

MODUL 4

FIREWALL

Wyne Habsari/L200160080

1. Percobaan 1 : Menghapus 'rules' pada iptables

- a. Cek aturan 'rules' di iptables pada server

```
root@wyne-VirtualBox:/home/wyne# iptables -L
```

- b. Hasilnya, belum ada rules yang terpasang karna baru saja menginstalasi server

```
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

- c. Untuk menghapus rule yang terpasang, menggunakan perintah

```
root@wyne-VirtualBox:/home/wyne# iptables -F
```

2. Percobaan 2: Blocking semua trafik

- a. Perintah untuk mengijinkan sesi sambungan untuk menerima trafik dari semua client

```
root@wyne-VirtualBox:/home/wyne# sudo iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
```

- b. Melakukan pengujian dari komputer client :

- i. Komputer client **terhubung** dengan server dengan tes ping

```
C:\Users\Asus-X453S>ping 192.168.43.82

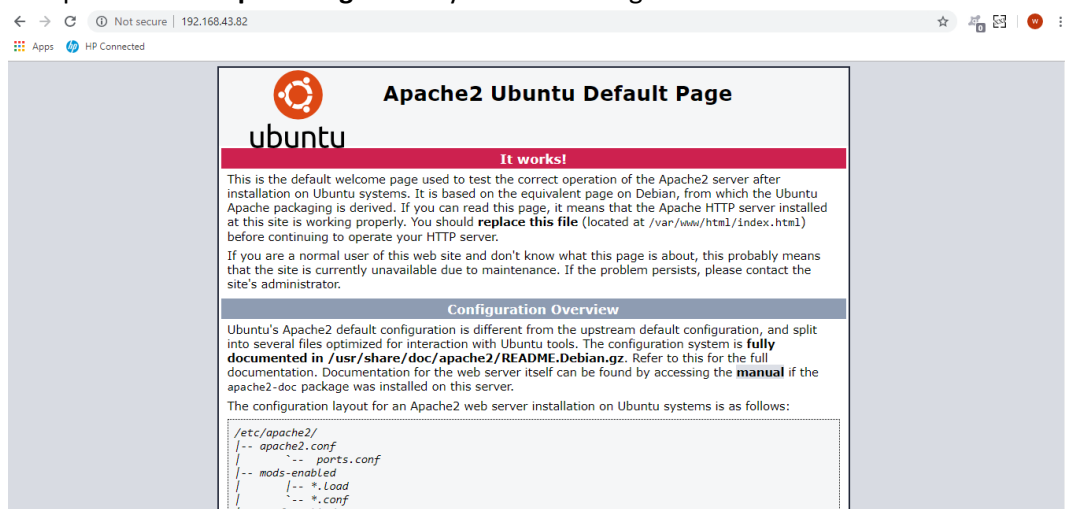
Pinging 192.168.43.82 with 32 bytes of data:
Reply from 192.168.43.82: bytes=32 time=5ms TTL=64
Reply from 192.168.43.82: bytes=32 time=2ms TTL=64
Reply from 192.168.43.82: bytes=32 time=3ms TTL=64
Reply from 192.168.43.82: bytes=32 time=3ms TTL=64

Ping statistics for 192.168.43.82:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 5ms, Average = 3ms
```

- ii. Komputer client **dapat mengakses** layanan SSH melalui software Putty

```
wyne@wyne-VirtualBox: ~  
login as: wyne  
wyne@192.168.43.82's password:  
Welcome to Ubuntu 16.04.3 LTS (GNU/Linux 4.10.0-28-generic x86_64)  
  
* Documentation:  https://help.ubuntu.com  
* Management:    https://landscape.canonical.com  
* Support:        https://ubuntu.com/advantage  
  
538 packages can be updated.  
351 updates are security updates.  
  
New release '18.04.2 LTS' available.  
Run 'do-release-upgrade' to upgrade to it.  
  
The programs included with the Ubuntu system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*/copyright.  
  
