Task 12: Log Monitoring & Analysis (Kali Linux)

Objective

To monitor and analyze system logs in Kali Linux to detect authentication events, identify anomalies, and understand incident detection techniques.

Tool Used

- Kali Linux system logs (systemd journal)

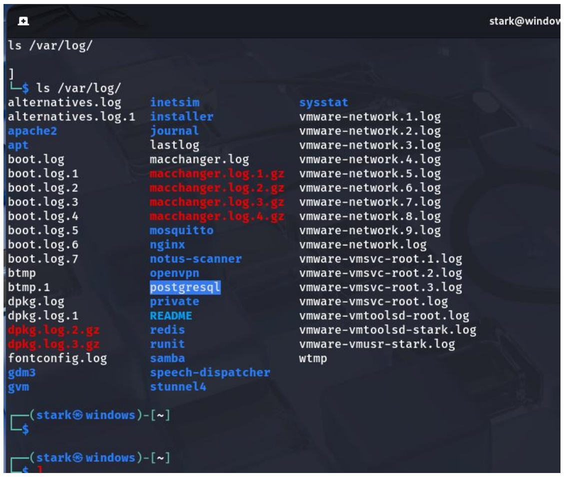
Log Storage in Kali Linux

In systemd-based Kali Linux, authentication and system logs are managed by **journald** instead of traditional auth.log files. Therefore, logs were analyzed using the journalctl command.

Log Monitoring & Analysis Steps

1. Accessing Log Files

System log files were explored from the /var/log/ directory to understand available log sources.



stark@windo

```
ls /var/log/

]
└─$ ls /var/log/
alternatives.log    inetsim              sysstat
alternatives.log.1  installer            vmware-network.1.log
apache2             journal              vmware-network.2.log
apt                 lastlog              vmware-network.3.log
boot.log            macchanger.log       vmware-network.4.log
boot.log.1          macchanger.log.1.gz  vmware-network.5.log
boot.log.2          macchanger.log.2.gz  vmware-network.6.log
boot.log.3          macchanger.log.3.gz  vmware-network.7.log
boot.log.4          macchanger.log.4.gz  vmware-network.8.log
boot.log.5          mosquitto            vmware-network.9.log
boot.log.6          nginx                vmware-network.log
boot.log.7          notus-scanner        vmware-vmsvc-root.1.log
btmp                openvpn              vmware-vmsvc-root.2.log
btmp.1              postgresql           vmware-vmsvc-root.3.log
dpkg.log            private              vmware-vmsvc-root.log
dpkg.log.1          README               vmware-vmtoolsd-root.log
dpkg.log.2.gz       redis                vmware-vmtoolsd-stark.log
dpkg.log.3.gz       runit                vmware-vmusr-stark.log
fontconfig.log      samba                wtmp
gdm3                speech-dispatcher
gvm                 stunnel4

┌──(stark㉿windows)-[~]
└─$

┌──(stark㉿windows)-[~]
```

