LAB 9: LINUX FORENSICS (LINUX AUDITING SYSTEM) PART II

Lab Requirements

1. Linux OS
2. Internet connection

Content

Part I: Linux Auditing System (auditd)

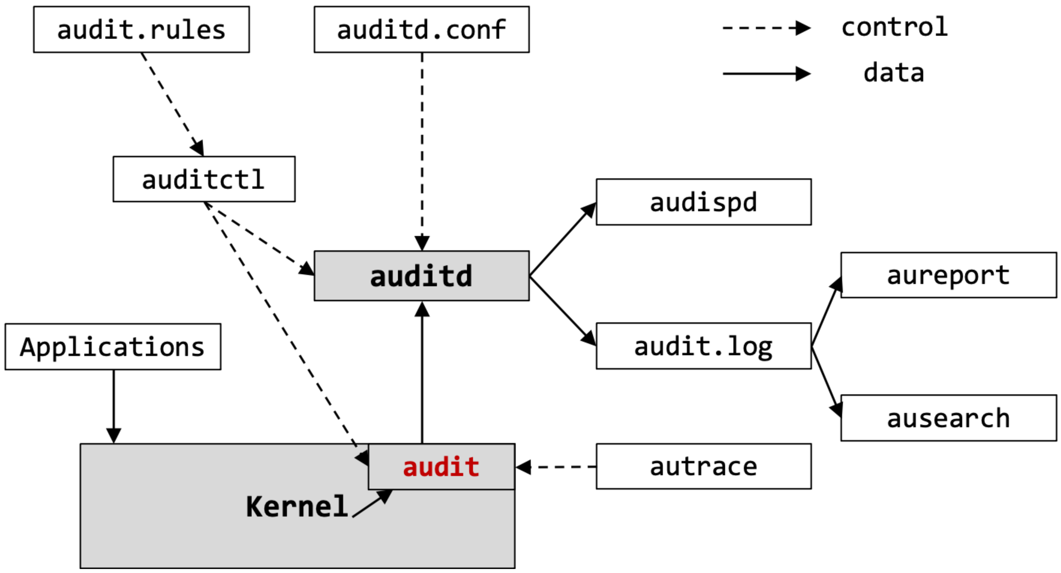
STEP 1: Linux audit system provide information about what is going on the system in great detail. This would help building up the system's security but auditing per se does not strengthen the security of the system.

STEP 2: Operating systems should provide auditing capabilities to conform with strands of protection profiles. For instance, Module 5.1.5, among other sections, of the **Protection Profile for General Purpose Operating Systems** proposed by the National Information Assurance Partnership (**NIAP**: USA) outlines the auditing requirements of operating systems. [Ref: https://www.niapccevs.org/MMO/PP/pp_os_v4.1.pdf]

STEP 3: Install `auditd` and start the daemon.

```

# Install auditd kali@kali [~] sudo apt-
get install auditd

# Display the status of auditd
kali@kali [~] systemctl status auditd | grep -i active
    Active: inactive (dead) since Tue 2022-03-29 00:05:13 EDT; 1min 24s ago

# Start auditd
kali@kali [~] systemctl start auditd
    Active: inactive (dead) since Tue 2022-03-29 00:05:13 EDT; 1min 24s ago
# Display the status of auditd
kali@kali [~]systemctl status auditd | grep -i active
    Active: active (running) since Tue 2022-03-29 00:07:40 EDT; 48s ago

```

Step 4: Linux Auditing System (`Audit`) is a native auditing system to Linux kernel. Linux audit consists of the following components (Ref: https://documentation.suse.com):



