

Name: Cristian Barreno

## Logwatch Intro

### Prerequisites

- Ubuntu 22.04 Server Powered up
- Ubuntu Server on Bridged mode
- From Host OS, ssh to the Ubuntu Server

```
Administrator: lynx@lynx ~
Microsoft Windows [Version 10.0.19045.4170]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Kristian Barreno>ssh lynx@192.168.0.47
Password:
Verification code:
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 5.15.0-100-generic x86_64)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/advantage

System information as of Tue Mar 19 01:55:36 PM UTC 2024

System load:          0.0751953125
Usage of /:           58.3% of 9.75GB
Memory usage:         10%
Swap usage:          0%
Processes:           108
Users logged in:     1
IPv4 address for enp0s3: 192.168.0.47
IPv6 address for enp0s3: 2600:8805:2101:fc00:a00:27ff:fe51:bf8a
IPv6 address for enp0s3: 2600:8805:2101:fc00:a00:27ff:fe51:bf8a

* Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s just raised the bar for easy, resilient and secure K8s cluster deployment.
  https://ubuntu.com/engage/secure-kubernetes-at-the-edge

Expanded Security Maintenance for Applications is not enabled.

80 updates can be applied immediately.
7 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

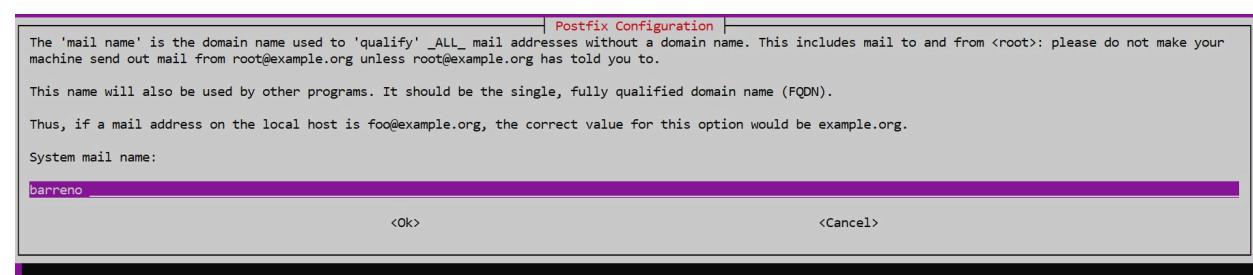
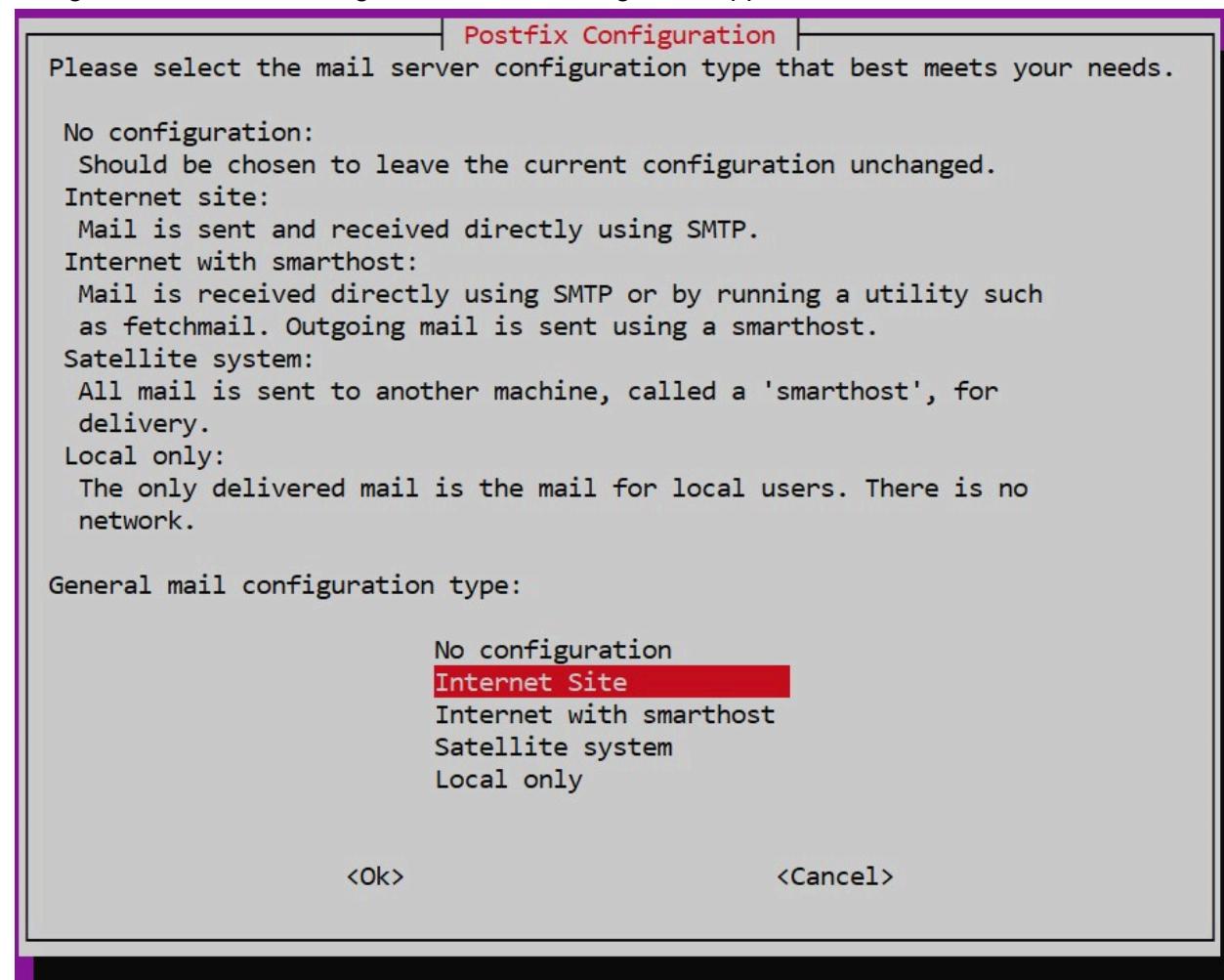
Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

Last login: Tue Mar 19 13:54:22 2024
lynx@lynx:~$
```

## EXERCISE 4 – Installing Logwatch

**sudo apt install logwatch -y**

Using the Advanced Package Tool install the Logwatch application.



```
lynx@lynx:~$ sudo apt install logwatch -y
[sudo] password for lynx:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libdate-manip-perl postfix ssl-cert
Suggested packages:
  libsys-cpu-perl libsys-meminfo-perl procmail postfix-mysql postfix-pgsql postfix-ldap postfix-pcre postfix-lmdb postfix-sqlite sasl2-bin | dovecot-common resolvconf
  postfix-cdb mail-reader postfix-mta-sts-resolver postfix-doc
The following NEW packages will be installed:
  libdate-manip-perl logwatch postfix ssl-cert
0 upgraded, 4 newly installed, 0 to remove and 73 not upgraded.
Need to get 2,589 kB of archives.
After this operation, 19.3 MB of additional disk space will be used.
Get:1 http://us.archive.ubuntu.com/ubuntu jammy/main amd64 ssl-cert all 1.1.2 [17.4 kB]
Get:2 http://us.archive.ubuntu.com/ubuntu jammy-updates/main amd64 postfix amd64 3.6.4-1ubuntu1.3 [1,248 kB]
Get:3 http://us.archive.ubuntu.com/ubuntu jammy/main amd64 libdate-manip-perl all 6.86-1 [946 kB]
Get:4 http://us.archive.ubuntu.com/ubuntu jammy/main amd64 logwatch all 7.5.6-1ubuntu1 [378 kB]
Fetched 2,589 kB in 0s (6,071 kB/s)
Preconfiguring packages ...
Selecting previously unselected package ssl-cert.
(Reading database ... 110836 files and directories currently installed.)
Preparing to unpack .../ssl-cert_1.1.2_all.deb ...
Unpacking ssl-cert (1.1.2) ...
Selecting previously unselected package postfix.
Preparing to unpack .../postfix_3.6.4-1ubuntu1.3_amd64.deb ...
Unpacking postfix (3.6.4-1ubuntu1.3) ...
Selecting previously unselected package libdate-manip-perl.
Preparing to unpack .../libdate-manip-perl_6.86-1_all.deb ...
Unpacking libdate-manip-perl (6.86-1) ...
Selecting previously unselected package logwatch.
Preparing to unpack .../logwatch_7.5.6-1ubuntu1_all.deb ...
Unpacking logwatch (7.5.6-1ubuntu1) ...
Setting up ssl-cert (1.1.2) ...
Setting up postfix (3.6.4-1ubuntu1.3) ...
Adding group `postfix' (GID 120) ...
Done.
Adding system user `postfix' (UID 114) ...
Adding new user `postfix' (UID 114) with group `postfix' ...
Not creating home directory `/var/spool/postfix'.
```

## EXERCISE 5 – Basic service usage

Create a Detailed Report for a Specific Service

To focus on a particular service, such as SSH, and get more detailed information, you can adjust the detail level and specify the service of interest.

```
sudo logwatch --service sshd --detail High --range 'Today' --output stdout
```

```
lynx@lynx:~$ sudo logwatch --service sshd --detail High --range 'Today' --output stdout
#####
Logwatch 7.5.6 (07/23/21) #####
Processing Initiated: Tue Mar 19 14:07:36 2024
Date Range Processed: today
          ( 2024-Mar-19 )
Period is day.
Detail Level of Output: 10
Type of Output/Format: stdout / text
LogFile for Host: lynx
#####

----- SSHD Begin -----

SSHD Started: 4 Times

Users logging in through sshd:
lynx:
 192.168.0.247: 2 Times

----- SSHD End -----



#####
Logwatch End #####
lynx@lynx:~$
```

## EXERCISE 6 – Examining logs over certain date ranges

Do not copy and paste the following command, it merely gives you options.

