ASSIGNMENT REPORT 3:LINUX SECURITY

CENG 3544, COMPUTER AND NETWORK SECURITY

Ahmet Oral
ahmetoral@posta.mu.edu.tr

Monday 7th June, 2021

Abstract

In this assignment, I located where the system log and configuration files stored. I researched types of log and configuration files with their usage areas. Lastly I researched a tools for detecting interferences and changes in system file integrity and alerting the user when these actions occurs.

1 Introduction

Log files are a set of records that Linux maintains for the administrators to keep track of important events. They contain messages about the server, including the kernel, services and applications running on it. By monitoring Linux log files, we can gain detailed insight on server performance, security, error messages and underlying issues.

My goal is to locate these log files and learn about their usage areas. Another goal is to find a tools for detecting interferences and changes in system file integrity .

2 Assignments

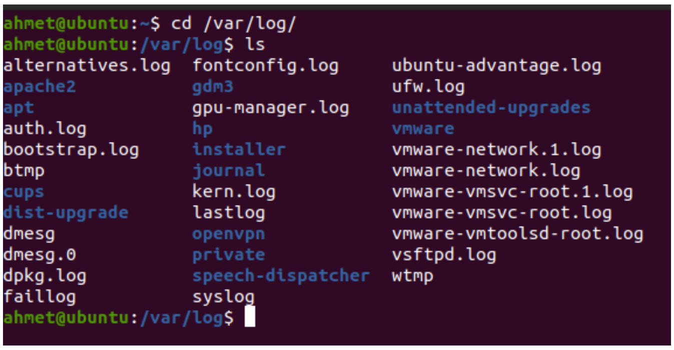
I have 2 main task in this assignment.

1) Locating and Defining System Log Files and Configurations
2) Finding a tool to Detect Changes In the System

2.1 Log Files and Configurations

Log Files

Linux system logs are a set of records that allow a system administrator to monitor critical and important events. In the Linux system, most of the log files are kept in the log folder under the /var/log directory. Inside this directory there are other sub directories that contain the logs of certain programs and services. We can access to the contents of this directory by executing the commands below:



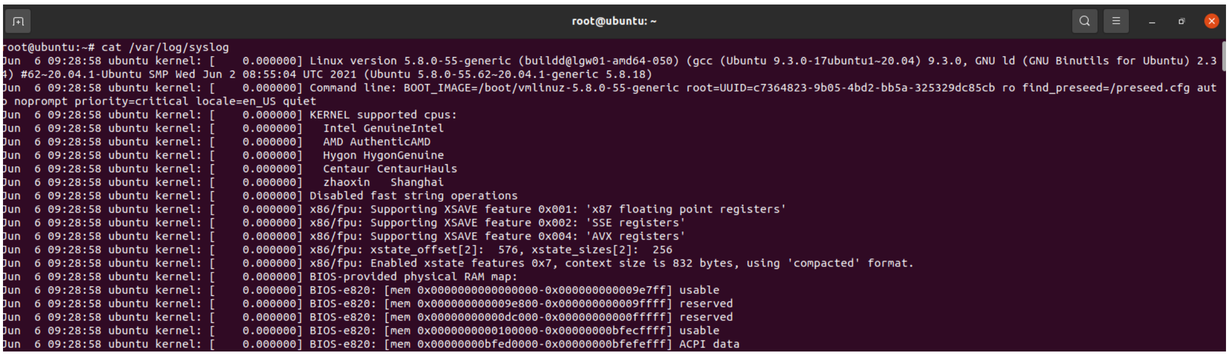
```
ahmet@ubuntu:~$ cd /var/log/
ahmet@ubuntu:/var/log$ ls
alternatives.log  fontconfig.log     ubuntu-advantage.log
apache2           gdm3               ufw.log
apt               gpu-manager.log    unattended-upgrades
auth.log          hp                 vmware
bootstrap.log     installer          vmware-network.1.log
btmp              journal            vmware-network.log
cups              kern.log           vmware-vmsvc-root.1.log
dist-upgrade      lastlog            vmware-vmsvc-root.log
dmesg             openvpn            vmware-vmtoolsd-root.log
dmesg.0           private            vsftpd.log
dpkg.log          speech-dispatcher  wtmp
faillog           syslog
ahmet@ubuntu:/var/log$ 
```

Figure 1: Log Files

This Linux is freshly installed, so there are no rotated files. After certain amount of time, log files are repeatedly overwritten by a certain number of files so that they do not take up much space on the hard disk. This process is called logrotate. Some of these log files can be read by all system users, while others can only be read by root.

