

Nama : Aliya Faradila

Kelas : ADSIS-E

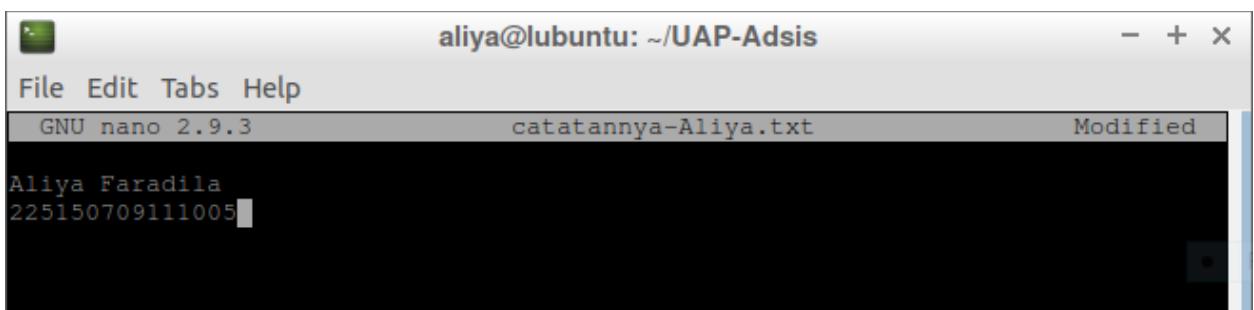
NIM : 225150709111005

1. Buat direktori dengan nama UAP-Adsis, isi dengan file txt dengan format penamaan catatannya-<nama kamu>.txt, kemudian isi file txt tersebut dengan nama dan NIM kamu. Kemudian atur permission view-only pada file tersebut untuk user biasa. Tunjukkan bukti berupa screenshot yang menunjukkan bahwa file tersebut berhasil diatur permissionnya menjadi view-only untuk user biasa.

Jawaban :

```
aliya@lubuntu:~$ mkdir UAP-Adsis
aliya@lubuntu:~$ ls
2023-05-19-135904_800x600_scrot.png  Desktop          susasadad.abw.bak~
2023-05-19-145333_800x600_scrot.png  Documents        Templates
2023-05-19-145334_800x600_scrot.png  Downloads        tesfile.txt
2023-05-19-145752_800x600_scrot.png  jcameron-key.asc testps.txt
2023-05-19-145753_800x600_scrot.png  Music           testpx.txt
2023-05-19-150735_800x600_scrot.png  Pictures         UAP-Adsis
aliy.txt                           Public          usus.txt
bashcase.sh                         sistemku.sh    Videos
bashtugas.sh                        sqlku.sh      susasadad.abw
cron.txt
aliya@lubuntu:~$ cd UAP-Adsis
aliya@lubuntu:~/UAP-Adsis$ touch catatannya-Aliya.txt
aliya@lubuntu:~/UAP-Adsis$ sudo nano catatannya-Aliya.txt
[sudo] password for aliya:
aliya@lubuntu:~/UAP-Adsis$
```

Membuat folder “UAP-Adsis” dan mengecek apakah berhasil membuat folder, selanjutnya membuat file “catatannya-Aliya.txt”



Menambahkan nama dan nim pada file “catatannya-Aliya.txt”

```
aliya@lubuntu:~/UAP-Adsis$ chmod 400 catatannya-Aliya.txt
aliya@lubuntu:~/UAP-Adsis$ ls -l
total 4
-r----- 1 aliyia aliyia 31 Jun 11 14:54 catatannya-Aliya.txt
aliya@lubuntu:~/UAP-Adsis$
```

Mengubah permission untuk user biasa hanya view/melihat

2. Lakukan konfigurasi alamat IP address sementara pada sistem dan default gateway.
(petunjuk 192.168.56.x | x adalah nomor absen)