**logwatch --range yesterday|today|all|help --detail low|medium|others**

One can mix and match the filters (or queries) to provide the appropriate output you seek.

If I just wanted today's logs:

**logwatch --range today**

```
lynx@lynx:~$ logwatch --range today
#####
# Logwatch 7.5.6 (07/23/21) #####
Processing Initiated: Tue Mar 19 14:11:10 2024
Date Range Processed: today
          ( 2024-Mar-19 )
Period is day.
Detail Level of Output: 0
Type of Output/Format: stdout / text
Logfiles for Host: lynx
#####

----- dpkg status changes Begin -----

Installed:
liblbddate-manip-perl:all 6.86-1
logwatch:all 7.5.6-1ubuntu1
postfix:amd64 3.6.4-1ubuntu1.3
ssl-cert:all 1.1.2

----- dpkg status changes End -----


----- Kernel Begin -----


WARNING: Kernel Errors Present
WARNING: Spectre v2 mitigation leaves CPU vulner ...: 2 Time(s)
[drm:vmw_host_printf [vmwgfx]] *ERROR* Failed to send ...: 2 Time(s)

----- Kernel End -----

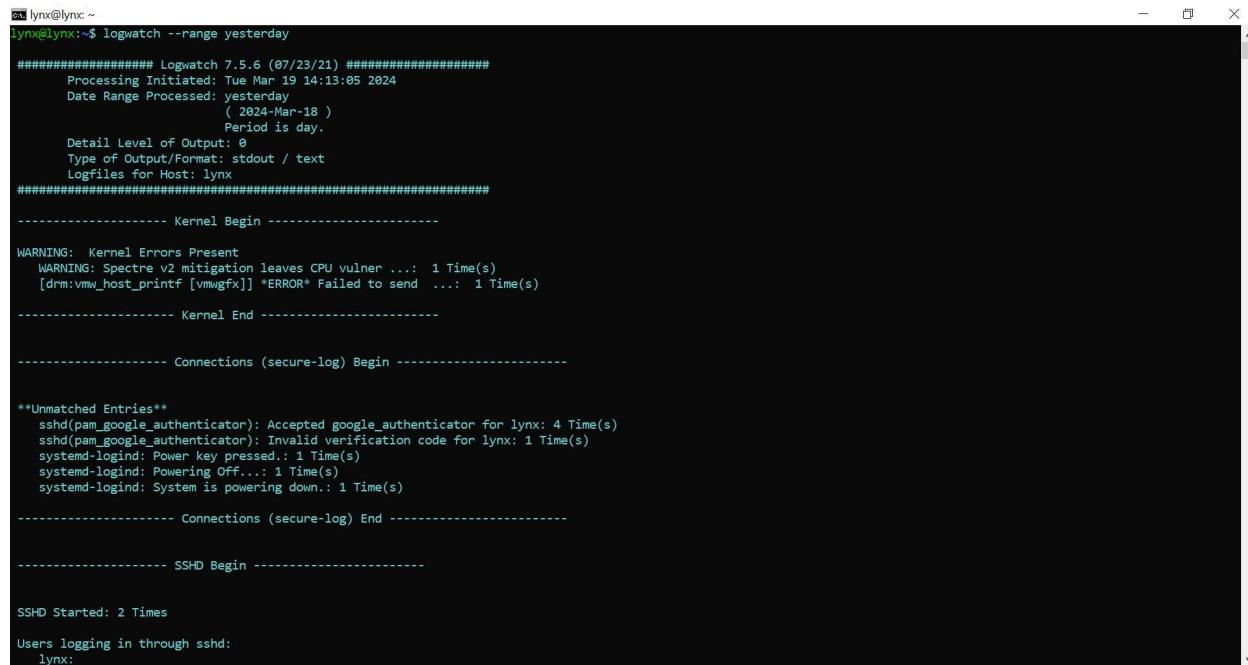

----- pam_unix Begin -----


sudo:
Sessions Opened:
lynx -> root(uid=0): 2 Time(s)

----- pam_unix End -----
```

If I just wanted yesterday's logs:

**logwatch --range yesterday**



```
lynx@lynx: ~
lynx@lynx:~$ logwatch --range yesterday
#####
Logwatch 7.5.6 (07/23/21) #####
Processing Initiated: Tue Mar 19 14:13:05 2024
Date Range Processed: yesterday
( 2024-Mar-18 )
Period is day.

Detail Level of Output: 0
Type of Output/Format: stdout / text
Logfiles for Host: lynx
#####

----- Kernel Begin -----

WARNING: Kernel Errors Present
WARNING: Spectre v2 mitigation leaves CPU vulner ...: 1 Time(s)
[drm:vmw_host_printf [vmwgfx]] *ERROR* Failed to send ...: 1 Time(s)

----- Kernel End -----


----- Connections (secure-log) Begin -----


**Unmatched Entries**
sshd(pam_google_authenticator): Accepted google_authenticator for lynx: 4 Time(s)
sshd(pam_google_authenticator): Invalid verification code for lynx: 1 Time(s)
systemd-logind: Power key pressed.: 1 Time(s)
systemd-logind: Powering Off...: 1 Time(s)
systemd-logind: System is powering down.: 1 Time(s)

----- Connections (secure-log) End -----


----- SSHD Begin -----


SSHD Started: 2 Times
Users logging in through sshd:
lynx:
```

## EXERCISE 7 – View the local Auth Log and compare it to the output of Logwatch

### Task 1. Review Raw Log Entries

First, inspect the raw log entries in /var/log/auth.log. You can view the contents of this file using a command like less or tail, depending on whether you want to read from the beginning or just see the most recent entries.

**sudo less /var/log/auth.log**



```
lynx@lynx: ~
lynx@lynx:~$ sudo less /var/log/auth.log
```

```

cd lynx@lynx: ~
Mar 17 15:33:10 lynx login[663]: pam_unix(login:session): session opened for user lynx(uid=1000) by LOGIN(uid=0)
Mar 17 15:33:19 lynx systemd-logind[655]: New session 1 of user lynx.
Mar 17 15:33:19 lynx systemd: pam_unix(systemd-user:session): session opened for user lynx(uid=1000) by (uid=0)
Mar 17 15:34:11 lynx sshd[pam_google_authenticator][978]: Accepted google_authenticator for lynx
Mar 17 15:34:11 lynx sshd[976]: pam_unix(sshd:session): session opened for user lynx(uid=1000) by (uid=0)
Mar 17 15:34:11 lynx sshd[976]: pam_unix(sshd:session): session opened for user lynx(uid=1000) by (uid=0)
Mar 17 15:34:11 lynx systemd-logind[655]: New session 3 of user lynx.
Mar 17 16:17:01 lynx CRON[1098]: pam_unix(cron:session): session opened for user root(uid=0) by (uid=0)
Mar 17 16:17:01 lynx CRON[1098]: pam_unix(cron:session): session closed for user root
Mar 17 17:17:01 lynx CRON[1188]: pam_unix(cron:session): session opened for user root(uid=0) by (uid=0)
Mar 17 17:17:01 lynx CRON[1188]: pam_unix(cron:session): session closed for user root
Mar 17 17:46:03 lynx sudo: lynx : TTY:/pts/0 ; PWD=/home/lynx ; USER=root ; COMMAND=/usr/bin/apt install unzip
Mar 17 17:46:03 lynx sudo: pam_unix(sudo:session): session opened for user root(uid=0) by lynx(uid=1000)
Mar 17 17:46:39 lynx sudo: pam_unix(sudo:session): session closed for user root
Mar 17 18:17:01 lynx CRON[1483]: pam_unix(cron:session): session opened for user root(uid=0) by (uid=0)
Mar 17 18:17:01 lynx CRON[1483]: pam_unix(cron:session): session closed for user root
Mar 17 18:22:05 lynx sshd[1023]: Received disconnect from 192.168.0.247 port 61937:11: disconnected by user
Mar 17 18:22:05 lynx sshd[1023]: Disconnected from user lynx 192.168.0.247 port 61937
Mar 17 18:22:05 lynx sshd[1023]: pam_unix(sshd:session): session closed for user lynx
Mar 17 18:22:05 lynx systemd-logind[655]: Session 3 logged out. Waiting for processes to exit.
Mar 17 18:22:05 lynx systemd-logind[655]: Removed session 3.
Mar 17 18:22:08 lynx systemd-logind[655]: Power key pressed.
Mar 17 18:22:08 lynx systemd-logind[655]: Powering Off...
Mar 17 18:22:08 lynx systemd-logind[655]: System is powering down.
Mar 18 14:36:57 lynx sshd[689]: Server listening on 0.0.0.0 port 22.
Mar 18 14:36:57 lynx sshd[689]: Server listening on :: port 22.
Mar 18 14:36:57 lynx systemd-logind[654]: New seat seat0.
Mar 18 14:36:58 lynx systemd-logind[654]: Watching system buttons on /dev/input/event0 (Power Button)
Mar 18 14:36:58 lynx systemd-logind[654]: Watching system buttons on /dev/input/event1 (Sleep Button)
Mar 18 14:36:58 lynx systemd-logind[654]: Watching system buttons on /dev/input/event2 (AT Translated Set 2 keyboard)
Mar 18 14:37:12 lynx login[662]: pam_unix(login:session): session opened for user lynx(uid=1000) by LOGIN(uid=0)
Mar 18 14:37:12 lynx systemd-logind[654]: New session 1 of user lynx.
Mar 18 14:37:12 lynx systemd: pam_unix(systemd-user:session): session opened for user lynx(uid=1000) by (uid=0)
Mar 18 14:38:10 lynx sshd[pam_google_authenticator][976]: Accepted google_authenticator for lynx
Mar 18 14:38:10 lynx sshd[974]: pam_unix(sshd:session): session opened for user lynx(uid=1000) by (uid=0)
Mar 18 14:38:10 lynx sshd[974]: pam_unix(sshd:session): session opened for user lynx(uid=1000) by (uid=0)
Mar 18 14:38:10 lynx systemd-logind[654]: New session 3 of user lynx.
Mar 18 14:52:02 lynx sshd[1030]: Received disconnect from 192.168.0.247 port 50816:11: disconnected by user
Mar 18 14:52:02 lynx sshd[1030]: Disconnected from user lynx 192.168.0.247 port 50816
Mar 18 14:52:02 lynx sshd[974]: pam_unix(sshd:session): session closed for user lynx