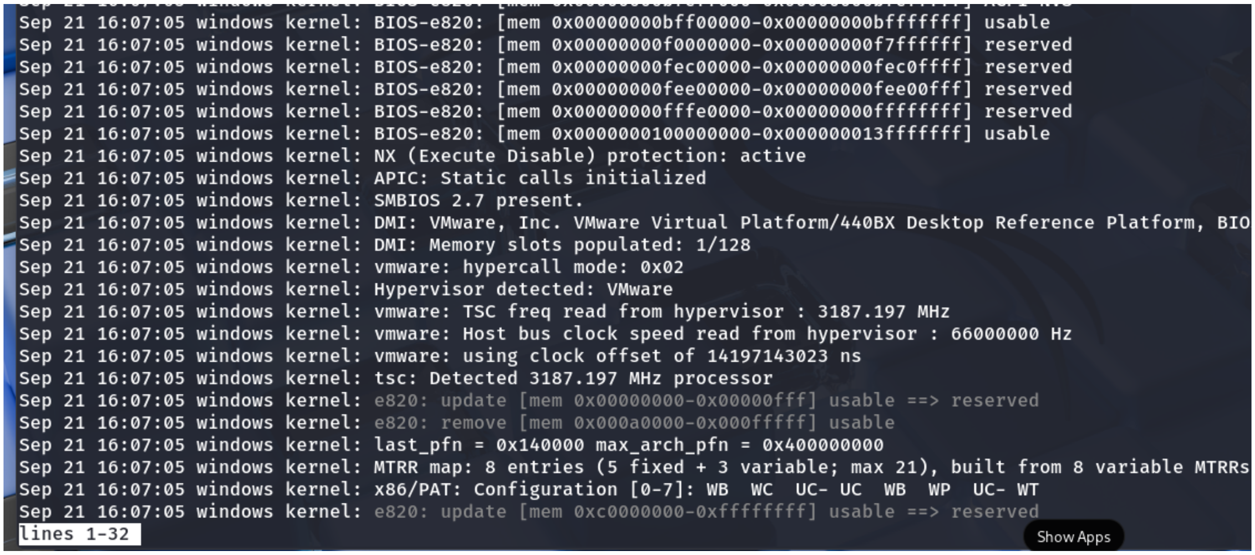
---

2. Analyzing System Logs Using journalctl

The systemd journal was accessed to view detailed system and security events.

Command used:

sudo journalctl



```
Sep 21 16:07:05 windows kernel: BIOS-e820: [mem 0x00000000bff00000-0x00000000bfffffff] usable
Sep 21 16:07:05 windows kernel: BIOS-e820: [mem 0x00000000f0000000-0x00000000f7ffffff] reserved
Sep 21 16:07:05 windows kernel: BIOS-e820: [mem 0x00000000fec00000-0x00000000fec0ffff] reserved
Sep 21 16:07:05 windows kernel: BIOS-e820: [mem 0x00000000fee00000-0x00000000fee00fff] reserved
Sep 21 16:07:05 windows kernel: BIOS-e820: [mem 0x00000000fffe0000-0x00000000ffffffff] reserved
Sep 21 16:07:05 windows kernel: BIOS-e820: [mem 0x0000000100000000-0x000000013fffffff] usable
Sep 21 16:07:05 windows kernel: NX (Execute Disable) protection: active
Sep 21 16:07:05 windows kernel: APIC: Static calls initialized
Sep 21 16:07:05 windows kernel: SMBIOS 2.7 present.
Sep 21 16:07:05 windows kernel: DMI: VMware, Inc. VMware Virtual Platform/440BX Desktop Reference Platform, BIO
Sep 21 16:07:05 windows kernel: DMI: Memory slots populated: 1/128
Sep 21 16:07:05 windows kernel: vmware: hypercall mode: 0x02
Sep 21 16:07:05 windows kernel: Hypervisor detected: VMware
Sep 21 16:07:05 windows kernel: vmware: TSC freq read from hypervisor : 3187.197 MHz
Sep 21 16:07:05 windows kernel: vmware: Host bus clock speed read from hypervisor : 66000000 Hz
Sep 21 16:07:05 windows kernel: vmware: using clock offset of 14197143023 ns
Sep 21 16:07:05 windows kernel: tsc: Detected 3187.197 MHz processor
Sep 21 16:07:05 windows kernel: e820: update [mem 0x00000000-0x00000fff] usable ==> reserved
Sep 21 16:07:05 windows kernel: e820: remove [mem 0x000a0000-0x000fffff] usable
Sep 21 16:07:05 windows kernel: last_pfn = 0x140000 max_arch_pfn = 0x400000000
Sep 21 16:07:05 windows kernel: MTRR map: 8 entries (5 fixed + 3 variable; max 21), built from 8 variable MTRRs
Sep 21 16:07:05 windows kernel: x86/PAT: Configuration [0-7]: WB  WC  UC- UC  WB  WP  UC- WT
Sep 21 16:07:05 windows kernel: e820: update [mem 0xc0000000-0xffffffff] usable ==> reserved
lines 1-32
```

