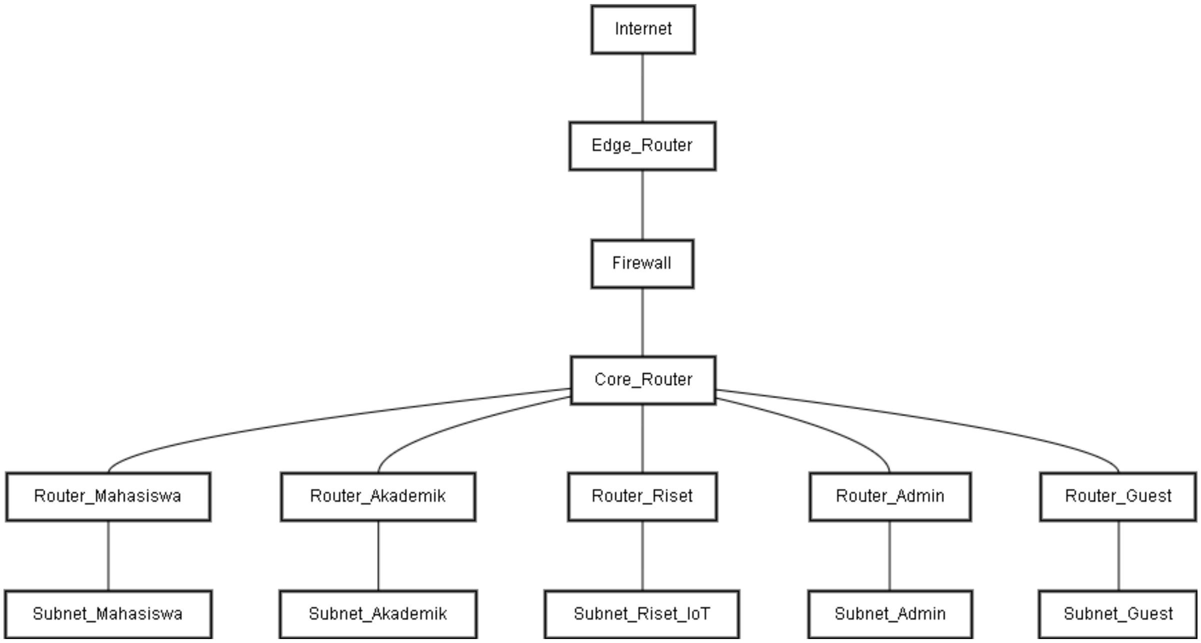
Laporan ITS Secure Network Challenge
Keamanan Jaringan Komputer (ET234302)

Nama Anggota:

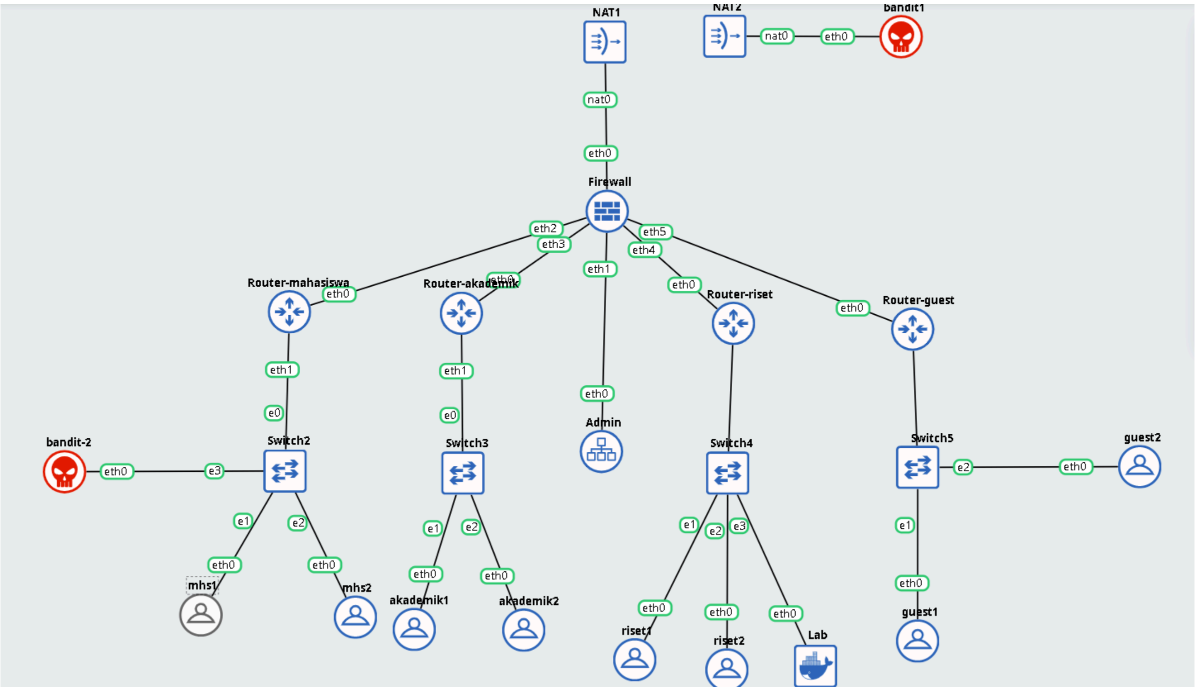
1.	Wira Samudra Siregar	(5027231041)
2.	Muhammad Farrel Rafli Al Fasya	(5027241075)
3.	Mochammad Atha Tajuddin	(5027241093)
4.	Jofanka Al-Kautsar Pangestu Abady	(5027241107)