```

# or to see the most recent entries

**sudo tail -n 100 /var/log/auth.log**

```

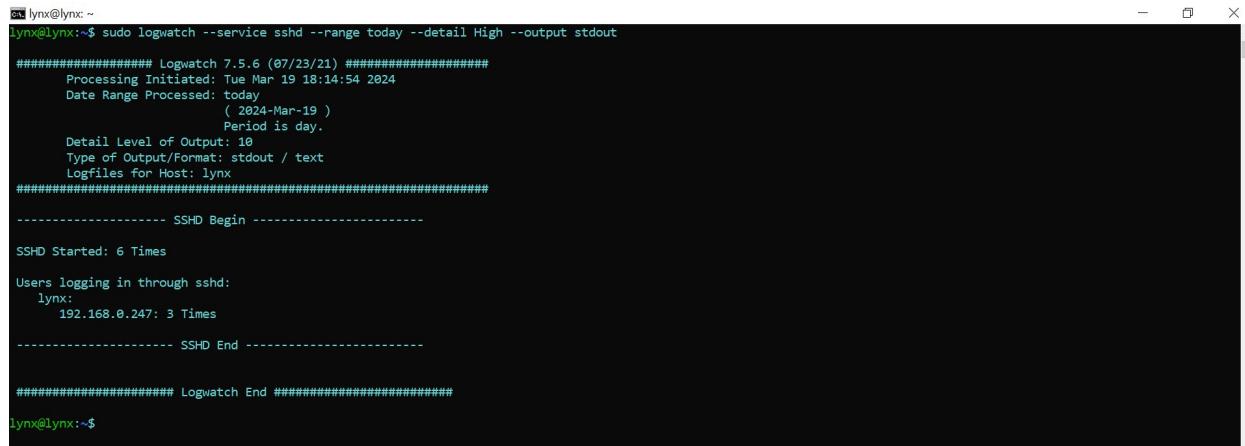
cd lynx@lynx: ~
lynx@lynx: ~$ sudo tail -n 100 /var/log/auth.log
Mar 18 14:52:35 lynx sshd[1083]: pam_unix(sshd:session): session opened for user lynx(uid=1000) by (uid=0)
Mar 18 14:52:35 lynx systemd-logind[654]: New session 4 of user lynx.
Mar 18 14:55:08 lynx sshd[pam_google_authenticator][1152]: Invalid verification code for lynx
Mar 18 14:55:10 lynx sshd[1150]: error: PAM: Authentication failure for lynx from 192.168.0.247
Mar 18 14:55:20 lynx sshd[pam_google_authenticator][1153]: Accepted google_authenticator for lynx
Mar 18 14:55:20 lynx sshd[1150]: Accepted keyboard-interactive/pam for lynx from 192.168.0.247 port 50891 ssh2
Mar 18 14:55:20 lynx sshd[1150]: pam_unix(sshd:session): session opened for user lynx(uid=1000) by (uid=0)
Mar 18 14:55:20 lynx systemd-logind[654]: New session 5 of user lynx.
Mar 18 14:55:20 lynx sshd[1207]: Received disconnect from 192.168.0.247 port 50891:11: disconnected by user
Mar 18 14:55:20 lynx sshd[1207]: Disconnected from user lynx 192.168.0.247 port 50891
Mar 18 14:55:20 lynx sshd[1150]: pam_unix(sshd:session): session closed for user lynx
Mar 18 14:55:20 lynx systemd-logind[654]: Session 5 logged out. Waiting for processes to exit.
Mar 18 14:55:20 lynx systemd-logind[654]: Removed session 5.
Mar 18 14:56:36 lynx sshd[pam_google_authenticator][1211]: Accepted google_authenticator for lynx
Mar 18 14:56:36 lynx sshd[1209]: Accepted keyboard-interactive/pam for lynx from 192.168.0.247 port 50897 ssh2
Mar 18 14:56:36 lynx sshd[1209]: pam_unix(sshd:session): session opened for user lynx(uid=1000) by (uid=0)
Mar 18 14:56:36 lynx systemd-logind[654]: New session 6 of user lynx.
Mar 18 14:56:37 lynx sshd[1265]: Received disconnect from 192.168.0.247 port 50897:11: disconnected by user
Mar 18 14:56:37 lynx sshd[1265]: Disconnected from user lynx 192.168.0.247 port 50897
Mar 18 14:56:37 lynx sshd[1209]: pam_unix(sshd:session): session closed for user lynx
Mar 18 14:56:37 lynx systemd-logind[654]: Session 6 logged out. Waiting for processes to exit.
Mar 18 14:56:37 lynx systemd-logind[654]: Removed session 6.
Mar 18 15:17:01 lynx CRON[1335]: pam_unix(cron:session): session opened for user root(uid=0) by (uid=0)
Mar 18 15:17:01 lynx CRON[1335]: pam_unix(cron:session): session closed for user root
Mar 18 16:17:01 lynx CRON[1508]: pam_unix(cron:session): session opened for user root(uid=0) by (uid=0)
Mar 18 16:17:01 lynx CRON[1508]: pam_unix(cron:session): session closed for user root
Mar 18 16:43:16 lynx sshd[1139]: Received disconnect from 192.168.0.247 port 50886:11: disconnected by user
Mar 18 16:43:16 lynx sshd[1139]: Disconnected from user lynx 192.168.0.247 port 50886
Mar 18 16:43:16 lynx systemd-logind[654]: Session 4 logged out. Waiting for processes to exit.
Mar 18 16:43:16 lynx sshd[1083]: pam_unix(sshd:session): session closed for user lynx
Mar 18 16:43:16 lynx systemd-logind[654]: Removed session 4.
Mar 18 16:43:31 lynx systemd-logind[654]: Power key pressed.
Mar 18 16:43:31 lynx systemd-logind[654]: Powering Off...
Mar 18 16:43:31 lynx systemd-logind[654]: System is powering down.
Mar 19 00:27:10 lynx sshd[693]: Server listening on 0.0.0.0 port 22.
Mar 19 00:27:10 lynx sshd[693]: Server listening on :: port 22.
Mar 19 00:27:11 lynx systemd-logind[653]: New seat seat0.
Mar 19 00:27:11 lynx systemd-logind[653]: Watching system buttons on /dev/input/event0 (Power Button)
Mar 19 00:27:11 lynx systemd-logind[653]: Watching system buttons on /dev/input/event1 (Sleep Button)
Mar 19 00:27:11 lynx systemd-logind[653]: Watching system buttons on /dev/input/event2 (AT Translated Set 2 keyboard)

```

## 2. Generate a Logwatch Report

Next, generate a Logwatch report that includes the authentication logs. You might need to specify the service (`--service sshd` for SSH logs, for example) and ensure the report covers the same date range as the entries you're examining in `auth.log`.

```
sudo logwatch --service sshd --range today --detail High --output stdout
```



```
lynx@lynx:~$ sudo logwatch --service sshd --range today --detail High --output stdout
#####
Logwatch 7.5.6 (07/23/21) #####
Processing Initiated: Tue Mar 19 18:14:54 2024
Date Range Processed: today
( 2024-Mar-19 )
Period is day.
Detail Level of Output: 10
Type of Output/Format: stdout / text
Logfiles for Host: lynx
#####
----- SSHD Begin -----
SSHD Started: 6 Times
Users logging in through sshd:
lynx:
 192.168.0.247: 3 Times
----- SSHD End -----
#####
Logwatch End #####
lynx@lynx:~$
```

This command tells Logwatch to generate a detailed report for SSH-related logs (sshd) from today. Adjust the `--range` parameter as necessary to match the period you're investigating in the raw logs.

