Syslog analysis on linux systems

Project overview

In this project I will be performing syslog analysis on a linux system (ubuntu).Syslog is a standard logging protocol that collects and stores log messages from various system processes and applications. The primary objectives of the project were to configure syslog, access and interpret log files, and analyze log data for troubleshooting and security monitoring.

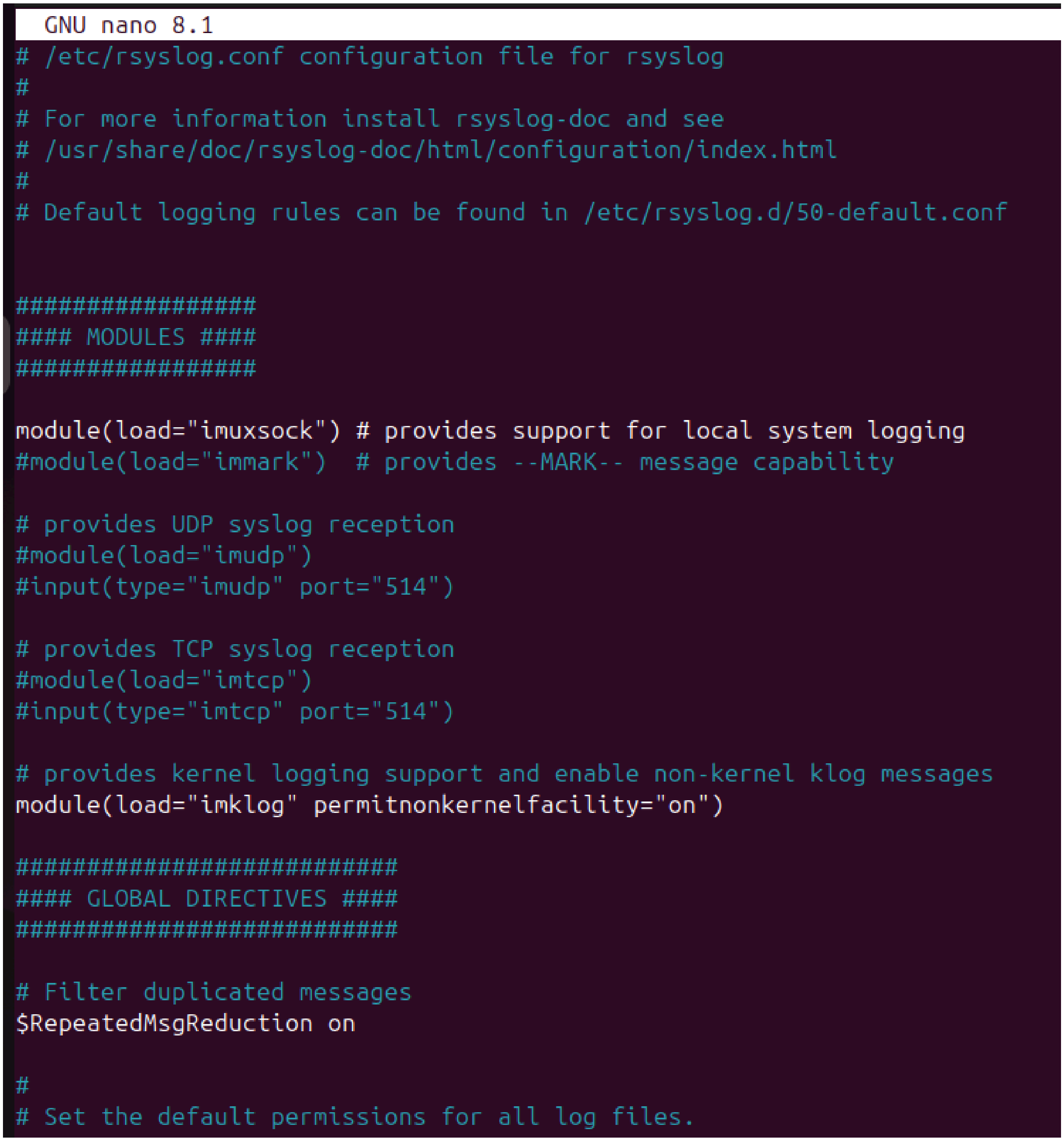
This project provided me with hands-on experience in understanding syslog configuration, exploring system logs, filtering log data, and performing detailed analysis of authentication logs.

Lab Setup and Tools

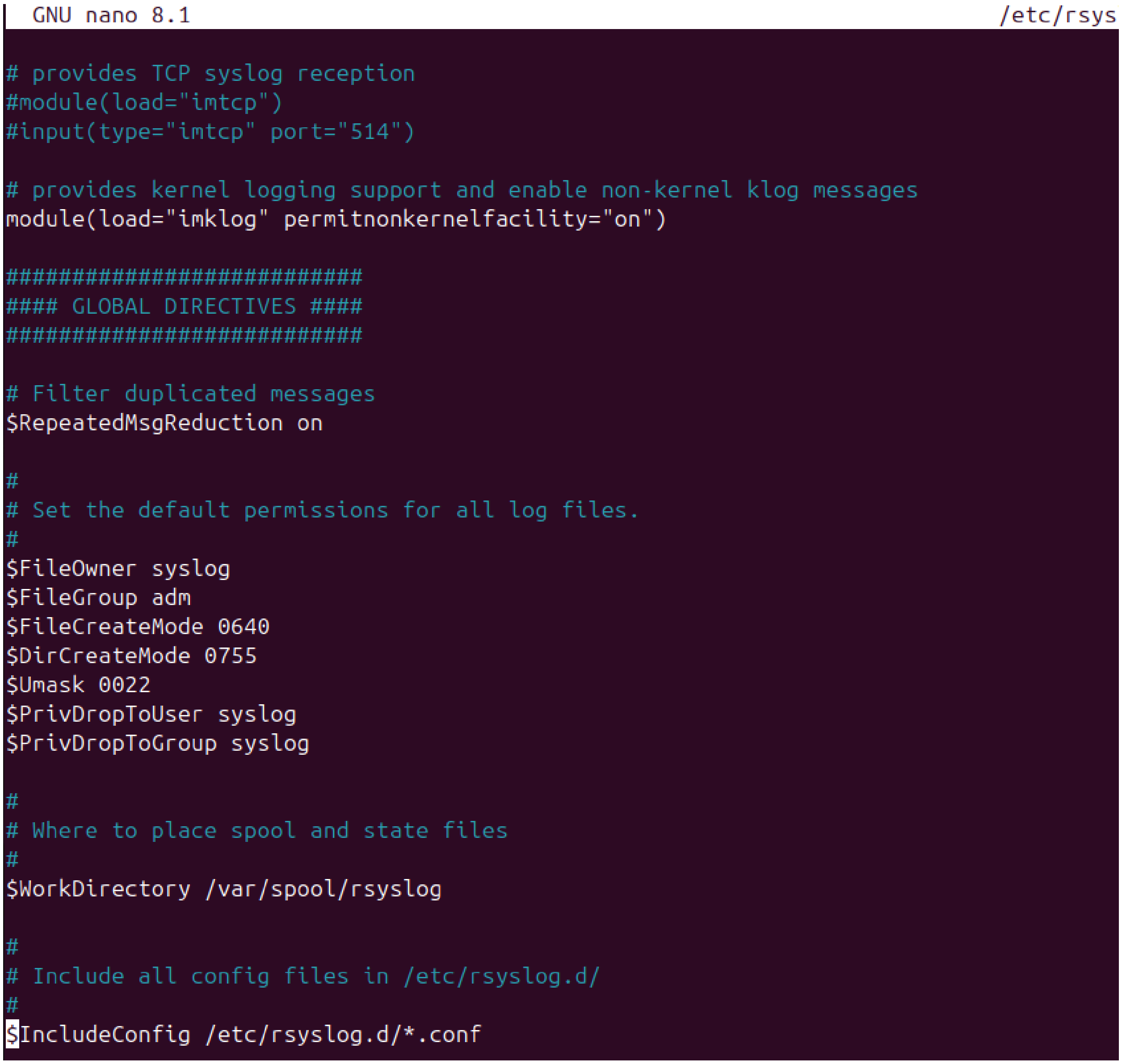
- Operating System: Ubuntu 20.04
- Syslog Files Location: `/var/log/`
- Tools Used: Built-in Linux tools such as nano, grep, awk, and less.