1. Konsep Topologi

Konsep awal/dasar:



Hasil Topologi di GN3:



2. ACL(Access Control List)

Tentukan aturan akses antar-subnet (siapa boleh akses apa). Buat matriks kebijakan akses (misal: Mahasiswa ke Admin -> Ditolak).
Contoh Matriks Aturan Akses (Access Rule Matrix):

Urutan	Dari Zona (Source)	Ke Zona (Dest)	Layanan / Port	Aksi	Penjelasan & Logika Script
1	ANY	ANY	ANY	ACCEPT	Stateful Inspection: Mengizinkan paket balasan (status ESTABLISHED, RELATED) agar koneksi lancar.
2	ANY	ANY	ANY	DROP	Invalid State: Membuang paket yang statusnya INVALID (rusak/tidak valid).
3	WAN	Router/LAN	ANY (Spoofed IP)	DROP	Anti-Spoofing WAN: Memblokir IP bogon/loopback (127.0.0.0/8, dll) yang datang dari internet.
4	Internal (ADM, MHS, dll)	ANY	ANY (Spoofed IP)	REJECT	Anti-Spoofing LAN: Menolak paket jika Source IP tidak sesuai dengan subnet asli interface-nya.
5	ANY	ANY	ICMP (Ping)	ACCEPT	Ping: Mengizinkan ping (Echo Request & Reply) untuk tes koneksi.
6	ADM (Admin)	SEMUA (WAN & LAN)	ANY	ACCEPT	Super Admin: Admin diizinkan mengakses jaringan apa pun dan internet.
7	ADM (Admin)	Router (Firewall)	ANY	ACCEPT	Admin Access: Admin diizinkan mengakses firewall itu sendiri.
8	MHS (Mahasiswa)	RST (Riset)	ANY	REJECT	Blacklist Riset: MHS dilarang keras mengakses IP Riset 192.168.8.2 dan 192.168.8.3.
9	MHS (Mahasiswa)	RST (Lab Host)	TCP: 22, 80, 443	ACCEPT	Lab Access: MHS hanya boleh akses ke Host Lab (192.168.8.4) untuk SSH/Web.

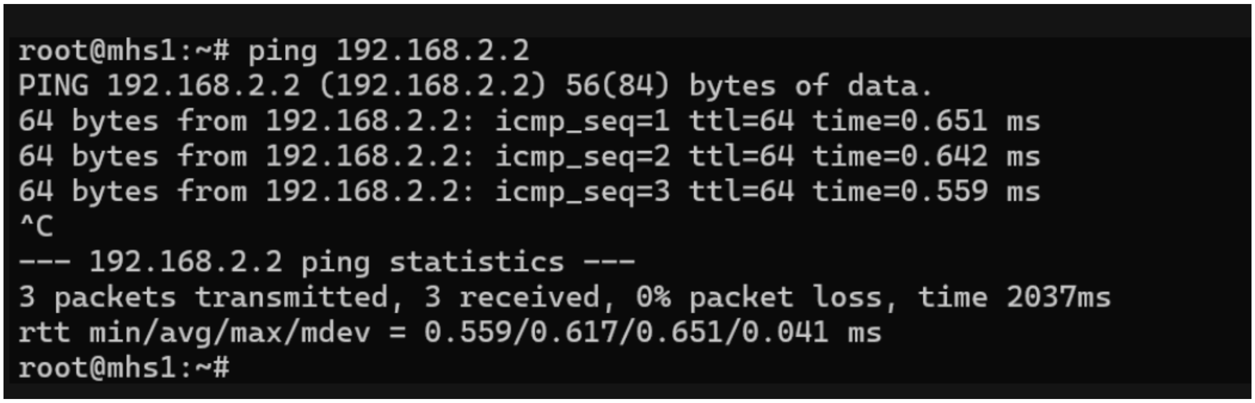
10	MHS (Mahasiswa)	WAN	TCP: 80, 443, 53UDP: 53	ACCEPT	Internet MHS: MHS boleh browsing (HTTP/HTTPS) dan query DNS.
11	AKD (Akademik)	WAN	ANY	ACCEPT	Internet AKD: Staf akademik memiliki akses internet penuh.
12	AKD (Akademik)	RST (Riset)	ANY	ACCEPT	Riset Access: Staf akademik boleh mengakses seluruh jaringan Riset.
13	RST (Riset)	WAN	TCP: 80, 443UDP: 53	ACCEPT	Internet Riset: Jaringan riset hanya boleh browsing dan DNS.
14	RST (Riset)	ADM (Admin)	TCP: 514, 9200	ACCEPT	Logging: Mengizinkan pengiriman log (Syslog/Elasticsearch) ke server di jaringan Admin.
15	GST (Guest)	WAN	TCP: 80, 443UDP: 53	ACCEPT	Internet Guest: Tamu hanya diizinkan browsing dan DNS. Tidak ada akses internal.
16	ADM (Admin)	Router (Firewall)	TCP: 22 (SSH)	ACCEPT	SSH Mgmt: (Redundan dengan aturan no 7, tapi spesifik) Mengamankan akses SSH router.
17	ANY (!ADM)	Router (Firewall)	TCP: 22 (SSH)	REJECT	SSH Protection: Menolak & mencatat log jika ada selain Admin yang mencoba SSH ke router.
18	WAN	Internal	ANY	DROP	Cleanup WAN: Membuang semua paket sisa dari internet secara diam-diam (SILENT_DROP).
19	Internal	Internal/WAN	ANY	REJECT	Cleanup LAN: Menolak semua trafik internal sisa yang tidak diizinkan di atas (LOG_REJECT).

