

# **Linux Security Monitoring and Auditing Lab Assignment: Implementing Security Monitoring and Auditing**

## **Part 1: Configuring Linux Logging and Auditing**

Configuring comprehensive logging and auditing on a Linux system to monitor security-relevant events

### **Deliverables:**

- Screenshot showing the configuration of rsyslog  
sudo apt update

```
(icdfa@icdfa)-[~]
$ sudo apt update
[sudo] password for icdfa:
Get:2 https://artifacts.elastic.co/packages/8.x/apt stable InRelease [3,248 B]
Get:3 https://artifacts.elastic.co/packages/8.x/apt stable/main amd64 Packages [87.9 kB]
Get:1 http://kali.download/kali kali-rolling InRelease [41.5 kB]
Get:4 http://kali.download/kali kali-rolling/main i386 Packages [20.7 MB]
Get:5 http://kali.download/kali kali-rolling/main amd64 Packages [21.2 MB]
Get:6 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [51.8 MB]
Get:7 http://kali.download/kali kali-rolling/main i386 Contents (deb) [48.1 MB]
Get:8 http://kali.download/kali kali-rolling/contrib i386 Packages [99.2 kB]
Get:9 http://kali.download/kali kali-rolling/contrib amd64 Packages [120 kB]
Get:10 http://kali.download/kali kali-rolling/contrib amd64 Contents (deb) [326 kB]
Get:11 http://kali.download/kali kali-rolling/contrib i386 Contents (deb) [182 kB]
Get:12 http://kali.download/kali kali-rolling/non-free i386 Packages [149 kB]
Get:13 http://kali.download/kali kali-rolling/non-free amd64 Packages [200 kB]
Get:14 http://kali.download/kali kali-rolling/non-free amd64 Contents (deb) [911 kB]
Get:15 http://kali.download/kali kali-rolling/non-free i386 Contents (deb) [859 kB]
Get:16 http://kali.download/kali kali-rolling/non-free-firmware amd64 Packages [11.3 kB]
Get:17 http://kali.download/kali kali-rolling/non-free-firmware i386 Packages [10.8 kB]
Get:18 http://kali.download/kali kali-rolling/non-free-firmware amd64 Contents (deb) [28.4 kB]
Get:19 http://kali.download/kali kali-rolling/non-free-firmware i386 Contents (deb) [28.4 kB]
Fetched 145 MB in 10min 37s (227 kB/s)
1404 packages can be upgraded. Run 'apt list --upgradable' to see them.
```

sudo apt install -y rsyslog

```
(icdfa@icdfa)-[~]
$ sudo apt install -y rsyslog
The following packages were automatically installed and are no longer required:
libcaes1  libevtx1t64  libolecf1  python3-acstore  python3-libcreg  python3-libfwsi  python3-lbscca  python3-zstd
libcreg1t64  libfws1t64  libopenh264-7  python3-cffi  python3-libesedb  python3-liblnk  python3-pefile
libdnnl3  libgapi-mesa  libssca1t64  python3-elasticsearch  python3-libevt  python3-lbmsiecf  python3-pycaes
libevt1t64  libmsiecf1t64  libxnpack0  python3-flor  python3-libevtx  python3-libolecf  python3-pycparser
Use 'sudo apt autoremove' to remove them.

Installing:
rsyslog

Installing dependencies:
libestr0  libfastjson4  liblognorm5

Suggested packages:
rsyslog-doc  rsyslog-mongodb  rsyslog-hiredis  rsyslog-docker  | rsyslog-gnutls
rsyslog-mysql  rsyslog-elasticsearch  rsyslog-snmp  rsyslog-clickhouse  rsyslog-gsapi
| rsyslog-pgsql  rsyslog-kafka  rsyslog-kubernetes  rsyslog-openssl  rsyslog-relp

Summary:
Upgrading: 0, Installing: 4, Removing: 0, Not Upgrading: 1404
Download size: 866 kB
Space needed: 2,343 kB / 4,693 MB available

Get:1 http://kali.download/kali kali-rolling/main amd64 libestr0 amd64 0.1.11-2 [9,048 B]
Get:2 http://kali.download/kali kali-rolling/main amd64 libfastjson4 amd64 1.2304.0-2 [28.9 kB]
Get:3 http://kali.download/kali kali-rolling/main amd64 liblognorm5 amd64 2.0.6-5 [66.5 kB]
Get:4 http://kali.download/kali kali-rolling/main amd64 rsyslog amd64 8.2506.0-4 [762 kB]
Fetched 866 kB in 4s (222 kB/s)
Selecting previously unselected package libestr0:amd64.
(Reading database ... 417547 files and directories currently installed.)
Preparing to unpack .../libestr0_0.1.11-2_amd64.deb ...
Unpacking libestr0:amd64 (0.1.11-2) ...
Selecting previously unselected package libfastjson4:amd64.
Preparing to unpack .../libfastjson4_1.2304.0-2_amd64.deb ...
Unpacking libfastjson4:amd64 (1.2304.0-2) ...
Selecting previously unselected package liblognorm5:amd64.
Preparing to unpack .../liblognorm5_2.0.6-5_amd64.deb ...
Unpacking liblognorm5:amd64 (2.0.6-5) ...
Selecting previously unselected package rsyslog.
Preparing to unpack .../rsyslog_8.2506.0-4_amd64.deb ...
Unpacking rsyslog (8.2506.0-4) ...
Setting up libestr0:amd64 (0.1.11-2) ...
Setting up libfastjson4:amd64 (1.2304.0-2) ...
Setting up liblognorm5:amd64 (2.0.6-5) ...
Setting up rsyslog (8.2506.0-4) ...
Created symlink '/etc/systemd/system/syslog.service' → '/usr/lib/systemd/system/rsyslog.service'.
Created symlink '/etc/systemd/system/multi-user.target.wants/rsyslog.service' → '/usr/lib/systemd/system/rsyslog.service'.
Processing triggers for kali-menu (2025.1.1) ...
Processing triggers for libc-bin (2.41-6) ...
Processing triggers for man-db (2.13.0-1) ...
```

```
(icdfa@icdfa) [~]
└─$ sudo nano /etc/rsyslog.d/security.config
[sudo] password for icdfa:

(icdfa@icdfa) [~]
└─$ sudo systemctl restart rsyslog
(icdfa@icdfa) [~]
└─$ sudo systemctl status rsyslog
● rsyslog.service - System Logging Service
    Loaded: loaded (/usr/lib/systemd/system/rsyslog.service; enabled; preset: enabled)
      Active: active (running) since Fri 2025-09-12 22:46:29 WAT; 16s ago
        Invocation: 998da4ca145348adaae7d67487a4e5e7
    TriggeredBy: ● syslog.socket
      Docs: man:rsyslogd(8)
             man:rsyslog.conf(5)
             https://www.rsyslog.com/doc/
     Main PID: 416182 (rsyslogd)
       Tasks: 4 (limit: 2207)
      Memory: 1.2M (peak: 2.4M)
         CPU: 62ms
      CGroup: /system.slice/rsyslog.service
              └─416182 /usr/sbin/rsyslogd -n -inone

Sep 12 22:46:29 icdfa systemd[1]: Starting rsyslog.service - System Logging Service ...
Sep 12 22:46:29 icdfa rsyslogd[416182]: imuxsock: Acquired UNIX socket '/run/systemd/journal/syslog' (fd 3) from system
Sep 12 22:46:29 icdfa systemd[1]: Started rsyslog.service - System Logging Service.
Sep 12 22:46:29 icdfa rsyslogd[416182]: [origin software="rsyslogd" swVersion="8.2506.0" x-pid="416182" x-info="https://www.rsyslog.com/doc/v8-stable/configuration/rsyslogd.html" x-time="2025-09-12T22:46:29+00:00"]
lines 1-19/19 (END)
```

Creating a security logging configuration and restarting rsyslog to apply changes.

```
(icdfa@icdfa) [~]
└─$ sudo tee /etc/rsyslog.d/security.conf > /dev/null << 'EOF'
# Log authentication messages to auth.log
auth,authpriv.*                                /var/log/auth.log

# Log kernel messages to kern.log
kern.*                                              /var/log/kern.log

# Create a dedicated security log file
if $programname == 'sudo' or $programname == 'su' or $programname == 'sshd' or $programname == 'firewalld' or $programname == 'fail2ban' then /var/log/security.log
& stop

# Remote logging (uncomment and configure for production use)
# *.* @logserver.example.com:514
EOF
[sudo] password for icdfa:

(icdfa@icdfa) [~]
└─$ sudo systemctl restart rsyslog
```

- Screenshots showing the configuration of auditd

### Install auditd

```
(icdfa@icdfa)[-]
$ sudo apt install -y auditd audisdp-plugins
The following packages were automatically installed and are no longer required:
libcaes1      libolecf1      python3-libcreg      python3-lbscca
libcreg1t64   libopenh264-7   python3-libesedb    python3-pefile
libdmn13      libscsa1t64    python3-libevtx     python3-pycaes
libevit1t64   libxnpack0     python3-libevtx     python3-pycparser
libevtx1t64   python3-astore  python3-libfswi    python3-zstd
libfws1t64    python3-cffi     python3-liblnk
libglapi-mesa python3-elasticsearch python3-lbmsiecf
libmsiecf1t64 python3-flor     python3-libolecf
Use 'sudo apt autoremove' to remove them.

Upgrading:
  libaudit-common libaudit1

Installing:
  audisdp-plugins auditd

Installing dependencies:
  libauparse0t64

Summary:
  Upgrading: 2, Installing: 3, Removing: 0, Not Upgrading: 1395
  Download size: 418 kB
  Space needed: 1,148 kB / 4,681 MB available

Get:1 http://kali.download/kali kali-rolling/main amd64 libaudit-common all 1:4.0.5-1 [13.
5 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 libaudit1 amd64 1:4.0.5-1 [59.4 kB]
]
Get:3 http://kali.download/kali kali-rolling/main amd64 libauparse0t64 amd64 1:4.0.5-1 [70
.1 kB]
Get:4 http://kali.download/kali kali-rolling/main amd64 auditd amd64 1:4.0.5-1 [225 kB]
Get:5 http://kali.download/kali kali-rolling/main amd64 audisdp-plugins amd64 1:4.0.5-1 [4
9.4 kB]
Fetched 418 kB in 5s (84.9 kB/s)
(Reading database ... 417824 files and directories currently installed.)
Preparing to unpack .../libaudit-common_1%3a4.0.5-1_all.deb ...
Unpacking libaudit-common (1:4.0.5-1) over (1:4.0.2-2) ...
Setting up libaudit-common (1:4.0.5-1) ...
(Reading database ... 417824 files and directories currently installed.)
Preparing to unpack .../libaudit1_1%3a4.0.5-1_amd64.deb ...
Unpacking libaudit1:amd64 (1:4.0.5-1) over (1:4.0.2-2+b1) ...
Setting up libaudit1:amd64 (1:4.0.5-1) ...
Selecting previously unselected package libauparse0t64:amd64.
(Reading database ... 417823 files and directories currently installed.)
Preparing to unpack .../libauparse0t64_1%3a4.0.5-1_amd64.deb ...
Adding 'diversion of /lib/x86_64-linux-gnu/libauparse.so.0 to /lib/x86_64-linux-gnu/libaup
arse.so.0.usr-is-merged by libauparse0t64'
Adding 'diversion of /lib/x86_64-linux-gnu/libauparse.so.0.0.0 to /lib/x86_64-linux-gnu/li
bauparse.so.0.0.0.usr-is-merged by libauparse0t64'
Unpacking libauparse0t64:amd64 (1:4.0.5-1) ...
Selecting previously unselected package auditd.
Preparing to unpack .../auditd_1%3a4.0.5-1_amd64.deb ...
Unpacking auditd (1:4.0.5-1) ...
Selecting previously unselected package audisdp-plugins.
Preparing to unpack .../audisdp-plugins_1%3a4.0.5-1_amd64.deb ...
Unpacking audisdp-plugins (1:4.0.5-1) ...
Setting up libauparse0t64:amd64 (1:4.0.5-1) ...
Setting up auditd (1:4.0.5-1) ...
update-rc.d: We have no instructions for the auditd init script.
update-rc.d: It looks like a non-network service, we enable it.
audit-rules.service is a disabled or a static unit, not starting it.
auditd.service is a disabled or a static unit, not starting it.
Setting up audisdp-plugins (1:4.0.5-1) ...
Processing triggers for libc-bin (2.41-6) ...
Processing triggers for man-db (2.13.0-1) ...
Processing triggers for kali-menu (2025.1.1) ...
```

Create a comprehensive audit configuration

```
(icdfa@icdfa)@[~]
$ >.....
-w /etc/security/opasswd -p wa -k identity

# Monitor system authentication
-w /etc/pam.d/ -p wa -k system-auth
-w /etc/nsswitch.conf -p wa -k system-auth
-w /etc/ssh/sshd_config -p wa -k system-auth

# Monitor system calls
-a always,exit -F arch=b64 -S execve -k exec
-a always,exit -F arch=b32 -S execve -k exec

# Monitor privileged commands
-a always,exit -F path=/usr/bin/sudo -F perm=x -k privileged
-a always,exit -F path=/usr/bin/su -F perm=x -k privileged
-a always,exit -F path=/usr/bin/passwd -F perm=x -k privileged
-a always,exit -F path=/usr/bin/chage -F perm=x -k privileged
-a always,exit -F path=/usr/bin/gpasswd -F perm=x -k privileged
-a always,exit -F path=/usr/bin/chsh -F perm=x -k privileged
-a always,exit -F path=/usr/bin/mount -F perm=x -k privileged
-a always,exit -F path=/usr/bin/umount -F perm=x -k privileged

# Monitor sensitive directories
-w /etc/ -p wa -k system-config
-w /var/log/ -p wa -k log-write
-w /usr/bin/ -p wa -k binary-modification
-w /usr/sbin/ -p wa -k binary-modification
-w /bin/ -p wa -k binary-modification
-w /sbin/ -p wa -k binary-modification

# Monitor unsuccessful events
-a always,exit -F arch=b64 -S open,openat,open_by_handle_at -F exit=-EACCES -k access
-a always,exit -F arch=b32 -S open,openat,open_by_handle_at -F exit=-EACCES -k access
-a always,exit -F arch=b64 -S open,openat,open_by_handle_at -F exit=-EPERM -k access
-a always,exit -F arch=b32 -S open,openat,open_by_handle_at -F exit=-EPERM -k access

# Make the configuration immutable - requires reboot to change
-e 2
EOF
```

Loading the new audit rules

```
(icdfa@icdfa)-[~]
└─$ sudo auditctl -R /etc/audit/rules.d/security-audit.rules

No rules
enabled 0
failure 1
pid 0
rate_limit 0
backlog_limit 8192
lost 0
backlog 0
backlog_wait_time 15000
backlog_wait_time_actual 0
enabled 0
failure 1
pid 0
rate_limit 0
backlog_limit 8192
lost 0
backlog 0
backlog_wait_time 15000
backlog_wait_time_actual 0
Old style watch rules are slower
perm used without an arch is slower
Old style watch rules are slower
enabled 2
failure 1
pid 0
rate_limit 0
backlog_limit 8192
lost 0
backlog 0
backlog_wait_time 15000
backlog_wait_time_actual 0
```