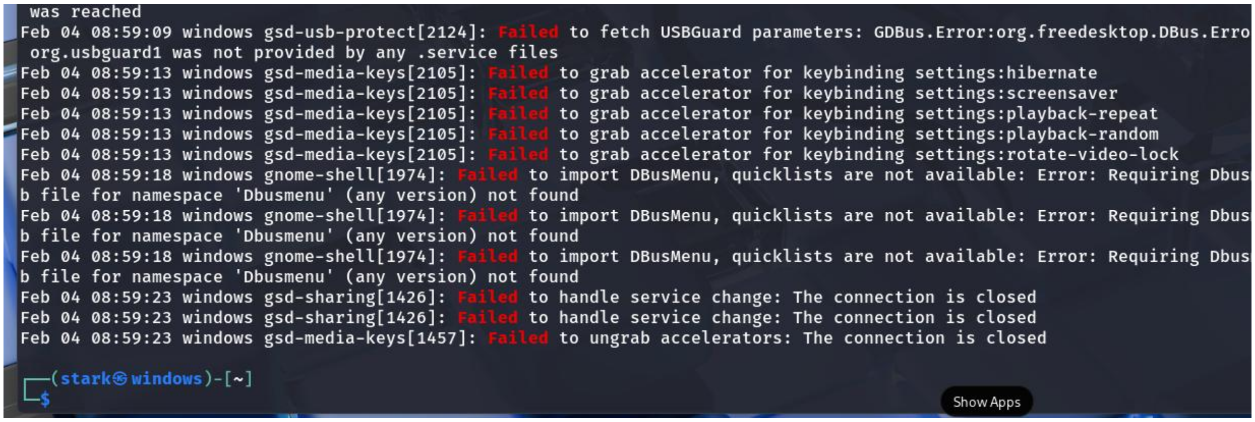
---

3. Identifying Failed Login Attempts

Failed authentication attempts were identified by filtering log entries.

Command used:

sudo journalctl | grep Failed



```
 was reached
Feb 04 08:59:09 windows gsd-usb-protect[2124]: Failed to fetch USBGuard parameters: GDBus.Error:org.freedesktop.DBus.Erro
 org.usbguard1 was not provided by any .service files
Feb 04 08:59:13 windows gsd-media-keys[2105]: Failed to grab accelerator for keybinding settings:hibernate
Feb 04 08:59:13 windows gsd-media-keys[2105]: Failed to grab accelerator for keybinding settings:screensaver
Feb 04 08:59:13 windows gsd-media-keys[2105]: Failed to grab accelerator for keybinding settings:playback-repeat
Feb 04 08:59:13 windows gsd-media-keys[2105]: Failed to grab accelerator for keybinding settings:playback-random
Feb 04 08:59:13 windows gsd-media-keys[2105]: Failed to grab accelerator for keybinding settings:rotate-video-lock
Feb 04 08:59:18 windows gnome-shell[1974]: Failed to import DBusMenu, quicklists are not available: Error: Requiring Dbus
b file for namespace 'Dbusmenu' (any version) not found
Feb 04 08:59:18 windows gnome-shell[1974]: Failed to import DBusMenu, quicklists are not available: Error: Requiring Dbus
b file for namespace 'Dbusmenu' (any version) not found
Feb 04 08:59:18 windows gnome-shell[1974]: Failed to import DBusMenu, quicklists are not available: Error: Requiring Dbus
b file for namespace 'Dbusmenu' (any version) not found
Feb 04 08:59:23 windows gsd-sharing[1426]: Failed to handle service change: The connection is closed
Feb 04 08:59:23 windows gsd-sharing[1426]: Failed to handle service change: The connection is closed
Feb 04 08:59:23 windows gsd-media-keys[1457]: Failed to ungrab accelerators: The connection is closed

┌──(stark㉿windows)-[~]
└─$
```