`auditd`: The audit daemon writes audit messages generated by the Kernel `audit` interface. The auditing functionality is controlled by the file `/etc/audit/auditd.conf`.

```


# List the content of the /etc/audit/ folder
kali@kali [~] sudo ls -l /etc/audit/ total
20
     -rw-r----- 1 root root  881 Feb 11 05:34 auditd.conf
     -rw-r----- 1 root root  107 Mar 20 18:10 audit.rules -rw-r---
     -- 1 root root  127 Feb 11 05:34 audit-stop.rules drwxr-x---
     2 root root 4096 Mar 20 18:10 plugins.d drwxr-x--- 2 root
     root 4096 Mar 20 18:10 rules.d

kali@kali [~] sudo cat /etc/audit/auditd.conf | head #
     # This file controls the configuration of the audit daemon
     #
     local_events = yes write_logs
     = yes
     log_file = /var/log/audit/audit.log
     log_group = adm log_format =
     ENRICHED flush = INCREMENTAL_ASYNC

```

`auditctl`: The utility control the audit system: the `audit` interface and the rule sets that determine the events to be tracked.

`audit rules`: The rules are stored as a sequence of `auditctl` commands file `/etc/audit/audit.rules`

`aureport`: This utility allows the user to generate reports out of the audit log file.

`ausearch`: This utility is used to search the audit log file for particular events using a variety of keys.

`audispd`: The audit dispatcher daemon can be used to relay event notifications to other applications instead of the audit log file.

`autrace`: This utility is used to trace particular processes (similar to `strace`). The output of autrace is logged t the audit log file.

STEP 5: The audit system can be controlled using the `auditctl` utility.

```



# Query the status of the audit daemon
kali@kali [~] sudo auditctl -s enabled
0 failure 1 pid 0 rate_limit 0
backlog_limit 64 lost 0 backlog 0
backlog_wait_time 15000
backlog_wait_time_actual 0
loginuid_immutable 0 unlocked



```

Flag	Meaning & Possible Values	Command
`enabled`	Enable or disable the audit system [**0**: disable, **1**: enable, **2**: enable and lockdown the configuration]	`auditctl -e [0|1|2]`
`failure`	Specify how the Kernel will handle critical errors.	`auditctl -f [0|1|2]`
	[**0**: silent, **1**: printk, **2**: panic]	
`pid`	Process ID of `auditd`	None

`rate_limit`	Set limit in messages/second (0: no limit). If the limit is exceeded, the failure flag is consulted by the kernel for action.	`auditctl -r rate`
`back_log_limit`	Set maximum number of outstanding audit buffers allowed (default: 64). If the limit is exceeded, the failure flag is consulted by the kernel for action.	`auditctl -b backlog`
`lost`	Count the number of lost audit messages	None
`backlog`	Count the number of current outstanding audit messages.	None
`backlog_wait_time`	Set the time for the kernel to wait (Kernel default 60*HZ) when the backlog limit is reached before queuing more audit events to be transferred to auditd.	None
`backlog_wait_time_actual`	The actual wait time	None

STEP 6: To enable the auditing system and display an event for analysis, use the following commands:

```
# Enable the audit system kali@kali
[~] sudo auditctl -e 1

# Display one audit event kali@kali [~] sudo cat /var/log/audit/audit.log |
grep -i syscall | head -n 1 type=SYSCALL msg=audit(1647814451.561:3):
arch=c000003e syscall=44 success=yes exit=60 a0=3 a1=7ffc2cb20ad0 a2=3c a3=0
items=0 ppid=209778 pid=209788 auid=4294967295 uid=0 gid=0 euid=0 suid=0
fsuid=0 egid=0 sgid=0 fsgid=0 tty=(none) ses=4294967295 comm="auditctl"
exe="/usr/sbin/auditctl" subj==unconfined key=(null)ARCH=x86_64 SYSCALL=sendto
AUID="unset"
     UID="root" GID="root" EUID="root" SUID="root" FSUID="root" EGID="root"
     SGID="root" FSGID="root"
```

type: The type of the event recorded. In this case, it is DAEMON_START (triggered when the audit daemon is started). DAEMON_CONFIG is triggered when daemon configuration change is detected, and SYSCALL is triggered to record a system call to the kernel, SYSTEM_BOOT to report system bootup, etc. CWD event is triggered to record the current working directory, and PATH is triggered to record file name path information. For a detailed list, refer to https://access.redhat.com/documentation/enus/red_hat_enterprise_linux/6/html/security_guide/sec-audit_record_types.

msg: The message id is enclosed in brackets (epoch time stamp: actual event id)

exe: The path to the binary program.