Understanding syslog configuration

I explored the syslog configuration file to understand how logging is set up and identified the various logging facilities and their corresponding log files by using the command `sudo nano /etc/rsyslog.conf` . This opens the rsyslog configuration file in the nano editor



```
  GNU nano 8.1
# /etc/rsyslog.conf configuration file for rsyslog
#
# For more information install rsyslog-doc and see
# /usr/share/doc/rsyslog-doc/html/configuration/index.html
#
# Default logging rules can be found in /etc/rsyslog.d/50-default.conf


#################
#### MODULES ####
#################

module(load="imuxsock") # provides support for local system logging
#module(load="immark")  # provides --MARK-- message capability

# provides UDP syslog reception
#module(load="imudp")
#input(type="imudp" port="514")

# provides TCP syslog reception
#module(load="imtcp")
#input(type="imtcp" port="514")

# provides kernel logging support and enable non-kernel klog messages
module(load="imklog" permitnonkernelfacility="on")

###########################
#### GLOBAL DIRECTIVES ####
###########################

# Filter duplicated messages
$RepeatedMsgReduction on

#
# Set the default permissions for all log files.
```



```
# provides TCP syslog reception
#module(load="imtcp")
#input(type="imtcp" port="514")

# provides kernel logging support and enable non-kernel klog messages
module(load="imklog" permitnonkernelfacility="on")

###########################
#### GLOBAL DIRECTIVES ####
###########################

# Filter duplicated messages
$RepeatedMsgReduction on

#
# Set the default permissions for all log files.
#
$FileOwner syslog
$FileGroup adm
$FileCreateMode 0640
$DirCreateMode 0755
$Umask 0022
$PrivDropToUser syslog
$PrivDropToGroup syslog

#
# Where to place spool and state files
#
$WorkDirectory /var/spool/rsyslog

#
# Include all config files in /etc/rsyslog.d/
#
$IncludeConfig /etc/rsyslog.d/*.conf
```

Here’s a **brief explanation** of the contents of /etc/rsyslog.conf, section by section:

1. Comments

- Lines starting with # are comments. They provide explanations or documentation.

2. Modules

- Modules add functionality to rsyslog. Examples:
    - module(load="imuxsock"): Enables logging for local applications and the system (e.g., logs generated by the syslog service).

    - #module(load="imudp"): (Commented out) Adds support for receiving syslog messages over UDP protocol on port 514.
    - #module(load="imtcp"): (Commented out) Adds support for receiving syslog messages over TCP protocol on port 514.
    - module(load="imklog"): Handles kernel log messages (e.g., messages generated by the Linux kernel).

3. Global Directives

These set global behavior for rsyslog:

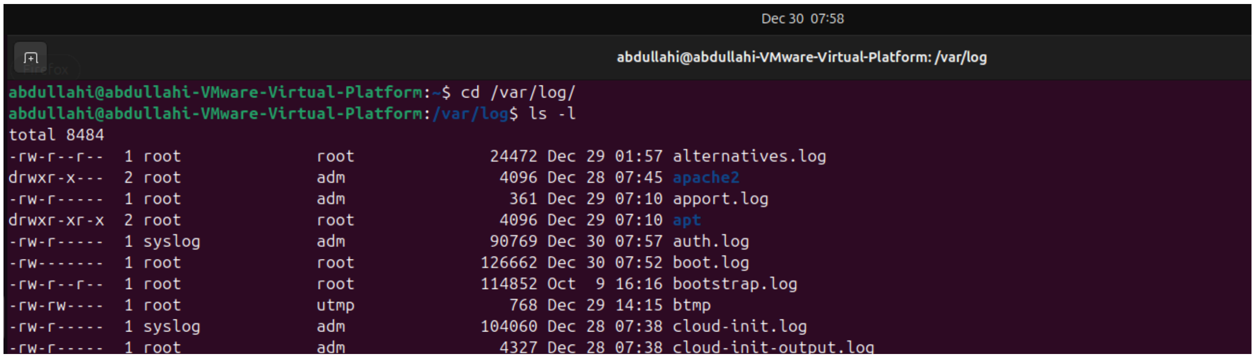
- $RepeatedMsgReduction on: Prevents duplicate log messages from being logged repeatedly.
- $FileOwner syslog and $FileGroup adm: Sets the owner and group of log files.
- $FileCreateMode 0640: Sets the default permissions for log files (rw-r-----).
- $DirCreateMode 0755: Sets permissions for log directories (rwxr-xr-x).
- $WorkDirectory /var/spool/rsyslog: Specifies where temporary and state files are stored.