Jawaban :

```
aliya@lubuntu:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 10.0.2.15 netmask 255.255.255.0 broadcast 10.0.2.255
        inet6 fe80::a00:27ff:fed:a1e9 prefixlen 64 scopeid 0x20<link>
          ether 08:00:27:da:1e:93 txqueuelen 1000 (Ethernet)
            RX packets 1119 bytes 122848 (122.8 KB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 1149 bytes 114597 (114.5 KB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

enp0s8: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 192.168.56.108 netmask 255.255.255.0 broadcast 192.168.56.255
        inet6 fe80::a00:27ff:fe54:ce85 prefixlen 64 scopeid 0x20<link>
          ether 08:00:27:54:ce:85 txqueuelen 1000 (Ethernet)
            RX packets 29 bytes 4771 (4.7 KB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 37 bytes 5362 (5.3 KB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
        inet 127.0.0.1 netmask 255.0.0.0
        inet6 ::1 prefixlen 128 scopeid 0x10<host>
          loop txqueuelen 1000 (Local Loopback)
            RX packets 204 bytes 15964 (15.9 KB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 204 bytes 15964 (15.9 KB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

aliya@lubuntu:~$
```

Mengecek ip awal pada enp0s8

```
aliya@lubuntu:~$ sudo ifconfig enp0s8 192.168.56.23 netmask 255.255.255.0
aliya@lubuntu:~$
```

Melakukan perubahan ip pada enp0s8

```
aliya@lubuntu:~$ ifconfig enp0s8
enp0s8: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 192.168.56.23 netmask 255.255.255.0 broadcast 192.168.56.255
        inet6 fe80::a00:27ff:fe54:ce85 prefixlen 64 scopeid 0x20<link>
          ether 08:00:27:54:ce:85 txqueuelen 1000 (Ethernet)
            RX packets 36 bytes 5383 (5.3 KB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 45 bytes 6934 (6.9 KB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

aliya@lubuntu:~$
```

Ip enp0s8 berhasil berubah

```

aliya@lubuntu:~$ sudo ip route add default via 192.168.56.1
aliya@lubuntu:~$ sudo route -n
Kernel IP routing table
Destination     Gateway         Genmask        Flags Metric Ref    Use Iface
0.0.0.0         192.168.56.1   0.0.0.0       UG    0      0        0 enp0s8
0.0.0.0         10.0.2.2       0.0.0.0       UG    100    0        0 enp0s3
10.0.2.0        0.0.0.0        255.255.255.0 U     100    0        0 enp0s3
192.168.56.0    0.0.0.0        255.255.255.0 U     101    0        0 enp0s8
192.168.56.0    0.0.0.0        255.255.255.0 U     101    0        0 enp0s8

```

Mengubah default gateway menjadi “192.168.56.1” dan mengecek apakah telah berhasil.

- Lakukan Instalasi Webmin lalu buatlah user bernama nama anda, lalu buat group Adsis_(kelas masing-masing) dan masukkan nama anda di group
- Jawaban :

```

aliya@lubuntu:~$ sudo apt-get install webmin
Reading package lists... Done
Building dependency tree
Reading state information... Done
webmin is already the newest version (2.021).
0 upgraded, 0 newly installed, 0 to remove and 591 not upgraded.

```

Sudah melakukan instalasi lanjut ke tahap berikutnya

The screenshot shows the Webmin interface with the 'Users and Groups' module open. At the top, there's a header with a star icon, the title 'Users and Groups', and a note 'Database type: Regular /etc/passwd & /etc/shadow'. Below the header, there are tabs for 'Local Users' (selected) and 'Local Groups'. A red box highlights the 'Create a new group' button. In the main area, there's a 'Create Group' dialog box. The dialog has a 'Group Details' section with fields for 'Group name' (set to 'Adsis_E'), 'Group ID' (set to 'Automatic' with value '1001'), and 'Password' options ('No password required' is selected). Below this, there are 'Members' sections for 'All users' (listing 'daemon', 'bin', 'sys') and 'Users in group' (listing 'aliya').

Membuat grup dengan nama Adsis_E dan memasukkan nama “aliya” pada grup Adsis_E

The screenshot shows the 'Users and Groups' section of the Webmin interface. At the top, it says 'Database type: Regular /etc/passwd & /etc/shadow'. Below that, there are tabs for 'Local Users' and 'Local Groups'. Under 'Local Groups', there is a table with columns: Group name, Group ID, and Members. A new group 'Adsis_E' has been created with Group ID 1001 and member 'aliya'. The row for 'Adsis_E' is highlighted with a red box.