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by  
applicable law.  
  
wyne@wyne-VirtualBox:~$
```

- iii. Komputer client **dapat mengakses** layanan web dengan browser



- c. Perintah untuk memblocking semua paket

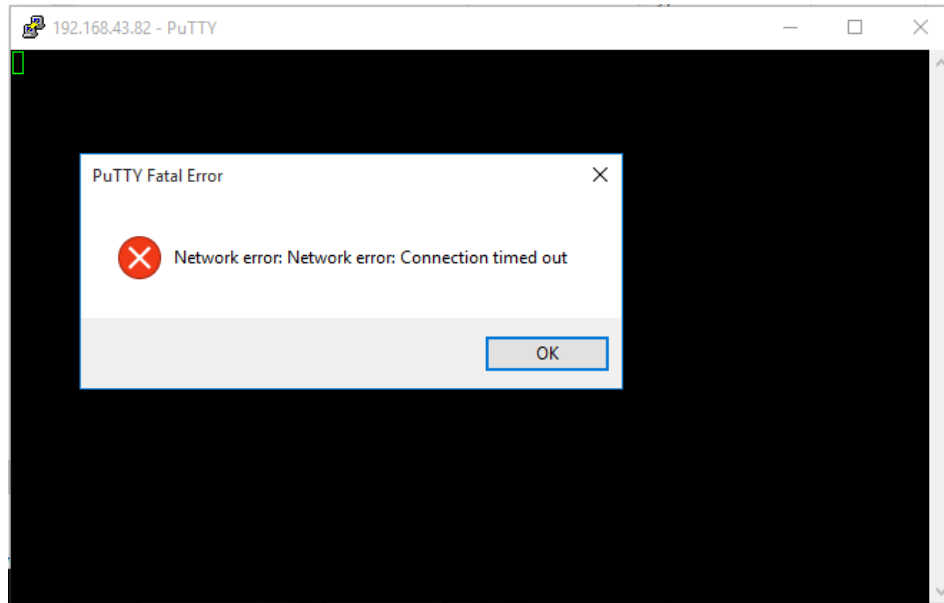
```
root@wyne-VirtualBox:/home/wyne# sudo iptables -A INPUT -j DROP
```

- d. Melakukan pengujian dari komputer client :

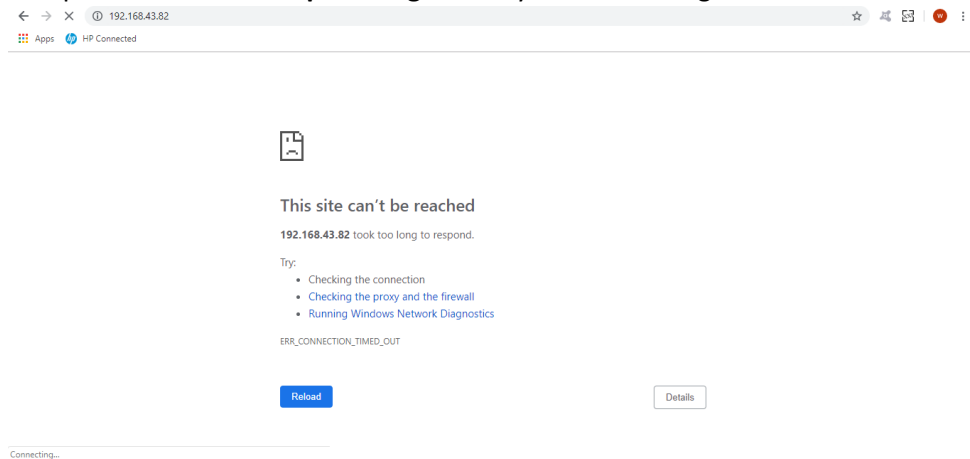
- i. Komputer client **tidak dapat** terhubung dengan server dengan tes ping

```
C:\Users\Asus-X453S>ping 192.168.43.82  
  
Pinging 192.168.43.82 with 32 bytes of data:  
Request timed out.  
Request timed out.  
Request timed out.  
Request timed out.  
  
