PRAKTIKUM KEAMANAN JARINGAN KOMPUTER

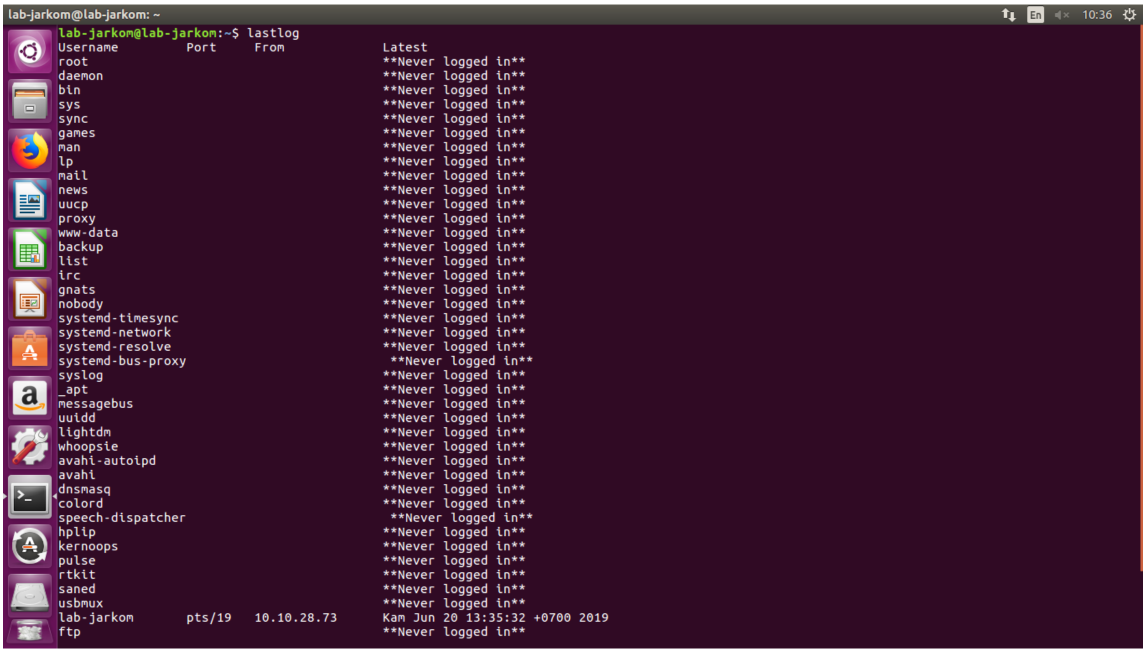
Modul 3

Nama : Tasya Farah Putri A.

