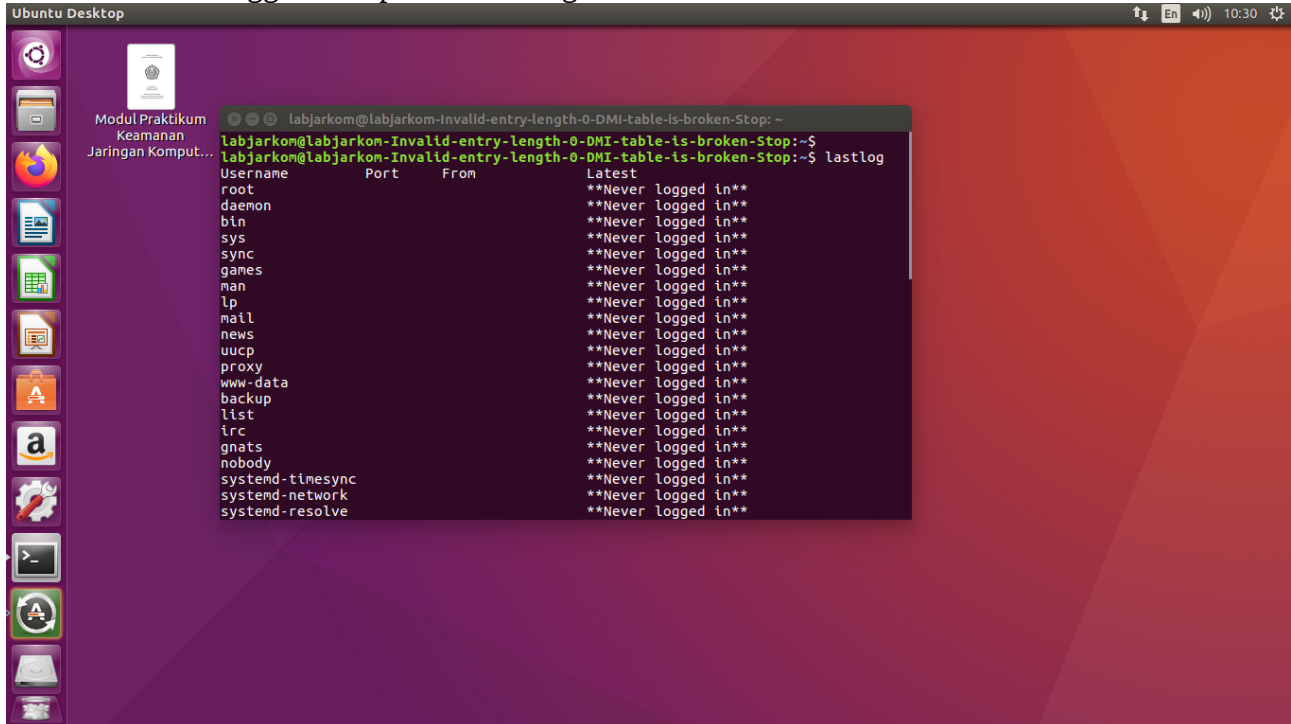


Nama : Reza Rivaldo Fakhry
NIM : L200170162

Laporan Praktikum Keamanan Jaringan Modul 3 Network Monitoring dan Log Analysis

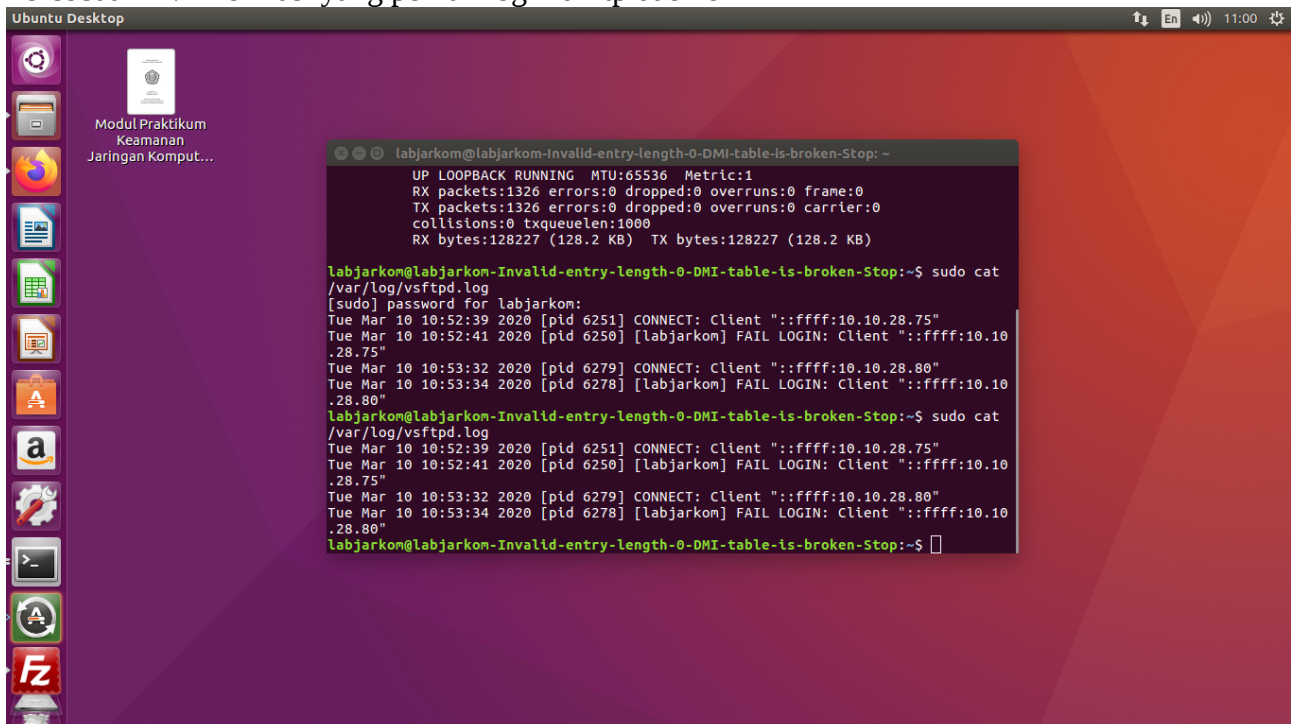
Percobaan 1 : Menggunakan perintah lastlog



The screenshot shows an Ubuntu Desktop environment with a terminal window open. The terminal displays the output of the `lastlog` command, which lists system users and their last login status. The output is as follows:

```
labjarkom@labjarkom-Invalid-entry-length-0-DMI-table-is-broken-Stop: ~  
labjarkom@labjarkom-Invalid-entry-length-0-DMI-table-is-broken-Stop:~$  
labjarkom@labjarkom-Invalid-entry-length-0-DMI-table-is-broken-Stop:~$ lastlog  
Username      Port      From      Latest  
root          **Never  logged in**  
daemon        **Never  logged in**  
bin           **Never  logged in**  
sys           **Never  logged in**  
sync          **Never  logged in**  
games         **Never  logged in**  
man           **Never  logged in**  
lp            **Never  logged in**  
mail          **Never  logged in**  
news          **Never  logged in**  
uucp          **Never  logged in**  
proxy         **Never  logged in**  
www-data      **Never  logged in**  
backup        **Never  logged in**  
list          **Never  logged in**  
irc           **Never  logged in**  
gnats         **Never  logged in**  
nobody        **Never  logged in**  
systemd-timesync **Never  logged in**  
systemd-network **Never  logged in**  
systemd-resolve **Never  logged in**
```