Enabling the audit service

```
(icdfa@icdfa)-[~]
└─$ sudo systemctl enable auditd
Synchronizing state of auditd.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable auditd
Created symlink '/etc/systemd/system/multi-user.target.wants/auditd.service' → '/usr/lib/systemd/system/auditd.service'.
```

starting the audit service

```
(icdfa@icdfa)-[~]
└─$ sudo systemctl restart auditd
```

```
(icdfa@icdfa)~]$ sudo auditctl -l
[sudo] password for icdfa:
-w /etc/passwd -p wa -k identity
-w /etc/group -p wa -k identity
-w /etc/shadow -p wa -k identity
-w /etc/gshadow -p wa -k identity
-w /etc/security/opasswd -p wa -k identity
-w /etc/pam.d -p wa -k system-auth
-w /etc/nsswitch.conf -p wa -k system-auth
-w /etc/ssh/sshd_config -p wa -k system-auth
-a always,exit -F arch=b64 -S execve -F key=exec
-a always,exit -F arch=b32 -S execve -F key=exec
-w /usr/bin/sudo -p x -k privileged
-w /usr/bin/su -p x -k privileged
-w /usr/bin/passwd -p x -k privileged
-w /usr/bin/chage -p x -k privileged
-w /usr/bin/gpasswd -p x -k privileged
-w /usr/bin/chsh -p x -k privileged
-w /usr/bin/mount -p x -k privileged
-w /usr/bin/umount -p x -k privileged
-w /etc -p wa -k system-config
-w /var/log -p wa -k log-write
-w /usr/bin -p wa -k binary-modification
-w /usr/sbin -p wa -k binary-modification
-w /bin -p wa -k binary-modification
-w /sbin -p wa -k binary-modification
-a always,exit -F arch=b64 -S open,openat,open_by_handle_at -F exit=-EACCES -F key=access
-a always,exit -F arch=b32 -S open,openat,open_by_handle_at -F exit=-EACCES -F key=access
-a always,exit -F arch=b64 -S open,openat,open_by_handle_at -F exit=-EPERM -F key=access
-a always,exit -F arch=b32 -S open,openat,open_by_handle_at -F exit=-EPERM -F key=access
```

Configuring log rotation to ensure logs are properly managed by creating a custom log rotation configuration for security logs

```
(icdfa@icdfa)~]$ sudo tee /etc/logrotate.d/security > /dev/null << 'EOF'
/var/log/auth.log
/var/log/kern.log
/var/log/security.log
/var/log/audit/audit.log {
    rotate 14
    daily
    missingok
   notifempty
    compress
    delaycompress
    sharedscripts
    postrotate
        /usr/lib/rsyslog/rsyslog-rotate
        systemctl restart audited >/dev/null 2>&1 || true
    endscript
    create 0640 root adm
}
EOF
$
```



- Screenshots showing the configuration of Fail2ban

#### Installing Fail2ban

```
(icdfa@icdfa)-[1]~$ sudo apt install -y fail2ban
The following packages were automatically installed and are no longer required:
  libcaes1   libglapi-mesa  python3-acstore  python3-libevt    python3-libscc
  libcreg1t64 libmsiecf1t64 python3-cffi     python3-libevtx  python3-pefile
  libdnnl3   libolecf1     python3-elasticsearch python3-libfws1  python3-pycaes
  libevtit64 libopenh264-7  python3-flor     python3-liblnk   python3-pycparser
  libevtx1t64 libssca1t64 python3-libcreg   python3-lombsiecf python3-zstd
  libfws1t64 libxnnpack0  python3-libesedb  python3-libolecf
Use 'sudo apt autoremove' to remove them.

Installing:
  fail2ban

Installing dependencies:
  python3-systemd

Suggested packages:
  monit ...

Summary:
  Upgrading: 0, Installing: 2, Removing: 0, Not Upgrading: 1395
  Download size: 507 kB
  Space needed: 2,461 kB / 4,676 MB available

Get:1 http://http.kali.org/kali kali-rolling/main amd64 python3-systemd amd64 235-1+b6 [40.8 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 fail2ban all 1.1.0-8 [466 kB]
Fetched 507 kB in 4s (123 kB/s)
Selecting previously unselected package python3-systemd.
(Reading database ... 417938 files and directories currently installed.)
Preparing to unpack .../python3-systemd_235-1+b6_amd64.deb ...
Unpacking python3-systemd (235-1+b6) ...
Selecting previously unselected package fail2ban.
Preparing to unpack .../fail2ban_1.1.0-8_all.deb ...
Unpacking fail2ban (1.1.0-8) ...
Setting up python3-systemd (235-1+b6) ...
Setting up fail2ban (1.1.0-8) ...
update-rc.d: We have no instructions for the fail2ban init script.
update-rc.d: It looks like a network service, we disable it.
fail2ban.service is a disabled or a static unit, not starting it.
Processing triggers for kali-menu (2025.1.1) ...
Processing triggers for man-db (2.13.0-1) ...
```

## Creating a custom Fail2ban configuration

```
[icdfa@icdfa]~$ sudo tee /etc/fail2ban/jail.local > /dev/null << 'EOF'
[DEFAULT]
# Ban hosts for 1 hour
bantime = 3600
# Check for new failed login attempts every 10 minutes
findtime = 600
# Ban after 5 failed login attempts
maxretry = 5
# Email to send notifications to (change to your email)
destemail = admin@example.com
# Email sender
sender = fail2ban@example.com
# Action to take when banning
action = %(action_mwl)s

[sshd]
enabled = true
port = ssh
filter = sshd
logpath = /var/log/auth.log

[sshd-ddos]
enabled = true
port = ssh
filter = sshd-ddos
logpath = /var/log/auth.log

[sudo]
enabled = true
filter = sudo
logpath = /var/log/auth.log
maxretry = 3
EOF

[icdfa@icdfa]~$ cat /etc/fail2ban/jail.local
[DEFAULT]
# Ban hosts for 1 hour
bantime = 3600
# Check for new failed login attempts every 10 minutes
findtime = 600
# Ban after 5 failed login attempts
maxretry = 5
# Email to send notifications to (change to your email)
destemail = admin@example.com
# Email sender
sender = fail2ban@example.com
# Action to take when banning
action = %(action_mwl)s

[sshd]
enabled = true
port = ssh
filter = sshd
logpath = /var/log/auth.log

[sshd-ddos]
enabled = true
port = ssh
filter = sshd-ddos
logpath = /var/log/auth.log

[sudo]
enabled = true
filter = sudo
logpath = /var/log/auth.log
maxretry = 3
```

## Enabling and starting Fail2ban

```
[icdfa@icdfa]~$ sudo systemctl enable fail2ban
Synchronizing state of fail2ban.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable fail2ban
Created symlink '/etc/systemd/system/multi-user.target.wants/fail2ban.service' → '/usr/lib/systemd/system/fail2ban.service'.

[icdfa@icdfa]~$ sudo systemctl restart fail2ban
```

```
(icdfa@icdfa) [~]
$ sudo systemctl status fail2ban
● fail2ban.service - Fail2Ban Service
  Loaded: loaded (/usr/lib/systemd/system/fail2ban.service; enabled; preset: disabled)
  Active: active (running) since Fri 2025-09-12 18:56:50 WAT; 4h 25min ago
    Invocation: 029a4cb2cf864dcba7f52de9ea530543
      Docs: man:fail2ban(1)
    Main PID: 15837 (fail2ban-server)
      Tasks: 5 (limit: 2207)
        Memory: 13.4M (peak: 28.1M, swap: 1.5M, swap peak: 1.5M)
          CPU: 11.124s
        CGroup: /system.slice/fail2ban.service
                └─15837 /usr/bin/python3 /usr/bin/fail2ban-server -xf start

Sep 12 18:56:50 icdfa systemd[1]: Started fail2ban.service - Fail2Ban Service.
Sep 12 18:56:50 icdfa fail2ban-server[15837]: 2025-09-12 18:56:50,534 fail2ban.configreader [15837]: ERROR Found >
Sep 12 18:56:50 icdfa fail2ban-server[15837]: 2025-09-12 18:56:50,534 fail2ban.jailreader [15837]: ERROR Unable >
Sep 12 18:56:50 icdfa fail2ban-server[15837]: 2025-09-12 18:56:50,534 fail2ban.jailsreader [15837]: ERROR Errors >
Sep 12 18:56:50 icdfa fail2ban-server[15837]: 2025-09-12 18:56:50,534 fail2ban.configreader [15837]: ERROR Found >
Sep 12 18:56:50 icdfa fail2ban-server[15837]: 2025-09-12 18:56:50,534 fail2ban.jailreader [15837]: ERROR Unable >
Sep 12 18:56:50 icdfa fail2ban-server[15837]: 2025-09-12 18:56:50,534 fail2ban.jailsreader [15837]: ERROR Errors >
Sep 12 18:56:50 icdfa fail2ban-server[15837]: Server ready
```

### Verifying status

```
(icdfa@icdfa) [~]
$ sudo fail2ban-client status sshd
Status for the jail: sshd
└─ Filter
  |  └─ Currently failed: 0
  |  └─ Total failed: 0
  |  └─ Journal matches: _SYSTEMD_UNIT=sshd.service + _COMM=sshd
└─ Actions
  |  └─ Currently banned: 0
  |  └─ Total banned: 0
  |  └─ Banned IP list:
```

### Creating a script to test the logging and auditing configuration

```
(icdfa@icdfa) [~]
$ cat > test_logging.sh << 'EOF'
#!/bin/bash
VMware
echo "Testing security logging and auditing configuration ..."

# Test authentication logging
echo "Testing failed login attempt ... "
ssh -o BatchMode=yes -o ConnectTimeout=5 nonexistentuser@localhost 2>/dev/null || true

# Test sudo logging
echo "Testing sudo command execution ... "
sudo ls -la /root

# Test file access monitoring
echo "Testing file access monitoring ... "
sudo touch /etc/test_audit_file
sudo rm /etc/test_audit_file

# Test unsuccessful access
echo "Testing unsuccessful access ... "
cat /etc/shadow 2>/dev/null || true

echo "Tests completed. Check logs for results."
EOF

(icdfa@icdfa) [~]
$ chmod +x test_logging.sh
```

- Output from the test script showing the logging and auditing in action  
Running the test script

```
(icdfa@icdfa)-[~]
$ ./test_logging.sh
Testing security logging and auditing configuration ...
Testing failed login attempt ...
Testing sudo command execution ...
total 96
drwx----- 10 root root 4096 May 11 13:41 .
drwxr-xr-x 19 root root 4096 May 11 00:03 ..
-rw-r--r-- 1 root root 5551 May 10 19:53 .bashrc
-rw-r--r-- 1 root root 607 May 10 19:53 .bashrc.original
drwx----- 7 root root 4096 May 11 05:07 .cache
drwx----- 6 root root 4096 May 11 06:41 .config
drwx----- 3 root root 4096 May 10 21:18 .dbus
-rw-r--r-- 1 root root 11656 May 10 20:11 .face
lrwxrwxrwx 1 root root 11 May 10 20:11 .face.icon → /root/.face
drwx----- 2 root root 4096 May 10 21:18 .gvfs
-rw-r--r-- 1 root root 1598 May 11 05:47 installation-report.txt
drwxr-xr-x 4 root root 4096 May 11 05:47 lab
drwxrwxr-x 3 root root 4096 May 10 21:18 .local
drwxr-xr-x 4 root root 4096 May 11 05:39 .npm
-rw-r--r-- 1 root root 132 Feb 17 2025 .profile
drwx----- 2 root root 4096 May 10 19:11 .ssh
-rw-r----- 1 root root 4 May 11 13:41 .vboxclient-display-svga-x11-tty1-control.pid
-rw-r--r-- 1 root root 210 May 11 11:16 .wget-hsts
-rw----- 1 root root 357 May 11 06:42 .zsh_history
-rw-r--r-- 1 root root 10988 May 11 05:47 .zshrc
Testing file access monitoring ...
Testing unsuccessful access ...
Tests completed. Check logs for results.

(icdfa@icdfa)-[~]
$ sleep 5
```