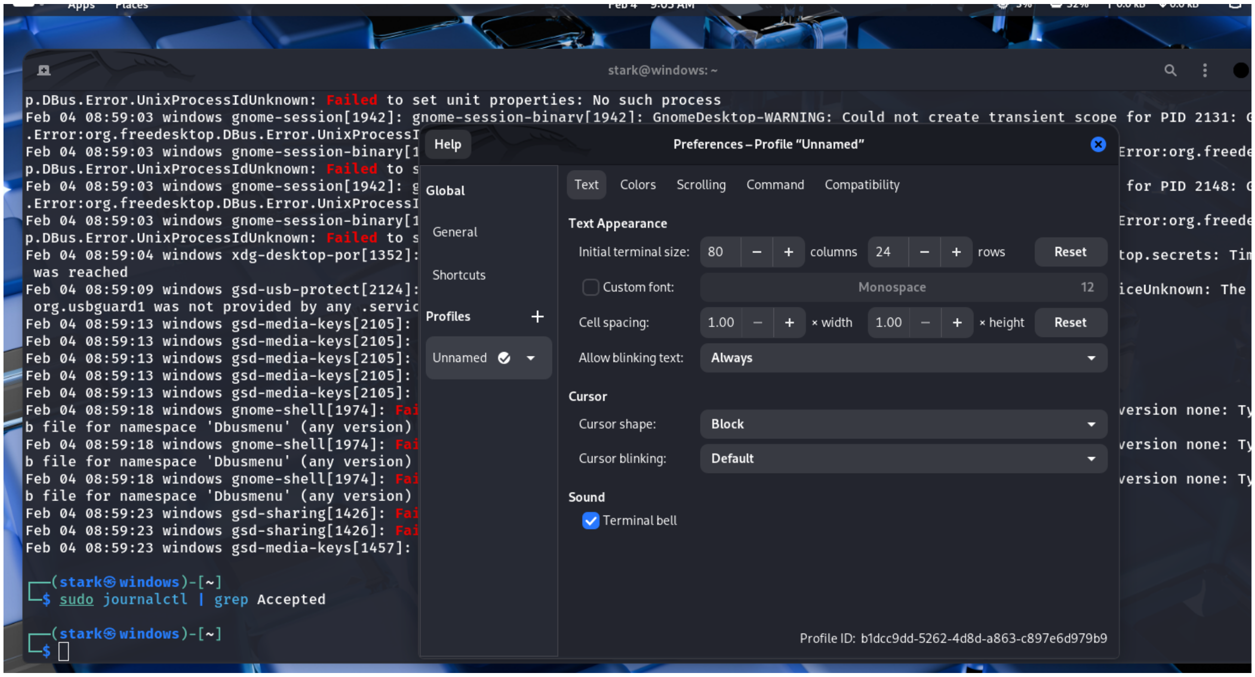
---

4. Identifying Successful Login Attempts

Successful authentication events were analyzed to understand normal user behavior.

Command used:

sudo journalctl | grep Accepted



```
p.DBus.Error.UnixProcessIdUnknown: Failed to set unit properties: No such process
Feb 04 08:59:03 windows gnome-session[1942]: gnome-session-binary[1942]: GnomeDesktop-WARNING: Could not create transient scope for PID 2131: G
.Error:org.freedesktop.DBus.Error.UnixProcessI
Feb 04 08:59:03 windows gnome-session-binary[1                                                         Error:org.freede
p.DBus.Error.UnixProcessIdUnknown: Failed to s
Feb 04 08:59:03 windows gnome-session[1942]: g                                                          for PID 2148: G
.Error:org.freedesktop.DBus.Error.UnixProcessI
Feb 04 08:59:03 windows gnome-session-binary[1                                                         Error:org.freede
p.DBus.Error.UnixProcessIdUnknown: Failed to s
Feb 04 08:59:04 windows xdg-desktop-por[1352]:                                                         top.secrets: Tim
 was reached
Feb 04 08:59:09 windows gsd-usb-protect[2124]:                                                         iceUnknown: The
 org.usbguard1 was not provided by any .servic
Feb 04 08:59:13 windows gsd-media-keys[2105]:
Feb 04 08:59:13 windows gsd-media-keys[2105]:
Feb 04 08:59:13 windows gsd-media-keys[2105]:
Feb 04 08:59:13 windows gsd-media-keys[2105]:
Feb 04 08:59:13 windows gsd-media-keys[2105]:
Feb 04 08:59:18 windows gnome-shell[1974]: Fai                                                         version none: Ty
b file for namespace 'Dbusmenu' (any version)
Feb 04 08:59:18 windows gnome-shell[1974]: Fai                                                         version none: Ty
b file for namespace 'Dbusmenu' (any version)
Feb 04 08:59:18 windows gnome-shell[1974]: Fai                                                         version none: Ty
b file for namespace 'Dbusmenu' (any version)
Feb 04 08:59:23 windows gsd-sharing[1426]: Fai
Feb 04 08:59:23 windows gsd-sharing[1426]: Fai
Feb 04 08:59:23 windows gsd-media-keys[1457]:

┌──(stark㉿windows)-[~]
└─$ sudo journalctl | grep Accepted

┌──(stark㉿windows)-[~]
└─$ 
```

Preferences – Profile "Unnamed"

Text Appearance

Initial terminal size: 80 columns 24 rows Reset

□ Custom font: Monospace 12

Cell spacing: 1.00 × width 1.00 × height Reset

Allow blinking text: Always

Cursor

Cursor shape: Block

Cursor blinking: Default

Sound

☑ Terminal bell

Profile ID: b1dcc9dd-5262-4d8d-a863-c897e6d979b9

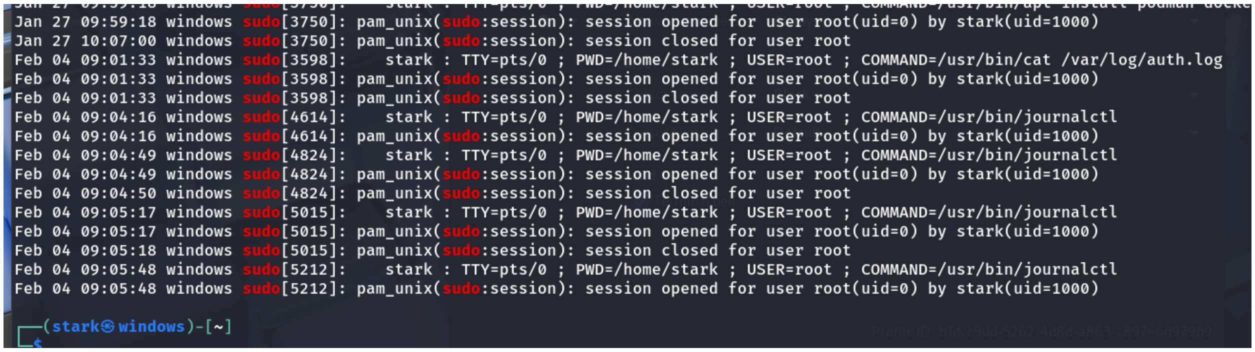
---

5. Monitoring sudo Activity

sudo command usage was reviewed to track privileged access attempts.