Ping statistics for 192.168.43.82:  
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

- ii. Komputer client **tidak dapat mengakses** layanan SSH melalui software Putty



- iv. Komputer client **tidak dapat mengakses** layanan web dengan browser



3. Percobaan 3 : Mengijinkan Traffic masuk hanya ke port SSH

- a. Menghapus 'rule' yang sudah terpasang di server

```
root@wyne-VirtualBox:/home/wyne# iptables -F
```

- b. Perintah untuk mengijinkan sesi sambungan untuk menerima traffic

```
root@wyne-VirtualBox:/home/wyne# sudo iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
```

- c. Untuk mengijinkan traffic masuk ke default port SSH 22, kita harus mengijinkan semua TCP traffic yang masuk ke port 22

```
root@wyne-VirtualBox:/home/wyne# sudo iptables -A INPUT -p tcp --dport ssh -j ACCEPT
```

- d. Cek aturan perintah diatas dengan

```
root@wyne-VirtualBox:/home/wyne# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source                destination           state RELATED,ESTABLISHED
ACCEPT     all  --  anywhere              anywhere              state RELATED,ESTABLISHED
ISNED
ACCEPT     tcp  --  anywhere              anywhere              tcp dpt:ssh

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
```

- e. Memblock traffic di akhir

```
root@wyne-VirtualBox:/home/wyne# sudo iptables -A INPUT -j DROP
root@wyne-VirtualBox:/home/wyne# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source                destination           state RELATED,ESTABLISHED
ACCEPT     all  --  anywhere              anywhere              state RELATED,ESTABLISHED
ISNED
ACCEPT     tcp  --  anywhere              anywhere              tcp dpt:ssh
DROP       all  --  anywhere              anywhere

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
```

- e. Melakukan pengujian dari komputer client :

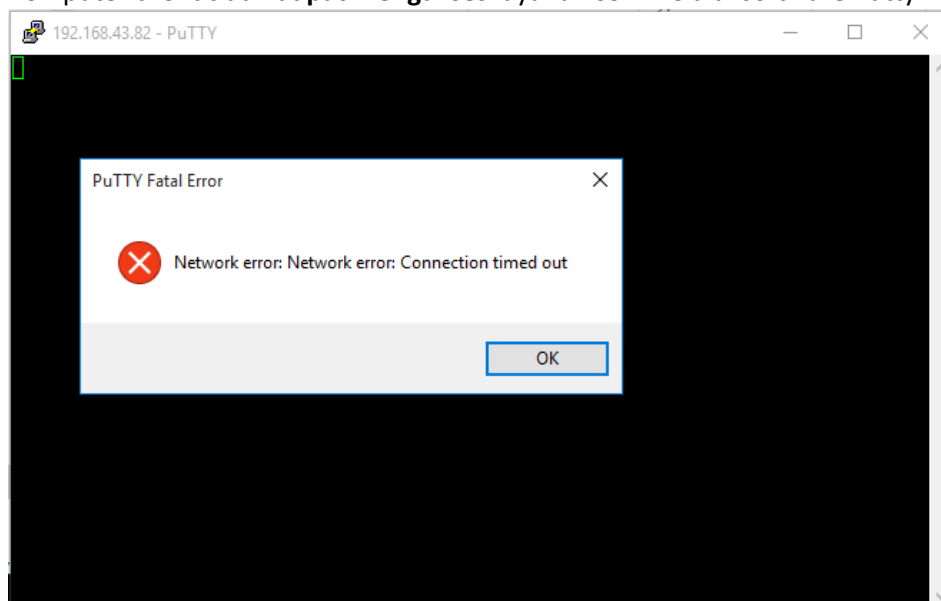
- i. Komputer client **tidak dapat** terhubung dengan server dengan tes ping

```
C:\Users\Asus-X453S>ping 192.168.43.82

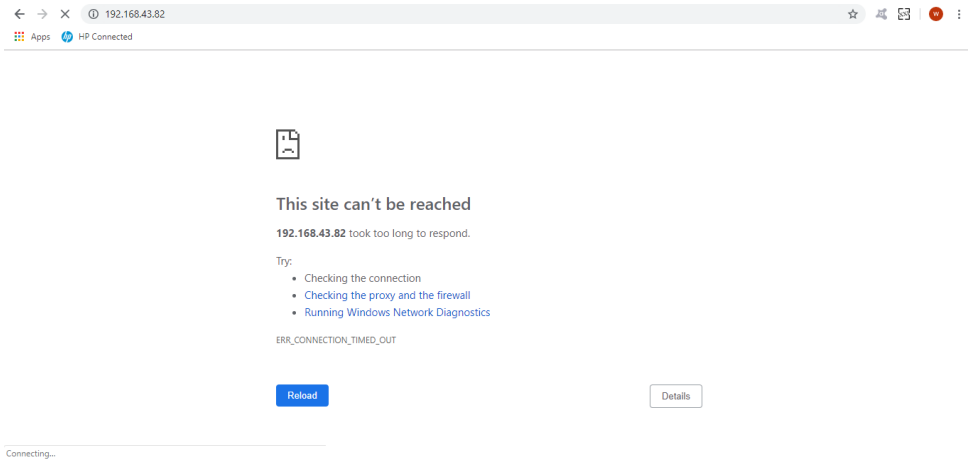
Pinging 192.168.43.82 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.43.82:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

- ii. Komputer client **tidak dapat mengakses** layanan SSH melalui software Putty



iii. Komputer client **tidak dapat mengakses** layanan web dengan browser



4. Percobaan 4 : Mengijinkan Traffic Masuk hanya ke port Web dan SSH

- a. Menghapus 'rule' yang sudah terpasang di server