Collecting the results

```
(icdfa@icdfa)~]$ echo "Authentication log entries:"  
Authentication log entries:  
  
(icdfa@icdfa)~]$ sudo grep -i "nonexistentuser\|sshd" /var/log/auth.log | tail -10  
2025-09-12T19:03:52.756752+01:00 icdfa sudo:    icdfa : TTY=pts/0 ; PWD=/home/icdfa ; USER=root ; COMMAND=/usr/bin/grep -i nonexistentuser\\|sshd /var/log/auth.log  
  
(icdfa@icdfa)~]$ echo "Sudo log entries:"  
Sudo log entries:  
  
(icdfa@icdfa)~]$ sudo grep -i "sudo" /var/log/auth.log | tail -10  
2025-09-12T19:01:28.935231+01:00 icdfa sudo: pam_unix(sudo:session): session opened for user root(uid=0) by icdfa(uid=1000)  
2025-09-12T19:01:28.946549+01:00 icdfa sudo: pam_unix(sudo:session): session closed for user root  
2025-09-12T19:01:28.961947+01:00 icdfa sudo:    icdfa : TTY=pts/0 ; PWD=/home/icdfa ; USER=root ; COMMAND=/usr/bin/rm /etc/test_audit_file  
2025-09-12T19:01:28.963155+01:00 icdfa sudo: pam_unix(sudo:session): session opened for user root(uid=0) by icdfa(uid=1000)  
2025-09-12T19:01:28.967976+01:00 icdfa sudo: pam_unix(sudo:session): session closed for user root  
2025-09-12T19:03:52.756752+01:00 icdfa sudo:    icdfa : TTY=pts/0 ; PWD=/home/icdfa ; USER=root ; COMMAND=/usr/bin/grep -i nonexistentuser\\|sshd /var/log/auth.log  
2025-09-12T19:03:52.758480+01:00 icdfa sudo: pam_unix(sudo:session): session opened for user root(uid=0) by icdfa(uid=1000)  
2025-09-12T19:03:52.764592+01:00 icdfa sudo: pam_unix(sudo:session): session closed for user root  
2025-09-12T19:04:22.511148+01:00 icdfa sudo:    icdfa : TTY=pts/0 ; PWD=/home/icdfa ; USER=root ; COMMAND=/usr/bin/grep -i sudo /var/log/auth.log  
2025-09-12T19:04:22.513539+01:00 icdfa sudo: pam_unix(sudo:session): session opened for user root(uid=0) by icdfa(uid=1000)  
  
(icdfa@icdfa)~]$ echo "Audit log entries:"  
Audit log entries:  
  
(icdfa@icdfa)~]$ sudo ausearch -ts today -k identity 2>/dev/null  
  
(icdfa@icdfa)~]$ sudo ausearch -ts today -k access 2>/dev/null
```

```
(icdfa@icdfa)@[~]
$ sudo ausearch -ts today -k access 2>/dev/null

time→Fri Sep 12 18:51:12 2025
type=PROCTITLE msg=audit(1757699472.207:5308): proctitle=73657470726976002D2D7265756964006D6
16E002D2D7265676964006D616E002D2D696E69742D67726F757073002D2D002F7573722F62696E2F6D616E64620
02D7071
type=PATH msg=audit(1757699472.207:5308): item=0 name="/root/.manpath" nametype=UNKNOWN cap_
fp=0 cap_fi=0 cap_fver=0 cap_frootid=0
type=CWD msg=audit(1757699472.207:5308): cwd="/"
type=SYSCALL msg=audit(1757699472.207:5308): arch=c000003e syscall=257 success=no exit=-13 a
0=fffffffffffff9c a1=5567f851c500 a2=0 a3=0 items=1 ppid=12896 pid=12897 auid=1000 uid=6 gi
d=12 euid=6 suid=6 egid=12 sgid=12 fsgid=12 tty=pts2 ses=2 comm="mandb" exe="/usr/bi
n/mandb" subj=unconfined key="access"

time→Fri Sep 12 18:58:36 2025
type=PROCTITLE msg=audit(1757699916.267:8130): proctitle=2F7573722F6C6962657865632F6C6F63616
C7365617263682D657874726163746F722D33002D2D736F636B65742D66640033
type=PATH msg=audit(1757699916.267:8130): item=0 name="/etc/ld.so.cache" inode=1107594 dev=0
8:01 mode=0100644 ouid=0 ogid=0 rdev=00:00 nametype=NORMAL cap_fp=0 cap_fi=0 cap_fe=0 cap_fv
er=0 cap_frootid=0
type=CWD msg=audit(1757699916.267:8130): cwd="/home/icdfa"
type=SYSCALL msg=audit(1757699916.267:8130): arch=c000003e syscall=257 success=no exit=-13 a
0=fffffff9c a1=7f121197921c a2=80000 a3=0 items=1 ppid=1233 pid=16710 auid=1000 uid=1000 gid=
1000 euid=1000 suid=1000 egid=1000 sgid=1000 fsgid=1000 tty=(none) ses=2 comm="lo
calsearch-ext" exe="/usr/libexec/localsearch-extractor-3" subj=unconfined key="access"

time→Fri Sep 12 18:58:36 2025
type=PROCTITLE msg=audit(1757699916.271:8131): proctitle=2F7573722F6C6962657865632F6C6F63616
C7365617263682D657874726163746F722D33002D2D736F636B65742D66640033
type=PATH msg=audit(1757699916.271:8131): item=0 name="/proc/filesystems" inode=4026532069 d
ev=00:17 mode=0100444 ouid=0 ogid=0 rdev=00:00 nametype=NORMAL cap_fp=0 cap_fi=0 cap_fe=0 ca
p_fver=0 cap_frootid=0
type=CWD msg=audit(1757699916.271:8131): cwd="/home/icdfa"
type=SYSCALL msg=audit(1757699916.271:8131): arch=c000003e syscall=257 success=no exit=-13 a
0=fffffffffffff9c a1=7f12109f1904 a2=80000 a3=0 items=1 ppid=1233 pid=16710 auid=1000 uid=1
000 gid=1000 euid=1000 suid=1000 egid=1000 sgid=1000 fsgid=1000 tty=(none) ses=2
comm="localsearch-ext" exe="/usr/libexec/localsearch-extractor-3" subj=unconfined key="acces
s"

time→Fri Sep 12 18:58:36 2025
type=PROCTITLE msg=audit(1757699916.283:8132): proctitle=2F7573722F6C6962657865632F6C6F63616
C7365617263682D657874726163746F722D33002D2D736F636B65742D66640033
type=PATH msg=audit(1757699916.283:8132): item=0 name="/usr/share/locale/locale.alias" inode
=1046639 dev=08:01 mode=0100644 ouid=0 ogid=0 rdev=00:00 nametype=NORMAL cap_fp=0 cap_fi=0 c
ap_fe=0 cap_fver=0 cap_frootid=0
type=CWD msg=audit(1757699916.283:8132): cwd="/home/icdfa"
```

```
type=SYSCALL msg=audit(1757699916.367:8133): arch=c000003e syscall=257 success=no exit=-13 a0=fffffffffffff9c a1=7f1210a5c855 a2=80000 a3=0 items=1 ppid=1233 pid=16710 auid=1000 uid=1000 gid=1000 euid=1000 suid=1000 fsuid=1000 egid=1000 sgid=1000 fsgid=1000 tty=(none) ses=2 comm="localsearch-ext" exe="/usr/libexec/localsearch-extractor-3" subj=unconfined key="access"
time→Fri Sep 12 18:58:36 2025
type=PROCTITLE msg=audit(1757699916.371:8134): proctitle=2F7573722F6C6962657865632F6C6F63616C7365617263682D657874726163746F722D33002D2D736F636B65742D66640033
type=PATH msg=audit(1757699916.371:8134): item=0 name="/etc/nsswitch.conf" inode=1104645 dev=08:01 mode=0100644 ouid=0 ogid=0 rdev=00:00 nametype=NORMAL cap_fp=0 cap_hi=0 cap_fe=0 cap_fver=0 cap_frootid=0
type=CWD msg=audit(1757699916.371:8134): cwd="/home/icdfa"
type=SYSCALL msg=audit(1757699916.371:8134): arch=c000003e syscall=257 success=no exit=-13 a0=ffffff9c a1=7f12113ee7f1 a2=80000 a3=0 items=1 ppid=1233 pid=16710 auid=1000 uid=1000 gid=1000 euid=1000 suid=1000 fsuid=1000 egid=1000 sgid=1000 fsgid=1000 tty=(none) ses=2 comm="localsearch-ext" exe="/usr/libexec/localsearch-extractor-3" subj=unconfined key="access"
time→Fri Sep 12 18:58:55 2025
type=PROCTITLE msg=audit(1757699935.323:8251): proctitle=2F7573722F6C6962657865632F6C6F63616C7365617263682D657874726163746F722D33002D2D736F636B65742D66640033
type=PATH msg=audit(1757699935.323:8251): item=0 name="/etc/ld.so.cache" inode=1107594 dev=08:01 mode=0100644 ouid=0 ogid=0 rdev=00:00 nametype=NORMAL cap_fp=0 cap_hi=0 cap_fe=0 cap_fver=0 cap_frootid=0
type=CWD msg=audit(1757699935.323:8251): cwd="/home/icdfa"
type=SYSCALL msg=audit(1757699935.323:8251): arch=c000003e syscall=257 success=no exit=-13 a0=ffffff9c a1=7f2cb17a221c a2=80000 a3=0 items=1 ppid=1233 pid=16872 auid=1000 uid=1000 gid=1000 euid=1000 suid=1000 fsuid=1000 egid=1000 sgid=1000 fsgid=1000 tty=(none) ses=2 comm="localsearch-ext" exe="/usr/libexec/localsearch-extractor-3" subj=unconfined key="access"
time→Fri Sep 12 18:58:55 2025
type=PROCTITLE msg=audit(1757699935.331:8252): proctitle=2F7573722F6C6962657865632F6C6F63616C7365617263682D657874726163746F722D33002D2D736F636B65742D66640033
type=PATH msg=audit(1757699935.331:8252): item=0 name="/proc/filesystems" inode=4026532069 dev=00:17 mode=0100444 ouid=0 ogid=0 rdev=00:00 nametype=NORMAL cap_fp=0 cap_hi=0 cap_fe=0 cap_fver=0 cap_frootid=0
type=CWD msg=audit(1757699935.331:8252): cwd="/home/icdfa"
type=SYSCALL msg=audit(1757699935.331:8252): arch=c000003e syscall=257 success=no exit=-13 a0=fffffffffffff9c a1=7f2cb0fd4904 a2=80000 a3=0 items=1 ppid=1233 pid=16872 auid=1000 uid=1000 gid=1000 euid=1000 suid=1000 fsuid=1000 egid=1000 sgid=1000 fsgid=1000 tty=(none) ses=2 comm="localsearch-ext" exe="/usr/libexec/localsearch-extractor-3" subj=unconfined key="access"
```

```

time→Fri Sep 12 18:58:55 2025
type=PROCTITLE msg=audit(1757699935.331:8253): proctitle=2F7573722F6C6962657865632F6C6F63616
C7365617263682D657874726163746F722D33002D2D736F636B65742D66640033
type=PATH msg=audit(1757699935.331:8253): item=0 name="/usr/share/locale/locale.alias" inode
=1046639 dev=08:01 mode=0100644 uid=0 ogid=0 rdev=00:00 nametype=NORMAL cap_fp=0 cap_fi=0 c
ap_fe=0 cap_fver=0 cap_frootid=0
type=CWD msg=audit(1757699935.331:8253): cwd="/home/icdfa"
type=SYSCALL msg=audit(1757699935.331:8253): arch=c000003e syscall=257 success=no exit=-13 a
0=ffffffff9c a1=7fffe8311b80 a2=80000 a3=0 items=1 ppid=1233 pid=16872 auid=1000 uid=1000 gid=
1000 euid=1000 suid=1000 fsuid=1000 egid=1000 sgid=1000 fsgid=1000 tty=(none) ses=2 comm="lo
calsearch-ext" exe="/usr/libexec/localsearch-extractor-3" subj=unconfined key="access"
_____
time→Fri Sep 12 18:58:55 2025
type=PROCTITLE msg=audit(1757699935.407:8254): proctitle=2F7573722F6C6962657865632F6C6F63616
C7365617263682D657874726163746F722D33002D2D736F636B65742D66640033
type=PATH msg=audit(1757699935.407:8254): item=0 name="/etc/fstab" inode=1046531 dev=08:01 m
ode=0100644 uid=0 ogid=0 rdev=00:00 nametype=NORMAL cap_fp=0 cap_fi=0 cap_fe=0 cap_fver=0 c
ap_frootid=0
type=CWD msg=audit(1757699935.407:8254): cwd="/home/icdfa"
type=SYSCALL msg=audit(1757699935.407:8254): arch=c000003e syscall=257 success=no exit=-13 a
0=ffffffffffff9c a1=7f2cb085c855 a2=80000 a3=0 items=1 ppid=1233 pid=16872 auid=1000 uid=1
000 gid=1000 euid=1000 suid=1000 fsuid=1000 egid=1000 sgid=1000 fsgid=1000 tty=(none) ses=2
comm="localsearch-ext" exe="/usr/libexec/localsearch-extractor-3" subj=unconfined key="acces
s"
_____
time→Fri Sep 12 18:58:55 2025
type=PROCTITLE msg=audit(1757699935.411:8255): proctitle=2F7573722F6C6962657865632F6C6F63616
C7365617263682D657874726163746F722D33002D2D736F636B65742D66640033
type=PATH msg=audit(1757699935.411:8255): item=0 name="/etc/nsswitch.conf" inode=1104645 dev
=08:01 mode=0100644 uid=0 ogid=0 rdev=00:00 nametype=NORMAL cap_fp=0 cap_fi=0 cap_fe=0 cap_
fver=0 cap_frootid=0
type=CWD msg=audit(1757699935.411:8255): cwd="/home/icdfa"
type=SYSCALL msg=audit(1757699935.411:8255): arch=c000003e syscall=257 success=no exit=-13 a
0=ffffffffffff9c a1=7f2cb12177f1 a2=80000 a3=0 items=1 ppid=1233 pid=16872 auid=1000 uid=1000
gid=1000 euid=1000 suid=1000 fsuid=1000 egid=1000 sgid=1000 fsgid=1000 tty=(none) ses=2 comm=
"localsearch-ext" exe="/usr/libexec/localsearch-extractor-3" subj=unconfined key="access"
_____
time→Fri Sep 12 19:01:28 2025
type=PROCTITLE msg=audit(1757700088.967:9260): proctitle=636174002F6574632F736861646F77
type=PATH msg=audit(1757700088.967:9260): item=0 name="/etc/shadow" inode=1046852 dev=08:01
mode=0100640 uid=0 ogid=42 rdev=00:00 nametype=NORMAL cap_fp=0 cap_fi=0 cap_fe=0 cap_fver=0
cap_frootid=0
type=CWD msg=audit(1757700088.967:9260): cwd="/home/icdfa"
type=SYSCALL msg=audit(1757700088.967:9260): arch=c000003e syscall=257 success=no exit=-13 a
0=ffffffffffff9c a1=7ffd736f4207 a2=0 a3=0 items=1 ppid=18233 pid=18247 auid=1000 uid=1000
gid=1000 euid=1000 suid=1000 fsuid=1000 egid=1000 sgid=1000 fsgid=1000 tty=pts0 ses=2 comm=
"cat" exe="/usr/bin/cat" subj=unconfined key="access"
_____
[icdfa@icdfa:~]
$ sudo ausearch -ts today -k privileged 2>/dev/null

[icdfa@icdfa:~]
$ echo "Fail2ban log entries:"
Fail2ban log entries:

[icdfa@icdfa:~]
$ sudo grep -i "fail2ban" /var/log/syslog | tail -10
2025-09-12T18:56:50.298528+01:00 icdfa systemd[1]: Started fail2ban.service - Fail2Ban Servi
ce.
2025-09-12T18:56:50.537040+01:00 icdfa fail2ban-server[15837]: 2025-09-12 18:56:50,534 fail2
ban.configreader [15837]: ERROR Found no accessible config files for 'filter.d/sshd-ddos'
under /etc/fail2ban
2025-09-12T18:56:50.537189+01:00 icdfa fail2ban-server[15837]: 2025-09-12 18:56:50,534 fail2
ban.jailreader [15837]: ERROR Unable to read the filter 'sshd-ddos'
2025-09-12T18:56:50.537217+01:00 icdfa fail2ban-server[15837]: 2025-09-12 18:56:50,534 fail2
ban.jailsreader [15837]: ERROR Errors in jail 'sshd-ddos'. Skipping ...
2025-09-12T18:56:50.537241+01:00 icdfa fail2ban-server[15837]: 2025-09-12 18:56:50,534 fail2
ban.configreader [15837]: ERROR Found no accessible config files for 'filter.d/sudo' und
er /etc/fail2ban
2025-09-12T18:56:50.537265+01:00 icdfa fail2ban-server[15837]: 2025-09-12 18:56:50,534 fail2
ban.jailreader [15837]: ERROR Unable to read the filter 'sudo'
2025-09-12T18:56:50.537289+01:00 icdfa fail2ban-server[15837]: 2025-09-12 18:56:50,534 fail2
ban.jailsreader [15837]: ERROR Errors in jail 'sudo'. Skipping ...
2025-09-12T18:56:50.615090+01:00 icdfa fail2ban-server[15837]: Server ready

```

- These logging and auditing mechanisms are often used to support security governance through insight provision of the current state of the system, which in turn supports the security frameworks that are built to support security governance.