System Log

The system log typically contains the greatest deal of information by default about your Ubuntu system. It is located at /var/log/syslog, and may contain information other logs do not. Consult the System Log when you can't locate the desired log information in another log.
We can read the contents of the syslog with the codes given below.



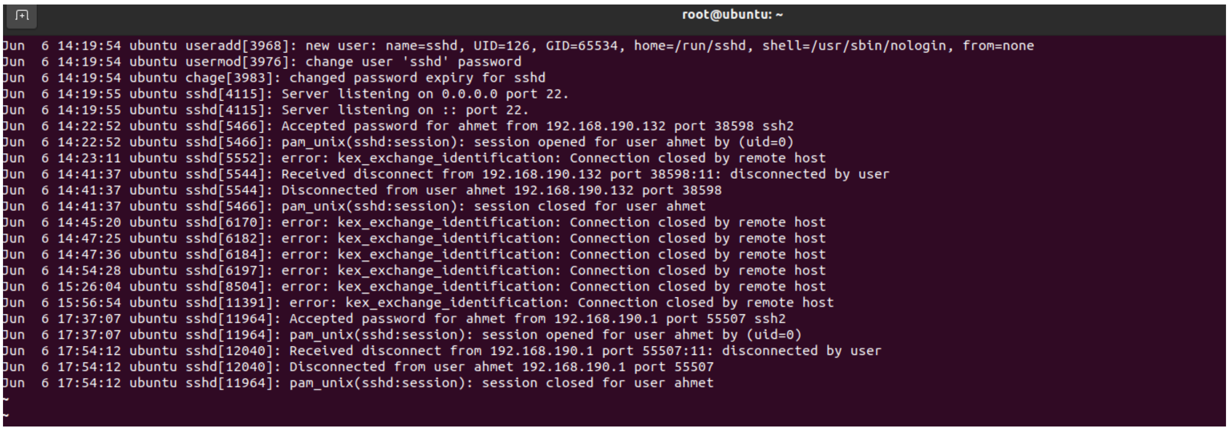
```
root@ubuntu:~# cat /var/log/syslog
Jun  6 09:28:58 ubuntu kernel: [    0.000000] Linux version 5.8.0-55-generic (buildd@lgw01-amd64-050) (gcc (Ubuntu 9.3.0-17ubuntu1~20.04) 9.3.0, GNU ld (GNU Binutils for Ubuntu) 2.3
4) #62~20.04.1-Ubuntu SMP Wed Jun 2 08:55:04 UTC 2021 (Ubuntu 5.8.0-55.62~20.04.1-generic 5.8.18)
Jun  6 09:28:58 ubuntu kernel: [    0.000000] Command line: BOOT_IMAGE=/boot/vmlinuz-5.8.0-55-generic root=UUID=c7364823-9b05-4bd2-bb5a-325329dc85cb ro find_preseed=/preseed.cfg aut
o noprompt priority=critical locale=en_US quiet
Jun  6 09:28:58 ubuntu kernel: [    0.000000] KERNEL supported cpus:
Jun  6 09:28:58 ubuntu kernel: [    0.000000]   Intel GenuineIntel
Jun  6 09:28:58 ubuntu kernel: [    0.000000]   AMD AuthenticAMD
Jun  6 09:28:58 ubuntu kernel: [    0.000000]   Hygon HygonGenuine
Jun  6 09:28:58 ubuntu kernel: [    0.000000]   Centaur CentaurHauls
Jun  6 09:28:58 ubuntu kernel: [    0.000000]   zhaoxin   Shanghai
Jun  6 09:28:58 ubuntu kernel: [    0.000000] Disabled fast string operations
Jun  6 09:28:58 ubuntu kernel: [    0.000000] x86/fpu: Supporting XSAVE feature 0x001: 'x87 floating point registers'
Jun  6 09:28:58 ubuntu kernel: [    0.000000] x86/fpu: Supporting XSAVE feature 0x002: 'SSE registers'
Jun  6 09:28:58 ubuntu kernel: [    0.000000] x86/fpu: Supporting XSAVE feature 0x004: 'AVX registers'
Jun  6 09:28:58 ubuntu kernel: [    0.000000] x86/fpu: xstate_offset[2]:  576, xstate_sizes[2]:  256
Jun  6 09:28:58 ubuntu kernel: [    0.000000] x86/fpu: Enabled xstate features 0x7, context size is 832 bytes, using 'compacted' format.
Jun  6 09:28:58 ubuntu kernel: [    0.000000] BIOS-provided physical RAM map:
Jun  6 09:28:58 ubuntu kernel: [    0.000000] BIOS-e820: [mem 0x0000000000000000-0x000000000009e7ff] usable
Jun  6 09:28:58 ubuntu kernel: [    0.000000] BIOS-e820: [mem 0x000000000009e800-0x000000000009ffff] reserved
Jun  6 09:28:58 ubuntu kernel: [    0.000000] BIOS-e820: [mem 0x00000000000dc000-0x00000000000fffff] reserved
Jun  6 09:28:58 ubuntu kernel: [    0.000000] BIOS-e820: [mem 0x0000000000100000-0x00000000bfecffff] usable
Jun  6 09:28:58 ubuntu kernel: [    0.000000] BIOS-e820: [mem 0x00000000bfed0000-0x00000000bfefefff] ACPI data
```