```
root@wyne-VirtualBox:/home/wyne# iptables -F
```

- b. Perintah untuk mengijinkan semua traffic web untuk masuk

```
root@wyne-VirtualBox:/home/wyne# sudo iptables -A INPUT -p tcp --sport 80 -j ACCEPT
```

- c. Perintah untuk mengijinkan semua traffic SSH masuk

```
root@wyne-VirtualBox:/home/wyne# sudo iptables -A INPUT -p tcp --sport 22 -j ACCEPT
```

- d. Mengecek aturan yang telah dibuat dengan perintah

```
root@wyne-VirtualBox:/home/wyne# sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source                destination           tcp spt:http
ACCEPT     tcp  --  anywhere              anywhere              tcp spt:ssh
ACCEPT     tcp  --  anywhere              anywhere              tcp spt:ssh

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
```

- e. Blocking traffic

```
root@wyne-VirtualBox:/home/wyne# sudo iptables -A INPUT -j DROP
root@wyne-VirtualBox:/home/wyne# sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source                destination           tcp spt:http
ACCEPT     tcp  --  anywhere              anywhere              tcp spt:ssh
ACCEPT     tcp  --  anywhere              anywhere              tcp spt:ssh
DROP       all  --  anywhere              anywhere

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
```

f. Melakukan pengujian dari komputer client :

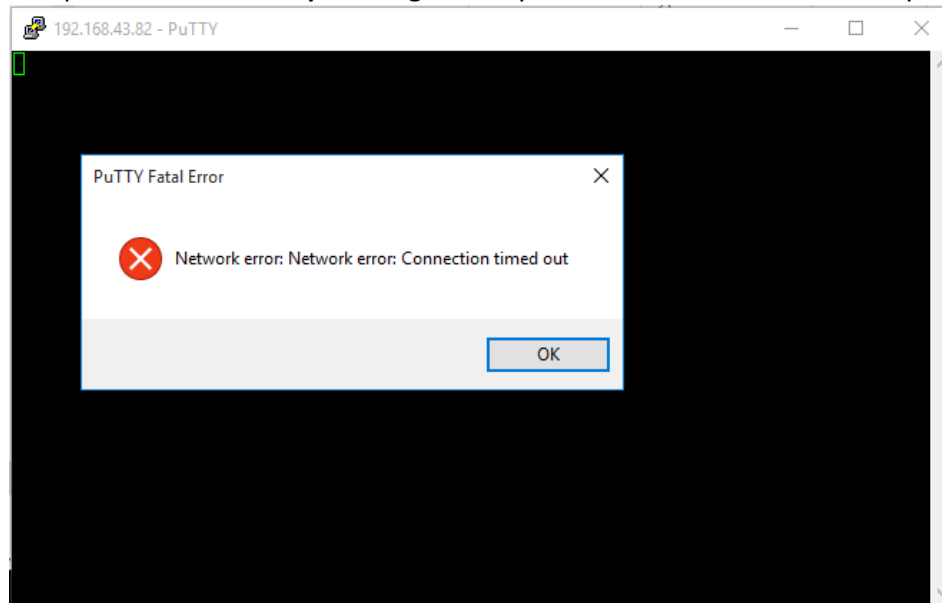
i. Komputer client **tidak dapat** terhubung dengan server dengan tes ping

```
C:\Users\Asus-X453S>ping 192.168.43.82

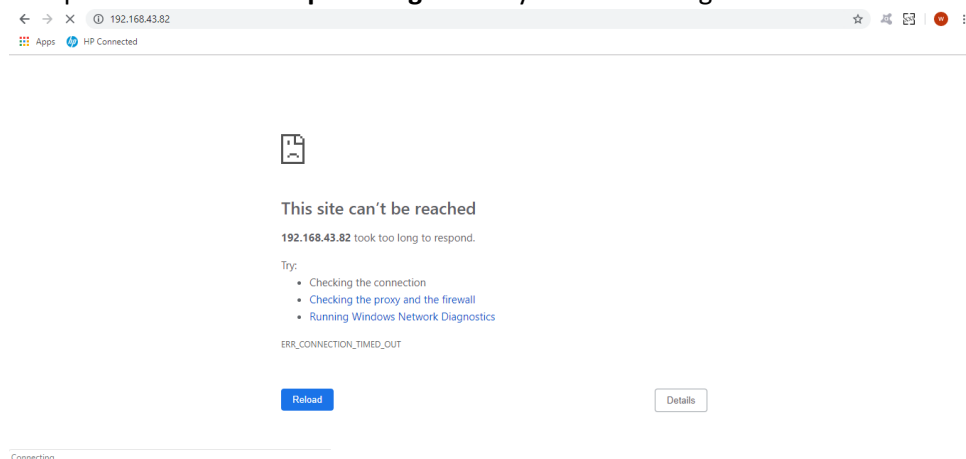
Pinging 192.168.43.82 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.43.82:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

ii. Komputer client **tidak dapat mengakses** layanan SSH melalui software Putty



iii. Komputer client **tidak dapat mengakses** layanan web dengan browser



5. Percobaan 5 : Blocking IP Address

a. Menghapus 'rule' yang sudah terpasang di server

```
root@wyne-VirtualBox:/home/wyne# iptables -F
```

b. Perintah untuk memblock IP Address

```
root@wyne-VirtualBox:/home/wyne# sudo iptables -I INPUT -s 192.168.43.111 -j DROP
```

c. Melakukan pengujian dari komputer client :