## Part 2: Implementing Security Monitoring Tools

### Deliverables:

- Screenshots showing the installation and configuration of AIDE  
Installing AIDE

```
(icdfa@icdfa)-[~]
$ sudo apt install -y aide
[sudo] password for icdfa:
The following packages were automatically installed and are no longer required:
  libcaes1   libglapi-mesa  python3-acstore  python3-libevt    python3-lbscca
  libcreg1t64 libmsiecf1t64  python3-cffi     python3-libevtx    python3-pefile
  libdnnl3    libolecf1     python3-elasticsearch  python3-libfwsi    python3-pycaes
  libevt1t64  libopenh264-7  python3-flor      python3-liblnk     python3-pycparser
  libevtx1t64 libscca1t64  python3-libcreg    python3-libsiecf  python3-zstd
  libfws1lt64 libxnnpack0   python3-libesedb   python3-libolecf
Use 'sudo apt autoremove' to remove them.

Installing:
  aide

Installing dependencies:
  aide-common

Summary:
  Upgrading: 0, Installing: 2, Removing: 0, Not Upgrading: 1395
  Download size: 277 kB
  Space needed: 891 kB / 4,651 MB available

Get:1 http://kali.download/kali kali-rolling/main amd64 aide amd64 0.19.2-2 [156 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 aide-common all 0.19.2-2 [121 kB]
Fetched 277 kB in 4s (70.0 kB/s)
Preconfiguring packages ...
Selecting previously unselected package aide.
(Reading database ... 418427 files and directories currently installed.)
Preparing to unpack .../aide_0.19.2-2_amd64.deb ...
Unpacking aide (0.19.2-2) ...
Selecting previously unselected package aide-common.
Preparing to unpack .../aide-common_0.19.2-2_all.deb ...
Unpacking aide-common (0.19.2-2) ...
Setting up aide (0.19.2-2) ...
Setting up aide-common (0.19.2-2) ...
Creating config file /etc/cron.daily/dailyaidecheck with new version
Creating config file /etc/aide/aide.conf with new version
Creating config file /etc/aide/aide.conf.d/21_aide_spamassassin with new version
Creating config file /etc/aide/aide.conf.d/31_aide_bandwidthd with new version
Creating config file /etc/aide/aide.conf.d/31_aide_hapsd with new version
Creating config file /etc/aide/aide.conf.d/70_aide_run with new version
Creating config file /etc/aide/aide.conf.d/31_aide_screen with new version
Creating config file /etc/aide/aide.conf.d/31_aide_fake-hwclock with new version
Creating config file /etc/aide/aide.conf.d/31_aide_tt-rss with new version
Creating config file /etc/aide/aide.conf.d/31_aide_trac with new version
Creating config file /etc/aide/aide.conf.d/31_aide_dcc-common with new version
```

```

Creating config file /etc/aide/aide.conf.d/31_aide_inn2 with new version
Creating config file /etc/aide/aide.conf.d/31_aide_run_systemd_netif with new version
Creating config file /etc/aide/aide.conf.d/31_aide_postfix with new version
Creating config file /etc/aide/aide.conf.d/31_aide_valkey with new version
Creating config file /etc/aide/aide.conf.d/31_aide_dbus with new version
Creating config file /etc/aide/aide.conf.d/31_aide_udev with new version
Creating config file /etc/aide/aide.conf.d/31_aide_pam_motd with new version
Creating config file /etc/aide/aide.conf.d/31_aide_php-fpm with new version
Creating config file /etc/aide/aide.conf.d/31_aide_anubis with new version
Creating config file /etc/aide/aide.conf.d/31_aide_tiger with new version
Creating config file /etc/aide/aide.conf.d/31_aide_console-setup with new version
Creating config file /etc/aide/aide.conf.d/31_aide_vsftpd with new version
Creating config file /etc/aide/aide.conf.d/31_aide_apache2 with new version
Creating config file /etc/aide/aide.conf.d/31_aide_fwupd with new version
Creating config file /etc/aide/aide.conf.d/31_aide_dlocate with new version
Creating config file /etc/aide/aide.conf.d/31_aide_amanda-client with new version
Creating config file /etc/aide/aide.conf.d/31_aide_mysql-server with new version
Creating config file /etc/aide/aide.conf.d/31_aide_uuidd-runtime with new version
Creating config file /etc/aide/aide.conf.d/31_aide_man with new version
Creating config file /etc/aide/aide.conf.d/31_aide_locales with new version
Creating config file /etc/aide/aide.conf.d/10_aide_bits with new version
Creating config file /etc/aide/aide.conf.d/31_aide_xe-guest-utilities with new version
Creating config file /etc/aide/aide.conf.d/31_aide_proftpd with new version
Creating config file /etc/aide/aide.conf.d/31_aide_amanda-server with new version
Creating config file /etc/aide/aide.conf.d/31_aide_logcheck with new version
Creating config file /etc/aide/aide.conf.d/31_aide_unbound with new version
Creating config file /etc/aide/aide.conf.d/31_aide_apt-cacher-ng with new version
Creating config file /etc/aide/aide.conf.d/31_aide_gnupg with new version
Creating config file /etc/aide/aide.conf.d/31_aide_dmeventd with new version
Creating config file /etc/aide/aide.conf.d/31_aide_mlocate with new version
Creating config file /etc/aide/aide.conf.d/70_aide_var with new version
Creating config file /etc/aide/aide.conf.d/31_aide_systemd-networkd with new version
Creating config file /etc/aide/aide.conf.d/31_aide_privoxy with new version
Creating config file /etc/aide/aide.conf.d/31_aide_util-linux with new version
Creating config file /etc/aide/aide.conf.d/31_aide_libapache2-mod-fastcgi with new version
Creating config file /etc/aide/aide.conf.d/31_aide_snmpd with new version
Creating config file /etc/aide/aide.conf.d/31_aide_cron-apt with new version
Creating config file /etc/aide/aide.settings.d/31_aide_trac_settings with new version
Creating config file /etc/aide/aide.settings.d/10_aide_sourceslist with new version
Creating config file /etc/aide/aide.settings.d/31_aide_svn-server_settings with new version
Creating config file /etc/aide/aide.settings.d/31_aide_apt_settings with new version
Creating config file /etc/aide/aide.settings.d/31_aide_torrus_settings with new version
Creating config file /etc/default/aide with new version
Creating group '_aide' with GID 990.

Creating user '_aide' (Advanced Intrusion Detection Environment) with UID 990 and GID 990.
Created symlink '/etc/systemd/system/timers.target.wants/dailyaidecheck.timer' → '/usr/lib/systemd/system/dailyaidecheck.timer'.
dailyaidecheck.service is a disabled or a static unit, not starting it.
dailyaidecheck-buildcache.service is a disabled or a static unit, not starting it.
dailyaidecheck-buildcache.service is a disabled or a static unit, not starting it.
dailyaidecheck.service is a disabled or a static unit, not starting it.
Processing triggers for man-db (2.13.0-1) ...
Processing triggers for kali-menu (2025.1.1) ...

```

```

└─(icdfa@icdfa)-[~]
$ █

```

Creating a custom AIDE configuration

```

└─(icdfa@icdfa)-[~]
$ sudo tee /etc/aide/aide.conf.d/90_custom.conf > /dev/null << 'EOF'
# Define custom rules
Binaries = p+i+n+u+g+s+b+m+c+sha1+sha256+rmd160
Logs = p+i+n+u+g+S
ConfigFiles = p+i+n+u+g+s+b+m+c+sha1+sha256+rmd160

# Monitor specific directories
/bin Binaries
/sbin Binaries
/usr/bin Binaries
/usr/sbin Binaries
/etc ConfigFiles
/var/log Logs
EOF

```

Initializing the AIDE database, moving the new database into place, and creating a daily check script

```
(icdfa@icdfa)~$ sudo aideinit
Running aide --init ...

(icdfa@icdfa)~$ sudo mv /var/lib/aide/aide.db.new /var/lib/aide/aide.db
(icdfa@icdfa)~$ sudo tee /etc/cron.daily/aide-check > /dev/null << 'EOF'
#!/bin/sh

# Run AIDE check and save results
/usr/bin/aide.wrapper --check > /var/log/aide/aide-check-$(date +%Y%m%d).log
# Send email notification if changes detected
if [ $? -ne 0 ]; then
    echo "AIDE detected changes on $(hostname) on $(date)" | mail -s "AIDE Integrity Check - Changes Detected" root
fi
EOF

(icdfa@icdfa)~$ sudo chmod +x /etc/cron.daily/aide-check
(icdfa@icdfa)~$ sudo mkdir -p /var/log/aide
(icdfa@icdfa)~$
```

- Screenshots showing the installation and configuration of Lynis

Installing Lynis

```
(icdfa@icdfa)~$ sudo apt install -y lynis
[sudo] password for icdfa:
lynis is already the newest version (3.1.4-1).
The following packages were automatically installed and are no longer required:
  libcaes1   libglapi-mesa  python3-acstore      python3-libevt      python3-lbscca
  libcreg1t64 libmsiecf1t64  python3-cffi       python3-libevtx      python3-pefile
  libdnnl3    libolecf1     python3-elasticsearch python3-libfws1      python3-pycaes
  libevtit64  libopenh264-7   python3-flor      python3-liblnk      python3-pyparser
  libevtx1t64 libscca1t64   python3-libcreg     python3-lbmsiecf   python3-zstd
  libfws1t64  libxnnpack0   python3-libesedb    python3-libolecf
Use 'sudo apt autoremove' to remove them.

Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 1395
```

## Running a system audit

```
(icdfa@icdfa)-[~]
$ sudo lynis audit system --quick
[ Lynis 3.1.4 ]

#####
Lynis comes with ABSOLUTELY NO WARRANTY. This is free software, and you are
welcome to redistribute it under the terms of the GNU General Public License.
See the LICENSE file for details about using this software.

2007-2024, CISOfy - https://cisofty.com/lynis/
Enterprise support available (compliance, plugins, interface and tools)
#####

[+] Initializing program
-----
- Detecting OS ... [ DONE ]
- Checking profiles ... [ DONE ]

-----
Program version: 3.1.4
Operating system: Linux
Operating system name: Kali Linux
Operating system version: Rolling release
Kernel version: 6.12.13
Hardware platform: x86_64
Hostname: icdfa

-----
Profiles: /etc/lynis/default.prf
Log file: /var/log/lynis.log
Report file: /var/log/lynis-report.dat
Report version: 1.0
Plugin directory: /etc/lynis/plugins

-----
Auditor: [Not Specified]
Language: en
Test category: all
Test group: all

-----
- Program update status ... [ NO UPDATE ]
```

- Show details of a test (lynis show details TEST-ID)
- Check the logfile for all details (less /var/log/lynis.log)
- Read security controls texts (<https://ciscofy.com>)
- Use --upload to upload data to central system (Lynis Enterprise users)

---

File Sy...

**Lynis security scan details:**

Hardening index : 67 [ ##### ]  
Tests performed : 277  
Plugins enabled : 1

**Components:**

- Firewall [V]
- Malware scanner [V]

**Scan mode:**

Normal [V] Forensics [ ] Integration [ ] Pentest [ ]

**Lynis modules:**

- Compliance status [?]
- Security audit [V]
- Vulnerability scan [V]

**Files:**

- Test and debug information : /var/log/lynis.log
- Report data : /var/log/lynis-report.dat

---

**Lynis 3.1.4**

Auditing, system hardening, and compliance for UNIX-based systems  
(Linux, macOS, BSD, and others)

2007-2024, CISOfy - <https://ciscofy.com/lynis/>  
**Enterprise support available (compliance, plugins, interface and tools)**

---

[TIP]: Enhance Lynis audits by adding your settings to custom.prf (see /etc/lynis/default.prf for all settings)

Saving the audit results

```
(icdfa@icdfa)-[~]
$ sudo lynis audit system --quick --report-file /var/log/lynis-audit.log

[sudo] password for icdfa:
Sorry, try again.
[sudo] password for icdfa:

[ Lynis 3.1.4 ]

#####
Lynis comes with ABSOLUTELY NO WARRANTY. This is free software, and
you are
welcome to redistribute it under the terms of the GNU General Publi
c License.
See the LICENSE file for details about using this software.

2007-2024, CISOfy - https://cisofy.com/lynis/
Enterprise support available (compliance, plugins, interface and to
ols)
#####

[+] Initializing program
-----
- Detecting OS ... [ DONE]
] - Checking profiles ... [ DONE]

-----
Program version: 3.1.4
Operating system: Linux
Operating system name: Kali Linux
Operating system version: Rolling release
Kernel version: 6.12.13
Hardware platform: x86_64
Hostname: icdfa

-----
Profiles: /etc/lynis/default.prf
Log file: /var/log/lynis.log
Report file: /var/log/lynis-audit.log
Report version: 1.0
Plugin directory: /etc/lynis/plugins
```

---

---

**Lynis security scan details:**

Hardening index : 67 [#####] Tests performed : 277 Plugins enabled : 1

**Components:**

- Firewall [V]
- Malware scanner [V]

**Scan mode:**

Normal [V] Forensics [ ] Integration [ ] Pentest [ ]

**Lynis modules:**

- Compliance status [?]
- Security audit [V]
- Vulnerability scan [V]

**Files:**

- Test and debug information : /var/log/lynis.log
  - Report data : /var/log/lynis-audit.log
- 

**Lynis 3.1.4**

Auditing, system hardening, and compliance for UNIX-based systems (Linux, macOS, BSD, and others)

2007-2024, CISOfy - <https://ciscofy.com/lynis/>

**Enterprise support available (compliance, plugins, interface and tools)**

---

---

- Screenshots showing the installation and configuration of Logwatch

Configure Logwatch for daily log analysis and reporting

Installing Logwatch

```
(icdfa@icdfa)~]$ sudo apt install -y logwatch
[sudo] password for icdfa:
The following packages were automatically installed and are no longer required:
  libcaes1   libglapi-mesa  python3-acstore  python3-libevt    python3-lbscca
  libcreg1t64 libmsiecf1t64  python3-cffi     python3-libevtx    python3-pefile
  libdnnn3   libolecf1      python3-elasticsearch  python3-libfws1    python3-pycaes
  libevt1t64 libopenh264-7  python3-flor     python3-liblnk     python3-pycparser
  libevtx1t64 libscca1t64  python3-libcreg    python3-lbmsiecf  python3-zstd
  libfws1t64 libxnnpack0   python3-libesedb   python3-libolecf
Use 'sudo apt autoremove' to remove them.

Installing:
  logwatch

Suggested packages:
  libsys-cpu-perl  libsys-meminfo-perl

Summary:
  Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 1395
  Download size: 390 kB
  Space needed: 2,451 kB / 4,631 MB available

Get:1 http://kali.download/kali kali-rolling/main amd64 logwatch all 7.12-3 [390 kB]
Fetched 390 kB in 2s (195 kB/s)
Selecting previously unselected package logwatch.
(Reading database ... 418714 files and directories currently installed.)
Preparing to unpack .../logwatch_7.12-3_all.deb ...
Unpacking logwatch (7.12-3) ...
Setting up logwatch (7.12-3) ...
Processing triggers for man-db (2.13.0-1) ...
Processing triggers for kali-menu (2025.1.1) ...
```

Creating a custom Logwatch configuration

```
(icdfa@icdfa)~]$ $ sudo tee /etc/logwatch/conf/logwatch.conf > /dev/null << 'EOF'
# Logwatch configuration
LogDir = /var/log
TmpDir = /var/cache/logwatch
Output = mail
Format = html
MailTo = root
MailFrom = logwatch@$(hostname)
Range = yesterday
Detail = High
Service = All
# Add custom services
Service = audit
Service = fail2ban
EOF
```

Running Logwatch manually to test  
<https://drive.google.com/file/d/1ZFEEnBQP985Etqh0ckudlxDJ0-Lg7nli6/view?usp=sharing>

```
[icdfa@icdfa]~$ sudo vim /etc/logwatch/conf/logwatch.conf
[icdfa@icdfa]~$ sudo logwatch --output file --filename /var/log/logwatch-report.html --detail High --range today

[icdfa@icdfa]~$ cat /var/log/logwatch-report.html
cat: /var/log/logwatch-report.html: Permission denied

[icdfa@icdfa]~$ sudo cat /var/log/logwatch-report.html
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN" "http://www.w3.org/TR/REC-html40/loose.dtd">
<html>
<head>
<title>Logwatch 7.12 ( 01/22/25 )</title>
<meta name="generator" content="Logwatch 7.12 ( 01/22/25 )">
<style type="text/css">
    h1 {color: gray; border-bottom: 3px double silver; font-family: sans-serif; }
```

- The security\_check\_report.txt file generated by your script

Creating a security check script

```
(icdfa@icdfa)-[~]
$ >....  
-10  
echo  
  
# Check for unowned files  
echo "Unowned files (sample):"  
sudo find / -nouser -o -nogroup -exec ls -la {} \; 2>/dev/null | head  
-10  
echo  
  
# Check for listening ports  
echo "Listening ports:"  
sudo netstat -tulpn | grep LISTEN  
echo  
  
# Check for failed login attempts  
echo "Recent failed login attempts:"  
grep "Failed password" /var/log/auth.log | tail -10  
echo war...  
  
# Check for successful logins  
echo "Recent successful logins:"  
grep "Accepted password" /var/log/auth.log | tail -10  
echo  
  
# Check for sudo usage  
echo "Recent sudo usage:"  
grep "sudo:" /var/log/auth.log | tail -10  
echo  
  
# Check system load  
echo "System load:"  
uptime  
echo  
  
# Check disk usage  
echo "Disk usage:"  
df -h  
echo  
  
# Check for updates  
echo "Available updates:"  
apt list --upgradable 2>/dev/null  
echo  
  
echo "Security check completed."  
  
(icdfa@icdfa)-[~]
$ chmod +x security_check.sh  
  
(icdfa@icdfa)-[~]
$ █
```