3. Simulai Serangan & Uji Koneksi

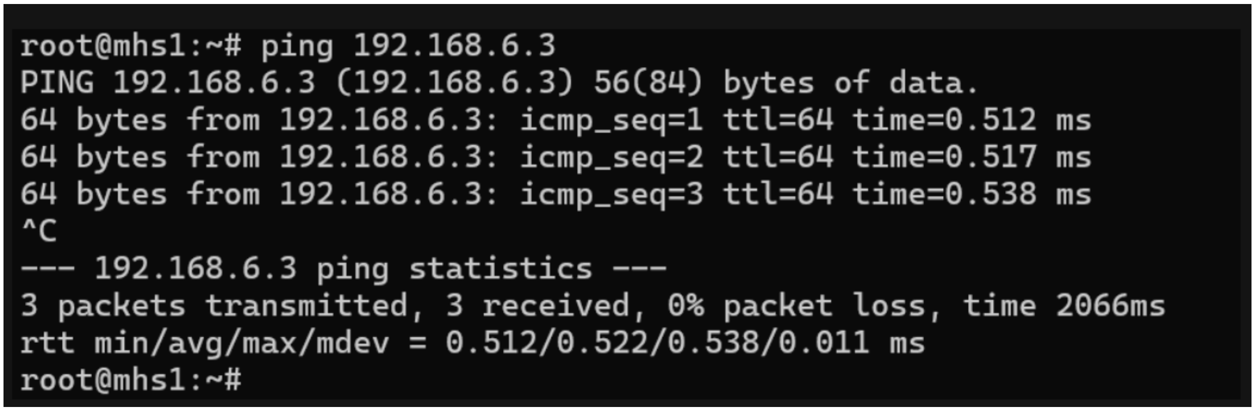
Uji Koneksi Daerah Internal

Mahasiswa

Client & Router MHS

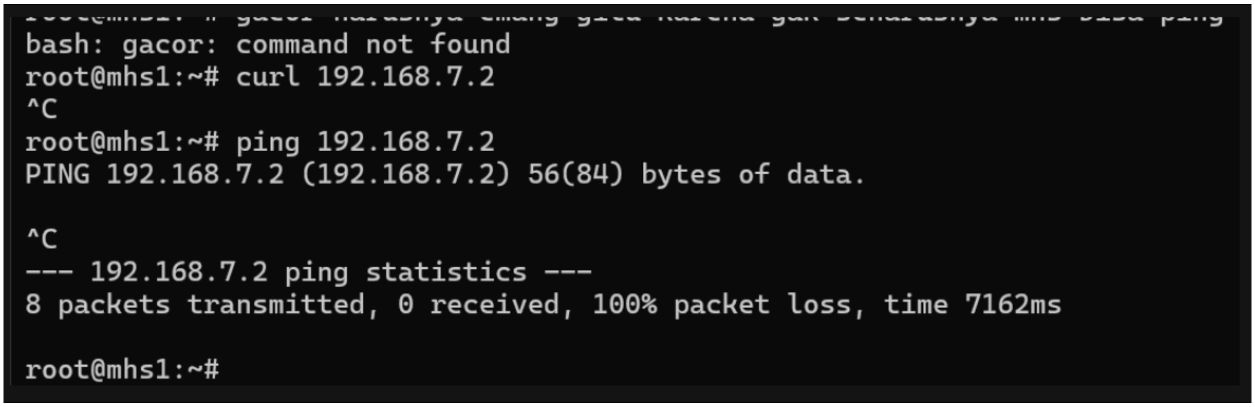


```
root@mhs1:~# ping 192.168.2.2
PING 192.168.2.2 (192.168.2.2) 56(84) bytes of data.
64 bytes from 192.168.2.2: icmp_seq=1 ttl=64 time=0.651 ms
64 bytes from 192.168.2.2: icmp_seq=2 ttl=64 time=0.642 ms
64 bytes from 192.168.2.2: icmp_seq=3 ttl=64 time=0.559 ms
^C
--- 192.168.2.2 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2037ms
rtt min/avg/max/mdev = 0.559/0.617/0.651/0.041 ms
root@mhs1:~#
```



```
root@mhs1:~# ping 192.168.6.3
PING 192.168.6.3 (192.168.6.3) 56(84) bytes of data.
64 bytes from 192.168.6.3: icmp_seq=1 ttl=64 time=0.512 ms
64 bytes from 192.168.6.3: icmp_seq=2 ttl=64 time=0.517 ms
64 bytes from 192.168.6.3: icmp_seq=3 ttl=64 time=0.538 ms
^C
--- 192.168.6.3 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2066ms
rtt min/avg/max/mdev = 0.512/0.522/0.538/0.011 ms
root@mhs1:~#
```