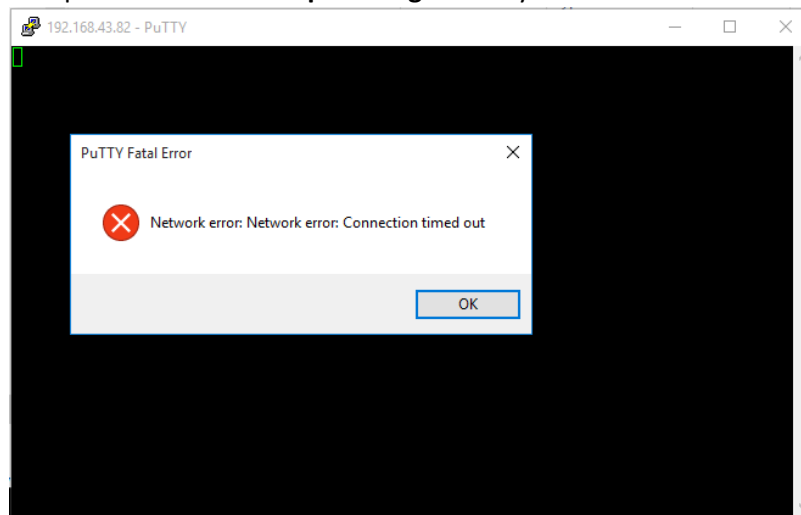
i. Komputer client **tidak dapat** terhubung dengan server dengan tes ping

```
C:\Users\Asus-X453S>ping 192.168.43.82

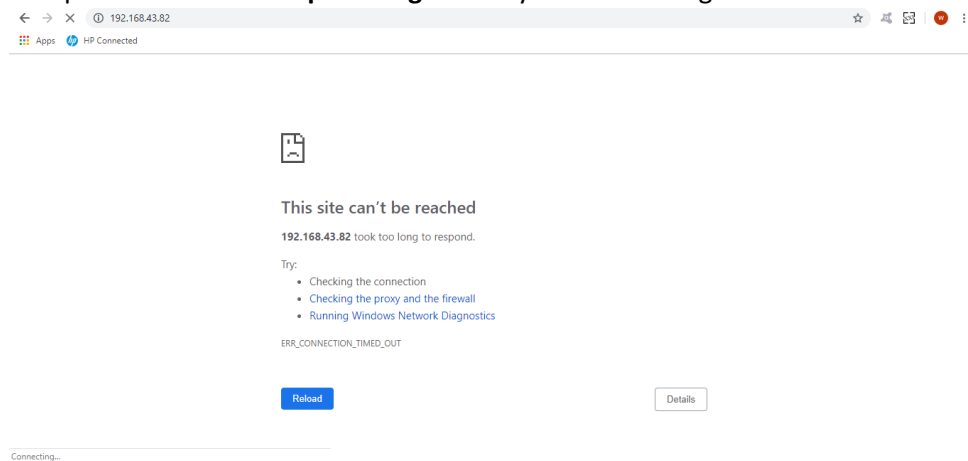
Pinging 192.168.43.82 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.43.82:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

ii. Komputer client **tidak dapat mengakses** layanan SSH melalui software Putty



iii. Komputer client **tidak dapat mengakses** layanan web dengan browser



d. Perintah untuk menghapus block IP Address

```
root@wyne-VirtualBox:/home/wyne# sudo iptables -D INPUT -s 192.168.43.111 -j DROP
```

- e. Melakukan pengujian dari komputer client :
- i. Komputer client **terhubung** dengan server dengan tes ping

```
C:\Users\Asus-X453S>ping 192.168.43.82

Pinging 192.168.43.82 with 32 bytes of data:
Reply from 192.168.43.82: bytes=32 time=5ms TTL=64
Reply from 192.168.43.82: bytes=32 time=2ms TTL=64
Reply from 192.168.43.82: bytes=32 time=3ms TTL=64
Reply from 192.168.43.82: bytes=32 time=3ms TTL=64

Ping statistics for 192.168.43.82:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 5ms, Average = 3ms
```

- ii. Komputer client **dapat mengakses** layanan SSH melalui software Putty

```
wyne@wyne-VirtualBox: ~
login as: wyne
wyne@192.168.43.82's password:
Welcome to Ubuntu 16.04.3 LTS (GNU/Linux 4.10.0-28-generic x86_64)

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

538 packages can be updated.
351 updates are security updates.