STEP 7: The `aureport` utility is used to create custom reports based on the audit log file content stored in `/var/log/audit/audit.log`. To read audit logs from a file, use the following command (I am using the standard audit log file, but any other file can be used):

```

# The option -if provided detailed output kali@kali
[~]sudo aureport -if /var/log/audit/audit.log
     Summary Report
     ======================
     Range of time in logs: 03/20/2022 18:14:11.535 - 03/28/2022 22:47:04.065
     Selected time for report: 03/20/2022 18:14:11 - 03/28/2022 22:47:04.065
     Number of changes in configuration: 10
     Number of changes to accounts, groups, or roles: 0
     Number of logins: 0
     Number of failed logins: 0
     Number of authentications: 13
     Number of failed authentications: 0
     Number of users: 4
     Number of terminals: 10
     Number of host names: 2
     Number of executables: 9
     Number of commands: 8
     Number of files: 22
     Number of AVC's: 0
     Number of MAC events: 0
     Number of failed syscalls: 10
     Number of anomaly events: 0
     Number of responses to anomaly events: 0
     Number of crypto events: 0
     Number of integrity events: 0
     Number of virt events: 0
     Number of keys: 0
     Number of process IDs: 171
     Number of events: 1217

```

STEP 8: More functionalities of the `aureport` utility.

```
# Attempted authentication kali@kali
[~] aureport -au
     Authentication Report
     ============================================
     # date time acct host term exe success event
     ============================================
     1.      03/20/2022 19:02:45 kali ? :1 /usr/sbin/lightdm yes 169
     2.      03/20/2022 19:03:01 kali ? /dev/pts/1 /usr/bin/sudo yes 176 3.
     03/20/2022 21:05:43 kali ? :1 /usr/sbin/lightdm yes 386
     4. 03/20/2022 21:07:11 kali ? /dev/pts/1 /usr/bin/sudo yes 393
     5. 03/20/2022 21:21:28 kali ? :1 /usr/sbin/lightdm yes 428

# Attempted logins kali@kali
[~]sudo aureport -l
     Login Report
     ============================================
     # date time auid host term exe success event
     ============================================
     <no events of interest were found>
# Failed events
kali@kali [~] sudo aureport --failed
     # Results are displayed here

# Successful events
kali@kali [~] sudo aureport --success
     # Results are displayed here

# ts: start time, te: end time kali@kali [~] sudo aureport
-ts yesterday -te now --success

     Success Summary Report
     ======================
     Range of time in logs: 03/20/2022 18:14:11.535 - 03/28/2022 23:02:52.071
     Selected time for report: 03/27/2022 00:00:00 - 03/28/2022 23:02:52
     Number of changes in configuration: 3
     Number of changes to accounts, groups, or roles: 0 ...

# User report (--summary option summarizes results)
# -I option will display the user name (Kali instead of 1000 and root instead
# of 0)
kali@kali [~] sudo aureport -u --summary
     User Summary Report
     =========================== total
     auid
     ===========================
     707  1000
     316  0
     283  -1
     18  130

# Events summary
```

```
kali@kali [~] sudo aureport -e -i --summary
     Event  Summary  Report
     ======================
     total  type
     ======================
     481  SYSCALL
     206  USER_ACCT
     204  USER_START
     197  CRED_DISP 197
     USER_END
     128  CRED_REFR
     123  USER_CMD
     82  CRED_ACQ
     76  LOGIN
     59  SERVICE_STOP
     39  SERVICE_START
     26  CONFIG_CHANGE
     15  USER_AUTH
     9  BPF
     2  DAEMON_START
     1  USER_LOGOUT
     1  SYSTEM_SHUTDOWN
     1 DAEMON_END

# Events report (better formatted display) kali@kali [~]
sudo aureport -e -ts yesterday -te now | head
     Event Report
     ===================================
     # date time event type auid success
     ===================================
     1.      03/28/2022 22:36:31 8521 DAEMON_START -1 yes
     2.      03/28/2022 22:36:31 49 SYSCALL -1 yes
     3.      03/28/2022 22:36:31 50 CONFIG_CHANGE -1 yes 4.
     03/28/2022 22:36:31 51 CONFIG_CHANGE -1 yes
     5. 03/28/2022 22:36:31 52 CONFIG_CHANGE -1 yes

# Processes report
kali@kali [~]sudo aureport -p | head

     Process ID Report
     ======================================
     # date time pid exe syscall auid event
     ======================================
     1.      03/20/2022 18:14:11 209775 ? 0 -1 834
     2.      03/20/2022 18:14:11 209788 /usr/sbin/auditctl 44
     -1 3 3. 03/20/2022 18:14:11 209788 /usr/sbin/auditctl 44
     -1 4
     4. 03/20/2022 18:14:11 209788 /usr/sbin/auditctl 44 -1 5
     5. 03/20/2022 18:14:11 1 /usr/lib/systemd/systemd 0 -1 6

# System call Events report kali@kali
[~]sudo aureport -s | head
```