Figure 2: Syslog

Authorization Log

The Authorization Log tracks usage of authorization systems, the mechanisms for authorizing users which prompt for user passwords, such as sudo command, remote logins to sshd and so on. The Authorization Log file may be accessed at /var/log/auth.log. This log is useful for learning about user logins and usage of the sudo command. Unsuccessful password attempts for root and other users are also written to this file.

For example, to see only information in the Authorization Log pertaining to sshd logins we can use ”grep sshd /var/log/auth.log — less” command. As you can see in the image below, ssh connections while I was doing the first assigment is visible:



```
Jun  6 14:19:54 ubuntu useradd[3968]: new user: name=sshd, UID=126, GID=65534, home=/run/sshd, shell=/usr/sbin/nologin, from=none
Jun  6 14:19:54 ubuntu usermod[3976]: change user 'sshd' password
Jun  6 14:19:54 ubuntu chage[3983]: changed password expiry for sshd
Jun  6 14:19:55 ubuntu sshd[4115]: Server listening on 0.0.0.0 port 22.
Jun  6 14:19:55 ubuntu sshd[4115]: Server listening on :: port 22.
Jun  6 14:22:52 ubuntu sshd[5466]: Accepted password for ahmet from 192.168.190.132 port 38598 ssh2
Jun  6 14:22:52 ubuntu sshd[5466]: pam_unix(sshd:session): session opened for user ahmet by (uid=0)
Jun  6 14:23:11 ubuntu sshd[5552]: error: kex_exchange_identification: Connection closed by remote host
Jun  6 14:41:37 ubuntu sshd[5544]: Received disconnect from 192.168.190.132 port 38598:11: disconnected by user
Jun  6 14:41:37 ubuntu sshd[5544]: Disconnected from user ahmet 192.168.190.132 port 38598
Jun  6 14:41:37 ubuntu sshd[5466]: pam_unix(sshd:session): session closed for user ahmet
Jun  6 14:45:20 ubuntu sshd[6170]: error: kex_exchange_identification: Connection closed by remote host
Jun  6 14:47:25 ubuntu sshd[6182]: error: kex_exchange_identification: Connection closed by remote host
Jun  6 14:47:36 ubuntu sshd[6184]: error: kex_exchange_identification: Connection closed by remote host
Jun  6 14:54:28 ubuntu sshd[6197]: error: kex_exchange_identification: Connection closed by remote host
Jun  6 15:26:04 ubuntu sshd[8504]: error: kex_exchange_identification: Connection closed by remote host
Jun  6 15:56:54 ubuntu sshd[11391]: error: kex_exchange_identification: Connection closed by remote host
Jun  6 17:37:07 ubuntu sshd[11964]: Accepted password for ahmet from 192.168.190.1 port 55507 ssh2
Jun  6 17:37:07 ubuntu sshd[11964]: pam_unix(sshd:session): session opened for user ahmet by (uid=0)
Jun  6 17:54:12 ubuntu sshd[12040]: Received disconnect from 192.168.190.1 port 55507:11: disconnected by user
Jun  6 17:54:12 ubuntu sshd[12040]: Disconnected from user ahmet 192.168.190.1 port 55507
Jun  6 17:54:12 ubuntu sshd[11964]: pam_unix(sshd:session): session closed for user ahmet
~
~
```