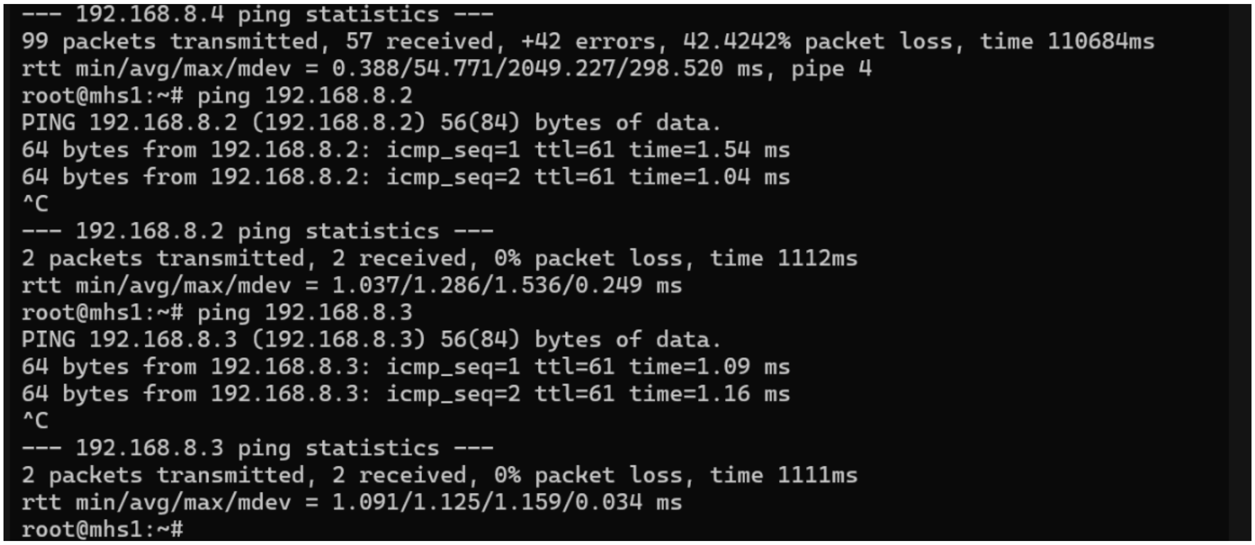
Client MHS1 mencoba ping ke client MHS lainnya



```
root@mhs1:~# gacor harusnya emang gitu karena gak seharusnya mhs bisa ping
bash: gacor: command not found
root@mhs1:~# curl 192.168.7.2
^C
root@mhs1:~# ping 192.168.7.2
PING 192.168.7.2 (192.168.7.2) 56(84) bytes of data.

^C
--- 192.168.7.2 ping statistics ---
8 packets transmitted, 0 received, 100% packet loss, time 7162ms

root@mhs1:~#
```

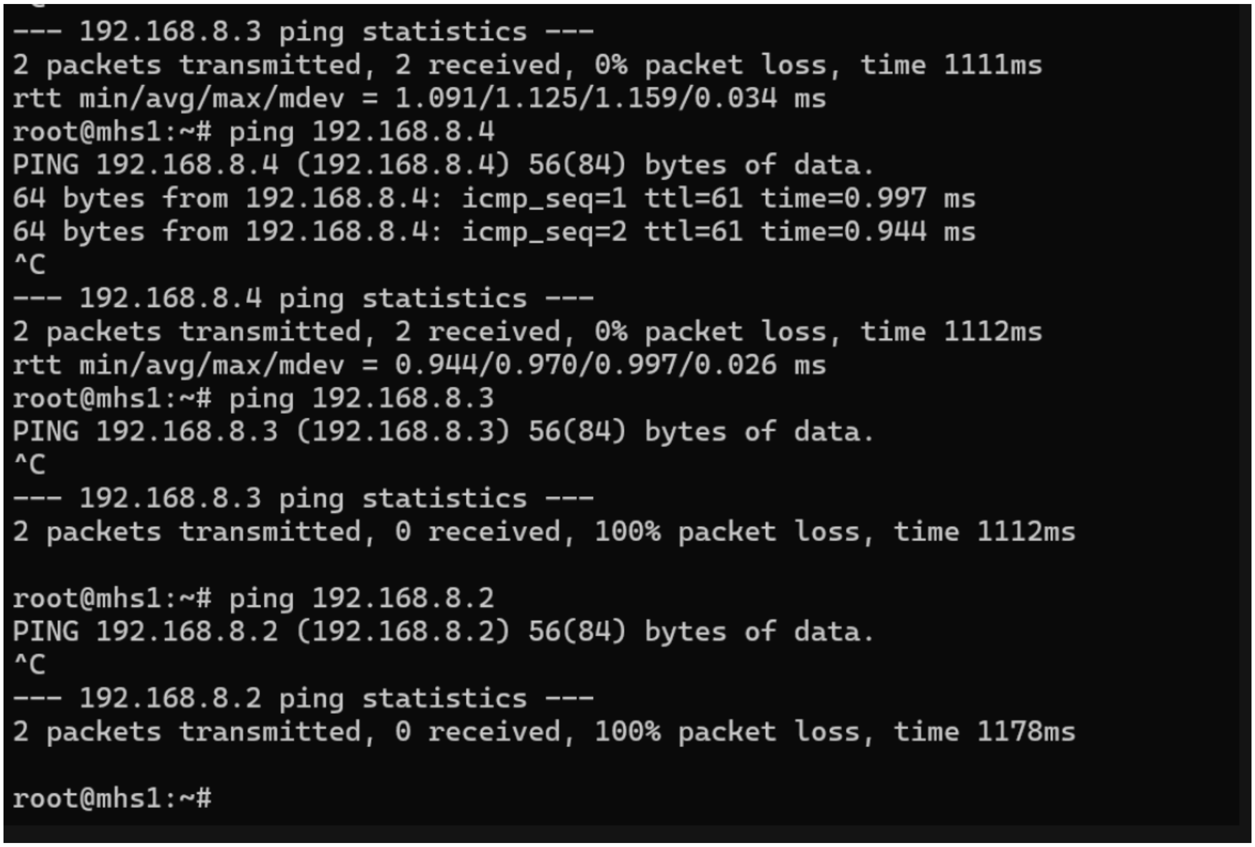
Client Mahasiswa mencoba terhubung dengan Akademik

Ini sudah benar karena tidak seharusnya mahasiswa dapat mengakses dari fitur-fitur atau benefit dari tendik/dosen.