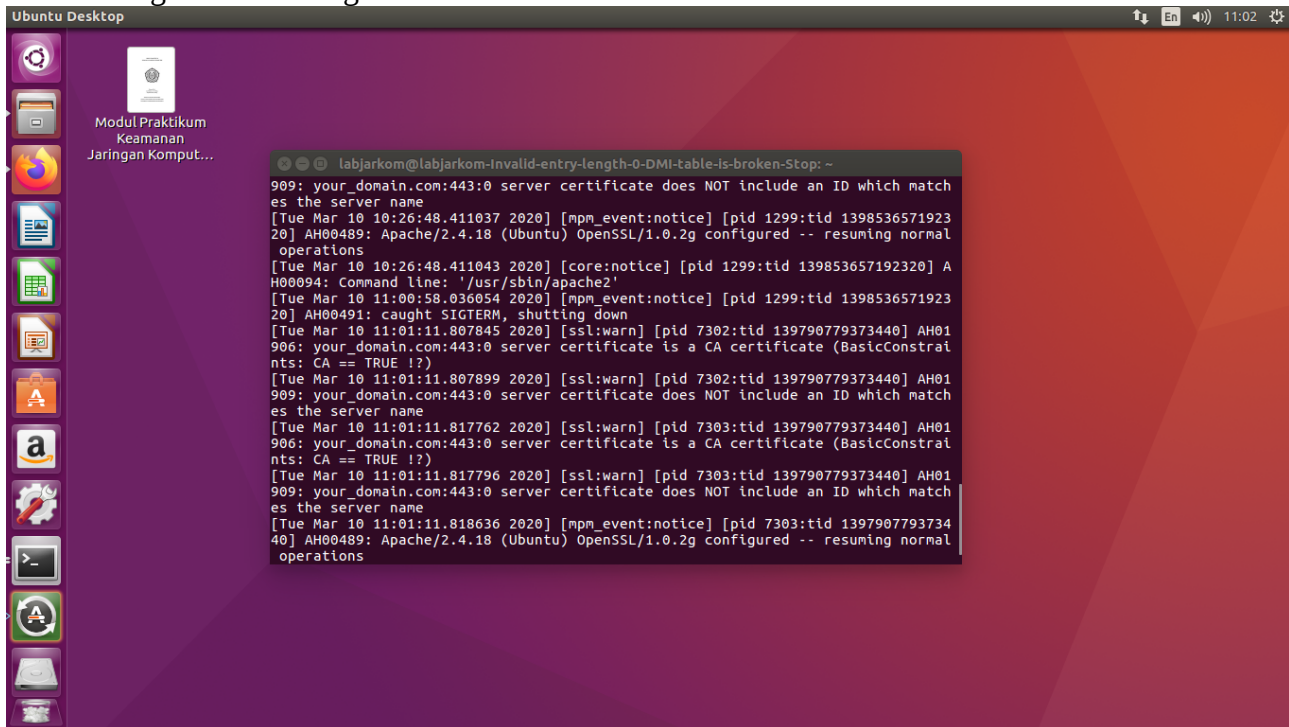
Percobaan 2 : Informasi yang pernah login di ftp daemon



The screenshot shows an Ubuntu Desktop environment with a terminal window open. The terminal displays the output of the `cat /var/log/vsftpd.log` command, which shows the log entries for the vsftpd daemon. The output is as follows:

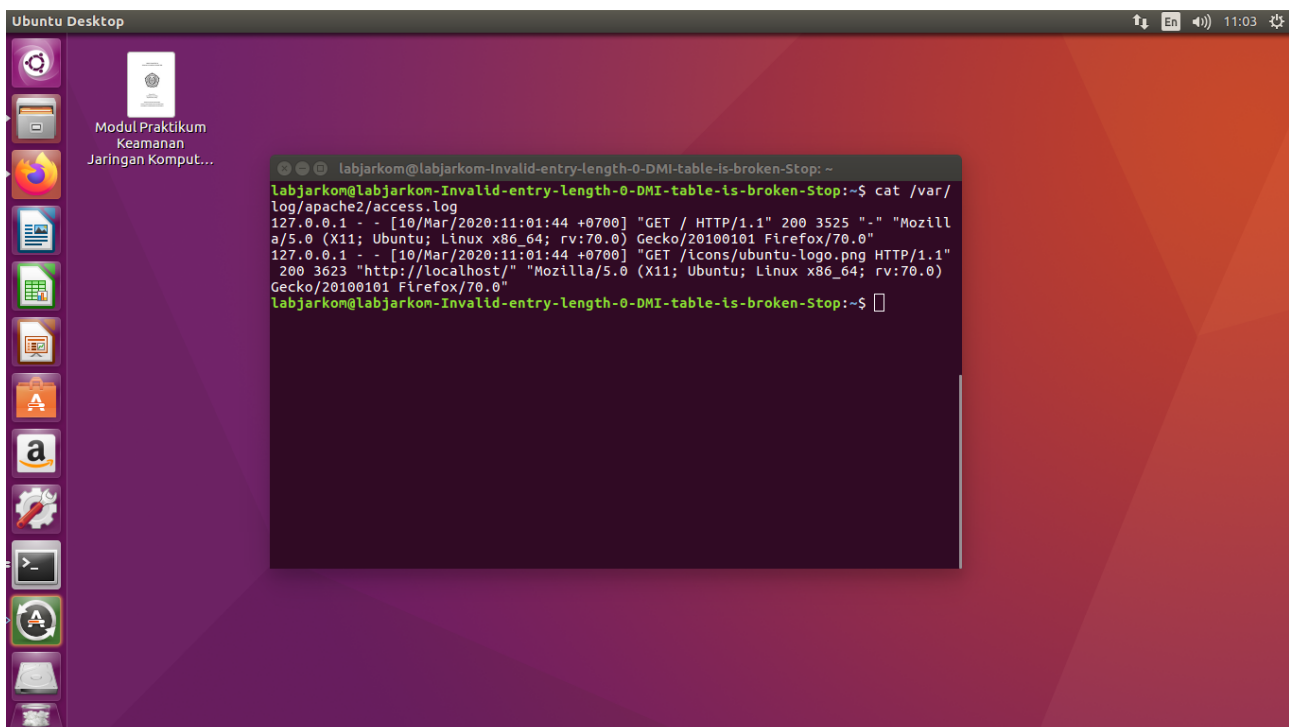
```
labjarkom@labjarkom-Invalid-entry-length-0-DMI-table-is-broken-Stop: ~  
UP LOOPBACK RUNNING MTU:65536 Metric:1  
RX packets:1326 errors:0 dropped:0 overruns:0 frame:0  
TX packets:1326 errors:0 dropped:0 overruns:0 carrier:0  
collisions:0 txqueuelen:1000  
RX bytes:128227 (128.2 KB) TX bytes:128227 (128.2 KB)  
  
labjarkom@labjarkom-Invalid-entry-length-0-DMI-table-is-broken-Stop:~$ sudo cat  
/var/log/vsftpd.log  
[sudo] password for labjarkom:  
Tue Mar 10 10:52:39 2020 [pid 6251] CONNECT: Client "::ffff:10.10.28.75"  
Tue Mar 10 10:52:41 2020 [pid 6250] [labjarkom] FAIL LOGIN: Client "::ffff:10.10.  
.28.75"  
Tue Mar 10 10:53:32 2020 [pid 6279] CONNECT: Client "::ffff:10.10.28.80"  
Tue Mar 10 10:53:34 2020 [pid 6278] [labjarkom] FAIL LOGIN: Client "::ffff:10.10.  
.28.80"  
labjarkom@labjarkom-Invalid-entry-length-0-DMI-table-is-broken-Stop:~$ sudo cat  
/var/log/vsftpd.log  
Tue Mar 10 10:52:39 2020 [pid 6251] CONNECT: Client "::ffff:10.10.28.75"  
Tue Mar 10 10:52:41 2020 [pid 6250] [labjarkom] FAIL LOGIN: Client "::ffff:10.10.  
.28.75"  
Tue Mar 10 10:53:32 2020 [pid 6279] CONNECT: Client "::ffff:10.10.28.80"  
Tue Mar 10 10:53:34 2020 [pid 6278] [labjarkom] FAIL LOGIN: Client "::ffff:10.10.  
.28.80"  
labjarkom@labjarkom-Invalid-entry-length-0-DMI-table-is-broken-Stop:~$
```

Percobaan 3 : Mengamati log pengaksesan sebuah halaman web file error.log dan access.log



The screenshot shows an Ubuntu Desktop environment with a purple background. On the left side, there is a vertical dock with various application icons. The desktop area contains a file manager icon and a folder named "Modul Praktikum Keamanan Jaringan Komput...". A terminal window is open in the center, displaying the following log output:

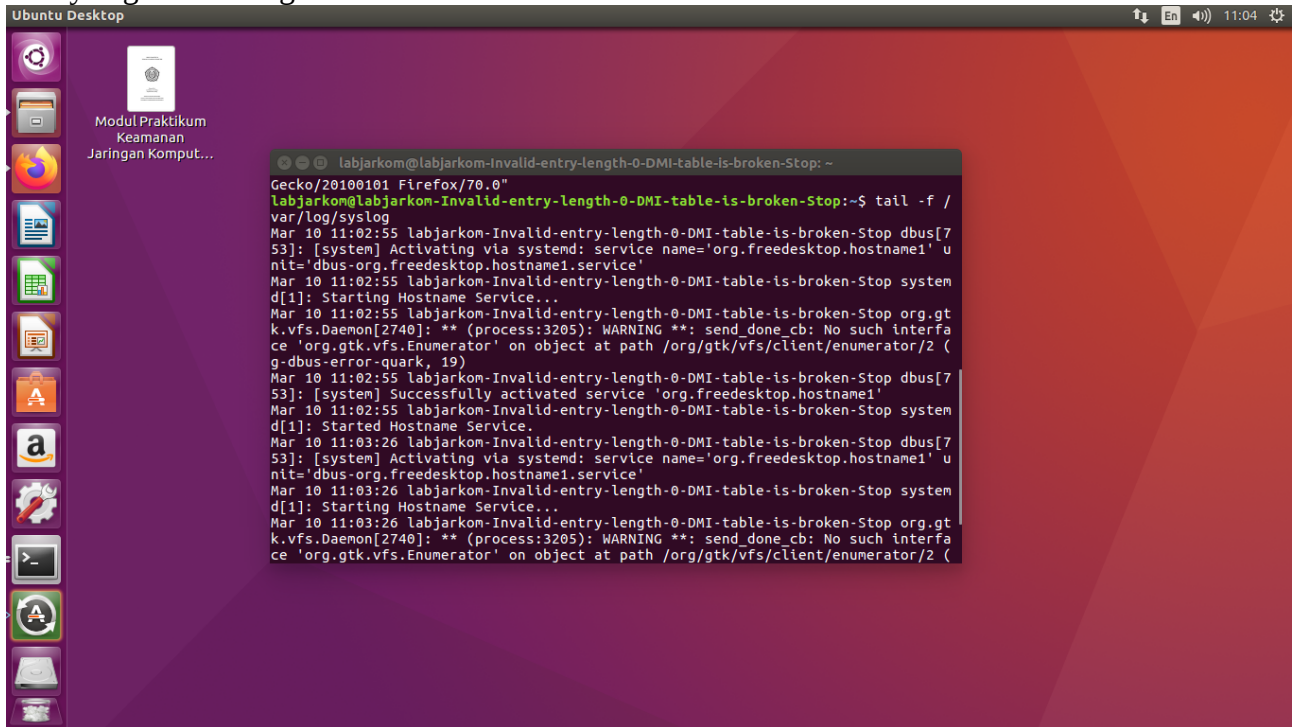
```
labjarkom@labjarkom-Invalid-entry-length-0-DMI-table-is-broken-Stop: ~  
909: your_domain.com:443:0 server certificate does NOT include an ID which matches the server name  
[Tue Mar 10 10:26:48.411037 2020] [mpm_event:notice] [pid 1299:tid 139853657192320] AH00489: Apache/2.4.18 (Ubuntu) OpenSSL/1.0.2g configured -- resuming normal operations  
[Tue Mar 10 10:26:48.411043 2020] [core:notice] [pid 1299:tid 139853657192320] AH0094: Command line: '/usr/sbin/apache2'  
[Tue Mar 10 11:00:58.036054 2020] [mpm_event:notice] [pid 1299:tid 139853657192320] AH00491: caught SIGTERM, shutting down  
[Tue Mar 10 11:01:11.807845 2020] [ssl:warn] [pid 7302:tid 139790779373440] AH01906: your_domain.com:443:0 server certificate is a CA certificate (BasicConstraints: CA == TRUE !?)  
[Tue Mar 10 11:01:11.807899 2020] [ssl:warn] [pid 7302:tid 139790779373440] AH01909: your_domain.com:443:0 server certificate does NOT include an ID which matches the server name  
[Tue Mar 10 11:01:11.817762 2020] [ssl:warn] [pid 7303:tid 139790779373440] AH01906: your_domain.com:443:0 server certificate is a CA certificate (BasicConstraints: CA == TRUE !?)  
[Tue Mar 10 11:01:11.817796 2020] [ssl:warn] [pid 7303:tid 139790779373440] AH01909: your_domain.com:443:0 server certificate does NOT include an ID which matches the server name  
[Tue Mar 10 11:01:11.818636 2020] [mpm_event:notice] [pid 7303:tid 139790779373440] AH00489: Apache/2.4.18 (Ubuntu) OpenSSL/1.0.2g configured -- resuming normal operations
```



The screenshot shows the same Ubuntu Desktop environment as the previous one. The terminal window now displays the output of the command `cat /var/log/apache2/access.log`:

```
labjarkom@labjarkom-Invalid-entry-length-0-DMI-table-is-broken-Stop:~$ cat /var/log/apache2/access.log  
127.0.0.1 - - [10/Mar/2020:11:01:44 +0700] "GET / HTTP/1.1" 200 3525 "-" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:70.0) Gecko/20100101 Firefox/70.0"  
127.0.0.1 - - [10/Mar/2020:11:01:44 +0700] "GET /icons/ubuntu-logo.png HTTP/1.1" 200 3623 "http://localhost/" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:70.0) Gecko/20100101 Firefox/70.0"  
labjarkom@labjarkom-Invalid-entry-length-0-DMI-table-is-broken-Stop:~$
```

file syslog dan messages



hasil