Figure 3: Auth.log

There are lots of other log files such as Daemon Log, Debug Log, Kernel Log, Application Logs and Non-Human-Readable Logs. Log Types etc. .The ones I explained above are 2 of the most important types of log types for me.

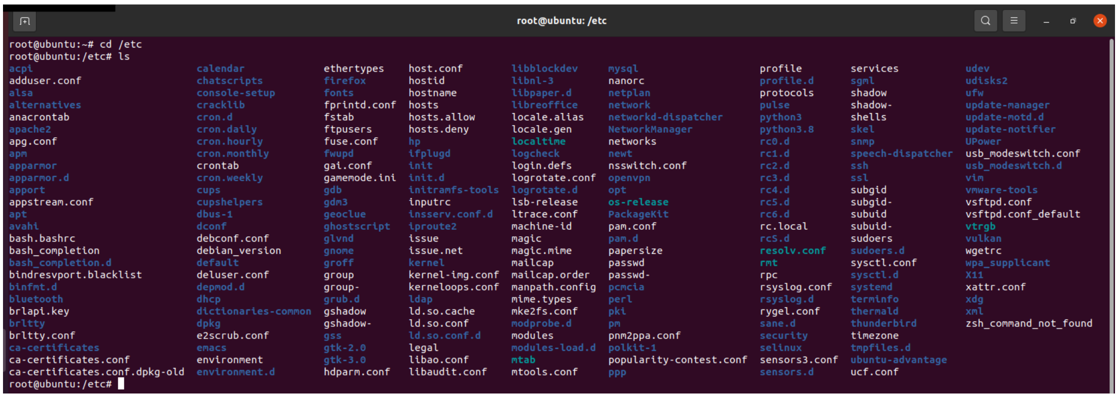
Configuration Files

Configuration files are used to configure the parameters and initial settings for most of programs. They are used for user applications, server processes and operating system settings. The behaviour of almost every program can be customized to our preferences or needs by modifying its configuration files. Some of the example files:

/etc/securetty: Contains the device names of tty lines (one per line, without leading /dev/) on which root is allowed to login.
/etc/shells: Holds the list of possible “shells” available to the system.
/etc/gated.version: Contains the version number of the gated daemon.

I can also give the ”vsft.pd.config” file that was used in the last assignment. This file was edited for enabling FTP encryption. Many programs config files can be edited like this to work under different conditions.