## 3. Compare the Information

With both the raw log entries and the Logwatch report open, you can start comparing the information:

- **Timestamps:** Check that events in the raw logs correspond to entries in the Logwatch report based on their timestamps.
- **Usernames and IP Addresses:** Look for mentions of specific usernames or IP addresses in the Logwatch report that you've seen in the raw logs.
- **Event Descriptions:** Compare the descriptions of events. Logwatch summarizes and categorizes events, so it may present information differently. For example, multiple failed login attempts might be summarized into a single line in the Logwatch report.

```

lynx@lynx:~$ sudo logwatch --service sshd --range today --detail High --output stdout

#####
Logwatch 7.5.6 (07/23/21) #####
Processing Initiated: Tue Mar 19 18:14:54 2024
Date Range Processed: today
( 2024-Mar-19 )
Period is day.
Detail Level of Output: 10
Type of Output/Format: stdout / text
Logfiles for Host: lynx
#####

----- SSHD Begin -----


SSHD Started: 6 Times

Users logging in through sshd:
lynx:
192.168.0.247: 3 Times

----- SSHD End -----


#####
Logwatch End #####

```

lynx@lynx:~\$

```

lynx@lynx:~$ sudo tail -n 100 /var/log/auth.log
Mar 18 14:52:35 lynx sshd[1083]: pam_unix(sshd:session): session opened for user lynx(uid=1000) by (uid=0)
Mar 18 14:52:35 lynx sshd[1083]: pam_unix(sshd:session): New session 4 of user lynx.
Mar 18 14:55:08 lynx sshd[pam_google_authenticator][1152]: Invalid verification code for lynx
Mar 18 14:55:18 lynx sshd[1150]: error: PAM: Authentication failure for lynx from 192.168.0.247
Mar 18 14:55:20 lynx sshd[pam_google_authenticator][1153]: Accepted google_authenticator for lynx
Mar 18 14:55:20 lynx sshd[1150]: Accepted keyboard-interactive/pam for lynx from 192.168.0.247 port 50891 ssh2
Mar 18 14:55:20 lynx sshd[1150]: pam_unix(sshd:session): session opened for user lynx(uid=1000) by (uid=0)
Mar 18 14:55:20 lynx systemd-logind[654]: New session 5 of user lynx.
Mar 18 14:55:20 lynx sshd[1207]: Received disconnect from 192.168.0.247 port 50891:11: disconnected by user
Mar 18 14:55:20 lynx sshd[1207]: Disconnected from user lynx 192.168.0.247 port 50891
Mar 18 14:55:20 lynx sshd[1150]: pam_unix(sshd:session): session closed for user lynx
Mar 18 14:55:20 lynx systemd-logind[654]: Session 5 logged out. Waiting for processes to exit.
Mar 18 14:55:28 lynx sshd[1150]: Removed session 5.
Mar 18 14:56:36 lynx sshd[pam_google_authenticator][1211]: Accepted google_authenticator for lynx
Mar 18 14:56:36 lynx sshd[1209]: Accepted keyboard-interactive/pam for lynx from 192.168.0.247 port 50897 ssh2
Mar 18 14:56:36 lynx sshd[1209]: pam_unix(sshd:session): session opened for user lynx(uid=1000) by (uid=0)
Mar 18 14:56:36 lynx systemd-logind[654]: New session 6 of user lynx.
Mar 18 14:56:37 lynx sshd[1265]: Received disconnect from 192.168.0.247 port 50897:11: disconnected by user
Mar 18 14:56:37 lynx sshd[1265]: Disconnected from user lynx 192.168.0.247 port 50897
Mar 18 14:56:37 lynx sshd[1209]: pam_unix(sshd:session): session closed for user lynx
Mar 18 14:56:37 lynx systemd-logind[654]: Session 6 logged out. Waiting for processes to exit.
Mar 18 14:56:37 lynx sshd[1150]: Removed session 6.
Mar 18 15:17:01 lynx CRON[1335]: pam_unix(cron:session): session opened for user root(uid=0) by (uid=0)
Mar 18 15:17:01 lynx CRON[1335]: pam_unix(cron:session): session closed for user root
Mar 18 16:17:01 lynx CRON[1508]: pam_unix(cron:session): session opened for user root(uid=0) by (uid=0)
Mar 18 16:17:01 lynx CRON[1508]: pam_unix(cron:session): session closed for user root
Mar 18 16:43:10 lynx sshd[1139]: Received disconnect from 192.168.0.247 port 50886:11: disconnected by user
Mar 18 16:43:10 lynx sshd[1139]: Disconnected from user lynx 192.168.0.247 port 50886
Mar 18 16:43:16 lynx sshd[1083]: Session 4 logged out. Waiting for processes to exit.
Mar 18 16:43:16 lynx sshd[1083]: pam_unix(sshd:session): session closed for user lynx
Mar 18 16:43:31 lynx systemd-logind[654]: Removed session 4.
Mar 18 16:43:31 lynx systemd-logind[654]: Power key pressed.
Mar 18 16:43:31 lynx systemd-logind[654]: Powering Off...
Mar 18 16:43:31 lynx systemd-logind[654]: System is powering down.
Mar 19 00:27:10 lynx sshd[693]: Server listening on :: port 22.
Mar 19 00:27:10 lynx sshd[693]: Server listening on :: port 22.
Mar 19 00:27:11 lynx systemd-logind[653]: New seat seat0.
Mar 19 00:27:11 lynx systemd-logind[653]: Watching system buttons on /dev/input/event0 (Power Button)
Mar 19 00:27:11 lynx systemd-logind[653]: Watching system buttons on /dev/input/event1 (Sleep Button)
Mar 19 00:27:11 lynx systemd-logind[653]: Watching system buttons on /dev/input/event2 (AT Translated Set 2 keyboard)

```

```

lynx@lynx: ~
Mar 17 15:33:10 lynx login[663]: pam_unix(login:session): session opened for user lynx(uid=1000) by LOGIN(uid=0)
Mar 17 15:33:19 lynx systemd-logind[655]: New session 1 of user lynx.
Mar 17 15:33:19 lynx systemd: pam_unix(systemd-user:session): session opened for user lynx(uid=1000) by (uid=0)
Mar 17 15:34:11 lynx sshd[pam_google_authenticator][978]: Accepted google_authenticator for lynx
Mar 17 15:34:11 lynx sshd[976]: Accepted keyboard-interactive/pam for lynx from 192.168.0.247 port 61937 ssh2
Mar 17 15:34:11 lynx sshd[976]: pam_unix(sshd:session): session opened for user lynx(uid=1000) by (uid=0)
Mar 17 15:34:11 lynx systemd-logind[655]: New session 3 of user lynx.
Mar 17 16:17:01 lynx CRON[1098]: pam_unix(cron:session): session opened for user root(uid=0) by (uid=0)
Mar 17 16:17:01 lynx CRON[1098]: pam_unix(cron:session): session closed for user root
Mar 17 17:17:01 lynx CRON[1188]: pam_unix(cron:session): session opened for user root(uid=0) by (uid=0)
Mar 17 17:17:01 lynx CRON[1188]: pam_unix(cron:session): session closed for user root
Mar 17 17:46:03 lynx sudo: lynx : TTY:/pts/0 ; PWD=/home/lynx ; USER=root ; COMMAND=/usr/bin/apt install unzip
Mar 17 17:46:03 lynx sudo: pam_unix(sudo:session): session opened for user root(uid=0) by lynx(uid=1000)
Mar 17 17:46:39 lynx sudo: pam_unix(sudo:session): session closed for user root
Mar 17 18:17:01 lynx CRON[1483]: pam_unix(cron:session): session closed for user root(uid=0) by (uid=0)
Mar 17 18:17:01 lynx CRON[1483]: pam_unix(cron:session): session closed for user root
Mar 17 18:22:05 lynx sshd[1023]: Received disconnect from 192.168.0.247 port 61937:11: disconnected by user
Mar 17 18:22:05 lynx sshd[1023]: Disconnected from user lynx 192.168.0.247 port 61937
Mar 17 18:22:05 lynx sshd[976]: pam_unix(sshd:session): session closed for user lynx
Mar 17 18:22:05 lynx systemd-logind[655]: Session 3 logged out. Waiting for processes to exit.
Mar 17 18:22:05 lynx systemd-logind[655]: Removed session 3.
Mar 17 18:22:08 lynx systemd-logind[655]: Power key pressed.
Mar 17 18:22:08 lynx systemd-logind[655]: Powering Off...
Mar 17 18:22:08 lynx systemd-logind[655]: System is powering down.
Mar 18 14:36:57 lynx sshd[689]: Server listening on 0.0.0.0 port 22.
Mar 18 14:36:57 lynx sshd[689]: Server listening on :: port 22.
Mar 18 14:36:57 lynx systemd-logind[654]: New seat seat0.
Mar 18 14:36:58 lynx systemd-logind[654]: Watching system buttons on /dev/input/event0 (Power Button)
Mar 18 14:36:58 lynx systemd-logind[654]: Watching system buttons on /dev/input/event1 (Sleep Button)
Mar 18 14:36:58 lynx systemd-logind[654]: Watching system buttons on /dev/input/event2 (AT Translated Set 2 keyboard)
Mar 18 14:37:12 lynx login[662]: pam_unix(login:session): session opened for user lynx(uid=1000) by LOGIN(uid=0)
Mar 18 14:37:12 lynx systemd-logind[654]: New session 1 of user lynx.
Mar 18 14:37:12 lynx systemd: pam_unix(systemd-user:session): session opened for user lynx(uid=1000) by (uid=0)
Mar 18 14:38:10 lynx sshd[pam_google_authenticator][976]: Accepted google_authenticator for lynx
Mar 18 14:38:10 lynx sshd[974]: Accepted keyboard-interactive/pam for lynx from 192.168.0.247 port 50816 ssh2
Mar 18 14:38:10 lynx sshd[974]: pam_unix(sshd:session): session opened for user lynx(uid=1000) by (uid=0)
Mar 18 14:38:10 lynx systemd-logind[654]: New session 3 of user lynx.
Mar 18 14:52:02 lynx sshd[1030]: Received disconnect from 192.168.0.247 port 50816:11: disconnected by user
Mar 18 14:52:02 lynx sshd[1030]: Disconnected from user lynx 192.168.0.247 port 50816
Mar 18 14:52:02 lynx sshd[974]: pam_unix(sshd:session): session closed for user lynx