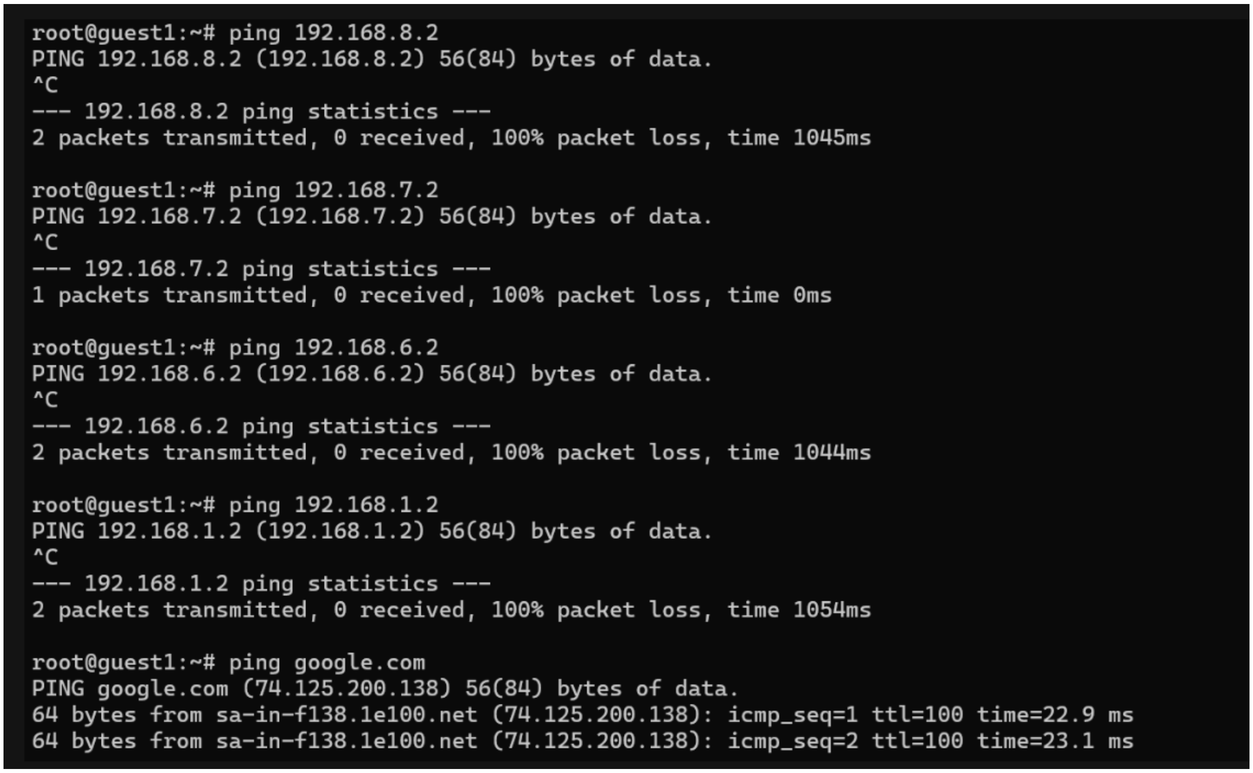
```
--- 192.168.8.4 ping statistics ---
99 packets transmitted, 57 received, +42 errors, 42.4242% packet loss, time 110684ms
rtt min/avg/max/mdev = 0.388/54.771/2049.227/298.520 ms, pipe 4
root@mhs1:~# ping 192.168.8.2
PING 192.168.8.2 (192.168.8.2) 56(84) bytes of data.
64 bytes from 192.168.8.2: icmp_seq=1 ttl=61 time=1.54 ms
64 bytes from 192.168.8.2: icmp_seq=2 ttl=61 time=1.04 ms
^C
--- 192.168.8.2 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1112ms
rtt min/avg/max/mdev = 1.037/1.286/1.536/0.249 ms
root@mhs1:~# ping 192.168.8.3
PING 192.168.8.3 (192.168.8.3) 56(84) bytes of data.
64 bytes from 192.168.8.3: icmp_seq=1 ttl=61 time=1.09 ms
64 bytes from 192.168.8.3: icmp_seq=2 ttl=61 time=1.16 ms
^C
--- 192.168.8.3 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1111ms
rtt min/avg/max/mdev = 1.091/1.125/1.159/0.034 ms
root@mhs1:~#
```