In Ubuntu OS, most of the Config files are located at "/etc" as seen in the image below:



```
root@ubuntu:~# cd /etc
root@ubuntu:/etc# ls
acpi                           calendar             ethertypes    host.conf        libblockdev     mysql                    profile        services           udev
adduser.conf                   chatscripts          firefox       hostid           libnl-3         nanorc                   profile.d      sgml               udisks2
alsa                           console-setup        fonts         hostname         libpaper.d      netplan                  protocols      shadow             ufw
alternatives                   cracklib             fprintd.conf  hosts            libreoffice     network                  pulse          shadow-            update-manager
anacrontab                     cron.d               fstab         hosts.allow      locale.alias    networkd-dispatcher      python3        shells             update-motd.d
apache2                        cron.daily           ftpusers      hosts.deny       locale.gen      NetworkManager           python3.8      skel               update-notifier
apg.conf                       cron.hourly          fuse.conf     hp               localtime       networks                 rc0.d          snmp               UPower
apm                            cron.monthly         fwupd         ifplugd          logcheck        newt                     rc1.d          speech-dispatcher  usb_modeswitch.conf
apparmor                       crontab              gai.conf      init             login.defs      nsswitch.conf            rc2.d          ssh                usb_modeswitch.d
apparmor.d                     cron.weekly          gamemode.ini  init.d           logrotate.conf  openvpn                  rc3.d          ssl                vim
apport                         cups                 gdb           initramfs-tools  logrotate.d     opt                      rc4.d          subgid             vmware-tools
appstream.conf                 cupshelpers          gdm3          inputrc          lsb-release     os-release               rc5.d          subgid-            vsftpd.conf
apt                            dbus-1               geoclue       insserv.conf.d   ltrace.conf     PackageKit               rc6.d          subuid             vsftpd.conf_default
avahi                          dconf                ghostscript   iproute2         machine-id      pam.conf                 rc.local       subuid-            vtrgb
bash.bashrc                    debconf.conf         glvnd         issue            magic           pam.d                    rcS.d          sudoers            vulkan
bash_completion                debian_version       gnome         issue.net        magic.mime      papersize                resolv.conf    sudoers.d          wgetrc
bash_completion.d              default              groff         kernel           mailcap         passwd                   rmt            sysctl.conf        wpa_supplicant
bindresvport.blacklist         deluser.conf         group         kernel-img.conf  mailcap.order   passwd-                  rpc            sysctl.d           X11
binfmt.d                       depmod.d             group-        kerneloops.conf  manpath.config  pcmcia                   rsyslog.conf   systemd            xattr.conf
bluetooth                      dhcp                 grub.d        ldap             mime.types      perl                     rsyslog.d      terminfo           xdg
brlapi.key                     dictionaries-common  gshadow       ld.so.cache      mke2fs.conf     pki                      rygel.conf     thermald           xml
brltty                         dpkg                 gshadow-      ld.so.conf       modprobe.d      pm                       sane.d         thunderbird        zsh_command_not_found
brltty.conf                    e2scrub.conf         gss           ld.so.conf.d     modules         pnm2ppa.conf             security       timezone
ca-certificates                emacs                gtk-2.0       legal            modules-load.d  polkit-1                 selinux        tmpfiles.d
ca-certificates.conf           environment          gtk-3.0       libao.conf       mtab            popularity-contest.conf  sensors3.conf  ubuntu-advantage
ca-certificates.conf.dpkg-old  environment.d        hdparm.conf   libaudit.conf    mtools.conf     ppp                      sensors.d      ucf.conf
root@ubuntu:/etc# 
```

Figure 4: Auth.log

2.2 Tools to Detect Changes In the System

Linux have specific tools for detecting any interference on the system. One of these tools are described below:

Tripwire

Tripwire is an open source host-based Intrusion Detection System. Tripwire can check for file integrity, and it will monitor and alert on file/directory change.

A Tripwire check compares the current filesystem state against a known baseline state and alerts on any changes it detects. The baseline and check behavior are controlled by a policy file, which specifies which files or directories to monitor, and which attributes to monitor on them, such as hashes, file permissions, and ownership.

When an expected change occurs, such as upgrading a package, the baseline database can be updated to the new known-good state. The policy can also be updated, for example, to reduce noise or cover a newly installed package.

3 Conclusion

In this assignment I learned about the log and configuration files. I learned what types of logs there are, their purposes and locations in the system. I also learned where most of the config files are stored and their usage areas. After that I researched a tool that can detect and interference on the system by checking system files and alerts the user. These interferences can be detected by humans after examining log files, but a tool is needed for making sure the system is safe because there are so many different variables and changes in the system.