## Running the security check script

```
└$ ./security_check.sh > security_check_report.txt
[sudo] password for icdfa:
[icdfa@icdfa] ~
└$ ./security_check.sh
Security Check Report - Fri 12 Sep 2025 23:35:02 WAT
=====
Users with empty passwords:
[sudo] password for icdfa:
root:!::20218:0:99999:7:::
systemd-network:!*:20218::::1
dhcpcd:!::20218:::::
_sentrypeer:!::20218:::::
tss:!::20218:::::
strongswan:!::20218:::::
systemd-timesync:!::20218::::1
Debian-exim:!::20218:::::
uidd:!::20218:::::
messagebus:!::20218:::::
clamav:!::20218:::::
tcpdump:!::20218:::::
redis:!::20218:::::
sshd:!::20218:::::
dnsmasq:!::20218:::::
postgres:!::20218:::::
avahi:!::20218:::::
speech-dispatcher:!::20218:::::
usbmux:!::20218:::::
nm-openvpn:!::20218:::::
inetsim:!::20218:::::
_defectdojo:!::20218:::::
nm-openconnect:!::20218:::::
lightdm;!::20218:::::
saned:!::20218:::::
polkitd;!::20218:::::
rtkit;!::20218:::::
colord;!::20218:::::
icdfa:$y$9T$jsCfLpD2oH.IX5Nf8x33p/$OpodUloLMtNXMup91mbrFQ0bpQse6esbbB5o.a3wsB1:20218:0:99999:7:::
_aide:!::20343:::::

Users with UID 0:
root:x:0:0:root:/root:/usr/bin/zsh

SUID/SID files (sample):
libtag2/kali-rolling 2.1.1-1 amd64 [upgradable from: 2.0.2-2]
libtag2/kali-rolling 2.1.1-1 i386 [upgradable from: 2.0.2-2]
libtalloc2/kali-rolling 2:2.4.3+samba4.22.4+dfsg-1 amd64 [upgradable from: 2:2.4.2+samba4.21.4+dfsg-1]
libtalloc8.6/kali-rolling 8.6.17+dfsg-1 amd64 [upgradable from: 8.6.16+dfsg-1]
libtdb1/kali-rolling 2:1.4.13+samba4.22.4+dfsg-1 amd64 [upgradable from: 2:1.4.12+samba4.21.4+dfsg-1]
libtevent0t64/kali-rolling 2:0.16.2+samba4.22.4+dfsg-1 amd64 [upgradable from: 2:0.16.1+samba4.21.4+dfsg-1]
libthunarx-3-0/kali-rolling 4.20.4-1 amd64 [upgradable from: 4.20.2-1]
libtiff6/kali-rolling 4.7.0-4 amd64 [upgradable from: 4.7.0-3]
libtiff6/kali-rolling 4.7.0-4 i386 [upgradable from: 4.7.0-3]
libtinystrsql-3.0-0/kali-rolling 3.8.2-7+b1 amd64 [upgradable from: 3.8.2-7]
libtirpc-common/kali-rolling,kali-rolling 1.3.6+ds-1 all [upgradable from: 1.3.4+ds-1.3]
libtirpc3t64/kali-rolling 1.3.6+ds-1 amd64 [upgradable from: 1.3.4+ds-1.3+b1]
libtk8.6/kali-rolling 8.6.17-1 amd64 [upgradable from: 8.6.16-1]
libtotem-plparser18/kali-rolling 3.26.6-2+b1 amd64 [upgradable from: 3.26.6-2]
libtsan2/kali-rolling 15.2.0-1 amd64 [upgradable from: 14.2.0-19]
libturbojpeg/kali-rolling 1:2.1.5-4 amd64 [upgradable from: 1:2.1.5-3.1]
libubusan1/kali-rolling 15.2.0-1 amd64 [upgradable from: 14.2.0-19]
libuchardet0/kali-rolling 0.0.8-2 amd64 [upgradable from: 0.0.8-1+b2]
libudev1/kali-rolling 257.7-1 amd64 [upgradable from: 257.5-2]
libudev1/kali-rolling 257.7-1 i386 [upgradable from: 257.5-2]
libudisks2-0/kali-rolling 2.10.90-3 amd64 [upgradable from: 2.10.1-11]
libunbound8/kali-rolling 1.23.1-1 amd64 [upgradable from: 1.22.0-1+b1]
libunbreak6/kali-rolling 6.1-3 amd64 [upgradable from: 6.1-2+b1]
libupower-glib3/kali-rolling 1.90.10-1 amd64 [upgradable from: 1.90.7-1]
liburcu8t64/kali-rolling 0.15.3-1 amd64 [upgradable from: 0.15.1-1]
liburing2/kali-rolling 2.11-1 amd64 [upgradable from: 2.9-1]
libusb-1.0-0/kali-rolling 2:1.0.29-2 amd64 [upgradable from: 2:1.0.28-1]
libusb-2.1-0/kali-rolling 2:1.0.29-2 i386 [upgradable from: 2:1.0.28-1]
libuuid1/kali-rolling 2.41.1-1 amd64 [upgradable from: 2.41-4]
libv4l-0t64/kali-rolling 1.30.1-1 amd64 [upgradable from: 1.28.1-1]
libv4l-0t64/kali-rolling 1.30.1-1 i386 [upgradable from: 1.28.1-1]
libv4lconvert0t64/kali-rolling 1.30.1-1 amd64 [upgradable from: 1.28.1-1]
libv4lconvert0t64/kali-rolling 1.30.1-1 i386 [upgradable from: 1.28.1-1]
libvolume-key1/kali-rolling 0.3.12-10 amd64 [upgradable from: 0.3.12-9]
libvpl2/kali-rolling 1:2.15.0-1 amd64 [upgradable from: 1:2.14.0-1+b1]
libvpx9/kali-rolling 1.15.0-2.1 amd64 [upgradable from: 1.15.0-2]
libvpx9/kali-rolling 1.15.0-2.1 i386 [upgradable from: 1.15.0-2]
libvte-2.91-0/kali-rolling 0.80.3-2 amd64 [upgradable from: 0.80.1-1]
libvte-2.91-common/kali-rolling 0.80.3-2 amd64 [upgradable from: 0.80.1-1]
libvulkan1/kali-rolling 1.4.321.0-1 amd64 [upgradable from: 1.4.309.0-1]
libvulkan1/kali-rolling 1.4.321.0-1 i386 [upgradable from: 1.4.309.0-1]
libwacom-common/kali-rolling,kali-rolling 2.16.1-1 all [upgradable from: 2.14.0-1]
libwacom9/kali-rolling 2.16.1-1 amd64 [upgradable from: 2.14.0-1]
```

Creating a cron job for daily security checks

```
└─(icdfa㉿icdfa)─[~]
$ echo "0 5 * * * root /path/to/security_check.sh > /var/log/security_check_$(date +\%Y\%m\%d).log 2>&1" | sudo tee /etc/cron.d/security_check
[sudo] password for icdfa:
5 * * * * root /path/to/security_check.sh > /var/log/security_check_20250912.log 2>&1
```

Creating a cron job for weekly AIDE checks

```
└─(icdfa㉿icdfa)─[~]
$ echo "0 4 * * 0 root /usr/bin/aide.wrapper --check > /var/log/aide/aide-check-$(date +\%Y\%m\%d).log 2>&1" | sudo tee /etc/cron.d/aide-weekly
0 4 * * 0 root /usr/bin/aide.wrapper --check > /var/log/aide/aide-check-20250912.log 2>&1
```

Creating a cron job for monthly Lynis audits

```
└─(icdfa㉿icdfa)─[~]
$ echo "0 3 1 * * root /usr/bin/lynis audit system --report-file /var/log/lynis-audit-$(date +\%Y\%m).log 2>&1" | sudo tee /etc/cron.d/lynis-monthly
0 3 1 * * root /usr/bin/lynis audit system --report-file /var/log/lynis-audit-202509.log 2>&1
```

- The Lynis audit report  
[https://drive.google.com/file/d/1OBQd3Os\\_IfbbaduJGInduC0V-iDBwW\\_4/view?usp=sharing](https://drive.google.com/file/d/1OBQd3Os_IfbbaduJGInduC0V-iDBwW_4/view?usp=sharing)

```
(icdfa@icdfa)~]$ sudo lynis audit system --quick > ./lynis-audit.log
2025-09-15 13:02:08,546 fail2ban.configreader [20257]: ERROR F
ound no accessible config files for 'filter.d/sshd-ddos' under /et
c/fail2ban
2025-09-15 13:02:08,550 fail2ban.jailreader [20257]: ERROR U
nable to read the filter 'sshd-ddos'
2025-09-15 13:02:08,550 fail2ban.jailsreader [20257]: ERROR E
rrors in jail 'sshd-ddos'. Skipping ...
2025-09-15 13:02:08,551 fail2ban.configreader [20257]: ERROR F
ound no accessible config files for 'filter.d/sudo' under /etc/fai
l2ban
2025-09-15 13:02:08,551 fail2ban.jailreader [20257]: ERROR U
nable to read the filter 'sudo'
2025-09-15 13:02:08,551 fail2ban.jailsreader [20257]: ERROR E
rrors in jail 'sudo'. Skipping ...

(icdfa@icdfa)~]$ cat lynis-audit.log

[ Lynis 3.1.4 ]

#####
##### Lynis comes with ABSOLUTELY NO WARRANTY. This is free software,
and you are
welcome to redistribute it under the terms of the GNU General Pu
blic License.
See the LICENSE file for details about using this software.

2007-2024, CISOfy - https://cisofy.com/lynis/
Enterprise support available (compliance, plugins, interface and
tools)
#####

[+] Initializing program

(icdfa@icdfa)~]$ sudo cp /var/log/lynis-audit.log /rol_monit/daily_securit
[sudo] password for icdfa:
(icdfa@icdfa)~]$
```

We installed and configured **Logwatch** for daily log analysis, created a **security check script**, and then set up cron jobs for daily, weekly, and monthly monitoring with **AIDE** and **Lynis**. These tools shall help detect anomalies, monitor system integrity, and generate reports automatically. By providing continuous oversight and regular audits, they strengthen the organization's security governance, support compliance, and enable a quick response to potential threats.

## Part 3: Security Log Analysis and Visualization

### Deliverables:

Creating a Python script to parse and analyze authentication logs:  
Creating a log analysis script

```
(icdfa@icdfa)-[~]
$ >....
```

```
# Check for compromised accounts
suspicious_users = [user for user, count in analysis_results['successful_users'].items() if count > 10]
    if suspicious_users:
        f.write("2. Unusually high number of logins for the following users:\n")
        for user in suspicious_users:
            f.write(f" - {user}: {analysis_results['successful_users'][user]}\n")
            f.write("   Recommendation: Verify if this activity is legitimate.\n\n")
    f.write("3. General recommendations:\n")
    f.write("   - Implement or strengthen fail2ban rules to block repeated failed login attempts\n")
    f.write("   - Consider implementing multi-factor authentication\n")
    f.write("   - Review user access regularly and remove unnecessary accounts\n")
    f.write("   - Ensure password policies enforce strong passwords\n")

if __name__ == "__main__":
    if len(sys.argv) < 2:
        print("Usage: python3 analyze_auth_logs.py <auth_log_file>")
        sys.exit(1)

log_file = sys.argv[1]
output_prefix = "auth_analysis"

# Parse and analyze the log file
data = parse_auth_log(log_file)
analysis_results = analyze_data(data)

# Generate visualizations
generate_visualizations(analysis_results, output_prefix)

# Generate report
generate_report(data, analysis_results, f"{output_prefix}_report.txt")

print(f"Analysis complete. Report saved to {output_prefix}_report.txt")
print(f"Visualizations saved as {output_prefix}_*.png")
EOF
```

```
(icdfa@icdfa)-[~]
$ chmod +x analyze_auth_logs.py
```

```
(icdfa@icdfa)-[~]
$ █
```

Installing required Python packages for the analysis script

```
(icdfa㉿icdfa) [~]
$ sudo apt install -y python3-pip
The following packages were automatically installed and are no longer required:
  libcaes1      libscca1t64          python3-libfwsi
  libcreg1t64   libbxnnpack0        python3-liblnk
  libdnnl3       python3-acstore    python3-libmsiecf
  libevt1t64    python3-cffi       python3-libolecf
  libevtx1t64   python3-elasticsearch python3-libscca
  libfwsi1t64   python3-flor       python3-pefile
  libglapi-mesa  python3-libcreg    python3-pycaes
  libmsiecf1t64 python3-libesedb   python3-pycparser
  libolecf1     python3-libevt     python3-zstd
  libopenh264-7  python3-libevtx
Use 'sudo apt autoremove' to remove them.

Upgrading:
  python3-pip  python3-pip-whl

Summary:
  Upgrading: 2, Installing: 0, Removing: 0, Not Upgrading: 1393
  Download size: 2,814 kB
  Freed space: 299 kB

Get:1 http://http.kali.org/kali kali-rolling/main amd64 python3-pip all 25
.2+dfsg-1 [1,386 kB]
Get:2 http://http.kali.org/kali kali-rolling/main amd64 python3-pip-whl al
l 25.2+dfsg-1 [1,428 kB]
Fetched 2,814 kB in 2s (1,640 kB/s)
(Reading database ... 419103 files and directories currently installed.)
Preparing to unpack .../python3-pip_25.2+dfsg-1_all.deb ...
Unpacking python3-pip (25.2+dfsg-1) over (25.0.1+dfsg-1) ...
Preparing to unpack .../python3-pip-whl_25.2+dfsg-1_all.deb ...
Unpacking python3-pip-whl (25.2+dfsg-1) over (25.0.1+dfsg-1) ...
Setting up python3-pip-whl (25.2+dfsg-1) ...
Setting up python3-pip (25.2+dfsg-1) ...
Processing triggers for man-db (2.13.0-1) ...
Processing triggers for kali-menu (2025.1.1) ...
```

```
(icdfa㉿icdfa) [~]
$ pip3 install matplotlib --break-system-packages
Defaulting to user installation because normal site-packages is not writeable
Requirement already satisfied: matplotlib in /usr/lib/python3/dist-packages (3.8.3)
Requirement already satisfied: contourpy>=1.0.1 in /usr/lib/python3/dist-packages (from matplotlib)
Requirement already satisfied: cycler>=0.10 in /usr/lib/python3/dist-packages (from matplotlib)
Requirement already satisfied: fonttools>=4.22.0 in /usr/lib/python3/dist-packages (from matplotlib)
Requirement already satisfied: kiwisolver>=1.3.1 in /usr/lib/python3/dist-packages (from matplotlib)
Requirement already satisfied: numpy<2,>=1.21 in /usr/lib/python3/dist-packages (from matplotlib)
Requirement already satisfied: packaging>=20.0 in /usr/lib/python3/dist-packages (from matplotlib)
Requirement already satisfied: pillow>=8 in /usr/lib/python3/dist-packages (from matplotlib)
Requirement already satisfied: pyparsing>=2.3.1 in /usr/lib/python3/dist-packages (from matplotlib)
Requirement already satisfied: python-dateutil>=2.7 in /usr/lib/python3/dist-packages (from matplotlib)
```