Mahasiswa dapat mengakses jaringan lab, namun tidak bisa akses ke riset dan & IoT device (upaya pemblokiran untuk mitigasi upaya penyerangan atau tindak ilegal)



```
--- 192.168.8.3 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1111ms
rtt min/avg/max/mdev = 1.091/1.125/1.159/0.034 ms
root@mhs1:~# ping 192.168.8.4
PING 192.168.8.4 (192.168.8.4) 56(84) bytes of data.
64 bytes from 192.168.8.4: icmp_seq=1 ttl=61 time=0.997 ms
64 bytes from 192.168.8.4: icmp_seq=2 ttl=61 time=0.944 ms
^C
--- 192.168.8.4 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1112ms
rtt min/avg/max/mdev = 0.944/0.970/0.997/0.026 ms
root@mhs1:~# ping 192.168.8.3
PING 192.168.8.3 (192.168.8.3) 56(84) bytes of data.
^C
--- 192.168.8.3 ping statistics ---
2 packets transmitted, 0 received, 100% packet loss, time 1112ms

root@mhs1:~# ping 192.168.8.2
PING 192.168.8.2 (192.168.8.2) 56(84) bytes of data.
^C
--- 192.168.8.2 ping statistics ---
2 packets transmitted, 0 received, 100% packet loss, time 1178ms

root@mhs1:~#
```

Guest

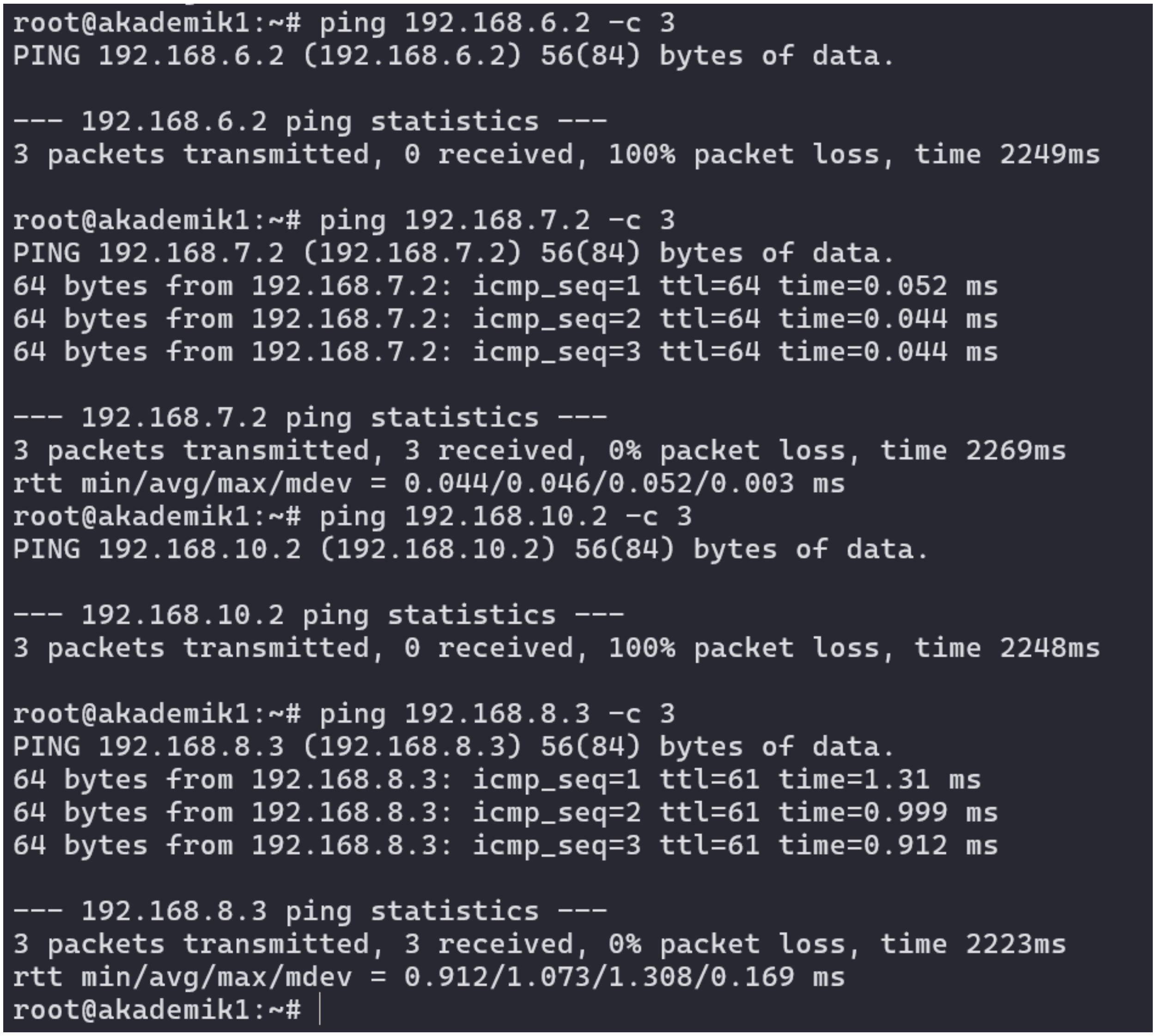


```
root@guest1:~# ping 192.168.8.2
PING 192.168.8.2 (192.168.8.2) 56(84) bytes of data.
^C
--- 192.168.8.2 ping statistics ---
2 packets transmitted, 0 received, 100% packet loss, time 1045ms

root@guest1:~# ping 192.168.7.2
PING 192.168.7.2 (192.168.7.2) 56(84) bytes of data.
^C
--- 192.168.7.2 ping statistics ---
1 packets transmitted, 0 received, 100% packet loss, time 0ms

root@guest1:~# ping 192.168.6.2
PING 192.168.6.2 (192.168.6.2) 56(84) bytes of data.
^C
--- 192.168.6.2 ping statistics ---
2 packets transmitted, 0 received, 100% packet loss, time 1044ms

root@guest1:~# ping 192.168.1.2
PING 192.168.1.2 (192.168.1.2) 56(84) bytes of data.
^C
--- 192.168.1.2 ping statistics ---
2 packets transmitted, 0 received, 100% packet loss, time 1054ms

root@guest1:~# ping google.com
PING google.com (74.125.200.138) 56(84) bytes of data.
64 bytes from sa-in-f138.1e100.net (74.125.200.138): icmp_seq=1 ttl=100 time=22.9 ms
64 bytes from sa-in-f138.1e100.net (74.125.200.138): icmp_seq=2 ttl=100 time=23.1 ms
```