4. Include Other Configurations

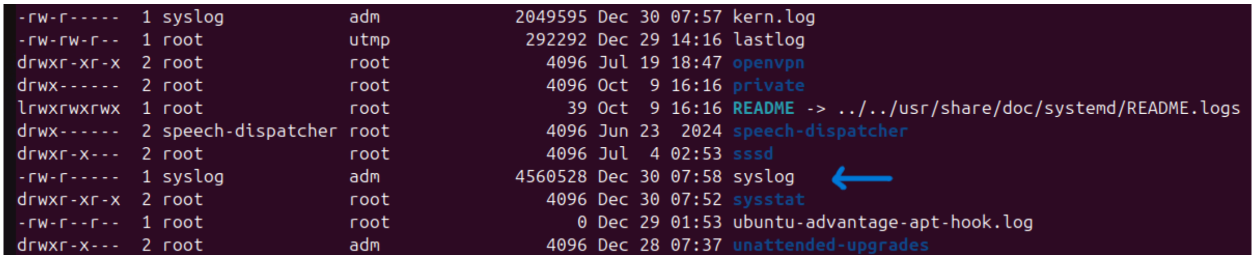
- $IncludeConfig /etc/rsyslog.d/*.conf: This includes additional configuration files from the /etc/rsyslog.d/ directory. It allows splitting configurations into smaller, modular files.

Accessing syslog files

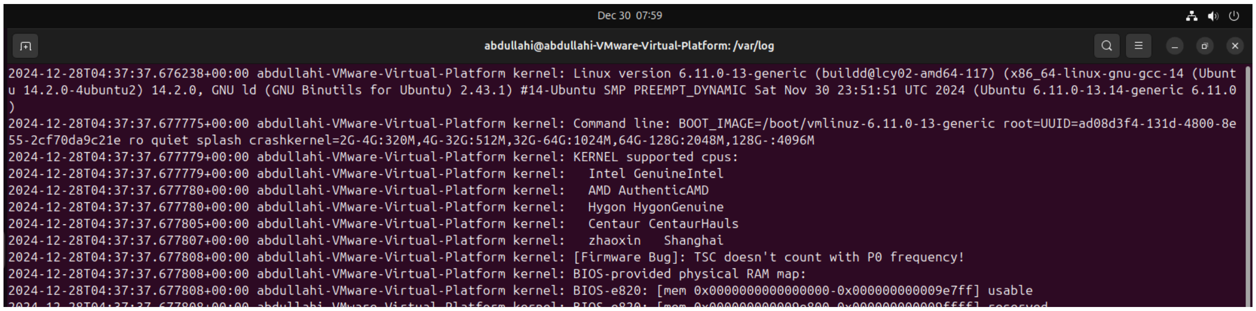
I accessed the syslog directory and examined the log files by Navigated to the syslog directory,listed the available syslog files and Opened the main syslog file using the command `less syslog`



```
abdullahi@abdullahi-VMware-Virtual-Platform:~$ cd /var/log/
abdullahi@abdullahi-VMware-Virtual-Platform:/var/log$ ls -l
total 8484
-rw-r--r--  1 root              root          24472 Dec 29 01:57 alternatives.log
drwxr-x---  2 root              adm            4096 Dec 28 07:45 apache2
-rw-r-----  1 root              adm             361 Dec 29 07:10 apport.log
drwxr-xr-x  2 root              root           4096 Dec 29 07:10 apt
-rw-r-----  1 syslog            adm           90769 Dec 30 07:57 auth.log
-rw-------  1 root              root         126662 Dec 30 07:52 boot.log
-rw-r--r--  1 root              root         114852 Oct  9 16:16 bootstrap.log
-rw-rw----  1 root              utmp            768 Dec 29 14:15 btmp
-rw-r-----  1 syslog            adm          104060 Dec 28 07:38 cloud-init.log
-rw-r-----  1 root              adm            4327 Dec 28 07:38 cloud-init-output.log
```



```
-rw-r-----  1 syslog            adm         2049595 Dec 30 07:57 kern.log
-rw-rw-r--  1 root              utmp         292292 Dec 29 14:16 lastlog
drwxr-xr-x  2 root              root           4096 Jul 19 18:47 openvpn
drwx------  2 root              root           4096 Oct  9 16:16 private
lrwxrwxrwx  1 root              root             39 Oct  9 16:16 README -> ../../usr/share/doc/systemd/README.logs
drwx------  2 speech-dispatcher root           4096 Jun 23  2024 speech-dispatcher
drwxr-x---  2 root              root           4096 Jul  4 02:53 sssd
-rw-r-----  1 syslog            adm         4560528 Dec 30 07:58 syslog
drwxr-xr-x  2 root              root           4096 Dec 30 07:52 sysstat
-rw-r--r--  1 root              root              0 Dec 29 01:53 ubuntu-advantage-apt-hook.log
drwxr-x---  2 root              adm            4096 Dec 28 07:37 unattended-upgrades
```



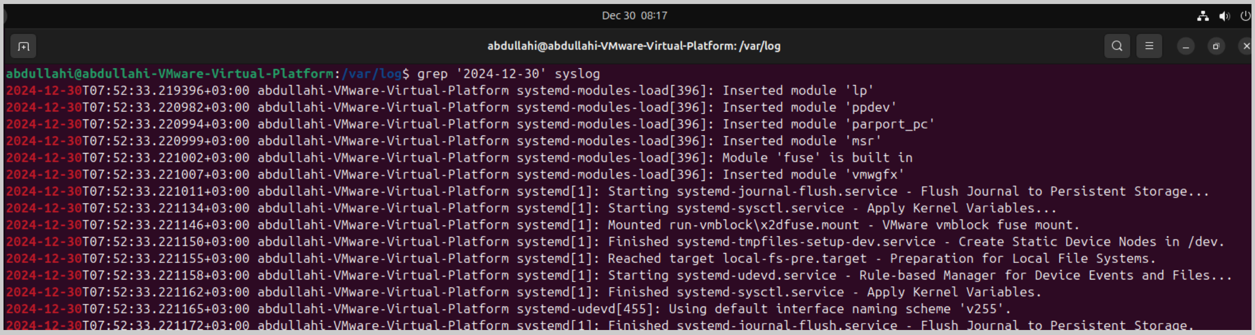
```
2024-12-28T04:37:37.676238+00:00 abdullahi-VMware-Virtual-Platform kernel: Linux version 6.11.0-13-generic (buildd@lcy02-amd64-117) (x86_64-linux-gnu-gcc-14 (Ubunt
u 14.2.0-4ubuntu2) 14.2.0, GNU ld (GNU Binutils for Ubuntu) 2.43.1) #14-Ubuntu SMP PREEMPT_DYNAMIC Sat Nov 30 23:51:51 UTC 2024 (Ubuntu 6.11.0-13.14-generic 6.11.0
)
2024-12-28T04:37:37.677775+00:00 abdullahi-VMware-Virtual-Platform kernel: Command line: BOOT_IMAGE=/boot/vmlinuz-6.11.0-13-generic root=UUID=ad08d3f4-131d-4800-8e
55-2cf70da9c21e ro quiet splash crashkernel=2G-4G:320M,4G-32G:512M,32G-64G:1024M,64G-128G:2048M,128G-:4096M
2024-12-28T04:37:37.677779+00:00 abdullahi-VMware-Virtual-Platform kernel: KERNEL supported cpus:
2024-12-28T04:37:37.677779+00:00 abdullahi-VMware-Virtual-Platform kernel:   Intel GenuineIntel
2024-12-28T04:37:37.677780+00:00 abdullahi-VMware-Virtual-Platform kernel:   AMD AuthenticAMD
2024-12-28T04:37:37.677780+00:00 abdullahi-VMware-Virtual-Platform kernel:   Hygon HygonGenuine
2024-12-28T04:37:37.677805+00:00 abdullahi-VMware-Virtual-Platform kernel:   Centaur CentaurHauls
2024-12-28T04:37:37.677807+00:00 abdullahi-VMware-Virtual-Platform kernel:   zhaoxin   Shanghai
2024-12-28T04:37:37.677808+00:00 abdullahi-VMware-Virtual-Platform kernel: [Firmware Bug]: TSC doesn't count with P0 frequency!
2024-12-28T04:37:37.677808+00:00 abdullahi-VMware-Virtual-Platform kernel: BIOS-provided physical RAM map:
2024-12-28T04:37:37.677808+00:00 abdullahi-VMware-Virtual-Platform kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000009e7ff] usable
2024-12-28T04:37:37.677808+00:00 abdullahi-VMware-Virtual-Platform kernel: BIOS-e820: [mem 0x000000000009e800-0x000000000009ffff] reserved
```