NIM : L200170146

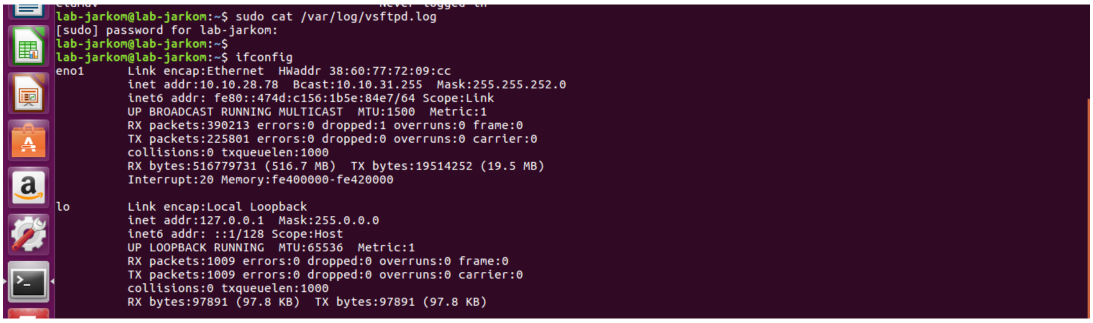
Kelas : A

I. **Percobaan 1 :** Menggunakan perintah lastlog



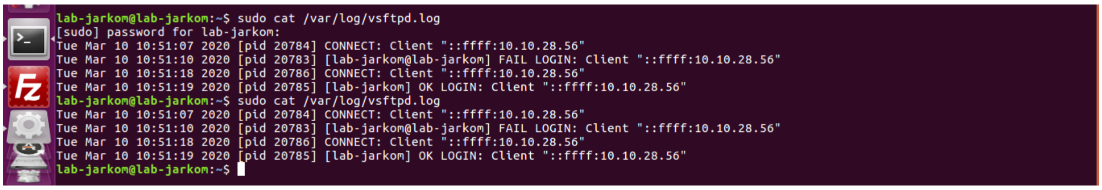
```
lab-jarkom@lab-jarkom:~$ lastlog
Username         Port     From             Latest
root                                       **Never logged in**
daemon                                     **Never logged in**
bin                                        **Never logged in**
sys                                        **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**
systemd-bus-proxy                           **Never logged in**
syslog                                     **Never logged in**
_apt                                       **Never logged in**
messagebus                                 **Never logged in**
uuidd                                      **Never logged in**
lightdm                                    **Never logged in**
whoopsie                                   **Never logged in**
avahi-autoipd                              **Never logged in**
avahi                                      **Never logged in**
dnsmasq                                    **Never logged in**
colord                                     **Never logged in**
speech-dispatcher                           **Never logged in**
hplip                                      **Never logged in**
kernoops                                   **Never logged in**
pulse                                      **Never logged in**
rtkit                                      **Never logged in**
saned                                      **Never logged in**
usbmux                                     **Never logged in**
lab-jarkom       pts/19   10.10.28.73      Kam Jun 20 13:35:32 +0700 2019
ftp                                        **Never logged in**
```

II. **Percobaan 2 :** Informai yang pernah loagin di ftp daemon



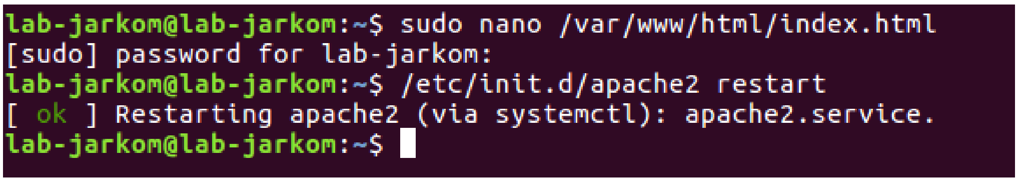
```
lab-jarkom@lab-jarkom:~$ sudo cat /var/log/vsftpd.log
[sudo] password for lab-jarkom:
lab-jarkom@lab-jarkom:~$
lab-jarkom@lab-jarkom:~$ ifconfig
eno1      Link encap:Ethernet  HWaddr 38:60:77:72:09:cc
          inet addr:10.10.28.78  Bcast:10.10.31.255  Mask:255.255.252.0
          inet6 addr: fe80::474d:c156:1b5e:84e7/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:390213 errors:0 dropped:1 overruns:0 frame:0
          TX packets:225801 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:516779731 (516.7 MB)  TX bytes:19514252 (19.5 MB)
          Interrupt:20 Memory:fe400000-fe420000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:1009 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1009 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:97891 (97.8 KB)  TX bytes:97891 (97.8 KB)
```

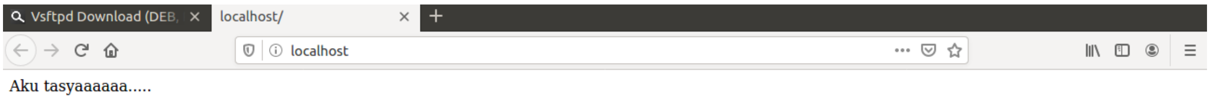


```
lab-jarkom@lab-jarkom:~$ sudo cat /var/log/vsftpd.log
[sudo] password for lab-jarkom:
Tue Mar 10 10:51:07 2020 [pid 20784] CONNECT: Client "::ffff:10.10.28.56"
Tue Mar 10 10:51:10 2020 [pid 20783] [lab-jarkom@lab-jarkom] FAIL LOGIN: Client "::ffff:10.10.28.56"
Tue Mar 10 10:51:18 2020 [pid 20786] CONNECT: Client "::ffff:10.10.28.56"
Tue Mar 10 10:51:19 2020 [pid 20785] [lab-jarkom] OK LOGIN: Client "::ffff:10.10.28.56"
lab-jarkom@lab-jarkom:~$ sudo cat /var/log/vsftpd.log
Tue Mar 10 10:51:07 2020 [pid 20784] CONNECT: Client "::ffff:10.10.28.56"
Tue Mar 10 10:51:10 2020 [pid 20783] [lab-jarkom@lab-jarkom] FAIL LOGIN: Client "::ffff:10.10.28.56"
Tue Mar 10 10:51:18 2020 [pid 20786] CONNECT: Client "::ffff:10.10.28.56"
Tue Mar 10 10:51:19 2020 [pid 20785] [lab-jarkom] OK LOGIN: Client "::ffff:10.10.28.56"
lab-jarkom@lab-jarkom:~$
```