STEP 9: Querying the audit log with `ausearch`.

```
# get the id f the current logged in user kali@kali [~] id uid=1000(kali)
gid=1000(kali)
groups=1000(kali),4(adm),20(dialout),24(cdrom),25(floppy),27(sudo),29(audio
),30(dip),44(video),46(plugdev),109(netdev),119(wireshark),122(bluetooth),1
     34(scanner),142(kaboxer)

# Search the events miniated by a given user (kali with uid 1000)
# ausearch -a event_id can be used to search for a particular event kali@kali
[~] ausearch -ui 1000 | head
     ---- time->Sun Mar 20 18:14:11 2022 type=USER_END
     msg=audit(1647814451.565:7): pid=209769 uid=1000 auid=1000
     ses=3 subj==unconfined msg='op=PAM:session_close
     grantors=pam_limits,pam_permit,pam_unix acct="root" exe="/usr/bin/sudo"
     hostname=? addr=? terminal=/dev/pts/1 res=success' ---- [truncated]
```

STEP 10: “When performing an `autrace` on a process, make sure that any audit rules are purged from the queue to avoid these rules clashing with the ones `autrace` adds itself. Delete the audit rules with the auditctl -D command. This stops all normal auditing.” [suse.com]

```
# Delete the audit rules (by default there are no rules)
kali@kali [~] auditctl -D No rules

# Trace the binary less
kali@kali [~] sudo autrace /usr/bin/less
     Waiting to execute: /usr/bin/less
     Missing filename ("less --help" for help)
     Cleaning up...
     Trace complete. You can locate the records with 'ausearch -i -p 122409'

# Search for all events related to /less in the audit log file  kali@kali
[~] sudo ausearch -i -p 122409
     # Results will be displayed here
```

Part II: Security Auditing using Lynis

STEP 11: Lynis is a security auditing tool for Linux, macOS, or UNIX operating systems. [https://cisofy.com/lynis/, https://cisofy.com/documentation/lynis/get-started/]

STEP 12: Lynis is used for 1) security auditing, 2) compliance testing (PCI, HIPAA, Sox, etc.), 3) penetration testing, 4) vulnerability detection, and 5) system hardening.

STEP 13: Performed tests by Lynis have unique identifiers (e.g., KRNL-1234). A complete list of controls is available at https://cisofy.com/lynis/controls/ **STEP 14:** Install Lynis using the following command:

```
kali@kali [~] sudo apt-get install lynis
```

STEP 15: Display the available commands as follows.

```
kali@kali [~] lynis show commands
     Commands: lynis
     audit lynis
     configure lynis
     generate lynis
     show lynis update
     lynis upload-only
```

STEP 16: Display Lynis settings.

```
kali@kali [~] lynis show settings #
     Colored screen output colors=1

     # Language language=en
      ...

     # Add --brief to hide descriptions, --configured-only to show configured
     items only, or --nocolors to remove colors
```