Command used:

sudo journalctl | grep sudo



```
Jan 27 09:59:18 windows sudo[3750]:    stark : TTY=pts/0 ; PWD=/home/stark ; USER=root ; COMMAND=/usr/bin/apt install podman docke
Jan 27 09:59:18 windows sudo[3750]: pam_unix(sudo:session): session opened for user root(uid=0) by stark(uid=1000)
Jan 27 10:07:00 windows sudo[3750]: pam_unix(sudo:session): session closed for user root
Feb 04 09:01:33 windows sudo[3598]:    stark : TTY=pts/0 ; PWD=/home/stark ; USER=root ; COMMAND=/usr/bin/cat /var/log/auth.log
Feb 04 09:01:33 windows sudo[3598]: pam_unix(sudo:session): session opened for user root(uid=0) by stark(uid=1000)
Feb 04 09:01:33 windows sudo[3598]: pam_unix(sudo:session): session closed for user root
Feb 04 09:04:16 windows sudo[4614]:    stark : TTY=pts/0 ; PWD=/home/stark ; USER=root ; COMMAND=/usr/bin/journalctl
Feb 04 09:04:16 windows sudo[4614]: pam_unix(sudo:session): session opened for user root(uid=0) by stark(uid=1000)
Feb 04 09:04:49 windows sudo[4824]:    stark : TTY=pts/0 ; PWD=/home/stark ; USER=root ; COMMAND=/usr/bin/journalctl
Feb 04 09:04:49 windows sudo[4824]: pam_unix(sudo:session): session opened for user root(uid=0) by stark(uid=1000)
Feb 04 09:04:50 windows sudo[4824]: pam_unix(sudo:session): session closed for user root
Feb 04 09:05:17 windows sudo[5015]:    stark : TTY=pts/0 ; PWD=/home/stark ; USER=root ; COMMAND=/usr/bin/journalctl
Feb 04 09:05:17 windows sudo[5015]: pam_unix(sudo:session): session opened for user root(uid=0) by stark(uid=1000)
Feb 04 09:05:18 windows sudo[5015]: pam_unix(sudo:session): session closed for user root
Feb 04 09:05:48 windows sudo[5212]:    stark : TTY=pts/0 ; PWD=/home/stark ; USER=root ; COMMAND=/usr/bin/journalctl
Feb 04 09:05:48 windows sudo[5212]: pam_unix(sudo:session): session opened for user root(uid=0) by stark(uid=1000)

┌──(stark㉿windows)-[~]
└─$
```

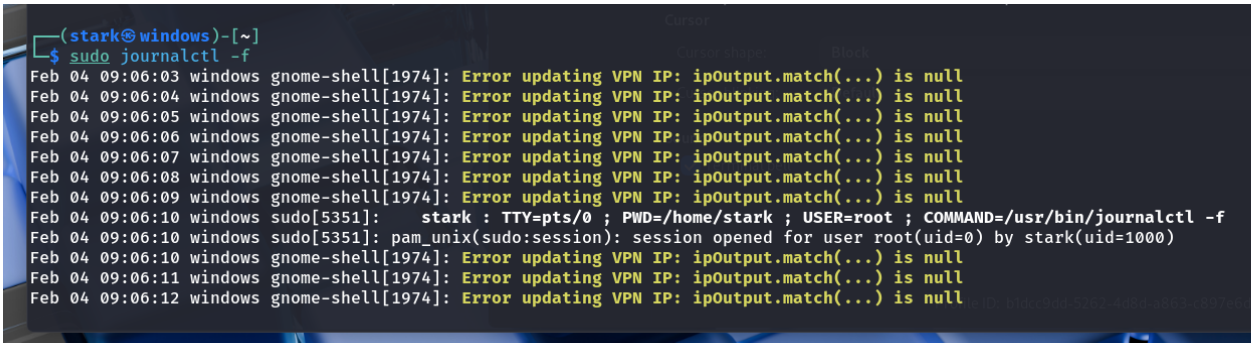
---

6. Monitoring Logs in Real Time

Logs were monitored in real time to observe live system events.