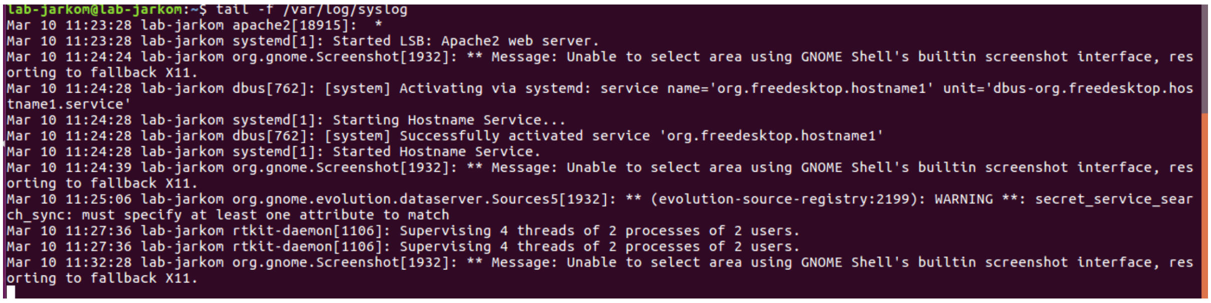
III. **Percobaan 3 :** Mengamati log pengaksesan ebuah halaman web



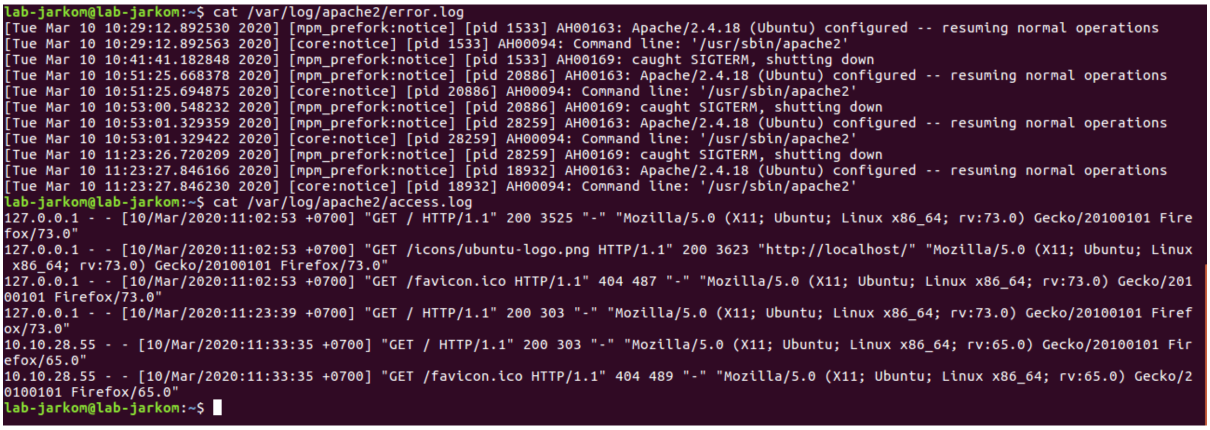
```
lab-jarkom@lab-jarkom:~$ sudo nano /var/www/html/index.html
[sudo] password for lab-jarkom:
lab-jarkom@lab-jarkom:~$ /etc/init.d/apache2 restart
[ ok ] Restarting apache2 (via systemctl): apache2.service.
lab-jarkom@lab-jarkom:~$
```