Group name	Group ID	Members
adm	4	syslog aliya
Adsis_E	1001	aliya

Berhasil membuat grup Adsis_E dan memasukkan “aliya” pada grup.

4. Lakukan ping ke alamat ip anda dan coba lakukan reject dan drop di webmin, lalu analisis apa yang terjadi?

Jawaban :

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.2.9200]
(c) 2012 Microsoft Corporation. All rights reserved.

C:\Users\user>ping 192.168.56.108

Pinging 192.168.56.108 with 32 bytes of data:
Reply from 192.168.56.108: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.56.108:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Ping statistics for 192.168.56.108:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
Appr
C:\Users\user>
```

Melakukan ping ke ip ubuntu dan Pada gambar diatas proses ping berhasil dilakukan dengan adanya reply dari server.

The screenshot shows the 'Linux IPTables Firewall' interface. It displays the IPv4 Firewall rules file located at /etc/webmin/firewall/iptables.save. The 'Showing IPTable:' dropdown is set to 'Packet filtering (filter)'. A message box states: 'Incoming packets (INPUT) - Only applies to packets addressed to this host. There are no rules defined for this chain.' A 'Set Default Action To:' dropdown is set to 'Accept'. A green 'Add Rule' button is visible in the bottom right corner.

Masuk pada webmin dan memilih incoming packets (INPUT) kemudian Add Rule.

- 1) Membuat rule Reject, kemudian save changes lalu klik apply configuration.

The screenshot shows the 'Add Rule' interface for the IPv4 Firewall. The 'Chain and action details' section specifies the rule applies to 'Incoming packets (INPUT)' and the 'Action to take' is 'Reject'. The 'Condition details' section shows no specific source or destination, but the 'Incoming interface' is set to 'enp0s3'. The 'Network protocol' is set to 'ICMP'. In the main list, there is one rule: 'Reject' for ICMP. At the bottom, the 'Apply Configuration' button is highlighted.

Chain and action details

Part of chain: Incoming packets (INPUT) - Only applies to packets addressed to this host

Rule comment:

Action to take:

- Do nothing
- Accept
- Drop
- Reject
- Userspace
- Exit chain

Reject with ICMP type:

- Default
- Type: icmp-net-unreachable

The action selected above will only be carried out if all the conditions below are met.

Condition details

Source address or network: <ignored>

Destination address or network: <ignored>

Incoming interface: <ignored> enp0s3

Outgoing interface: <ignored> enp0s3

Fragmentation:

- Ignored
- Is fragmented
- Is not fragmented

Network protocol: Equals ICMP

Incoming packets (INPUT) - Only applies to packets addressed to this host

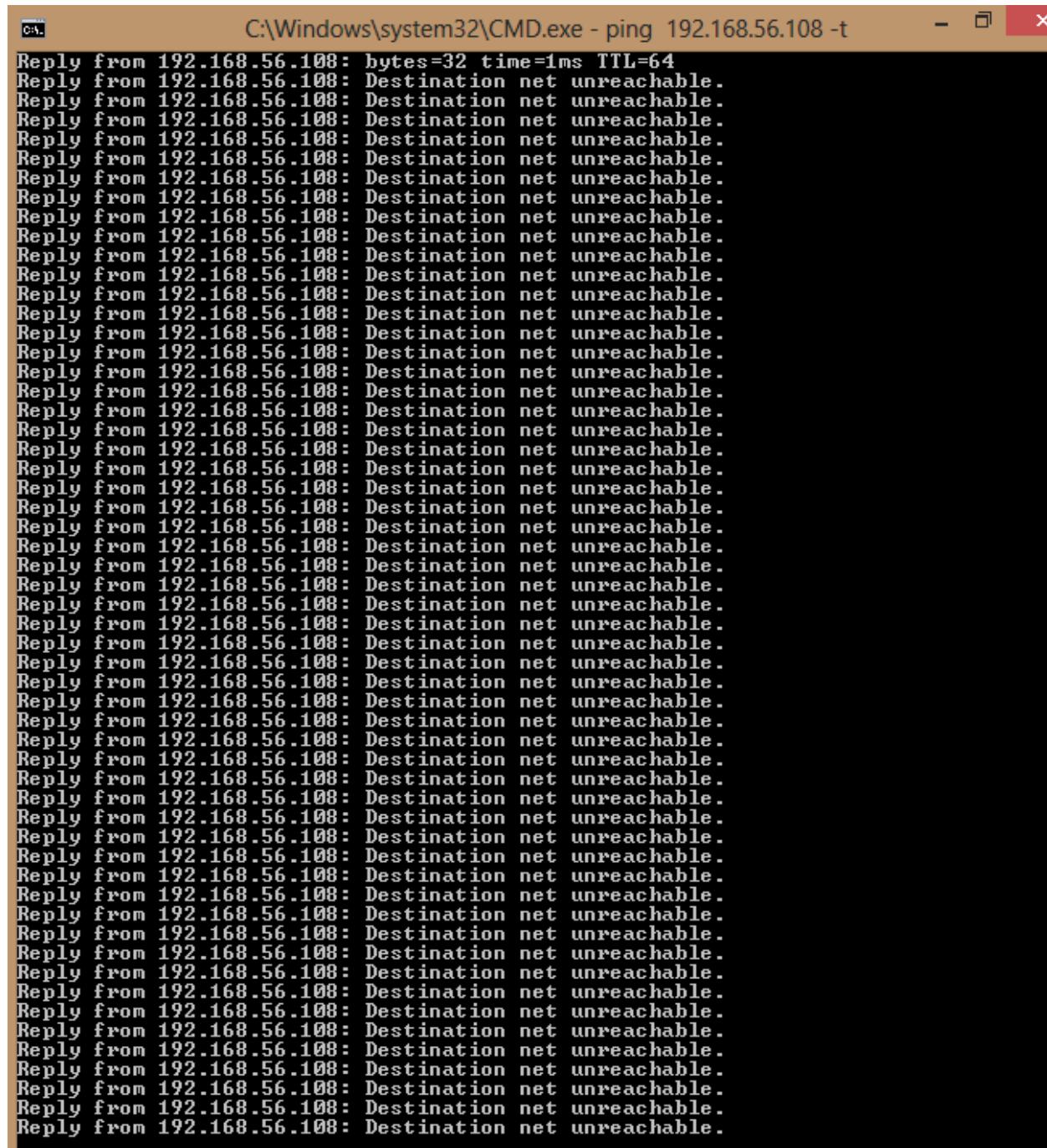
Select all Invert selection

Action	Condition	Move	Add
<input checked="" type="checkbox"/> Reject	If protocol is ICMP	<input type="button" value="Move"/>	<input type="button" value="Add"/>

Apply Configuration Click this button to make the firewall configuration listed above active. Any firewall rules currently in effect will be flushed and replaced.

Revert Configuration Click this button to reset the configuration listed above to the one that is currently active.

Paket ICMP atau Ping berhasil di reject. Melakukan test ping lagi kepada ip ubuntu dan gagal hal ini dikarenakan kita telah membuat sebuah rule firewall pada ipv4 yang dimana kita tidak bisa memping atau memblok sehingga muncul destination net unreachable.



C:\Windows\system32\CMD.exe - ping 192.168.56.108 -t