```

## TCPDump

### Basic Usage

Capture packets on an interface: `tcpdump -i enp0s3`

```

lynx@lynx: ~
lynx@lynx: $ sudo tcpdump -i enp0s3
tcpdump: verbose output suppressed, use -v[V]... for full protocol decode
listening on enp0s3, link-type EN10MB (Ethernet), snapshot length 262144 bytes
20:42:42.228308 IP lynx.ssh > 192.168.0.247.54444: Flags [.], seq 3123675921:3123676029, ack 4109583206, win 501, length 108
20:42:42.228428 IP lynx.ssh > 192.168.0.247.54444: Flags [.], seq 108:272, ack 1, win 501, length 164
20:42:42.228487 IP lynx.ssh > 192.168.0.247.54444: Flags [.], ack 108, win 4100, length 0
20:42:42.228537 IP lynx.ssh > 192.168.0.247.54444: Flags [.], seq 272:340, ack 1, win 501, length 68
20:42:42.228635 IP lynx.ssh > 192.168.0.247.54444: Flags [.], seq 340:376, ack 1, win 501, length 36
20:42:42.228667 IP 192.168.0.247.54444 > lynx.ssh: Flags [.], ack 346, win 4106, length 0
20:42:42.269271 IP 192.168.0.247.54444 > lynx.ssh: Flags [.], ack 376, win 4106, length 0
20:42:42.329098 IP lynx.51355 > cdns1.cox.net.domain: 33309+ [iau] PTR 247.0.168.192.in-addr.arpa. (55)
20:42:42.344644 IP cdns1.cox.net.domain > lynx.51355: 33309 NXDomain 0/0/1 (55)
20:42:42.344841 IP cdns1.cox.net.domain: 33309+ [iau] PTR 247.0.168.192.in-addr.arpa. (44)
20:42:42.361028 IP cdns1.cox.net.domain > lynx.51355: 33309 NXDomain 0/0/0 (44)
20:42:42.362287 IP lynx.36895 > cdns1.cox.net.domain: 51505+ [iau] PTR 47.0.168.192.in-addr.arpa. (54)
20:42:42.376068 IP cdns1.cox.net.domain > lynx.36895: 51505 NXDomain 0/0/1 (54)
20:42:42.376263 IP lynx.36895 > cdns1.cox.net.domain: 51505+ [iau] PTR 47.0.168.192.in-addr.arpa. (43)
20:42:42.387940 IP cdns1.cox.net.domain > lynx.36895: 51505 NXDomain 0/0/0 (43)
20:42:42.389183 IP lynx.ssh > 192.168.0.247.54444: Flags [.], seq 376:540, ack 1, win 501, length 164
20:42:42.389834 IP lynx.ssh > 192.168.0.247.54444: Flags [.], seq 540:576, ack 1, win 501, length 36
20:42:42.390274 IP 192.168.0.247.54444 > lynx.ssh: Flags [.], ack 576, win 4105, length 0
20:42:42.396393 IP lynx.ssh > 192.168.0.247.54444: Flags [.], seq 576:716, ack 1, win 501, length 140
20:42:42.396837 IP lynx.ssh > 192.168.0.247.54444: Flags [.], seq 716:752, ack 1, win 501, length 36
20:42:42.391446 IP 192.168.0.247.54444 > lynx.ssh: Flags [.], ack 752, win 4104, length 0
20:42:42.391692 IP lynx.ssh > 192.168.0.247.54444: Flags [.], seq 752:876, ack 1, win 501, length 124
20:42:42.392181 IP lynx.ssh > 192.168.0.247.54444: Flags [.], seq 876:912, ack 1, win 501, length 36
20:42:42.392327 IP lynx.ssh > 192.168.0.247.54444: Flags [.], seq 912:1052, ack 1, win 501, length 140
20:42:42.392793 IP 192.168.0.247.54444 > lynx.ssh: Flags [.], ack 912, win 4104, length 0
20:42:42.399038 IP lynx.ssh > 192.168.0.247.54444: Flags [.], seq 1052:1088, ack 1, win 501, length 36
20:42:42.395447 IP 192.168.0.247.54444 > lynx.ssh: Flags [.], ack 1088, win 4103, length 0
20:42:42.395643 IP lynx.ssh > 192.168.0.247.54444: Flags [.], seq 1088:1228, ack 1, win 501, length 140
20:42:42.394038 IP lynx.ssh > 192.168.0.247.54444: Flags [.], seq 1228:1264, ack 1, win 501, length 36
20:42:42.394252 IP lynx.ssh > 192.168.0.247.54444: Flags [.], seq 1264:1388, ack 1, win 501, length 124
20:42:42.394529 IP 192.168.0.247.54444 > lynx.ssh: Flags [.], ack 1264, win 4102, length 0
20:42:42.394765 IP lynx.ssh > 192.168.0.247.54444: Flags [.], seq 1388:1424, ack 1, win 501, length 36
20:42:42.395191 IP 192.168.0.247.54444 > lynx.ssh: Flags [.], ack 1424, win 4102, length 0
20:42:42.395339 IP lynx.ssh > 192.168.0.247.54444: Flags [.], seq 1424:1548, ack 1, win 501, length 124
20:42:42.395718 IP lynx.ssh > 192.168.0.247.54444: Flags [.], seq 1548:1584, ack 1, win 501, length 36
20:42:42.396148 IP 192.168.0.247.54444 > lynx.ssh: Flags [.], ack 1584, win 4101, length 0
20:42:42.431356 IP lynx.56360 > cdns1.cox.net.domain: 58268+ [iau] PTR 11.28.105.68.in-addr.arpa. (54)
20:42:42.446351 IP cdns1.cox.net.domain > lynx.56360: 58268 0/0/1 PTR cdns1.cox.net. (81)

```

## Capture only N packets: **tcpdump -c N -i enp0s3**

```
lynx@lynx:~$ sudo tcpdump -c 5 -i enp0s3
tcpdump: verbose output suppressed, use -v[V]... for full protocol decode
listening on enp0s3, link-type EN10MB (Ethernet), snapshot length 262144 bytes
20:50:23.567288 IP lynx.ssh > 192.168.0.247.54444: Flags [P.], seq 3123848461:3123848569, ack 4109590850, win 501, length 108
20:50:23.567411 IP lynx.ssh > 192.168.0.247.54444: Flags [P.], seq 108:272, ack 1, win 501, length 164
20:50:23.567470 IP 192.168.0.247.54444 > lynx.ssh: Flags [.], ack 108, win 4105, length 0
20:50:23.567522 IP lynx.ssh > 192.168.0.247.54444: Flags [P.], seq 272:340, ack 1, win 501, length 68
20:50:23.567620 IP lynx.ssh > 192.168.0.247.54444: Flags [P.], seq 340:376, ack 1, win 501, length 36
5 packets captured
28 packets received by filter
0 packets dropped by kernel
lynx@lynx:~$
```