Findings

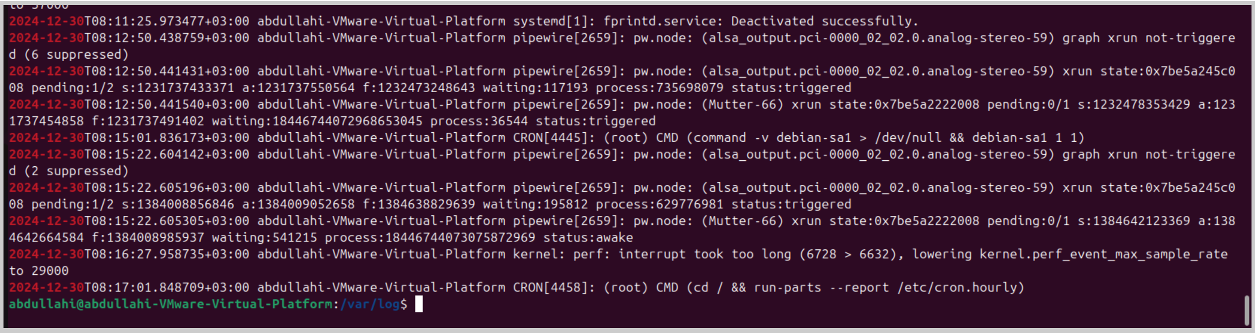
- Discovered various log files, including syslog and auth.log.
- The syslog file contains general system logs.

Filtering syslog entries

I filtered syslog entries to extract specific information, such as logs for a particular date or process by using grep command which allows searching for specific patterns in the log file. For example, to filter logs for a specific date like "2024-12-29," I used the command: `grep '2024-12-29' syslog`