Aku tasyaaaaaa.....



```
lab-jarkom@lab-jarkom:~$ tail -f /var/log/syslog
Mar 10 11:23:28 lab-jarkom apache2[18915]:  *
Mar 10 11:23:28 lab-jarkom systemd[1]: Started LSB: Apache2 web server.
Mar 10 11:24:24 lab-jarkom org.gnome.Screenshot[1932]: ** Message: Unable to select area using GNOME Shell's builtin screenshot interface, res
orting to fallback X11.
Mar 10 11:24:28 lab-jarkom dbus[762]: [system] Activating via systemd: service name='org.freedesktop.hostname1' unit='dbus-org.freedesktop.hos
tname1.service'
Mar 10 11:24:28 lab-jarkom systemd[1]: Starting Hostname Service...
Mar 10 11:24:28 lab-jarkom dbus[762]: [system] Successfully activated service 'org.freedesktop.hostname1'
Mar 10 11:24:28 lab-jarkom systemd[1]: Started Hostname Service.
Mar 10 11:24:39 lab-jarkom org.gnome.Screenshot[1932]: ** Message: Unable to select area using GNOME Shell's builtin screenshot interface, res
orting to fallback X11.
Mar 10 11:25:06 lab-jarkom org.gnome.evolution.dataserver.Sources5[1932]: ** (evolution-source-registry:2199): WARNING **: secret_service_sear
ch_sync: must specify at least one attribute to match
Mar 10 11:27:36 lab-jarkom rtkit-daemon[1106]: Supervising 4 threads of 2 processes of 2 users.
Mar 10 11:27:36 lab-jarkom rtkit-daemon[1106]: Supervising 4 threads of 2 processes of 2 users.
Mar 10 11:32:28 lab-jarkom org.gnome.Screenshot[1932]: ** Message: Unable to select area using GNOME Shell's builtin screenshot interface, res
orting to fallback X11.
```



```
lab-jarkom@lab-jarkom:~$ cat /var/log/apache2/error.log
[Tue Mar 10 10:29:12.892530 2020] [mpm_prefork:notice] [pid 1533] AH00163: Apache/2.4.18 (Ubuntu) configured -- resuming normal operations
[Tue Mar 10 10:29:12.892563 2020] [core:notice] [pid 1533] AH00094: Command line: '/usr/sbin/apache2'
[Tue Mar 10 10:41:41.182848 2020] [mpm_prefork:notice] [pid 1533] AH00169: caught SIGTERM, shutting down
[Tue Mar 10 10:51:25.668378 2020] [mpm_prefork:notice] [pid 20886] AH00163: Apache/2.4.18 (Ubuntu) configured -- resuming normal operations
[Tue Mar 10 10:51:25.694875 2020] [core:notice] [pid 20886] AH00094: Command line: '/usr/sbin/apache2'
[Tue Mar 10 10:53:00.548232 2020] [mpm_prefork:notice] [pid 20886] AH00169: caught SIGTERM, shutting down
[Tue Mar 10 10:53:01.329359 2020] [mpm_prefork:notice] [pid 28259] AH00163: Apache/2.4.18 (Ubuntu) configured -- resuming normal operations
[Tue Mar 10 10:53:01.329422 2020] [core:notice] [pid 28259] AH00094: Command line: '/usr/sbin/apache2'
[Tue Mar 10 11:23:26.720209 2020] [mpm_prefork:notice] [pid 28259] AH00169: caught SIGTERM, shutting down
[Tue Mar 10 11:23:27.846166 2020] [mpm_prefork:notice] [pid 18932] AH00163: Apache/2.4.18 (Ubuntu) configured -- resuming normal operations
[Tue Mar 10 11:23:27.846230 2020] [core:notice] [pid 18932] AH00094: Command line: '/usr/sbin/apache2'
lab-jarkom@lab-jarkom:~$ cat /var/log/apache2/access.log
127.0.0.1 - - [10/Mar/2020:11:02:53 +0700] "GET / HTTP/1.1" 200 3525 "-" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:73.0) Gecko/20100101 Fire
fox/73.0"
127.0.0.1 - - [10/Mar/2020:11:02:53 +0700] "GET /icons/ubuntu-logo.png HTTP/1.1" 200 3623 "http://localhost/" "Mozilla/5.0 (X11; Ubuntu; Linux
 x86_64; rv:73.0) Gecko/20100101 Firefox/73.0"
127.0.0.1 - - [10/Mar/2020:11:02:53 +0700] "GET /favicon.ico HTTP/1.1" 404 487 "-" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:73.0) Gecko/201
00101 Firefox/73.0"
127.0.0.1 - - [10/Mar/2020:11:23:39 +0700] "GET / HTTP/1.1" 200 303 "-" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:73.0) Gecko/20100101 Firef
ox/73.0"
10.10.28.55 - - [10/Mar/2020:11:33:35 +0700] "GET / HTTP/1.1" 200 303 "-" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:65.0) Gecko/20100101 Fir
efox/65.0"
10.10.28.55 - - [10/Mar/2020:11:33:35 +0700] "GET /favicon.ico HTTP/1.1" 404 489 "-" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:65.0) Gecko/2
0100101 Firefox/65.0"
lab-jarkom@lab-jarkom:~$
```