Command used:

sudo journalctl -f



```
┌──(stark㉿windows)-[~]
└─$ sudo journalctl -f
Feb 04 09:06:03 windows gnome-shell[1974]: Error updating VPN IP: ipOutput.match(...) is null
Feb 04 09:06:04 windows gnome-shell[1974]: Error updating VPN IP: ipOutput.match(...) is null
Feb 04 09:06:05 windows gnome-shell[1974]: Error updating VPN IP: ipOutput.match(...) is null
Feb 04 09:06:06 windows gnome-shell[1974]: Error updating VPN IP: ipOutput.match(...) is null
Feb 04 09:06:07 windows gnome-shell[1974]: Error updating VPN IP: ipOutput.match(...) is null
Feb 04 09:06:08 windows gnome-shell[1974]: Error updating VPN IP: ipOutput.match(...) is null
Feb 04 09:06:09 windows gnome-shell[1974]: Error updating VPN IP: ipOutput.match(...) is null
Feb 04 09:06:10 windows sudo[5351]:    stark : TTY=pts/0 ; PWD=/home/stark ; USER=root ; COMMAND=/usr/bin/journalctl -f
Feb 04 09:06:10 windows sudo[5351]: pam_unix(sudo:session): session opened for user root(uid=0) by stark(uid=1000)
Feb 04 09:06:10 windows gnome-shell[1974]: Error updating VPN IP: ipOutput.match(...) is null
Feb 04 09:06:11 windows gnome-shell[1974]: Error updating VPN IP: ipOutput.match(...) is null
Feb 04 09:06:12 windows gnome-shell[1974]: Error updating VPN IP: ipOutput.match(...) is null
```