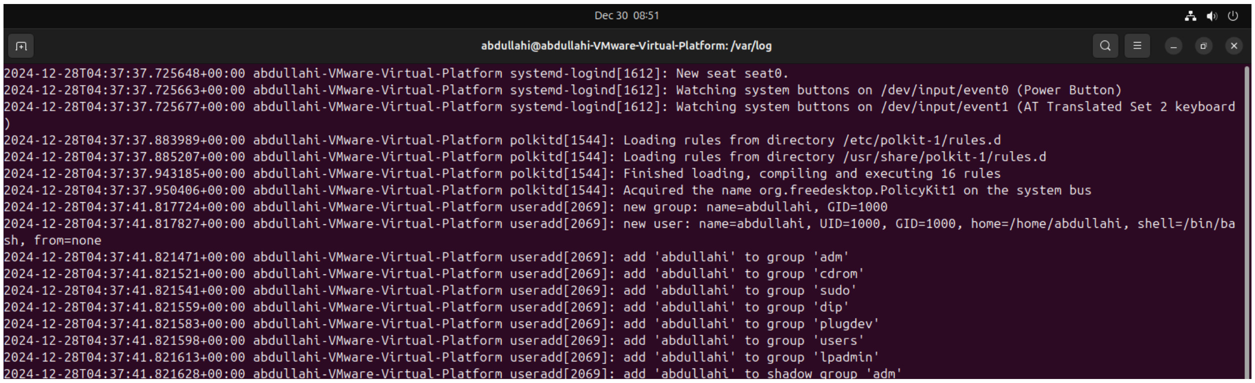
```
abdullahi@abdullahi-VMware-Virtual-Platform:/var/log$ grep '2024-12-30' syslog
2024-12-30T07:52:33.219396+03:00 abdullahi-VMware-Virtual-Platform systemd-modules-load[396]: Inserted module 'lp'
2024-12-30T07:52:33.220982+03:00 abdullahi-VMware-Virtual-Platform systemd-modules-load[396]: Inserted module 'ppdev'
2024-12-30T07:52:33.220994+03:00 abdullahi-VMware-Virtual-Platform systemd-modules-load[396]: Inserted module 'parport_pc'
2024-12-30T07:52:33.220999+03:00 abdullahi-VMware-Virtual-Platform systemd-modules-load[396]: Inserted module 'msr'
2024-12-30T07:52:33.221002+03:00 abdullahi-VMware-Virtual-Platform systemd-modules-load[396]: Module 'fuse' is built in
2024-12-30T07:52:33.221007+03:00 abdullahi-VMware-Virtual-Platform systemd-modules-load[396]: Inserted module 'vmwgfx'
2024-12-30T07:52:33.221011+03:00 abdullahi-VMware-Virtual-Platform systemd[1]: Starting systemd-journal-flush.service - Flush Journal to Persistent Storage...
2024-12-30T07:52:33.221134+03:00 abdullahi-VMware-Virtual-Platform systemd[1]: Starting systemd-sysctl.service - Apply Kernel Variables...
2024-12-30T07:52:33.221146+03:00 abdullahi-VMware-Virtual-Platform systemd[1]: Mounted run-vmblock\x2dfuse.mount - VMware vmblock fuse mount.
2024-12-30T07:52:33.221150+03:00 abdullahi-VMware-Virtual-Platform systemd[1]: Finished systemd-tmpfiles-setup-dev.service - Create Static Device Nodes in /dev.
2024-12-30T07:52:33.221155+03:00 abdullahi-VMware-Virtual-Platform systemd[1]: Reached target local-fs-pre.target - Preparation for Local File Systems.
2024-12-30T07:52:33.221158+03:00 abdullahi-VMware-Virtual-Platform systemd[1]: Starting systemd-udevd.service - Rule-based Manager for Device Events and Files...
2024-12-30T07:52:33.221162+03:00 abdullahi-VMware-Virtual-Platform systemd[1]: Finished systemd-sysctl.service - Apply Kernel Variables.
2024-12-30T07:52:33.221165+03:00 abdullahi-VMware-Virtual-Platform systemd-udevd[455]: Using default interface naming scheme 'v255'.
2024-12-30T07:52:33.221172+03:00 abdullahi-VMware-Virtual-Platform systemd[1]: Finished systemd-journal-flush.service - Flush Journal to Persistent Storage.
```



```
to 37000
2024-12-30T08:11:25.973477+03:00 abdullahi-VMware-Virtual-Platform systemd[1]: fprintd.service: Deactivated successfully.
2024-12-30T08:12:50.438759+03:00 abdullahi-VMware-Virtual-Platform pipewire[2659]: pw.node: (alsa_output.pci-0000_02_02.0.analog-stereo-59) graph xrun not-triggere
d (6 suppressed)
2024-12-30T08:12:50.441431+03:00 abdullahi-VMware-Virtual-Platform pipewire[2659]: pw.node: (alsa_output.pci-0000_02_02.0.analog-stereo-59) xrun state:0x7be5a245c0
08 pending:1/2 s:1231737433371 a:1231737550564 f:1232473248643 waiting:117193 process:735698079 status:triggered
2024-12-30T08:12:50.441540+03:00 abdullahi-VMware-Virtual-Platform pipewire[2659]: pw.node: (Mutter-66) xrun state:0x7be5a2222008 pending:0/1 s:1232478353429 a:123
1737454858 f:1231737491402 waiting:18446744072968653045 process:36544 status:triggered
2024-12-30T08:15:01.836173+03:00 abdullahi-VMware-Virtual-Platform CRON[4445]: (root) CMD (command -v debian-sa1 > /dev/null && debian-sa1 1 1)
2024-12-30T08:15:22.604142+03:00 abdullahi-VMware-Virtual-Platform pipewire[2659]: pw.node: (alsa_output.pci-0000_02_02.0.analog-stereo-59) graph xrun not-triggere
d (2 suppressed)
2024-12-30T08:15:22.605196+03:00 abdullahi-VMware-Virtual-Platform pipewire[2659]: pw.node: (alsa_output.pci-0000_02_02.0.analog-stereo-59) xrun state:0x7be5a245c0
08 pending:1/2 s:1384008856846 a:1384009052658 f:1384638829639 waiting:195812 process:629776981 status:triggered
2024-12-30T08:15:22.605305+03:00 abdullahi-VMware-Virtual-Platform pipewire[2659]: pw.node: (Mutter-66) xrun state:0x7be5a2222008 pending:0/1 s:1384642123369 a:138
4642664584 f:1384008985937 waiting:541215 process:18446744073075872969 status:awake
2024-12-30T08:16:27.958735+03:00 abdullahi-VMware-Virtual-Platform kernel: perf: interrupt took too long (6728 > 6632), lowering kernel.perf_event_max_sample_rate
to 29000
2024-12-30T08:17:01.848709+03:00 abdullahi-VMware-Virtual-Platform CRON[4458]: (root) CMD (cd / && run-parts --report /etc/cron.hourly)
abdullahi@abdullahi-VMware-Virtual-Platform:/var/log$ 
```

Analyzing and filtering Authentication Logs

I analyzed authentication logs to identify login events and user activity, and filtered the data to extract specific entries, such as logs related to a particular date or process. I started with opening the authentication log file using `less auth.log` command.