Run the log analysis script on the authentication logs

```
[icdfa@icdfa]~$ python3 analyze_auth_logs.py /var/log/auth.log
Analysis complete. Report saved to auth_analysis_report.txt
Visualizations saved as auth_analysis_*.png
```

Creating a Python script to analyze and visualize audit logs

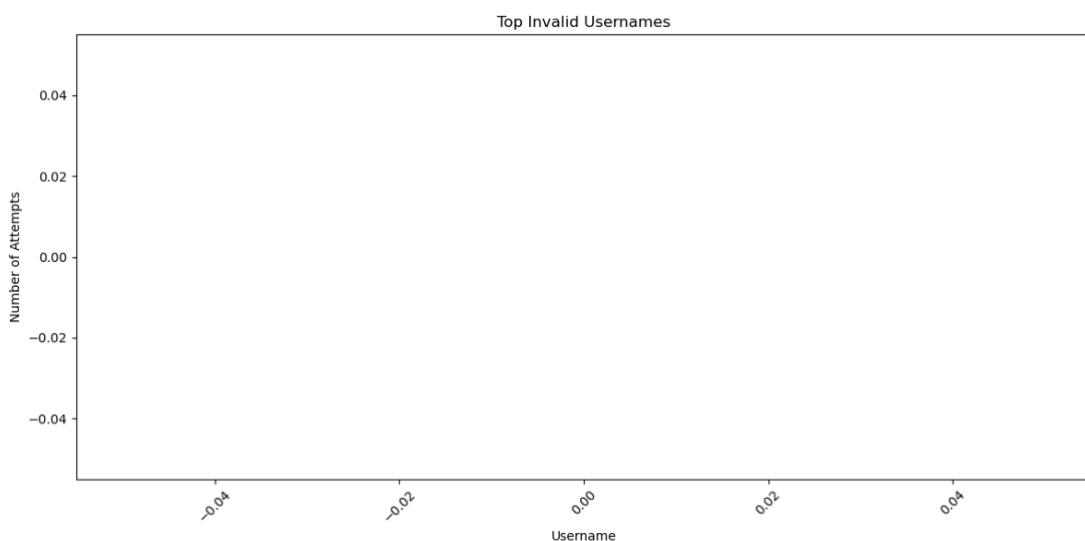
```
[icdfa@icdfa]~$ >....  
# Check for unusual executables  
common_exes = {'/usr/bin/sudo', '/usr/bin/su', '/usr/bin/passwd',  
'/usr/bin/ssh'}  
unusual_exes = [exe for exe in analysis_results['event_executables'] if exe not in common_exes and analysis_results['event_executables'][exe] > 5]  
  
if unusual_exes:  
    f.write("2. Review usage of these executables with high audit event counts:\n")  
    for exe in unusual_exes[:5]:  
        f.write(f" - {exe}: {analysis_results['event_executables'][exe]} events\n")  
        f.write("\n")  
  
    f.write("3. General recommendations:\n")  
    f.write(" - Review audit configuration to ensure all security-relevant events are captured\n")  
    f.write(" - Implement regular review of audit logs as part of security operations\n")  
    f.write(" - Consider implementing automated alerting for suspicious audit events\n")  
    f.write(" - Ensure audit logs are backed up and retained according to policy\n")  
  
if __name__ == "__main__":  
    output_prefix = "audit_analysis"  
  
    # Get and parse audit data  
    audit_data = get_audit_data()  
    parsed_data = parse_audit_data(audit_data)  
  
    # Analyze the data  
    analysis_results = analyze_audit_data(parsed_data)  
  
    # Generate visualizations  
    generate_visualizations(analysis_results, output_prefix)  
  
    # Generate report  
    generate_report(parsed_data, analysis_results, f"{output_prefix}_report.txt")  
    print(f"Analysis complete. Report saved to {output_prefix}_report.txt")  
    print(f"Visualizations saved as {output_prefix}_*.png")  
EOF  
[icdfa@icdfa]~$
```

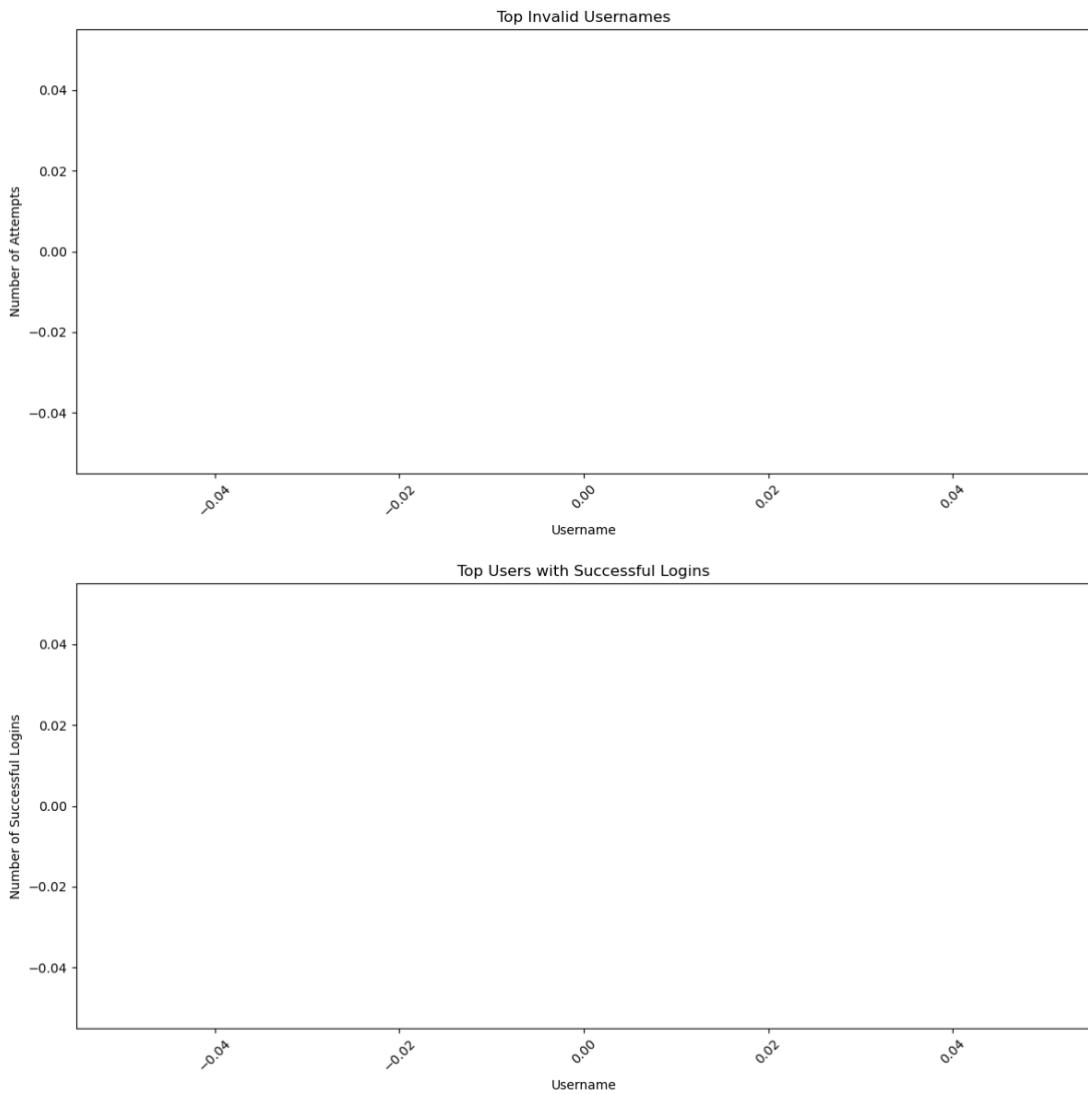
```
(icdfa@icdfa)~]$ chmod +x security_dashboard.py
chmod: cannot access 'security_dashboard.py': No such file or directory
(icdfa@icdfa)~]$
```

Run the dashboard script

```
(icdfa@icdfa)~]$ python3 security_dashboard.py
python3: can't open file '/home/icdfa/security_dashboard.py': [Errno 2] No
such file or directory
(icdfa@icdfa)~]$
```

- The auth\_analysis\_report.txt file generated by the script  
<https://drive.google.com/file/d/1BUVZtDziRmdB8Nx1jfflTqmx-oiXZZEQ/view?usp=sharing>





- The audit\_analysis\_report.txt file generated by the script  
[https://drive.google.com/file/d/1lAOTwSu5y\\_FvvAyx0UoNHw9t6vqfShAt/view?usp=sharing](https://drive.google.com/file/d/1lAOTwSu5y_FvvAyx0UoNHw9t6vqfShAt/view?usp=sharing)

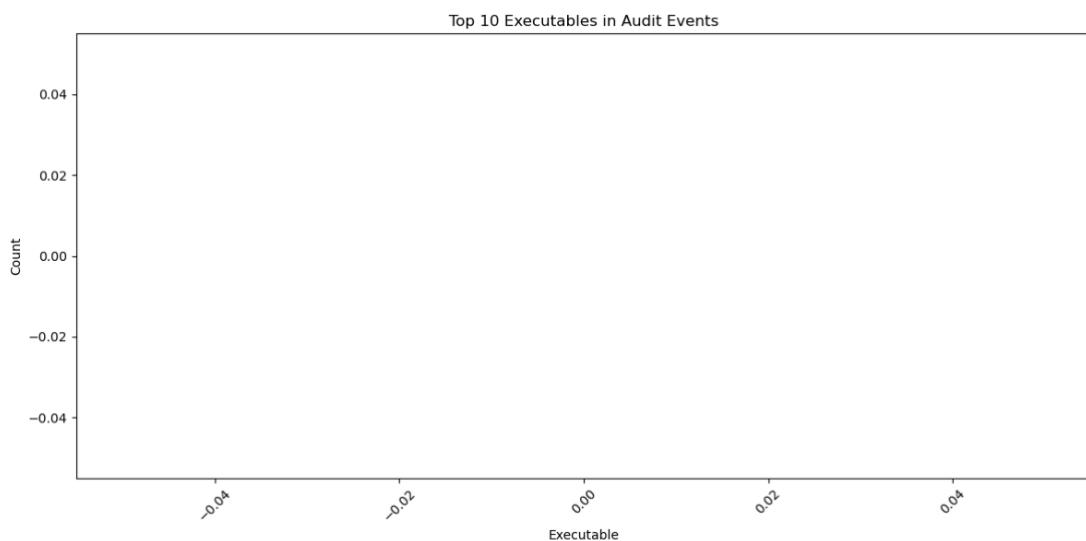
- The Security\_dashboard.html file  
[https://drive.google.com/file/d/1iBMNssTVOzNaVLwaaTtgkpZxFlXP\\_1hz/view?usp=sharing](https://drive.google.com/file/d/1iBMNssTVOzNaVLwaaTtgkpZxFlXP_1hz/view?usp=sharing)