---

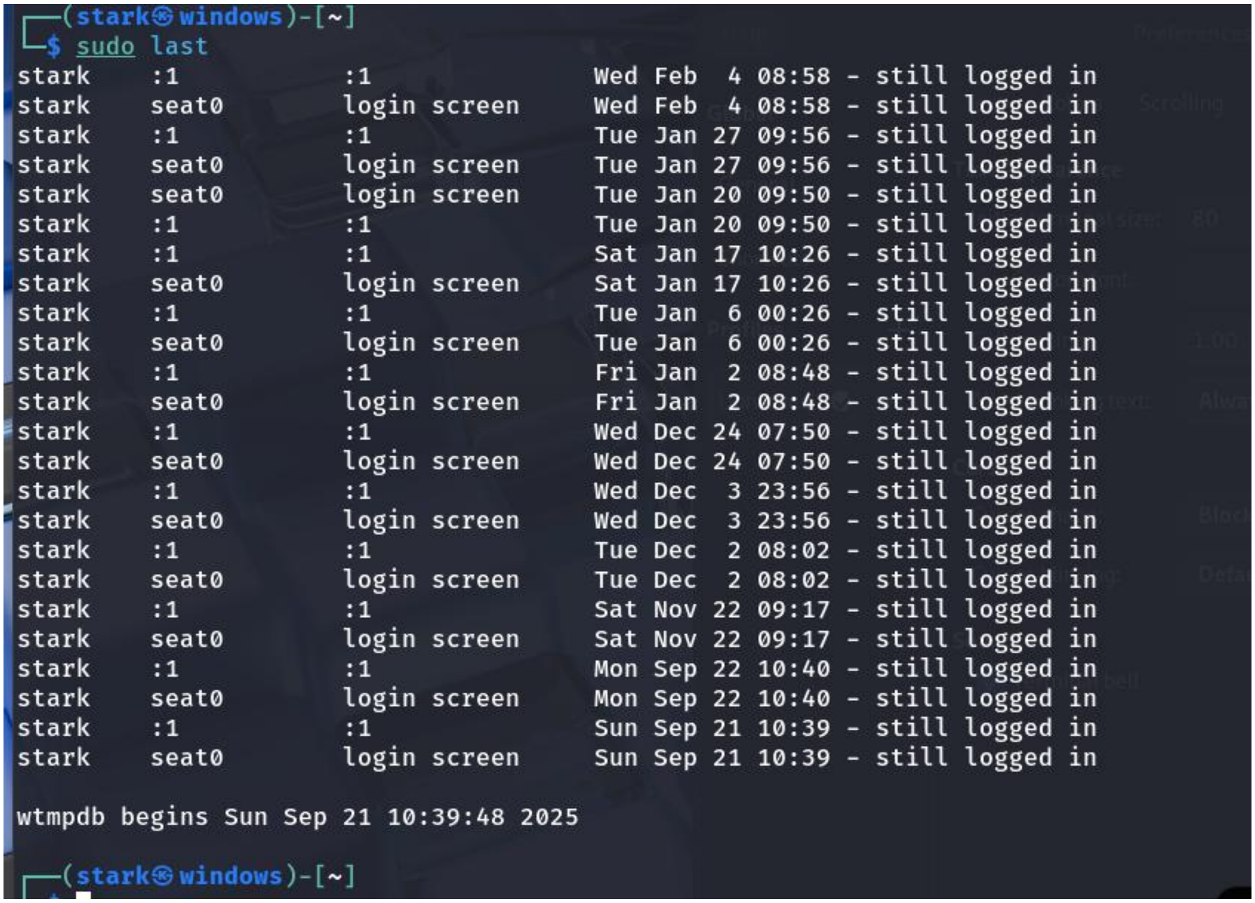
7. Reviewing Login History

User login history was reviewed to identify past successful and failed logins.

Commands used:

last

sudo lastb



```
┌──(stark㉿windows)-[~]
└─$ sudo last
stark    :1           :1                Wed Feb  4 08:58 - still logged in
stark    seat0        login screen      Wed Feb  4 08:58 - still logged in
stark    :1           :1                Tue Jan 27 09:56 - still logged in
stark    seat0        login screen      Tue Jan 27 09:56 - still logged in
stark    seat0        login screen      Tue Jan 20 09:50 - still logged in
stark    :1           :1                Tue Jan 20 09:50 - still logged in
stark    :1           :1                Sat Jan 17 10:26 - still logged in
stark    seat0        login screen      Sat Jan 17 10:26 - still logged in
stark    :1           :1                Tue Jan  6 00:26 - still logged in
stark    seat0        login screen      Tue Jan  6 00:26 - still logged in
stark    :1           :1                Fri Jan  2 08:48 - still logged in
stark    seat0        login screen      Fri Jan  2 08:48 - still logged in
stark    :1           :1                Wed Dec 24 07:50 - still logged in
stark    seat0        login screen      Wed Dec 24 07:50 - still logged in
stark    :1           :1                Wed Dec  3 23:56 - still logged in
stark    seat0        login screen      Wed Dec  3 23:56 - still logged in
stark    :1           :1                Tue Dec  2 08:02 - still logged in
stark    seat0        login screen      Tue Dec  2 08:02 - still logged in
stark    :1           :1                Sat Nov 22 09:17 - still logged in
stark    seat0        login screen      Sat Nov 22 09:17 - still logged in
stark    :1           :1                Mon Sep 22 10:40 - still logged in
stark    seat0        login screen      Mon Sep 22 10:40 - still logged in
stark    :1           :1                Sun Sep 21 10:39 - still logged in
stark    seat0        login screen      Sun Sep 21 10:39 - still logged in

wtmpdb begins Sun Sep 21 10:39:48 2025

┌──(stark㉿windows)-[~]
```

Observations

- systemd journal contains detailed authentication and system logs
- Multiple failed login attempts may indicate brute-force attacks
- sudo logs help track privileged access
- Real-time monitoring assists in early incident detection

Deliverable

Log Analysis Report including:

- Logs analyzed
- Commands used

- Screenshots
- Observations

Final Outcome

Developed incident detection skills by monitoring and analyzing Kali Linux logs using systemd journal and identifying suspicious authentication activities.