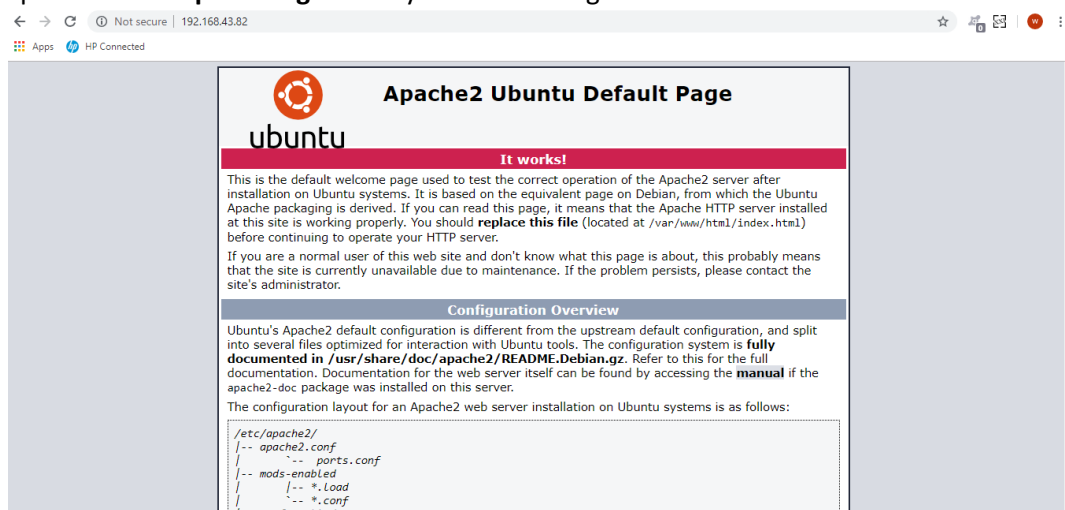
New release '18.04.2 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.


wyne@wyne-VirtualBox:~$
```

- iii. Komputer client **dapat mengakses** layanan web dengan browser



← → ↻ ⓘ Not secure | 192.168.43.82

Apps HP Connected



Apache2 Ubuntu Default Page

ubuntu

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in `/usr/share/doc/apache2/README.Debian.gz`**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the `apache2-doc` package was installed on this server.

The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

```
/etc/apache2/
|-- apache2.conf
/   |-- ports.conf
|-- mods-enabled
/   |-- *.load
/   |-- *.conf
-- conf-enabled
```


6. Percobaan 5 : Blocking MAC Address

- a. Menghapus 'rule' yang sudah terpasang di server

```
root@wyne-VirtualBox:/home/wyne# iptables -F
```

- b. Perintah untuk memblock IP Address

```
root@wyne-VirtualBox:/home/wyne# sudo iptables -A INPUT -m mac -mac-source fe80::304d:68f0:1558:37e2 -j DROP
```

- c. Melakukan pengujian dari komputer client :

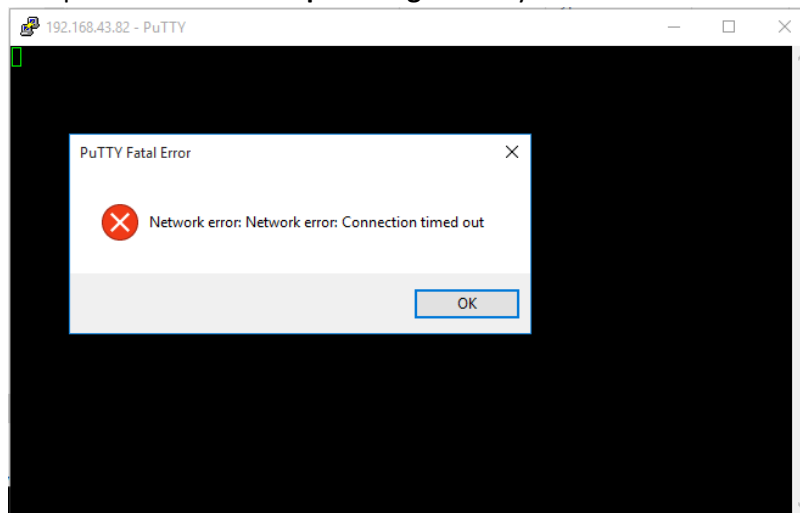
- i. Komputer client **tidak dapat** terhubung dengan server dengan tes ping