```
Reply from 192.168.56.108: bytes=32 time=1ms TTL=64
Reply from 192.168.56.108: Destination net unreachable.
```

- 2) Membuat rule Drop, kemudian save changes lalu klik apply configuration.

Add Rule
IPv4 Firewall

Chain and action details

Part of chain: Incoming packets (INPUT) - Only applies to packets addressed to this host

Rule comment:

Action to take:

- Do nothing
- Accept
- Drop
- Reject
- Log packet
- Run chain

Reject with ICMP type: Default Type: icmp-net-unreachable

The action selected above will only be carried out if all the conditions below are met.

Condition details

Source address or network	<Ignored>		
Destination address or network	<Ignored>		
Incoming interface	<Ignored>	enp0s3	
Outgoing interface	<Ignored>	enp0s3	
Fragmentation	<input checked="" type="radio"/> Ignored	<input type="radio"/> Is fragmented	<input type="radio"/> Is not fragmented
Network protocol	Equals	ICMP	

Incoming packets (INPUT) - Only applies to packets addressed to this host

Select all

Action	Condition	Move	Add
<input checked="" type="checkbox"/> Drop	If protocol is ICMP	<input type="button" value="↑"/>	<input type="button" value="↓"/>
<input checked="" type="checkbox"/> Select all	<input type="button" value="Invert selection"/>		

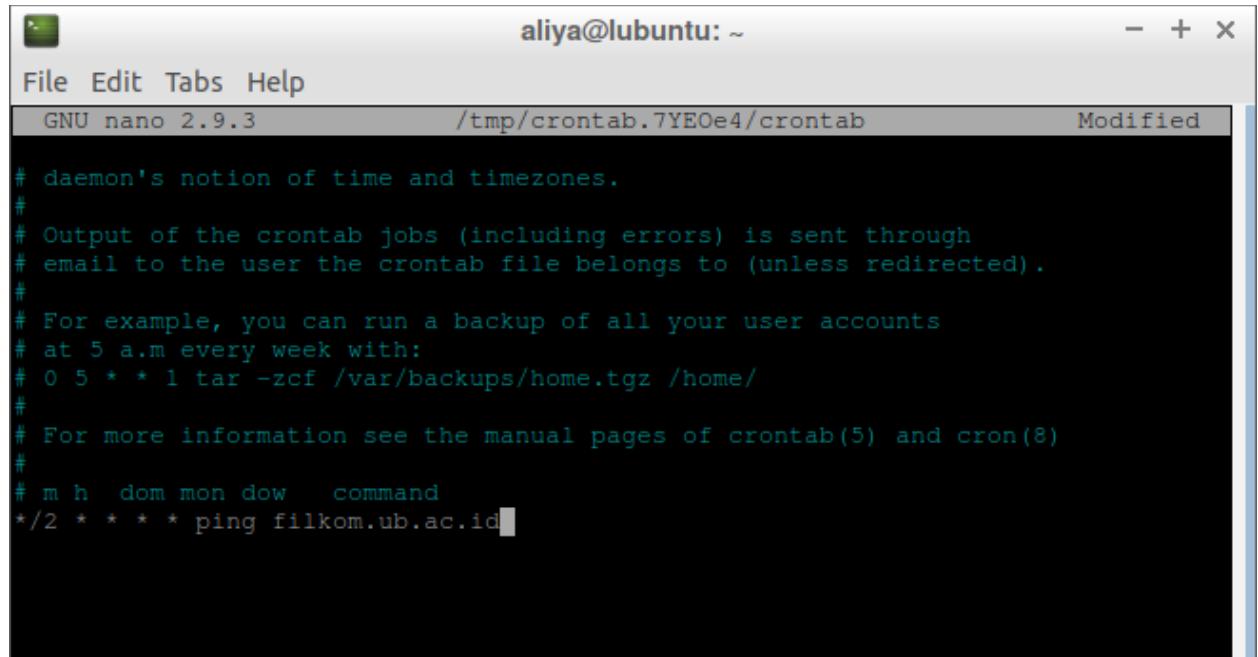
Paket ICMP atau Ping berhasil di drop. Melakukan test ping lagi kepada ip ubuntu dan gagal sehingga Request Timed Out.

5. Buatlah perintah otomatis yang berfungsi untuk ping www.filkom.ub.ac.id

Jawaban :