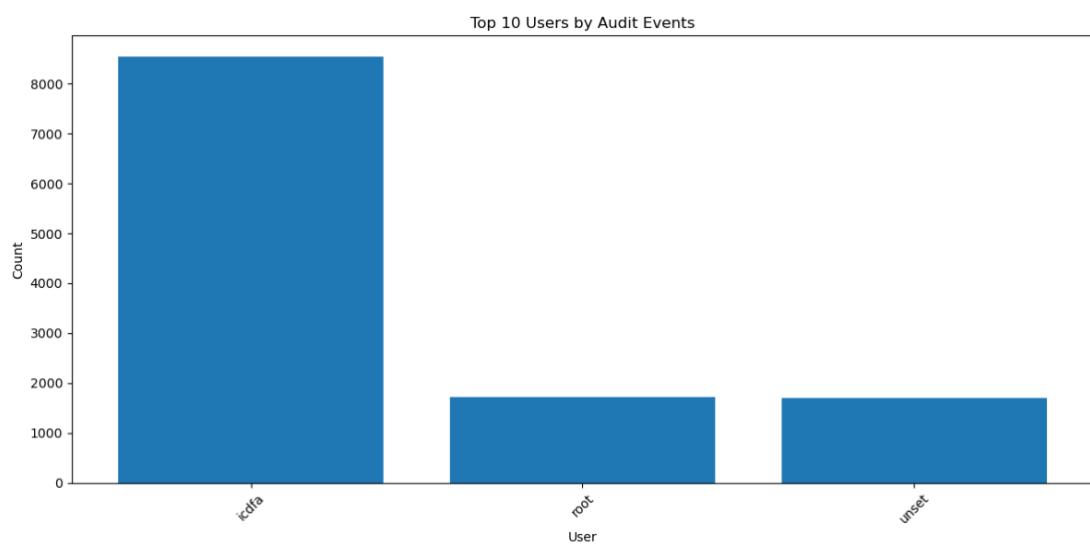
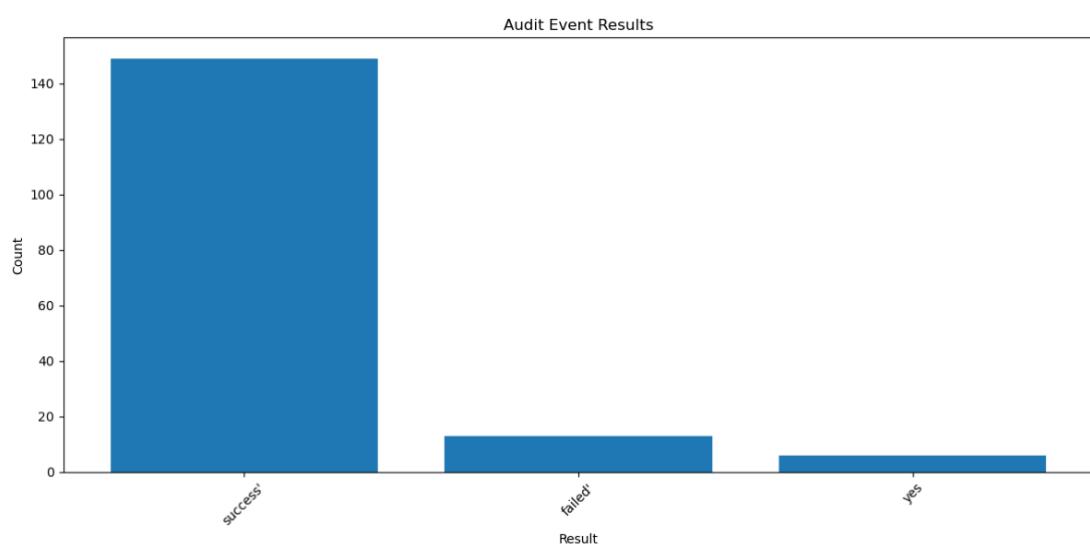
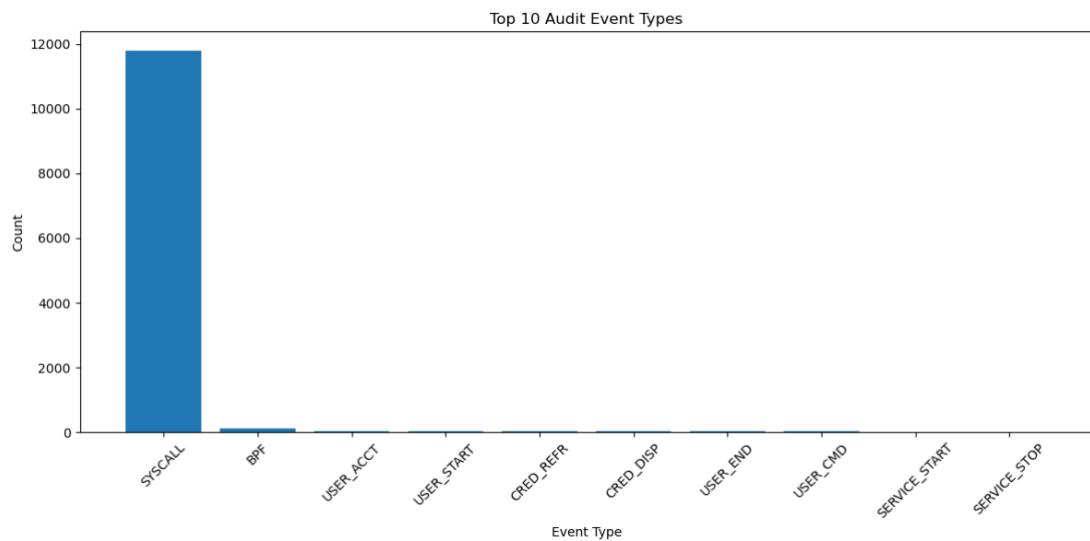
```
└─(icdfa㉿icdfa)-[~]
$ chmod +x security_dashboard.py

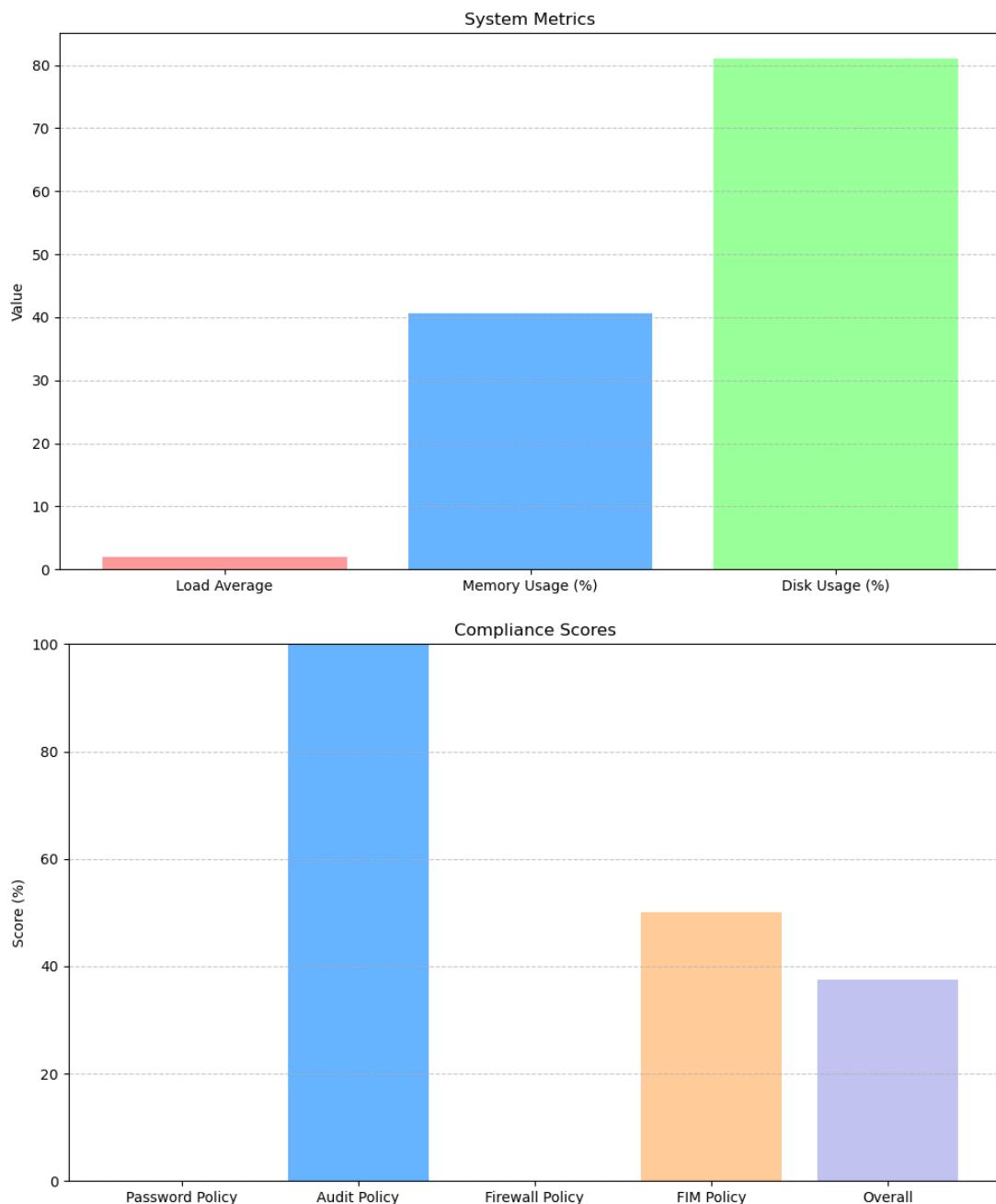
└─(icdfa㉿icdfa)-[~]
$ ./security_dashboard.py
/home/icdfa/.:/security_dashboard.py:110: SyntaxWarning: invalid escape sequence '\*'
    empty_passwords = run_command("sudo grep -v ':\*:' /etc/shadow | grep -c ':::'").strip()
/home/icdfa/.:/security_dashboard.py:115: SyntaxWarning: invalid escape sequence '\('
    uid_files = int(run_command("sudo find /home -type f \(-perm -4000 -o -perm -2000 \) | wc -l").strip())
[sudo] password for icdfa:
Security dashboard generated: security_dashboard.html

└─(icdfa㉿icdfa)-[~]
$
```

- Screenshots of the visualizations generated by your scripts







The log analysis and visualization tools help to improve security monitoring by providing structured insights into authentication and system events. Since raw logs are not easy to interpret, automated scripts are used to summarize failed logins, unusual audit events, and suspicious activities. Visual dashboards are used to make it easy to understand patterns, such as brute force attempts in system activity. The collaboration of these tools supports detection and response, thus strengthening security governance.

## Part 4: Implementing Continuous Monitoring

Create a comprehensive security monitoring script that runs daily checks:

Create a daily security monitoring script

```
└$ >....
UPDATES=$(apt list --upgradable 2>/dev/null | grep -c upgradable)
if [ "$UPDATES" -gt 0 ]; then
    echo "- RECOMMENDATION: Updates available: $UPDATES" >> $REPORT_FILE
fi

# Check for high system load
LOAD=$(cat /proc/loadavg | awk '{print $1}')
if (( $(echo "$LOAD > 2.0" | bc -l) )); then
    echo "- WARNING: High system load: $LOAD" >> $REPORT_FILE
fi

# Check for disk space
DISK_USAGE=$(df / | tail -1 | awk '{print $5}' | tr -d '%')
if [ "$DISK_USAGE" -gt 90 ]; then
    echo "- WARNING: High disk usage: $DISK_USAGE%" >> $REPORT_FILE
fi

# Check for failed logins
FAILED_LOGINS=$(grep "Failed password" /var/log/auth.log | grep "$(date "+%b %e")" | wc -l)
if [ "$FAILED_LOGINS" -gt 10 ]; then
    echo "- WARNING: High number of failed logins today: $FAILED_LOGINS" >
> $REPORT_FILE
fi

# Generate HTML dashboard
if [ -f /usr/bin/python3 ]; then
    # Run the security dashboard script if it exists
    if [ -f /path/to/security_dashboard.py ]; then
        python3 /path/to/security_dashboard.py
        cp security_dashboard.html $HTML_REPORT
    fi
fi

echo "" >> $REPORT_FILE
echo "Report completed at $(date)" >> $REPORT_FILE

# Send email notification (uncomment and configure for production use)
# mail -s "Daily Security Report - $(hostname) - $(date +%Y-%m-%d)" admin@
example.com < $REPORT_FILE

echo "Security monitoring completed. Report saved to $REPORT_FILE"
if [ -f $HTML_REPORT ]; then
    echo "HTML dashboard saved to $HTML_REPORT"
fi
EOF
```

```
└(icdfa@icdfa)-[~]
$ chmod +x daily_security_monitor.sh

└(icdfa@icdfa)-[~]
$ █
```

Creating a script to monitor for security control changes:

```
└$ >....  
    echo "Previous checksum: $BASELINE_SHADOW_MD5" >> $REPORT_FILE  
    echo "Current checksum: $CURRENT_SHADOW_MD5" >> $REPORT_FILE  
    echo "" >> $REPORT_FILE  
  
    # Update baseline  
    echo "$CURRENT_SHADOW_MD5" > "$SHADOW_FILE"  
else  
    echo "UNCHANGED: User passwords (/etc/shadow)" >> $REPORT_FILE  
fi  
else  
    # Create baseline if it doesn't exist  
    echo "$CURRENT_SHADOW_MD5" > "$SHADOW_FILE"  
    echo "BASELINE CREATED: User passwords (/etc/shadow)" >> $REPORT_FILE  
fi  
  
# Check group file  
CURRENT_GROUP_MD5=$(md5sum /etc/group | awk '{print $1}')  
if [ -f "$GROUP_FILE" ]; then  
    BASELINE_GROUP_MD5=$(cat "$GROUP_FILE")  
    if [ "$CURRENT_GROUP_MD5" != "$BASELINE_GROUP_MD5" ]; then  
        echo "CHANGED: Group accounts (/etc/group)" >> $REPORT_FILE  
        echo "Previous checksum: $BASELINE_GROUP_MD5" >> $REPORT_FILE  
        echo "Current checksum: $CURRENT_GROUP_MD5" >> $REPORT_FILE  
        echo "" >> $REPORT_FILE  
  
        # Update baseline  
        echo "$CURRENT_GROUP_MD5" > "$GROUP_FILE"  
    else  
        echo "UNCHANGED: Group accounts (/etc/group)" >> $REPORT_FILE  
    fi  
else  
    # Create baseline if it doesn't exist  
    echo "$CURRENT_GROUP_MD5" > "$GROUP_FILE"  
    echo "BASELINE CREATED: Group accounts (/etc/group)" >> $REPORT_FILE  
fi  
  
echo "" >> $REPORT_FILE  
echo "Report completed at $(date)" >> $REPORT_FILE  
  
# Send email notification (uncomment and configure for production use)  
# mail -s "Security Control Changes - $(hostname) - $(date +%Y-%m-%d)" adm  
in@example.com < $REPORT_FILE  
  
echo "Security control monitoring completed. Report saved to $REPORT_FILE"  
EOF
```

```
└(icdfa@icdfa)-[~]  
$ chmod +x monitor_security_controls.sh  
└(icdfa@icdfa)-[~]  
$ █
```

## Creating a security metrics script

```
$ >....
```

```
def save_metrics_history(metrics):
    history_file = "/var/lib/security_metrics/metrics_history.json"
    os.makedirs(os.path.dirname(history_file), exist_ok=True)

    # Load existing history
    history = []
    if os.path.exists(history_file):
        try:
            with open(history_file, 'r') as f:
                history = json.load(f)
        except:
            history = []

    # Add current metrics with timestamp
    metrics['timestamp'] = datetime.datetime.now().isoformat()
    history.append(metrics)

    # Keep only last 30 days
    if len(history) > 30:
        history = history[-30:]

    # Save updated history
    with open(history_file, 'w') as f:
        json.dump(history, f, indent=2)

if __name__ == "__main__":
    output_prefix = "security_metrics"
    output_file = f"{output_prefix}_report.txt"

    # Get metrics
    metrics = get_metrics()

    # Generate visualizations
    generate_visualizations(metrics, output_prefix)

    # Generate report
    generate_report(metrics, output_file)

    # Save metrics history
    save_metrics_history(metrics)

    print(f"Security metrics generated. Report saved to {output_file}")
    print(f"Visualizations saved as {output_prefix}.*.png")
EOF
```

```
(icdfa@icdfa)-[~]
$ chmod +x security_metrics.py

(icdfa@icdfa)-[~]
$ █
```

Schedule the monitoring scripts to run automatically:

Creating cron jobs for the monitoring scripts

[https://drive.google.com/file/d/1Yel1p\\_UOghIG2NAHBUZhf0frfZK0Ph2G/view?usp=sharing](https://drive.google.com/file/d/1Yel1p_UOghIG2NAHBUZhf0frfZK0Ph2G/view?usp=sharing)

```
[icdfa@icdfa]~]$ echo "0 6 * * * root /path/to/daily_security_monitor.sh > /var/log/security_reports/daily_monitor_$(date +\%Y\%m\%d).log 2>&1" | sudo tee /etc/cron.d/daily-security-monitor
[sudo] password for icdfa:
0 6 * * * root /path/to/daily_security_monitor.sh > /var/log/security_reports/daily_monitor_$(date +\%Y\%m\%d).log 2>&1

[icdfa@icdfa]~]$
```

```
[icdfa@icdfa]~]$ echo "0 7 * * * root /path/to/monitor_security_controls.sh > /var/log/security_reports/control_monitor_$(date +\%Y\%m\%d).log 2>&1" | sudo tee /etc/cron.d/security-control-monitor
0 7 * * * root /path/to/monitor_security_controls.sh > /var/log/security_reports/control_monitor_$(date +\%Y\%m\%d).log 2>&1

[icdfa@icdfa]~]$
```

```
[icdfa@icdfa]~]$ echo "0 8 * * * root /path/to/security_metrics.py > /var/log/security_reports/metrics_$(date +\%Y\%m\%d).log 2>&1" | sudo tee /etc/cron.d/security-metrics
0 8 * * * root /path/to/security_metrics.py > /var/log/security_reports/metrics_$(date +\%Y\%m\%d).log 2>&1

[icdfa@icdfa]~]$
```

Create a script to simulate security events for testing:  
Creating a script to simulate security events

```
(icdfa@icdfa)-
$ echo "0 8 * * * root /path/to/security_metrics.py > /var/log/security_
reports/metrics_$(date +\%Y\%m\%d).log 2>&1" | sudo tee /etc/cron.d/secur
ity-metrics

0 8 * * * root /path/to/security_metrics.py > /var/log/security_reports/me
trics_$(date +\%Y\%m\%d).log 2>&1

(icdfa@icdfa)-
$ cat > simulate_security_events.sh << 'EOF'
#!/bin/bash

echo "Simulating security events for testing ..."

# Simulate failed login attempts
for i in {1..5}; do
    ssh -o BatchMode=yes -o ConnectTimeout=5 nonexistentuser@localhost 2>/
dev/null || true
    ssh -o BatchMode=yes -o ConnectTimeout=5 root@localhost 2>/dev/null ||
true
done

# Simulate successful login
sudo su - $(whoami) -c "echo 'Simulated login'"

# Simulate file access
sudo cat /etc/shadow 2>/dev/null || true

# Simulate file changes
sudo touch /tmp/test_security_file
sudo rm /tmp/test_security_file

# Simulate sudo usage
sudo ls -la /root

# Simulate failed sudo
echo "wrongpassword" | sudo -S ls 2>/dev/null || true

echo "Security events simulation completed."
EOF
```

```
(icdfa@icdfa)-
$ chmod +x simulate_security_events.sh

(icdfa@icdfa)-
$ █
```

