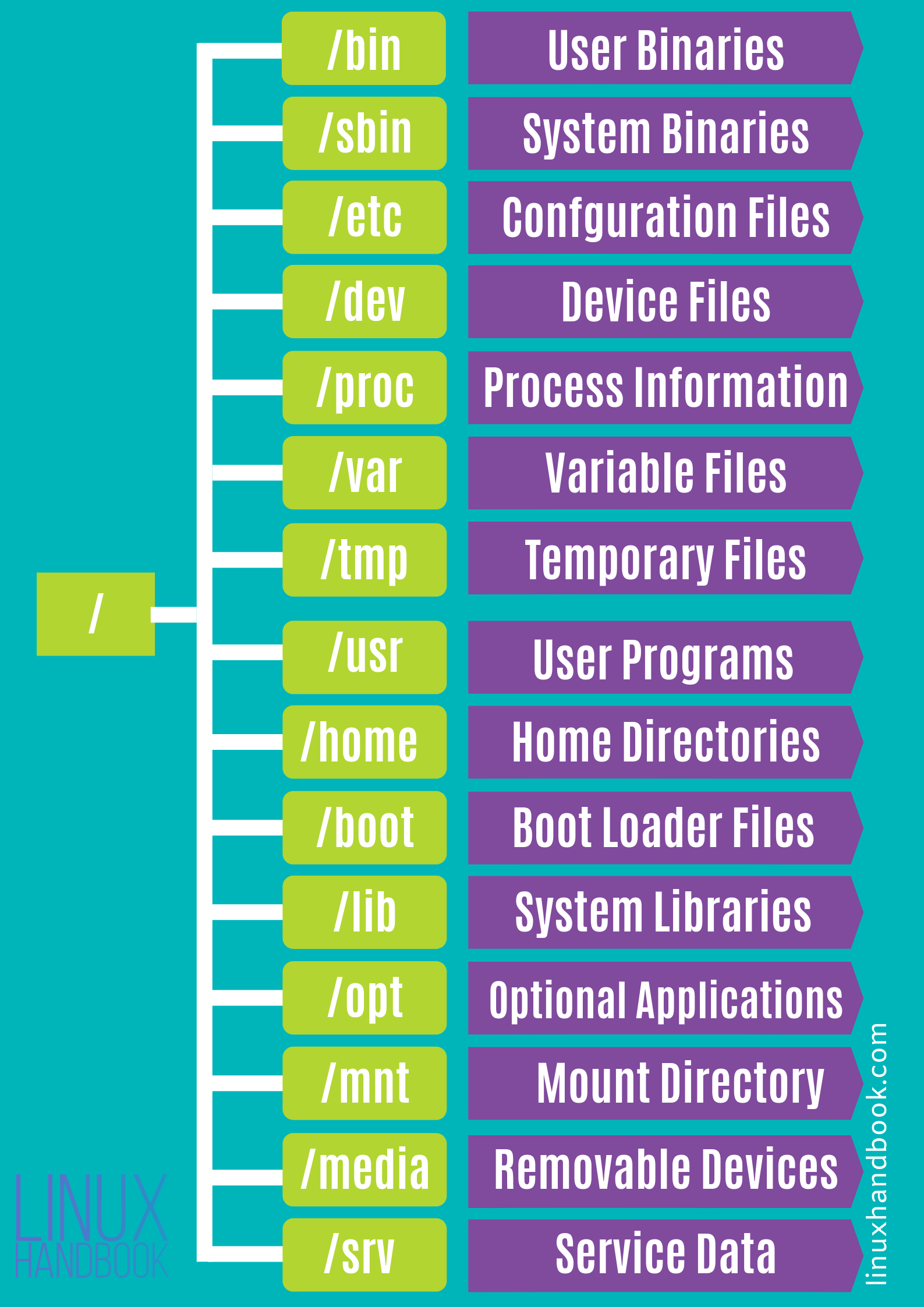
**Lab #01 \_A Activities File Work:**

1. Perform this Experiment and make a list of 10 critical events you come across in the Windows Logs.
2. Review Critical Log Event IDs and learn about their mitigation steps as per the below table.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Windows Log** | **Source** | **Event ID** | **General Info** | **Mitigation Steps** |
|  |  |  | Write in your own words about the event by searching vendor sites, search engines or CVE Details | Write in your own words about the event by searching vendor sites, search engines or CVE Details |
|  |  |  |  |  |
|  |  |  |  |  |

Bonus: Find your PC’s boot time using event viewer.

**Using Linux Event Logs for Security**



There are several ways to view logs in Linux:

Following are commonly used Linux log files:

* **/var/log/syslog or /var/log/messages** – general system activity logs. Used to detect problems that may occur during startup or to isolate application service errors. RedHat-based systems store information in the messages folder while Debian-based systems store them in the syslog folder.
* **/var/log/auth.log or /var/log/secure** – all authentication and authorization logs. Used to investigate failed login attempts. RedHat-based systems store these in the auth.log folder while Debian-based systems store them in the secure folder.
* **/var/log/kern.log** – kernel activity logs, including custom kernels.
* **/var/log/faillog** – failed login attempts.
* **/var/log/maillog or var/log/mail.log** – logs related to mail servers. Used to track issues like emails tagged as spam, and suspicious use of postfix or smtpd.
* Access the directory cd /var/log.
* Use the dmesg (diagnostic message) command to browse through all system logs (dmesg command lets you peer into the hidden world of the Linux startup processes)
* sudo dmesg | less
* sudo dmesg -H (Human Timestamps)
* sudo dmesg -T (Human readable timestamps)
* sudo dmesg –-follow (watch live events)
* sudo dmesg | last -10 (retrieve last 10 messages)
* sudo dmesg | grep -i usb (search for specific term like usb, global regular expression print)
* sudo dmesg | grep -E "memory|tty|dma" (search for multiple terms at once)

## Using Log Levels

Every message logged to the kernel ring buffer has a level attached to it. The level represents the importance of the information in the message. The levels are:

* **emerg**: System is unusable.
* **alert**: Action must be taken immediately.
* **crit**: Critical conditions.
* **err**: Error conditions.
* **warn**: Warning conditions.
* **notice**: Normal but significant condition.
* **info**: Informational.
* **debug**: Debug-level messages
* sudo dmesg -l info
* sudo dmesg -l debug,notice (combine log)

## The Facility Categories

The dmesg messages are grouped into categories called "facilities." The list of facilities is:

* **kern**: Kernel messages.
* **user**: User-level messages.
* **mail**: Mail system.
* **daemon**: System daemons.
* **auth**: Security/authorization messages.
* **syslog**: Internal syslogd messages.
* **lpr**: Line printer subsystem.
* **news**: Network news subsystem.
* sudo dmesg -f daemon
* sudo dmesg -f syslog, daemon (mix both)

## Combining Facility and Level

* sudo dmesg -x

Use the tail command, which displays the last lines written to a certain log file, where problems are usually found.

* tail -f geek-1.log ( track files in real time)
* tail -f /var/log/syslog
* tail -n 11 /var/log/mail.log
* tail -f geek-1.log | grep average ( only relevant info like average)
* tail -f -s 5 geek-1.log ( track file in every 5 sec in real time)

**Lab #01\_B Activities File Work:**

* **Write steps to check logs in Linux with screenshots.**
* **Include important commands and log details (for various levels and categories of logs).**