Dari sini Client guest tidak dapat melakukan akses pada internal seperti admin,mahasiswa, akademik, riset, namun guest masih bisa terhubung ke jaringan dengan dibuktikan dapat ping google.com dan apt update

Akademik

Untuk akademik diperbolehkan untuk mengakses hampir semua node lain, terkecuali Mahasiswa dan Admin.

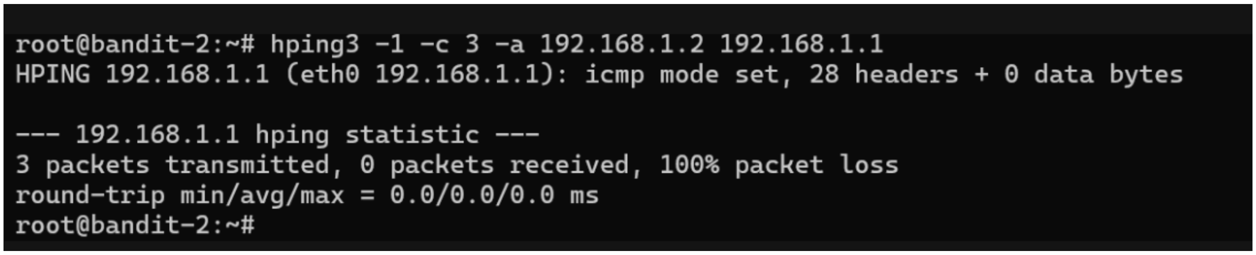


```
root@akademik1:~# ping 192.168.6.2 -c 3
PING 192.168.6.2 (192.168.6.2) 56(84) bytes of data.

--- 192.168.6.2 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2249ms

root@akademik1:~# ping 192.168.7.2 -c 3
PING 192.168.7.2 (192.168.7.2) 56(84) bytes of data.
64 bytes from 192.168.7.2: icmp_seq=1 ttl=64 time=0.052 ms
64 bytes from 192.168.7.2: icmp_seq=2 ttl=64 time=0.044 ms
64 bytes from 192.168.7.2: icmp_seq=3 ttl=64 time=0.044 ms

--- 192.168.7.2 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2269ms
rtt min/avg/max/mdev = 0.044/0.046/0.052/0.003 ms
root@akademik1:~# ping 192.168.10.2 -c 3
PING 192.168.10.2 (192.168.10.2) 56(84) bytes of data.

--- 192.168.10.2 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2248ms

root@akademik1:~# ping 192.168.8.3 -c 3
PING 192.168.8.3 (192.168.8.3) 56(84) bytes of data.
64 bytes from 192.168.8.3: icmp_seq=1 ttl=61 time=1.31 ms
64 bytes from 192.168.8.3: icmp_seq=2 ttl=61 time=0.999 ms
64 bytes from 192.168.8.3: icmp_seq=3 ttl=61 time=0.912 ms

--- 192.168.8.3 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2223ms
rtt min/avg/max/mdev = 0.912/1.073/1.308/0.169 ms
root@akademik1:~#
```

Dapat dilihat pada gambar tersebut bahwa akses kepada Mahasiswa (192.168.6.2) dan Admin (192.168.10.2) diblokir. Hal ini membuktikan bahwa konfigurasi berhasil diterapkan.

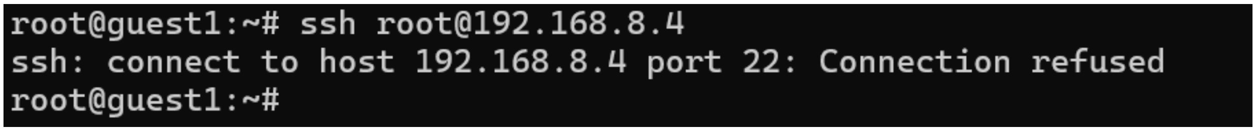
Uji Simulasi Serangan

Simulasi serangan yang paling mendasar ialah dengan melakukan request secara besar besaran pada firewall (***seperti teknik request atau floodng***) atau membanjiri request ke node firewall.