## Display captured packets in verbose mode: **tcpdump -v -i enp0s3**

```
lynx@lynx:~$ sudo tcpdump -v -i enp0s3
tcpdump: listening on enp0s3, link-type EN10MB (Ethernet), snapshot length 262144 bytes
20:54:47.407664 IP (tos 0x10, ttl 64, id 31488, offset 0, flags [DF], proto TCP (6), length 84)
    lynx.ssh > 192.168.0.247.54444: Flags [P..], cksum 0x82bd (incorrect -> 0x45c6), seq 3132527937:3132527981, ack 4109598750, win 501, length 44
20:54:47.407750 IP (tos 0x10, ttl 64, id 31489, offset 0, flags [DF], proto TCP (6), length 108)
    lynx.ssh > 192.168.0.247.54444: Flags [P..], cksum 0x82cd (incorrect -> 0xb5c9), seq 44:104, ack 1, win 501, length 60
20:54:47.407899 IP (tos 0x0, ttl 128, id 1609, offset 0, flags [DF], proto TCP (6), length 40)
    192.168.0.247.54444 > lynx.ssh: Flags [P..], cksum 0x835e (correct), ack 44, win 4102, length 0
20:54:47.407908 IP (tos 0x10, ttl 64, id 31490, offset 0, flags [DF], proto TCP (6), length 108)
    lynx.ssh > 192.168.0.247.54444: Flags [P..], cksum 0x82d5 (incorrect -> 0x53d5), seq 104:172, ack 1, win 501, length 68
20:54:47.408012 IP (tos 0x10, ttl 64, id 31491, offset 0, flags [DF], proto TCP (6), length 144)
    lynx.ssh > 192.168.0.247.54444: Flags [P..], cksum 0x82f9 (incorrect -> 0xa7ad), seq 172:276, ack 1, win 501, length 104
20:54:47.408091 IP (tos 0x0, ttl 64, id 1610, offset 0, flags [DF], proto TCP (6), length 40)
    192.168.0.247.54444 > lynx.ssh: Flags [P..], cksum 0x82df (correct), ack 172, win 4101, length 0
20:54:47.408223 IP (tos 0x0, ttl 128, id 1611, offset 0, flags [DF], proto TCP (6), length 40)
    192.168.0.247.54444 > lynx.ssh: Flags [P..], cksum 0x8277 (correct), ack 276, win 4101, length 0
20:54:47.507415 IP (tos 0x10, ttl 64, id 31492, offset 0, flags [DF], proto TCP (6), length 172)
    lynx.ssh > 192.168.0.247.54444: Flags [P..], cksum 0x8315 (incorrect -> 0xedf0), seq 276:408, ack 1, win 501, length 132
20:54:47.507590 IP (tos 0x10, ttl 64, id 31493, offset 0, flags [DF], proto TCP (6), length 76)
    lynx.ssh > 192.168.0.247.54444: Flags [P..], cksum 0x82b5 (incorrect -> 0x7737), seq 408:444, ack 1, win 501, length 36
20:54:47.507730 IP (tos 0x0, ttl 128, id 1612, offset 0, flags [DF], proto TCP (6), length 40)
    192.168.0.247.54444 > lynx.ssh: Flags [P..], cksum 0x81d0 (correct), ack 444, win 4100, length 0
20:54:47.507852 IP (tos 0x0, ttl 64, id 11517, offset 0, flags [none], proto UDP (17), length 83)
    lynx.ssh > 28795+[au] PTR? 47.0.168.192.in-addr.arpa. (55)
20:54:47.526330 IP (tos 0x0, ttl 60, id 10523, offset 0, flags [DF], proto UDP (17), length 83)
    cdns1.cox.net.domain > lynx.ssh: Flags [P.], cksum 0x8111 (incorrect -> 0x1111), seq 28795:NXDomain 0/0/0 (55)
20:54:47.526441 IP (tos 0x0, ttl 64, id 11518, offset 0, flags [none], proto UDP (17), length 72)
    lynx.ssh > 28795+[au] PTR? 47.0.168.192.in-addr.arpa. (44)
20:54:47.554190 IP (tos 0x0, ttl 60, id 10537, offset 0, flags [DF], proto UDP (17), length 72)
    cdns1.cox.net.domain > lynx.ssh: Flags [P.], cksum 0x8000 (incorrect -> 0x0000), seq 28795:NXDomain 0/0/0 (44)
20:54:47.555963 IP (tos 0x0, ttl 64, id 10660, offset 0, flags [none], proto UDP (17), length 82)
    lynx.ssh > 53125> cdns1.cox.net.domain: 38815+[au] PTR? 47.0.168.192.in-addr.arpa. (54)
20:54:47.571236 IP (tos 0x0, ttl 60, id 62699, offset 0, flags [DF], proto UDP (17), length 82)
    cdns1.cox.net.domain > lynx.ssh: Flags [P.], cksum 0x8111 (incorrect -> 0x1111), seq 38815:NXDomain 0/0/0 (54)
20:54:47.571525 IP (tos 0x0, ttl 64, id 10661, offset 0, flags [none], proto UDP (17), length 71)
    lynx.ssh > 53125> cdns1.cox.net.domain: 38815+[au] PTR? 47.0.168.192.in-addr.arpa. (43)
20:54:47.584123 IP (tos 0x0, ttl 60, id 62708, offset 0, flags [DF], proto UDP (17), length 71)
    cdns1.cox.net.domain > lynx.ssh: Flags [P.], cksum 0x8000 (incorrect -> 0x0000), seq 38815:NXDomain 0/0/0 (43)
20:54:47.585661 IP (tos 0x10, ttl 64, id 31494, offset 0, flags [DF], proto TCP (6), length 220)
    lynx.ssh > 192.168.0.247.54444: Flags [P..], cksum 0x8345 (incorrect -> 0x77ca), seq 444:624, ack 1, win 501, length 180
20:54:47.586269 IP (tos 0x10, ttl 64, id 31495, offset 0, flags [DF], proto TCP (6), length 76)
    lynx@lynx:~$
```

## Write captured packets to a file: **tcpdump -w file.pcap -i enp0s3**

```
lynx@lynx:~$ sudo tcpdump -w file.pcap -i enp0s3
tcpdump: listening on enp0s3, link-type EN10MB (Ethernet), snapshot length 262144 bytes
^C10 packets captured
0 packets received by filter
0 packets dropped by kernel
lynx@lynx:~$
```

## Read packets from a file: **tcpdump -r file.pcap**

```
lynx@lynx:~$ sudo tcpdump -r file.pcap
reading from file file.pcap, link-type EN10MB (Ethernet), snapshot length 262144
21:07:14.022212 IP lynx.ssh > 192.168.0.247.54444: Flags [P..], seq 3132579893:3132579937, ack 4109605790, win 501, length 44
21:07:14.022270 IP lynx.ssh > 192.168.0.247.54444: Flags [P..], seq 44:104, ack 1, win 501, length 60
21:07:14.022380 IP 192.168.0.247.54444 > lynx.ssh: Flags [.], ack 44, win 4100, length 0
21:07:14.022391 IP lynx.ssh > 192.168.0.247.54444: Flags [P..], seq 104:172, ack 1, win 501, length 68
21:07:14.022450 IP lynx.ssh > 192.168.0.247.54444: Flags [P..], seq 172:276, ack 1, win 501, length 104
21:07:14.022519 IP 192.168.0.247.54444 > lynx.ssh: Flags [.], ack 172, win 4100, length 0
21:07:14.062318 IP 192.168.0.247.54444 > lynx.ssh: Flags [.], ack 276, win 4105, length 0
21:07:15.380190 IP _gateway > ip6-allnodes: ICMP6, router advertisement, length 80
21:07:15.399985 IP lynx > ff02::1: HBH ICMP6, multicast listener report v2, 2 group record(s), length 48
21:07:15.475198 IP lynx > ff02::1: HBH ICMP6, multicast listener report v2, 2 group record(s), length 48
lynx@lynx:~$
```

## Use Cases and Examples

### 1. Monitoring Specific Ports

- Capture HTTP traffic: **tcpdump port 80 -i enp0s3**
- This is useful for troubleshooting web server issues or inspecting HTTP request and response headers.

The screenshot shows a dual-pane interface. On the left is a web browser window titled "Apache2 Default Page" from "Ubuntu". It features the Ubuntu logo and the text "It works!". Below the page content, there is a "Configuration Overview" section with some descriptive text and a file tree view showing the directory structure under "/etc/apache2/". On the right is a terminal window titled "lynx@lynx:~" showing the output of the command "sudo tcpdump port 80 -i enp0s3". The terminal output displays several network packets captured by tcpdump, showing details like source and destination IP addresses, ports, and packet content.

```
lynx@lynx:~$ sudo tcpdump port 80 -i enp0s3
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on enp0s3, link-type EN10MB (Ethernet), snapshot length 262144 bytes
21:16:21.282323 IP 192.168.0.247.55045 > lynx.http: Flags [F.], seq 3386714272, ack 797826579, win 4106, length 0
21:16:21.282323 IP 192.168.0.247.55046 > lynx.http: Flags [F.], seq 2968935927, ack 2571714301, win 4106, length 0
21:16:21.282358 IP lynx.http > 192.168.0.247.55045: Flags [.], ack 1, win 502, length 0
21:16:21.282370 IP lynx.http > 192.168.0.247.55046: Flags [.], ack 1, win 502, length 0
21:16:21.282866 IP 192.168.0.247.55051 > lynx.http: Flags [S], seq 2088698216, win 64240, options [mss 1460,nop,wscale 8,nop,nop,sackOK], length 0
21:16:21.282887 IP lynx.http > 192.168.0.247.55051: Flags [S.], seq 1893986321, ack 2088698217, win 64240, options [mss 1460,nop,nop,sackOK,nop,wscale 7], length 0
21:16:21.283069 IP 192.168.0.247.55051 > lynx.http: Flags [.], ack 1, win 4106, length 0
21:16:21.283305 IP 192.168.0.247.55052 > lynx.http: Flags [S], seq 2703891977, win 64240, options [mss 1460,nop,wscale 8,nop,nop,sackOK], length 0
21:16:21.283321 IP lynx.http > 192.168.0.247.55052: Flags [S.], seq 2315671829, ack 2703891978, win 64240, options [mss 1460,nop,nop,sackOK,nop,wscale 7], length 0
21:16:21.283497 IP 192.168.0.247.55052 > lynx.http: Flags [.], ack 1, win 4106, length 0
```