Run the simulation script

```
[icdfa@icdfa]~]$ ./simulate_security_events.sh
Simulating security events for testing ...
Simulated login
root::!20218:0:99999:7:::
daemon:*20218:0:99999:7:::
bin::*20218:0:99999:7:::
sys::*20218:0:99999:7:::
sync::*20218:0:99999:7:::
games::*20218:0:99999:7:::
man::*20218:0:99999:7:::
lp::*20218:0:99999:7:::
mail::*20218:0:99999:7:::
news::*20218:0:99999:7:::
uucp::*20218:0:99999:7:::
proxy::*20218:0:99999:7:::
www-data::*20218:0:99999:7:::
backup::*20218:0:99999:7:::
list::*20218:0:99999:7:::
irc::*20218:0:99999:7:::
_apt::*20218:0:99999:7:::
nobody::*20218:0:99999:7:::
systemd-network:!*:20218::::1:
dhpcd:!20218:::::
_sentrypeer:!20218:::::
tss:!20218:::::
strongswan:!20218:::::
systemd-timesync:!*:20218::::1:
Debian-exim:!20218:::::
uuidd:!20218:::::
messagebus:!20218:::::
clamav:!20218:::::
tcpdump:!20218:::::
redis:!20218:::::
sshd:!20218:::::
dnsmasq:!20218:::::
postgres:!20218:::::
avahi:!20218:::::
speech-dispatcher:!20218:::::
usbmux:!20218:::::
nm-openvpn:!20218:::::
inetsim:!20218:::::
_defectdojo:!20218:::::
nm-openconnect:!20218:::::
lightdm:!20218:::::
saned:!20218:::::
polkitd:!*:20218:::::
```

```
rtkit:!:20218:::::  
colord:!:20218:::::  
icdfa:$y$j9T$jscDlPD2oH.IX5Nf8x33p/$OpodUloLMtNXMup91mbrFQ0bpQse6esbbB5o.a  
3wsB1:20218:0:99999:7 :::  
aide:!*:20343:::::  
total 96  
drwx----- 10 root root 4096 May 11 13:41 .  
drwxr-xr-x 19 root root 4096 Sep 12 20:41 ..  
-rw-r--r-- 1 root root 5551 May 10 19:53 .bashrc  
-rw-r--r-- 1 root root 607 May 10 19:53 .bashrc.original  
drwx----- 7 root root 4096 May 11 05:07 .cache  
drwx----- 6 root root 4096 May 11 06:41 .config  
drwx----- 3 root root 4096 May 10 21:18 .dbus  
-rw-r--r-- 1 root root 11656 May 10 20:11 .face  
lrwxrwxrwx 1 root root 11 May 10 20:11 .face.icon → /root/.face  
drwx----- 2 root root 4096 May 10 21:18 .gvfs  
-rw-r--r-- 1 root root 1598 May 11 05:47 installation-report.txt  
drwxr-xr-x 4 root root 4096 May 11 05:47 lab  
drwxrwxr-x 3 root root 4096 May 10 21:18 .local  
drwxr-xr-x 4 root root 4096 May 11 05:39 .npm  
-rw-r--r-- 1 root root 132 Feb 17 2025 .profile  
drwx----- 2 root root 4096 May 10 19:11 .ssh  
-rw-r----- 1 root root 4 May 11 13:41 .vboxclient-display-svga-x11-tt  
y1-control.pid  
-rw-r--r-- 1 root root 210 May 11 11:16 .wget-hsts  
-rw----- 1 root root 357 May 11 06:42 .zsh_history  
-rw-r--r-- 1 root root 10988 May 11 05:47 .zshrc  
analyze_audit_logs.py Music  
analyze_auth_logs.py Pictures  
auth_analysis_failed_ips.png Public  
auth_analysis_invalid_users.png security_check_report.txt  
auth_analysis_report.txt security_check.sh  
auth_analysis_successful_users.png security_metrics.py  
daily_security_monitor.sh simulate_security_events.sh  
Desktop Templates  
Documents test_logging.sh  
Downloads time_decode_env  
get-pip.py tools  
installation-report.txt Videos  
lab Vinetto  
monitor_security_controls.sh  
Security events simulation completed.
```

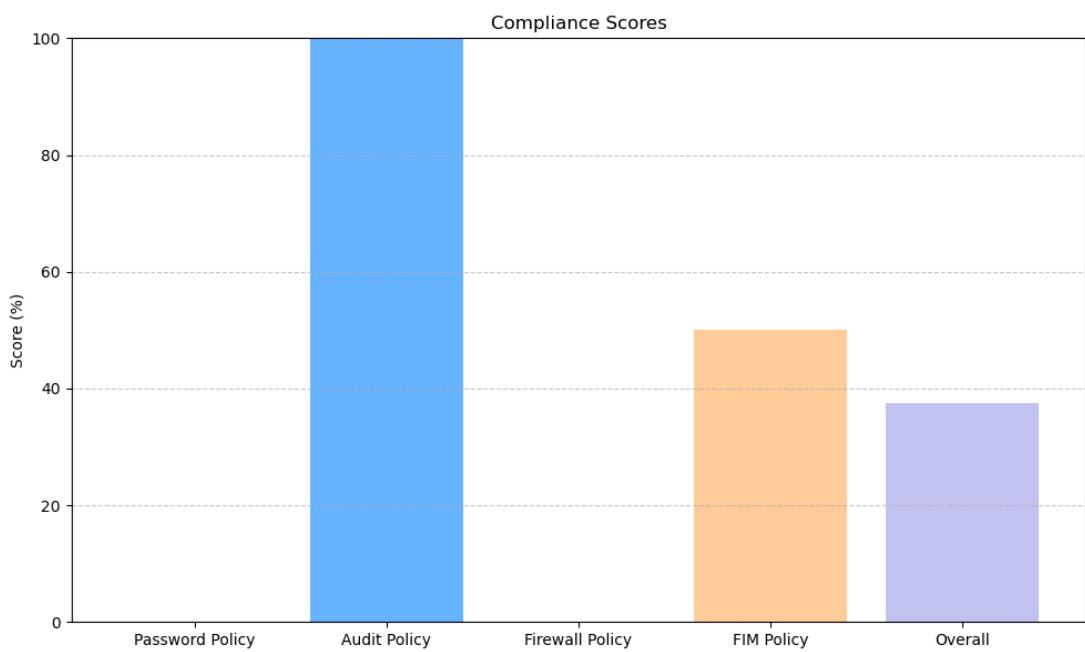
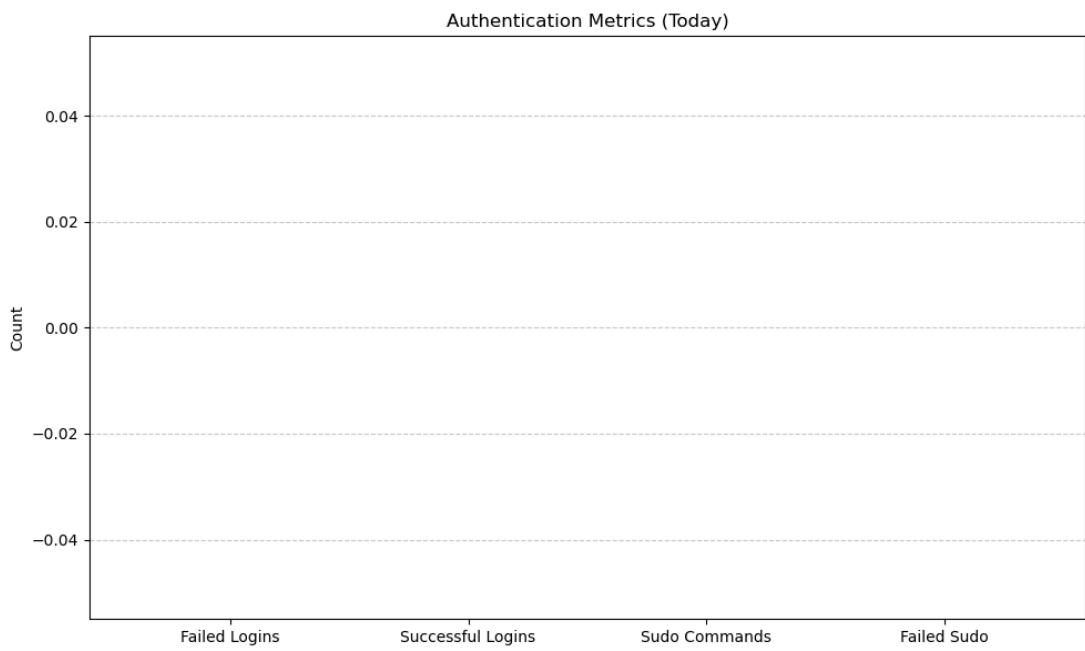
```
└─(icdfa@icdfa)─[~]  
└─$ ┌─
```

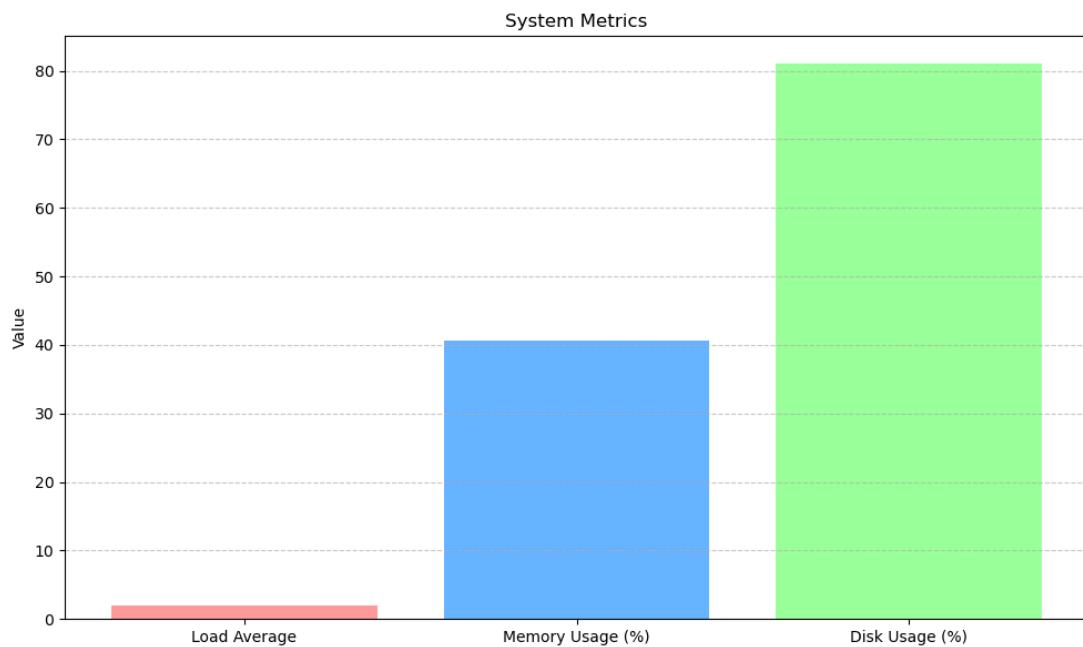
## Run the monitoring scripts

```
(icdfa@icdfa)-[~]
└─$ cat /var/log/control_changes.txt
=====
Control Change Monitoring
Sat 13 Sep 2025 00:42:14 WAT
-r--r----- 1 root root 1714 Feb 9 2025 /etc/sudoers
76d0f5775326cea72600a8d590342ca1173403e5bee040fbfc9bded896492c98 /etc/sudoers
-w /etc/passwd -p wa -k identity
-w /etc/group -p wa -k identity
-w /etc/shadow -p wa -k identity
-w /etc/gshadow -p wa -k identity
-w /etc/security/opasswd -p wa -k identity
-w /etc/pam.d -p wa -k system-auth
-w /etc/nsswitch.conf -p wa -k system-auth
-w /etc/ssh/sshd_config -p wa -k system-auth
-a always,exit -F arch=b64 -S execve -F key=exec
-a always,exit -F arch=b32 -S execve -F key=exec
-w /usr/bin/sudo -p x -k privileged
-w /usr/bin/su -p x -k privileged
-w /usr/bin/passwd -p x -k privileged
-w /usr/bin/chage -p x -k privileged
-w /usr/bin/gpasswd -p x -k privileged
-w /usr/bin/chsh -p x -k privileged
-w /usr/bin/mount -p x -k privileged
-w /usr/bin/umount -p x -k privileged
-w /etc -p wa -k system-config
-w /var/log -p wa -k log-write
-w /usr/bin -p wa -k binary-modification
-w /usr/sbin -p wa -k binary-modification
-w /bin -p wa -k binary-modification
-w /sbin -p wa -k binary-modification
-a always,exit -F arch=b64 -S open,openat,open_by_handle_at -F exit=-EACCES -F key=access
-a always,exit -F arch=b32 -S open,openat,open_by_handle_at -F exit=-EACCES -F key=access
-a always,exit -F arch=b64 -S open,openat,open_by_handle_at -F exit=-EPERM -F key=access
-a always,exit -F arch=b32 -S open,openat,open_by_handle_at -F exit=-EPERM -F key=access
```

```
(icdfa@icdfa)-[~]
└─$ sudo python3 security_metrics.py
Security metrics generated. Report saved to security_metrics_report.txt
Visualizations saved as security_metrics_*.png
report.txt k_report.txt rics_auth_me rics_complia
└─$
```

- The security\_report.txt file generated by the daily monitoring script  
<https://drive.google.com/file/d/18lsjCb079w15wJkqwDraMd0c1gtVc6NT/view?usp=sharing>
- The security\_metrics\_report.txt file and associated visualizations  
[https://drive.google.com/file/d/1HZxqsAAv8rU9qTCN\\_wlzKSa8DItkRFA/view?usp=sharing](https://drive.google.com/file/d/1HZxqsAAv8rU9qTCN_wlzKSa8DItkRFA/view?usp=sharing)





Consistently checking and detecting deviations of critical controls are strategies for continuous monitoring that support security governance. Automated scripts collect integrity results (AIDE), audit findings (Lynis), and real-time intrusion prevention data (Fail2ban), making the security posture transparent. Scheduled cron jobs are used to ensure monitoring runs smoothly without human intervention, while simulation tests verify that alert triggers are correct. Monitoring enables organizations to detect risks faster and maintain compliance with governance frameworks.

**GROUP 2 NAMES**

<b>1</b>	<b>Gean Bernard</b>
<b>2</b>	<b>Khumo Tsoeu</b>
<b>3</b>	<b>Tosin Oyewole</b>
<b>4</b>	<b>Odion Shalom Ebosetale</b>
<b>5</b>	<b>Akinleye Abidat Bolanle</b>
<b>6</b>	<b>Comfort Tosin Olowookere</b>
<b>7</b>	<b>Muminat Lamidi</b>
<b>8</b>	<b>Vandana Mygapu</b>
<b>9</b>	<b>Precious Ogwumike</b>
<b>10</b>	<b>Nabirye Zahara</b>
<b>11</b>	<b>Dolapo Ajibade</b>
<b>12</b>	<b>Nneamaka Edwin</b>
<b>13</b>	<b>Adeola Bamigboye</b>
<b>14</b>	<b>Hussein Kaosara Dolapo</b>
<b>15</b>	<b>Tinyang Stacey Enjeck</b>
<b>16</b>	<b>Stella Oluwabukola Adejumo</b>
<b>17</b>	<b>Azeezat Animashaun</b>
<b>18</b>	<b>Taiwo Olasupo Owolebi</b>
<b>19</b>	<b>Ibrahim Zainab</b>
<b>20</b>	<b>Oluwatimilehin Oluwagbemi</b>
<b>21</b>	<b>Yusroh Titilayo Oduola</b>
<b>22</b>	<b>Olubukola Esther Obisanya</b>
<b>23</b>	<b>Linda Oluwadamilare Ogunsuyi</b>
<b>24</b>	<b>Rachael Gakanyi</b>
<b>25</b>	<b>Halima Abubakar</b>
<b>26</b>	<b>Magdalene Akpan</b>
<b>27</b>	<b>Ojeah Laura</b>