STEP 17: Use the following command to perform security auditing of the system. Detailed information of the audit will be stored in the log file `/var/log/lynis.log`, and data will be stored in `/var/log/lynis-report.dat`.

```
kali@kali [~] sudo lynis audit system
    # Results [Very long] will be displayed here
    # You might wish to use the --quick option
```

STEP 18: Lynis displays a report at the end of the auditing process that includes Warnings and Suggestions, each with a unique identifier.

```

-[ Lynis 3.0.7 Results ]-

  Warnings (1):
  ----------------------------
  ! Couldn't find 2 responsive nameservers [NETW-2705]
https://cisofy.com/lynis/controls/NETW-2705/

  Suggestions (60):
  ----------------------------
 *    Install libpam-tmpdir to set $TMP and $TMPDIR for PAM sessions [DEB-0280]
 https://cisofy.com/lynis/controls/DEB-0280/

 *    Install apt-listbugs to display a list of critical bugs prior to each APT
 installation. [DEB-0810]
      https://cisofy.com/lynis/controls/DEB-0810/ ...
```

STEP 19: To get more details about any of the performed tests, which either resulted in a warning or suggestion, use the lynis show details command.

```
kali@kali [~] sudo lynis show details NETW-2705
    2022-03-29 00:26:47 Performing test ID NETW-2705 (Check availability two
    nameservers)
    2022-03-29 00:26:47 Result: less than 2 responsive nameservers found
    2022-03-29 00:26:47 Warning: Couldn't find 2 responsive nameservers
    [test:NETW-2705] [details:-] [solution:-]
    2022-03-29 00:26:47 Note: Non responsive nameservers can give problems for
    your system(s). Like the lack of recursive lookups, bad connectivity to
    update servers etc.
    2022-03-29 00:26:47 Suggestion: Check your resolv.conf file and fill in a
    backup nameserver if possible [test:NETW-2705] [details:-] [solution:-]
    2022-03-29 00:26:47 Hardening: assigned partial number of hardening points
    (1 of 2). Currently having 106 points (out of 166) 2022-03-29
    00:26:47 ====
```

STEP 20: Let us check the content of the resolv.conf.

```
kali@kali [~] sudo su

# Display the content of the /etc/resolv.conf file kali@kali
[/home/kali] # cat /etc/resolv.conf
     # Generated by NetworkManager
     search localdomain nameserver
     172.16.200.2

# Add more public DNS servers kali@kali [/home/kali] # echo nameserver
8.8.8.8>> /etc/resolv.conf kali@kali [/home/kali] # echo nameserver
75.75.75.75>> /etc/resolv.conf kali@kali [/home/kali] # echo nameserver
75.75.76.76>> /etc/resolv.conf
# Display the content of the /etc/resolv.conf file kali@kali
[/home/kali] # cat /etc/resolv.conf
     # Generated by NetworkManager
     search localdomain nameserver
     172.16.200.2 nameserver
     8.8.8.8 nameserver
     75.75.75.75 nameserver
     75.75.76.76
```

STEP 21: Perform system security auditing again to check if the warning disappears. Geat, the warning disappeared!

```
kali@kali [~] sudo lynis audit system
     -[ Lynis 3.0.7 Results ]-

       Great, no warnings

       Suggestions (58):
       ----------------------------
     * Install libpam-tmpdir to set $TMP and $TMPDIR for PAM sessions [DEB-
     0280]  https://cisofy.com/lynis/controls/DEB-0280/

     * Install apt-listbugs to display a list of critical bugs prior to each APT
     installation. [DEB-0810]
     https://cisofy.com/lynis/controls/DEB-0810/ ...
```

STEP 22: Lynis provides a hardening score (unique to Lynis). After fixing all the suggestions, the hardening index improves.

```
    Lynis security scan details:

```

```
    Hardening index : 61 [############        ]
    Tests performed : 267
    Plugins enabled : 1
```