### 2. Capturing Packets from Specific IP

- Capture traffic from a specific IP: **tcpdump src host 192.168.0.47 -i enp0s3**
- This can help in analyzing traffic from a suspicious source or debugging network issues related to a specific device.

```
lynx@lynx:~
```

```
lynx@lynx:~$ sudo tcpdump src host 192.168.0.47 -i enp0s3
tcpdump: verbose output suppressed, use -v[V]... for full protocol decode
listening on enp0s3, link-type EN10MB (Ethernet), snapshot length 262144 bytes
21:26:25.215381 IP lynx.ssh > 192.168.0.247.54444: Flags [P..], seq 1312768861:3132768969, ack 4109615934, win 501, length 108
21:26:25.215622 IP lynx.ssh > 192.168.0.247.54444: Flags [P..], seq 108:204, ack 1, win 501, length 96
21:26:25.215765 IP lynx.ssh > 192.168.0.247.54444: Flags [P..], seq 204:272, ack 1, win 501, length 68
21:26:25.215980 IP lynx.ssh > 192.168.0.247.54444: Flags [P..], seq 272:340, ack 1, win 501, length 68
21:26:25.216027 IP lynx.ssh > 192.168.0.247.54444: Flags [P..], seq 340:376, ack 1, win 501, length 36
21:26:25.316394 IP lynx.45652 > cdns1.cox.net.domain: 7565+ [lau] PTR? 247.0.168.192.in-addr.arpa. (55)
21:26:25.339348 IP lynx.45652 > cdns1.cox.net.domain: 7565+ PTR? 247.0.168.192.in-addr.arpa. (44)
21:26:25.353565 IP lynx.48458 > cdns1.cox.net.domain: 17616+ [lau] PTR? 47.0.168.192.in-addr.arpa. (54)
21:26:25.368291 IP lynx.48458 > cdns1.cox.net.domain: 17616+ PTR? 47.0.168.192.in-addr.arpa. (43)
21:26:25.386461 IP lynx.ssh > 192.168.0.247.54444: Flags [P..], seq 376:540, ack 1, win 501, length 164
21:26:25.386745 IP lynx.ssh > 192.168.0.247.54444: Flags [P..], seq 540:576, ack 1, win 501, length 36
21:26:25.387049 IP lynx.ssh > 192.168.0.247.54444: Flags [P..], seq 576:716, ack 1, win 501, length 140
21:26:25.387202 IP lynx.ssh > 192.168.0.247.54444: Flags [P..], seq 716:752, ack 1, win 501, length 36
21:26:25.387279 IP lynx.ssh > 192.168.0.247.54444: Flags [P..], seq 752:892, ack 1, win 501, length 140
21:26:25.387485 IP lynx.ssh > 192.168.0.247.54444: Flags [P..], seq 892:928, ack 1, win 501, length 36
21:26:25.387579 IP lynx.ssh > 192.168.0.247.54444: Flags [P..], seq 928:1068, ack 1, win 501, length 140
21:26:25.387763 IP lynx.ssh > 192.168.0.247.54444: Flags [P..], seq 1068:1104, ack 1, win 501, length 36
21:26:25.387851 IP lynx.ssh > 192.168.0.247.54444: Flags [P..], seq 1104:1244, ack 1, win 501, length 140
21:26:25.388087 IP lynx.ssh > 192.168.0.247.54444: Flags [P..], seq 1244:1280, ack 1, win 501, length 36
21:26:25.419793 IP lynx.ssh > 192.168.0.247.54444: Flags [P..], seq 1280:1420, ack 1, win 501, length 140
21:26:25.420843 IP lynx.ssh > 192.168.0.247.54444: Flags [P..], seq 1420:1456, ack 1, win 501, length 36
21:26:25.420813 IP lynx.ssh > 192.168.0.247.54444: Flags [P..], seq 1456:1588, ack 1, win 501, length 132
21:26:25.420819 IP lynx.ssh > 192.168.0.247.54444: Flags [P..], seq 1588:1624, ack 1, win 501, length 36
21:26:25.420729 IP lynx.ssh > 192.168.0.247.54444: Flags [P..], seq 1624:1764, ack 1, win 501, length 140
21:26:25.420889 IP lynx.ssh > 192.168.0.247.54444: Flags [P..], seq 1764:1880, ack 1, win 501, length 36
21:26:25.421062 IP lynx.ssh > 192.168.0.247.54444: Flags [P..], seq 1880:1932, ack 1, win 501, length 132
21:26:25.421221 IP lynx.ssh > 192.168.0.247.54444: Flags [P..], seq 1932:1968, ack 1, win 501, length 36
21:26:25.421314 IP lynx.ssh > 192.168.0.247.54444: Flags [P..], seq 1968:2108, ack 1, win 501, length 140
21:26:25.421453 IP lynx.ssh > 192.168.0.247.54444: Flags [P..], seq 2108:2144, ack 1, win 501, length 36
21:26:25.421541 IP lynx.ssh > 192.168.0.247.54444: Flags [P..], seq 2144:2284, ack 1, win 501, length 140
21:26:25.421687 IP lynx.ssh > 192.168.0.247.54444: Flags [P..], seq 2284:2320, ack 1, win 501, length 36
21:26:25.421848 IP lynx.ssh > 192.168.0.247.54444: Flags [P..], seq 2320:2460, ack 1, win 501, length 140
21:26:25.421988 IP lynx.ssh > 192.168.0.247.54444: Flags [P..], seq 2460:2496, ack 1, win 501, length 36
21:26:25.422212 IP lynx.ssh > 192.168.0.247.54444: Flags [P..], seq 2496:2636, ack 1, win 501, length 140
21:26:25.422389 IP lynx.ssh > 192.168.0.247.54444: Flags [P..], seq 2636:2672, ack 1, win 501, length 36
21:26:25.422573 IP lynx.ssh > 192.168.0.247.54444: Flags [P..], seq 2672:2812, ack 1, win 501, length 140
21:26:25.422710 IP lynx.ssh > 192.168.0.247.54444: Flags [P..], seq 2812:2848, ack 1, win 501, length 36
21:26:25.422998 IP lynx.ssh > 192.168.0.247.54444: Flags [P..], seq 2848:2988, ack 1, win 501, length 140
```

### 3. Filtering by Protocol

- Capture only TCP packets: **tcpdump tcp -i enp0s3**
- Useful for focusing on TCP traffic, which might be necessary for troubleshooting TCP connection issues.

```
lynx@lynx:~
```