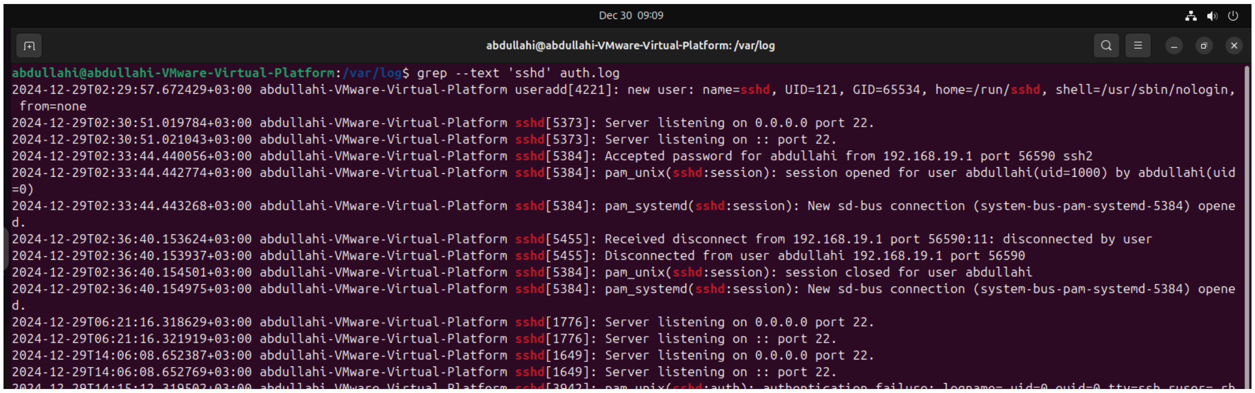


```
2024-12-28T04:37:37.725648+00:00 abdullahi-VMware-Virtual-Platform systemd-logind[1612]: New seat seat0.
2024-12-28T04:37:37.725663+00:00 abdullahi-VMware-Virtual-Platform systemd-logind[1612]: Watching system buttons on /dev/input/event0 (Power Button)
2024-12-28T04:37:37.725677+00:00 abdullahi-VMware-Virtual-Platform systemd-logind[1612]: Watching system buttons on /dev/input/event1 (AT Translated Set 2 keyboard
)
2024-12-28T04:37:37.883989+00:00 abdullahi-VMware-Virtual-Platform polkitd[1544]: Loading rules from directory /etc/polkit-1/rules.d
2024-12-28T04:37:37.885207+00:00 abdullahi-VMware-Virtual-Platform polkitd[1544]: Loading rules from directory /usr/share/polkit-1/rules.d
2024-12-28T04:37:37.943185+00:00 abdullahi-VMware-Virtual-Platform polkitd[1544]: Finished loading, compiling and executing 16 rules
2024-12-28T04:37:37.950406+00:00 abdullahi-VMware-Virtual-Platform polkitd[1544]: Acquired the name org.freedesktop.PolicyKit1 on the system bus
2024-12-28T04:37:41.817724+00:00 abdullahi-VMware-Virtual-Platform useradd[2069]: new group: name=abdullahi, GID=1000
2024-12-28T04:37:41.817827+00:00 abdullahi-VMware-Virtual-Platform useradd[2069]: new user: name=abdullahi, UID=1000, GID=1000, home=/home/abdullahi, shell=/bin/ba
sh, from=none
2024-12-28T04:37:41.821471+00:00 abdullahi-VMware-Virtual-Platform useradd[2069]: add 'abdullahi' to group 'adm'
2024-12-28T04:37:41.821521+00:00 abdullahi-VMware-Virtual-Platform useradd[2069]: add 'abdullahi' to group 'cdrom'
2024-12-28T04:37:41.821541+00:00 abdullahi-VMware-Virtual-Platform useradd[2069]: add 'abdullahi' to group 'sudo'
2024-12-28T04:37:41.821559+00:00 abdullahi-VMware-Virtual-Platform useradd[2069]: add 'abdullahi' to group 'dip'
2024-12-28T04:37:41.821583+00:00 abdullahi-VMware-Virtual-Platform useradd[2069]: add 'abdullahi' to group 'plugdev'
2024-12-28T04:37:41.821598+00:00 abdullahi-VMware-Virtual-Platform useradd[2069]: add 'abdullahi' to group 'users'
2024-12-28T04:37:41.821613+00:00 abdullahi-VMware-Virtual-Platform useradd[2069]: add 'abdullahi' to group 'lpadmin'
2024-12-28T04:37:41.821628+00:00 abdullahi-VMware-Virtual-Platform useradd[2069]: add 'abdullahi' to shadow group 'adm'
```

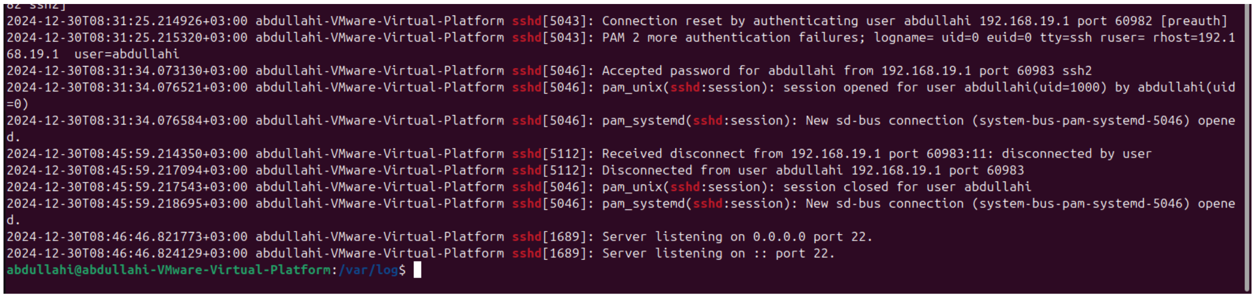
The log entries show a series of system events, including the creation of a new user named 'abdullahi' and the assignment of this user to multiple system groups (such as sudo, adm, and cdrom). It also records a password change for the 'abdullahi' user, followed by session activities for the 'gdm' user, including session openings and related system connections (e.g., SD-bus connections). Additionally, there are logs related to system services such as polkitd (handling policy authentication), gnome-keyring-daemon (managing keyring services), and gdm-launch-environment (handling login environments), with some warnings about the keyring daemon and a failure to locate a control file for gdm-password.

This is just the first page of a large log file, so it's better to use commands such as grep to extract specific information.

I ran the command `grep --text 'sshd' auth.log` to search for any SSH-related logs in the authentication file. This command filters out all entries that are related to SSH, helping to identify login attempts or authentication events.