```
C:\Users\Asus-X453S>ping 192.168.43.82

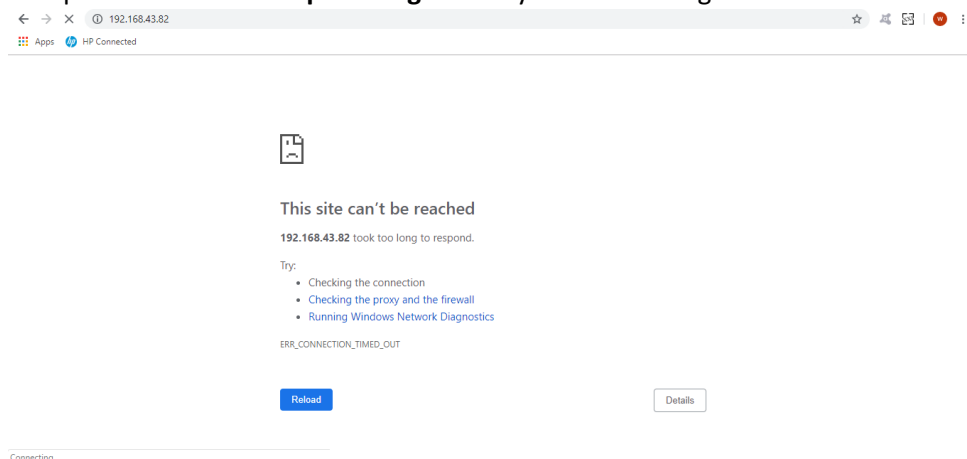
Pinging 192.168.43.82 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.43.82:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

- ii. Komputer client **tidak dapat mengakses** layanan SSH melalui software Putty



- iii. Komputer client **tidak dapat mengakses** layanan web dengan browser



- d. Perintah untuk menghapus block IP Address

```
root@wyne-VirtualBox:/home/wyne# sudo iptables -A INPUT -m mac -mac-source fe80::304d:68f0:1558:37e2 -j DROP
```

- e. Melakukan pengujian dari komputer client :
- i. Komputer client **terhubung** dengan server dengan tes ping

```
C:\Users\Asus-X453S>ping 192.168.43.82

Pinging 192.168.43.82 with 32 bytes of data:
Reply from 192.168.43.82: bytes=32 time=5ms TTL=64
Reply from 192.168.43.82: bytes=32 time=2ms TTL=64
Reply from 192.168.43.82: bytes=32 time=3ms TTL=64
Reply from 192.168.43.82: bytes=32 time=3ms TTL=64

Ping statistics for 192.168.43.82:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 5ms, Average = 3ms
```

- ii. Komputer client **dapat mengakses** layanan SSH melalui software Putty

```
wyne@wyne-VirtualBox: ~
login as: wyne
wyne@192.168.43.82's password:
Welcome to Ubuntu 16.04.3 LTS (GNU/Linux 4.10.0-28-generic x86_64)

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

538 packages can be updated.
351 updates are security updates.

New release '18.04.2 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.


Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

wyne@wyne-VirtualBox:~$
```

- iii. Komputer client **dapat mengakses** layanan web dengan browser

← → ↻ ⓘ Not secure | 192.168.43.82

Apps HP Connected



Apache2 Ubuntu Default Page

ubuntu

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in `/usr/share/doc/apache2/README.Debian.gz`**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the `apache2-doc` package was installed on this server.

The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

```
/etc/apache2/
|-- apache2.conf
/   |-- ports.conf
|-- mods-enabled
/   |-- *.load
/   |-- *.conf
-- conf-enabled
```