```
aliya@lubuntu:~$ sudo crontab -e
```

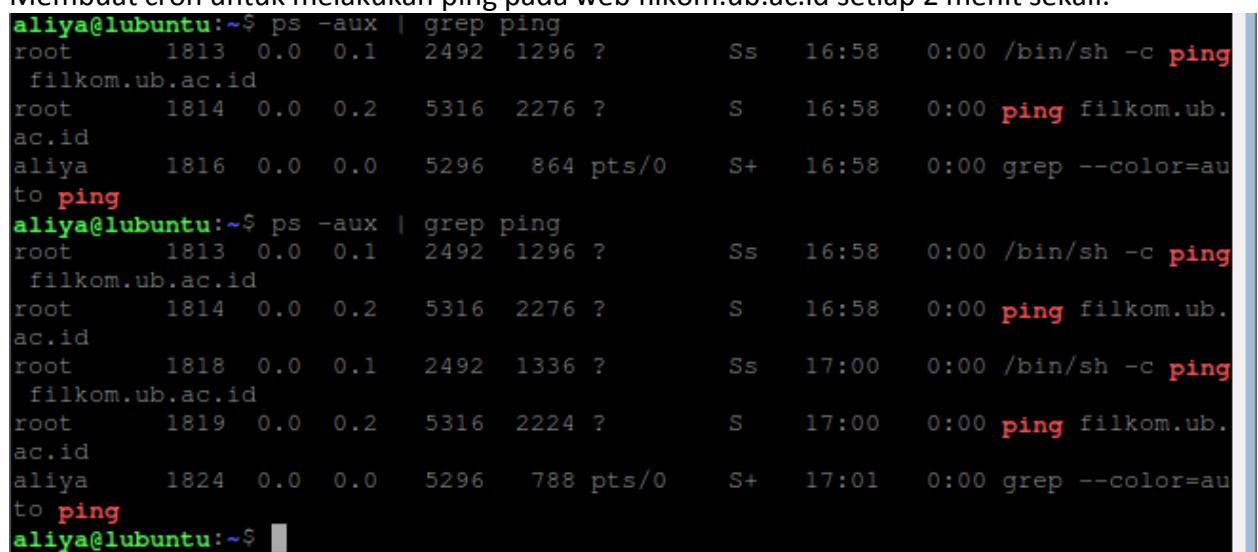
Buka Crontab untuk menyetting perintah otomatis



The screenshot shows a terminal window with the title bar "aliya@lubuntu: ~". The menu bar includes "File Edit Tabs Help". The window content is a terminal session where the user is editing a crontab file using the nano editor. The file path is "/tmp/crontab.7YE0e4/crontab". The text in the editor is:

```
# daemon's notion of time and timezones.  
#  
# Output of the crontab jobs (including errors) is sent through  
# email to the user the crontab file belongs to (unless redirected).  
#  
# For example, you can run a backup of all your user accounts  
# at 5 a.m every week with:  
# 0 5 * * 1 tar -zcf /var/backups/home.tgz /home/  
#  
# For more information see the manual pages of crontab(5) and cron(8)  
#  
# m h dom mon dow   command  
*/2 * * * * ping filkom.ub.ac.id
```

Membuat cron untuk melakukan ping pada web filkom.ub.ac.id setiap 2 menit sekali.



The screenshot shows a terminal session with the title bar "aliya@lubuntu: ~". The user runs the "ps -aux | grep ping" command to check if the cron job is running. The output shows several processes named "ping" running at different times. The output is:

```
aliya@lubuntu:~$ ps -aux | grep ping  
root      1813  0.0  0.1  2492  1296 ?          Ss   16:58  0:00 /bin/sh -c ping  
filkom.ub.ac.id  
root      1814  0.0  0.2  5316  2276 ?          S    16:58  0:00 ping filkom.ub.  
ac.id  
aliya    1816  0.0  0.0  5296   864 pts/0     S+   16:58  0:00 grep --color=au  
to ping  
aliya@lubuntu:~$ ps -aux | grep ping  
root      1813  0.0  0.1  2492  1296 ?          Ss   16:58  0:00 /bin/sh -c ping  
filkom.ub.ac.id  
root      1814  0.0  0.2  5316  2276 ?          S    16:58  0:00 ping filkom.ub.  
ac.id  
root      1818  0.0  0.1  2492  1336 ?          Ss   17:00  0:00 /bin/sh -c ping  
filkom.ub.ac.id  
root      1819  0.0  0.2  5316  2224 ?          S    17:00  0:00 ping filkom.ub.  
ac.id  
aliya    1824  0.0  0.0  5296   788 pts/0     S+   17:01  0:00 grep --color=au  
to ping  
aliya@lubuntu:~$
```

Berhasil memping web filkom.ub.ac.id setiap 2 menit.