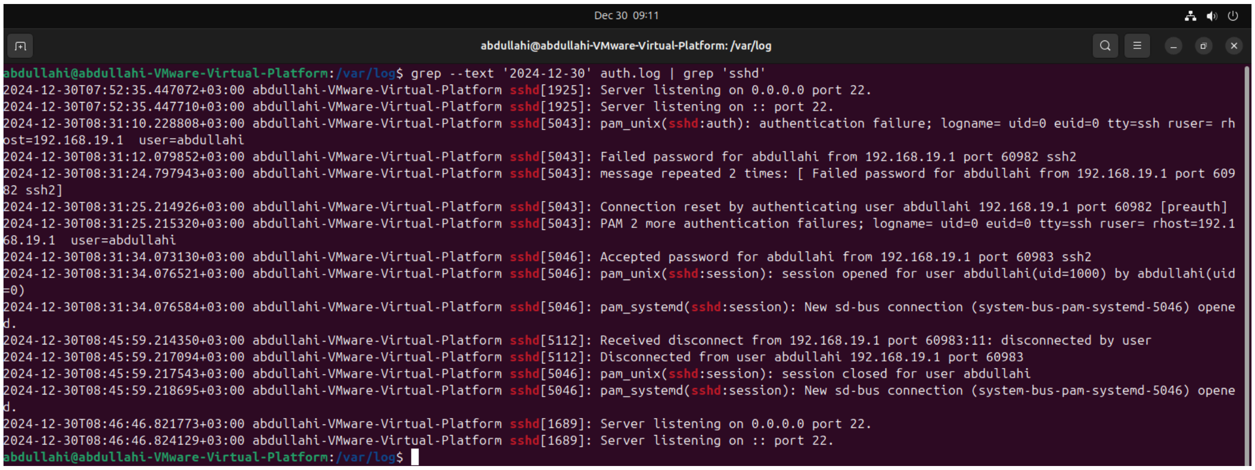


```
abdullahi@abdullahi-VMware-Virtual-Platform:/var/log$ grep --text 'sshd' auth.log
2024-12-29T02:29:57.672429+03:00 abdullahi-VMware-Virtual-Platform useradd[4221]: new user: name=sshd, UID=121, GID=65534, home=/run/sshd, shell=/usr/sbin/nologin,
 from=none
2024-12-29T02:30:51.019784+03:00 abdullahi-VMware-Virtual-Platform sshd[5373]: Server listening on 0.0.0.0 port 22.
2024-12-29T02:30:51.021043+03:00 abdullahi-VMware-Virtual-Platform sshd[5373]: Server listening on :: port 22.
2024-12-29T02:33:44.440056+03:00 abdullahi-VMware-Virtual-Platform sshd[5384]: Accepted password for abdullahi from 192.168.19.1 port 56590 ssh2
2024-12-29T02:33:44.442774+03:00 abdullahi-VMware-Virtual-Platform sshd[5384]: pam_unix(sshd:session): session opened for user abdullahi(uid=1000) by abdullahi(uid
=0)
2024-12-29T02:33:44.443268+03:00 abdullahi-VMware-Virtual-Platform sshd[5384]: pam_systemd(sshd:session): New sd-bus connection (system-bus-pam-systemd-5384) opene
d.
2024-12-29T02:36:40.153624+03:00 abdullahi-VMware-Virtual-Platform sshd[5455]: Received disconnect from 192.168.19.1 port 56590:11: disconnected by user
2024-12-29T02:36:40.153937+03:00 abdullahi-VMware-Virtual-Platform sshd[5455]: Disconnected from user abdullahi 192.168.19.1 port 56590
2024-12-29T02:36:40.154501+03:00 abdullahi-VMware-Virtual-Platform sshd[5384]: pam_unix(sshd:session): session closed for user abdullahi
2024-12-29T02:36:40.154975+03:00 abdullahi-VMware-Virtual-Platform sshd[5384]: pam_systemd(sshd:session): New sd-bus connection (system-bus-pam-systemd-5384) opene
d.
2024-12-29T06:21:16.318629+03:00 abdullahi-VMware-Virtual-Platform sshd[1776]: Server listening on 0.0.0.0 port 22.
2024-12-29T06:21:16.321919+03:00 abdullahi-VMware-Virtual-Platform sshd[1776]: Server listening on :: port 22.
2024-12-29T14:06:08.652387+03:00 abdullahi-VMware-Virtual-Platform sshd[1649]: Server listening on 0.0.0.0 port 22.
2024-12-29T14:06:08.652769+03:00 abdullahi-VMware-Virtual-Platform sshd[1649]: Server listening on :: port 22.
2024-12-29T14:15:12.319502+03:00 abdullahi-VMware-Virtual-Platform sshd[3942]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rh
```



```
82 ssh2]
2024-12-30T08:31:25.214926+03:00 abdullahi-VMware-Virtual-Platform sshd[5043]: Connection reset by authenticating user abdullahi 192.168.19.1 port 60982 [preauth]
2024-12-30T08:31:25.215320+03:00 abdullahi-VMware-Virtual-Platform sshd[5043]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.1
68.19.1  user=abdullahi
2024-12-30T08:31:34.073130+03:00 abdullahi-VMware-Virtual-Platform sshd[5046]: Accepted password for abdullahi from 192.168.19.1 port 60983 ssh2
2024-12-30T08:31:34.076521+03:00 abdullahi-VMware-Virtual-Platform sshd[5046]: pam_unix(sshd:session): session opened for user abdullahi(uid=1000) by abdullahi(uid
=0)
2024-12-30T08:31:34.076584+03:00 abdullahi-VMware-Virtual-Platform sshd[5046]: pam_systemd(sshd:session): New sd-bus connection (system-bus-pam-systemd-5046) opene
d.
2024-12-30T08:45:59.214350+03:00 abdullahi-VMware-Virtual-Platform sshd[5112]: Received disconnect from 192.168.19.1 port 60983:11: disconnected by user
2024-12-30T08:45:59.217094+03:00 abdullahi-VMware-Virtual-Platform sshd[5112]: Disconnected from user abdullahi 192.168.19.1 port 60983
2024-12-30T08:45:59.217543+03:00 abdullahi-VMware-Virtual-Platform sshd[5046]: pam_unix(sshd:session): session closed for user abdullahi
2024-12-30T08:45:59.218695+03:00 abdullahi-VMware-Virtual-Platform sshd[5046]: pam_systemd(sshd:session): New sd-bus connection (system-bus-pam-systemd-5046) opene
d.
2024-12-30T08:46:46.821773+03:00 abdullahi-VMware-Virtual-Platform sshd[1689]: Server listening on 0.0.0.0 port 22.
2024-12-30T08:46:46.824129+03:00 abdullahi-VMware-Virtual-Platform sshd[1689]: Server listening on :: port 22.
abdullahi@abdullahi-VMware-Virtual-Platform:/var/log$
```