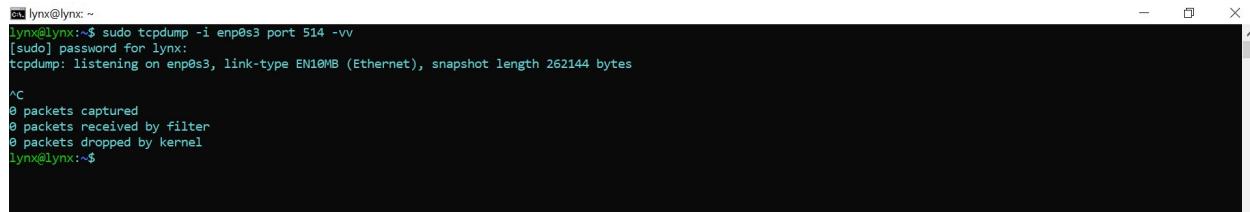
```
lynx@lynx:~$ sudo tcpdump tcp -i enp0s3
tcpdump: verbose output suppressed, use -v[V]... for full protocol decode
listening on enp0s3, link-type EN10MB (Ethernet), snapshot length 262144 bytes
21:28:42.723203 IP lynx.ssh > 192.168.0.247.54444: Flags [P..], seq 3132791193, ack 4109617946, win 501, length 108
21:28:42.723321 IP lynx.ssh > 192.168.0.247.54444: Flags [P..], seq 108:272, ack 1, win 501, length 164
21:28:42.723382 IP 192.168.0.247.54444 > lynx.ssh: Flags [.], ack 108, win 4102, length 0
21:28:42.723431 IP lynx.ssh > 192.168.0.247.54444: Flags [P..], seq 272:340, ack 1, win 501, length 68
21:28:42.723548 IP lynx.ssh > 192.168.0.247.54444: Flags [P..], seq 340:376, ack 1, win 501, length 36
21:28:42.723598 IP 192.168.0.247.54444 > lynx.ssh: Flags [.], ack 340, win 4101, length 0
21:28:42.723632 IP 192.168.0.247.54444 > lynx.ssh: Flags [.], ack 376, win 4101, length 0
21:28:43.033339 IP lynx.ssh > 192.168.0.247.54444: Flags [P..], seq 376:540, ack 1, win 501, length 164
21:28:43.033488 IP lynx.ssh > 192.168.0.247.54444: Flags [P..], seq 540:576, ack 1, win 501, length 36
21:28:43.033534 IP lynx.ssh > 192.168.0.247.54444: Flags [P..], seq 576:716, ack 1, win 501, length 140
21:28:43.033614 IP lynx.ssh > 192.168.0.247.54444: Flags [P..], seq 716:752, ack 1, win 501, length 36
21:28:43.033768 IP lynx.ssh > 192.168.0.247.54444: Flags [P..], seq 752:876, ack 1, win 501, length 124
21:28:43.033749 IP 192.168.0.247.54444 > lynx.ssh: Flags [.], ack 576, win 4101, length 0
21:28:43.033822 IP 192.168.0.247.54444 > lynx.ssh: Flags [.], ack 752, win 4106, length 0
21:28:43.033869 IP lynx.ssh > 192.168.0.247.54444: Flags [P..], seq 876:912, ack 1, win 501, length 36
21:28:43.033954 IP 192.168.0.247.54444 > lynx.ssh: Flags [.], ack 912, win 4105, length 0
21:28:43.033976 IP lynx.ssh > 192.168.0.247.54444: Flags [P..], seq 912:1052, ack 1, win 501, length 140
21:28:43.034120 IP lynx.ssh > 192.168.0.247.54444: Flags [P..], seq 1052:1088, ack 1, win 501, length 36
21:28:43.034158 IP lynx.ssh > 192.168.0.247.54444: Flags [P..], seq 1088:1228, ack 1, win 501, length 140
21:28:43.034262 IP lynx.ssh > 192.168.0.247.54444: Flags [P..], seq 1228:1264, ack 1, win 501, length 36
21:28:43.034322 IP 192.168.0.247.54444 > lynx.ssh: Flags [.], ack 1088, win 4104, length 0
21:28:43.034357 IP lynx.ssh > 192.168.0.247.54444: Flags [P..], seq 1264:1388, ack 1, win 501, length 124
21:28:43.034387 IP 192.168.0.247.54444 > lynx.ssh: Flags [.], ack 1264, win 4104, length 0
21:28:43.034497 IP lynx.ssh > 192.168.0.247.54444: Flags [P..], seq 1388:1424, ack 1, win 501, length 36
21:28:43.034583 IP lynx.ssh > 192.168.0.247.54444: Flags [P..], seq 1424:1548, ack 1, win 501, length 124
21:28:43.034683 IP 192.168.0.247.54444 > lynx.ssh: Flags [.], ack 1424, win 4103, length 0
21:28:43.034867 IP lynx.ssh > 192.168.0.247.54444: Flags [P..], seq 1548:1584, ack 1, win 501, length 36
21:28:43.035186 IP 192.168.0.247.54444 > lynx.ssh: Flags [.], ack 1584, win 4103, length 0
21:28:43.135063 IP lynx.ssh > 192.168.0.247.54444: Flags [P..], seq 1584:1724, ack 1, win 501, length 140
21:28:43.135457 IP lynx.ssh > 192.168.0.247.54444: Flags [P..], seq 1724:1760, ack 1, win 501, length 36
21:28:43.135555 IP lynx.ssh > 192.168.0.247.54444: Flags [P..], seq 1760:1980, ack 1, win 501, length 140
21:28:43.136284 IP 192.168.0.247.54444 > lynx.ssh: Flags [.], ack 1760, win 4102, length 0
21:28:43.136488 IP lynx.ssh > 192.168.0.247.54444: Flags [P..], seq 1900:1936, ack 1, win 501, length 36
21:28:43.136798 IP 192.168.0.247.54444 > lynx.ssh: Flags [.], ack 1936, win 4101, length 0
21:28:43.136776 IP lynx.ssh > 192.168.0.247.54444: Flags [P..], seq 1936:2076, ack 1, win 501, length 140
21:28:43.137049 IP lynx.ssh > 192.168.0.247.54444: Flags [P..], seq 2076:2112, ack 1, win 501, length 36
21:28:43.137282 IP lynx.ssh > 192.168.0.247.54444: Flags [P..], seq 2112:2252, ack 1, win 501, length 140
21:28:43.137332 IP 192.168.0.247.54444 > lynx.ssh: Flags [.], ack 2112, win 4100, length 0
```

## Capturing Syslog Messages

### Example Command

```
tcpdump -i enp0s3 port 514 -vv
```

- **-i eth0:** Specifies the interface to listen on.
- **port 514:** Filters packets for UDP port 514, the standard port for syslog messages.
- **-vv:** Verbose output, to see more details of each packet. You might not need this.



```
lynx@lynx:~$ sudo tcpdump -i enp0s3 port 514 -vv
[sudo] password for lynx:
tcpdump: listening on enp0s3, link-type EN10MB (Ethernet), snapshot length 262144 bytes
^C
0 packets captured
0 packets received by filter
0 packets dropped by kernel
lynx@lynx:~$
```

A screenshot of a terminal window titled 'lynx'. The window shows the command 'sudo tcpdump -i enp0s3 port 514 -vv' being run. It asks for a password and then displays the output of the command. The output shows that no packets were captured, received, or dropped. The window has a standard OS X style with a close button in the top right corner.

### Example Command (2)

```
tcpdump -port 514
```

- More simple and to the point if you are just validating syslog traffic.

## EXERCISE 8 – Syslog in Linux

### Configuration

- **/etc/rsyslog.conf:** The main configuration file for rsyslog. It defines global directives, module loading, and rules for how to handle and where to route log messages.

```
cd lynx@lynx:/etc$ cat rsyslog.conf
# /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 #####
#####

#
# Use traditional timestamp format.
# To enable high precision timestamps, comment out the following line.
#
$ActionFileDefaultTemplate RSYSLOG_TraditionalFileFormat

# Filter duplicated messages
$RepeatedMsgReduction on
#
```

- **/etc/rsyslog.d/**: A directory that can contain additional configuration files. Files in this directory are included in the configuration in alphabetical order, allowing for modular configuration setups.

```
cd lynx@lynx:/etc/rsyslog.d/
lynx@lynx:/etc/rsyslog.d$ ls -l
total 16
-rw-r--r-- 1 root root 314 Sep 19 2021 20-ufw.conf
-rw-r--r-- 1 root root 255 Jun 28 2023 21-cloudinit.conf
-rw-r--r-- 1 root root 1124 Nov 16 2021 50-default.conf
-rw-r--r-- 1 root root 242 Jan 29 08:02 postfix.conf
lynx@lynx:/etc/rsyslog.d$
```

## Task 1. Configure Syslog

Configure Syslog to send to Host OS

The screenshot shows two terminal sessions. The top session displays the contents of the /etc/rsyslog.conf file, which includes various log entries and system configurations. The bottom session shows the command `sudo tail /var/log/syslog` being run, followed by a series of kernel log messages indicating system initialization and device activity.

```
lynx@lynx:/etc
#input(type="imtcp" port="514")
# provides kernel logging support and enable non-kernel klog messages
module(load="imklog" permitnonkernelfacility="on")

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

#
# Use traditional timestamp format.
# To enable high precision timestamps, comment out the following line.
#
$ActionFileDefaultTemplate RSYSLOG_TraditionalFileFormat

# Filter duplicated messages
$RepeatedMsgReduction on

#
# Set the default permissions for all log files.
#
$fileOwner syslog
$fileGroup adm
$fileCreateMode 0640
$DirCreateMode 0755
$Mask 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

.* @192.168.0.47:514
-- INSERT --
```

```
lynx@lynx:~$ sudo tail /var/log/syslog
Mar 28 23:24:59 lynx kernel: [ 6928.463455] Bluetooth: L2CAP socket layer initialized
Mar 28 23:24:59 lynx kernel: [ 6928.463458] Bluetooth: SCO socket layer initialized
Mar 28 23:24:59 lynx kernel: [ 6928.469387] device enp0s3 entered promiscuous mode
Mar 28 23:26:07 lynx kernel: [ 6996.969736] device enp0s3 left promiscuous mode
Mar 28 23:46:08 lynx systemd[1]: session-6.scope: Deactivated successfully.
Mar 28 23:46:08 lynx systemd[1]: session-6.scope: Consumed 9.149s CPU time.
Mar 28 23:46:51 lynx systemd[1]: Started Session 8 of User lynx.
Mar 28 23:52:11 lynx lynx: test test test
Mar 28 23:52:34 lynx lynx: TEST TEST TEST
Mar 28 23:53:50 lynx lynx: test test test
lynx@lynx:~$
```

## Task 1. Tcpdump

**Task 2.** Using `tcpdump`, detect syslog traffic by running the following command:

```
sudo tcpdump -i any udp port 514 -w syslog_traffic.pcap
```

The screenshot shows a terminal session where the command `sudo tcpdump -i any udp port 514 -w syslog_traffic.pcap` is executed. The output indicates that tcpdump is listening on any interface, using link-type LINUX\_SLL2, and has a snapshot length of 262144 bytes.

```
lynx@lynx:~$ sudo tcpdump -i any udp port 514 -w syslog_traffic.pcap
tcpdump: data link type LINUX_SLL2
tcpdump: listening on any, link-type LINUX_SLL2 (Linux cooked v2), snapshot length 262144 bytes
```

Here's a breakdown of the command:

- **sudo:** Runs tcpdump with superuser privileges, which are usually required for capturing packets.

- **-i any:** Specifies the network interface on which to capture the traffic. Using any listens on all network interfaces.
- **udp port 514:** Filters the capture to only include UDP traffic on port 514, the default port for syslog messages.
- **-w syslog\_traffic.pcap:** Writes the captured packets to a file named **syslog\_traffic.pcap** instead of displaying them on the screen.

This command captures all syslog traffic across all network interfaces and saves it to a file for later analysis. You can then use tools like Wireshark or even **tcpdump** itself to read and analyze the captured data.