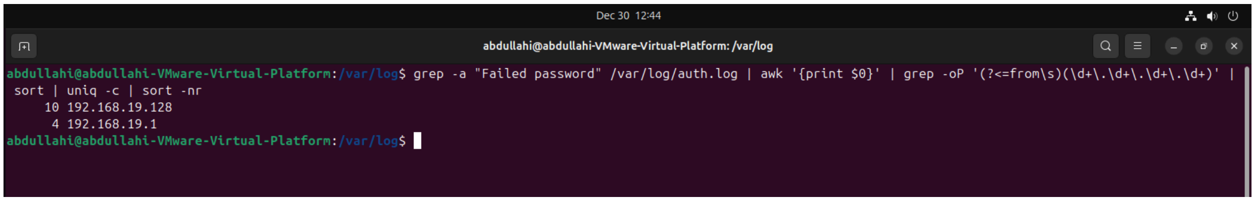
Next, I ran the command `grep --text '2024-12-30' auth.log | grep 'sshd'` to filter the authentication logs for entries from the specific date '2024-12-30' and then search for SSH-related logs. This allows me to narrow down the logs to a particular day and focus on relevant SSH login attempts or activities.



```
abdullahi@abdullahi-VMware-Virtual-Platform:/var/log$ grep --text '2024-12-30' auth.log | grep 'sshd'
2024-12-30T07:52:35.447072+03:00 abdullahi-VMware-Virtual-Platform sshd[1925]: Server listening on 0.0.0.0 port 22.
2024-12-30T07:52:35.447710+03:00 abdullahi-VMware-Virtual-Platform sshd[1925]: Server listening on :: port 22.
2024-12-30T08:31:10.228808+03:00 abdullahi-VMware-Virtual-Platform sshd[5043]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rh
ost=192.168.19.1  user=abdullahi
2024-12-30T08:31:12.079852+03:00 abdullahi-VMware-Virtual-Platform sshd[5043]: Failed password for abdullahi from 192.168.19.1 port 60982 ssh2
2024-12-30T08:31:24.797943+03:00 abdullahi-VMware-Virtual-Platform sshd[5043]: message repeated 2 times: [ Failed password for abdullahi from 192.168.19.1 port 609
82 ssh2]
2024-12-30T08:31:25.214926+03:00 abdullahi-VMware-Virtual-Platform sshd[5043]: Connection reset by authenticating user abdullahi 192.168.19.1 port 60982 [preauth]
2024-12-30T08:31:25.215320+03:00 abdullahi-VMware-Virtual-Platform sshd[5043]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.1
68.19.1  user=abdullahi
2024-12-30T08:31:34.073130+03:00 abdullahi-VMware-Virtual-Platform sshd[5046]: Accepted password for abdullahi from 192.168.19.1 port 60983 ssh2
2024-12-30T08:31:34.076521+03:00 abdullahi-VMware-Virtual-Platform sshd[5046]: pam_unix(sshd:session): session opened for user abdullahi(uid=1000) by abdullahi(uid
=0)
2024-12-30T08:31:34.076584+03:00 abdullahi-VMware-Virtual-Platform sshd[5046]: pam_systemd(sshd:session): New sd-bus connection (system-bus-pam-systemd-5046) opene
d.
2024-12-30T08:45:59.214350+03:00 abdullahi-VMware-Virtual-Platform sshd[5112]: Received disconnect from 192.168.19.1 port 60983:11: disconnected by user
2024-12-30T08:45:59.217094+03:00 abdullahi-VMware-Virtual-Platform sshd[5112]: Disconnected from user abdullahi 192.168.19.1 port 60983
2024-12-30T08:45:59.217543+03:00 abdullahi-VMware-Virtual-Platform sshd[5046]: pam_unix(sshd:session): session closed for user abdullahi
2024-12-30T08:45:59.218695+03:00 abdullahi-VMware-Virtual-Platform sshd[5046]: pam_systemd(sshd:session): New sd-bus connection (system-bus-pam-systemd-5046) opene
d.
2024-12-30T08:46:46.821773+03:00 abdullahi-VMware-Virtual-Platform sshd[1689]: Server listening on 0.0.0.0 port 22.
2024-12-30T08:46:46.824129+03:00 abdullahi-VMware-Virtual-Platform sshd[1689]: Server listening on :: port 22.
abdullahi@abdullahi-VMware-Virtual-Platform:/var/log$
```

Summarizing log data

I summarized log data to extract meaningful insights for example to summarize failed login attempts by ip addressesi used the command `grep "Failed password" /var/log/auth.log | awk '{print $0}' | grep -oP '(?<=from\s)(\d+\.\d+\.\d+\.\d+)' | sort | uniq -c | sort -nr`



```
abdullahi@abdullahi-VMware-Virtual-Platform:/var/log$ grep -a "Failed password" /var/log/auth.log | awk '{print $0}' | grep -oP '(?<=from\s)(\d+\.\d+\.\d+\.\d+)' |
 sort | uniq -c | sort -nr
     10 192.168.19.128
      4 192.168.19.1
abdullahi@abdullahi-VMware-Virtual-Platform:/var/log$
```

Breakdown of the command:

`grep -a "Failed password" /var/log/auth.log:`

- Searches the file `/var/log/auth.log` for lines containing the text **"Failed password"** (indicating failed login attempts).
- The `-a` option treats binary files as text, useful if the file has any non-text data.

`awk '{print $0}'`:

- Prints each matching line (redundant here, as `grep` already outputs the lines).

`grep -oP '(?<=from\s)(\d+\.\d+\.\d+\.\d+)'`:

- Extracts only the IP addresses from the lines using a Perl-compatible regular expression (`-P`).
- The regex `(?<=from\s)(\d+\.\d+\.\d+\.\d+)` matches an IP address after the word "from".

`sort`:

- Sorts the extracted IP addresses in ascending order, grouping duplicates together.

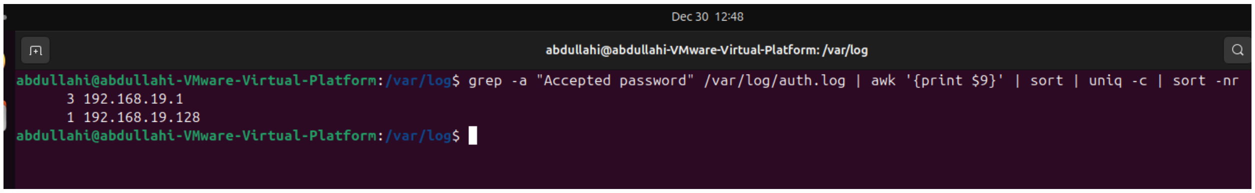
`uniq -c`:

- Counts the number of occurrences of each unique IP address.

`sort -nr`:

- Sorts the counted results in **numerical reverse order**, showing the IP with the most failed attempts at the top.

To summarize successful logins per user I ran the command grep -a "Accepted password" /var/log/auth.log | awk '{print $9}' | sort | uniq -c | sort -nr



```
abdullahi@abdullahi-VMware-Virtual-Platform:/var/log$ grep -a "Accepted password" /var/log/auth.log | awk '{print $9}' | sort | uniq -c | sort -nr
      3 192.168.19.1
      1 192.168.19.128
abdullahi@abdullahi-VMware-Virtual-Platform:/var/log$ 
```

This command analyzes the `/var/log/auth.log` file to summarize successful logins by user. It starts by using `grep` to search for lines containing the text **"Accepted password,"** which logs successful logins. The awk command then extracts the **username** from the 9th column of each matching line. These usernames are sorted to group duplicates together, and `uniq -c` counts how many times each username appears. Finally, the results are sorted in descending order (`sort -nr`), listing the users with the most successful logins at the top. This provides a clear summary of successful logins categorized by user.

Conclusion

In conclusion, this project provided valuable hands-on experience in syslog analysis, enhancing my skills in configuring and managing syslog on a Linux system (Ubuntu). I gained practical knowledge of syslog configuration files, exploring the contents of /etc/rsyslog.conf and understanding how various modules and directives affect logging behavior. I learned to efficiently navigate system log files, filter and search logs using tools like grep, awk, and less to extract specific data for analysis. A key focus was on authentication logs, where I analyzed SSH login attempts and identified potential security concerns. Through this project, I strengthened my troubleshooting, log analysis, and security monitoring skills, which are crucial in system administration and cybersecurity. The project helped me develop a deeper understanding of log management and its role in maintaining a secure and well-functioning system.

---

abdullahi-cybersecurity-portfolio