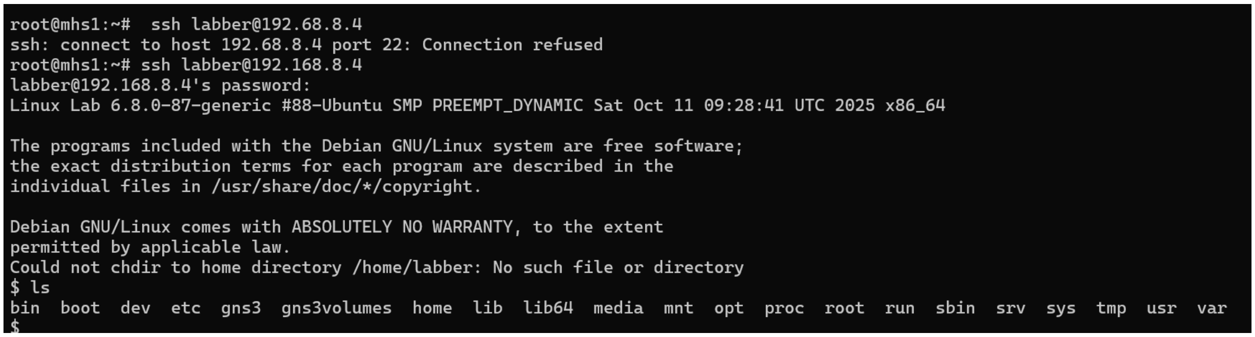
```
root@bandit-2:~# hping3 -1 -c 3 -a 192.168.1.2 192.168.1.1
HPING 192.168.1.1 (eth0 192.168.1.1): icmp mode set, 28 headers + 0 data bytes

--- 192.168.1.1 hping statistic ---
3 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
root@bandit-2:~#
```

Dari hasil uji tersebut hasilnya menunjukkan bahwasannya packet yang di transmisikan tidak berhasil diterima dan juga adanya status Packet Loss 100%, in menjadi bukti jika dari firewall sudah mumpuni untuk pemblokiran serangan terkait dengan ***IP Flooding***.



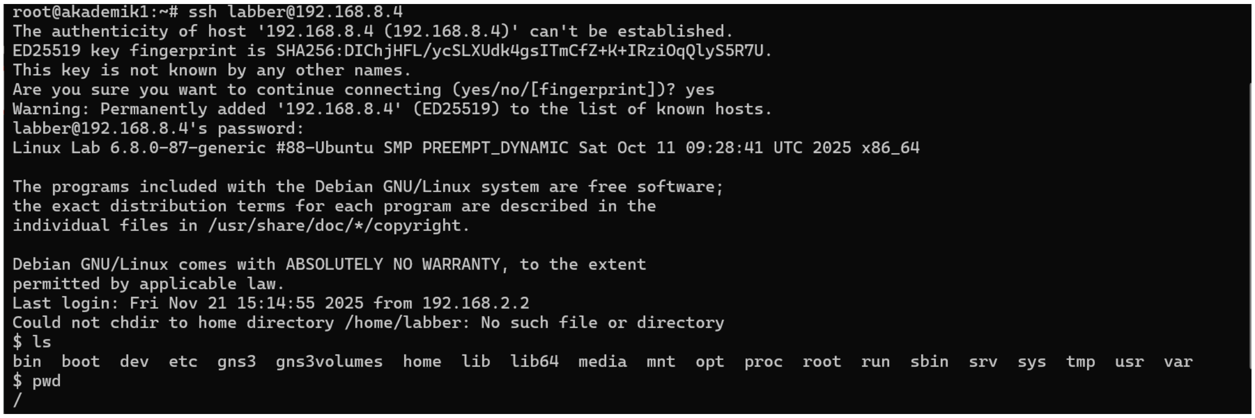
```
root@guest1:~# ssh root@192.168.8.4
ssh: connect to host 192.168.8.4 port 22: Connection refused
root@guest1:~#
```

Dari node Guest jika ingin melakukan SSH pada Lab maka akan diblokir oleh rules firewall yang sudah di setup atau dijalankan.



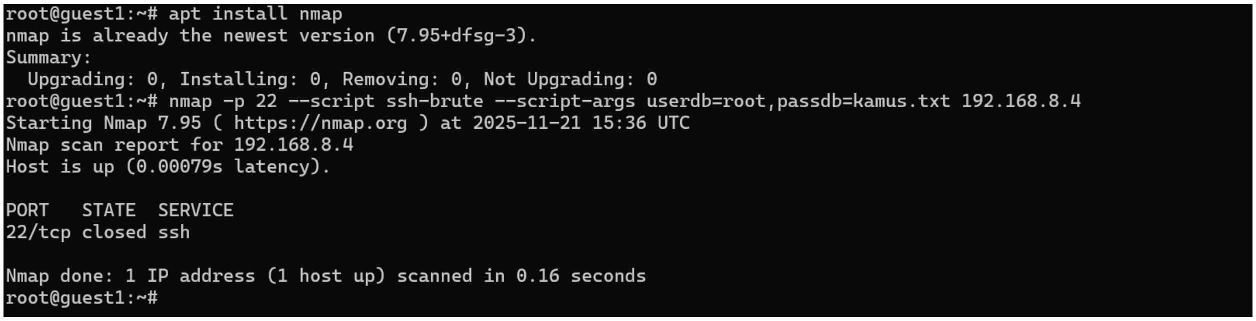
```
root@mhs1:~#  ssh labber@192.68.8.4
ssh: connect to host 192.68.8.4 port 22: Connection refused
root@mhs1:~# ssh labber@192.168.8.4
labber@192.168.8.4's password:
Linux Lab 6.8.0-87-generic #88-Ubuntu SMP PREEMPT_DYNAMIC Sat Oct 11 09:28:41 UTC 2025 x86_64

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

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Could not chdir to home directory /home/labber: No such file or directory
$ ls
bin  boot  dev  etc  gns3  gns3volumes  home  lib  lib64  media  mnt  opt  proc  root  run  sbin  srv  sys  tmp  usr  var
$
```

Dari mahasiswa melakukan koneksi SSH pada Lab dan karena diizinkan pada rules Firewall maka dapat login dengan baik.



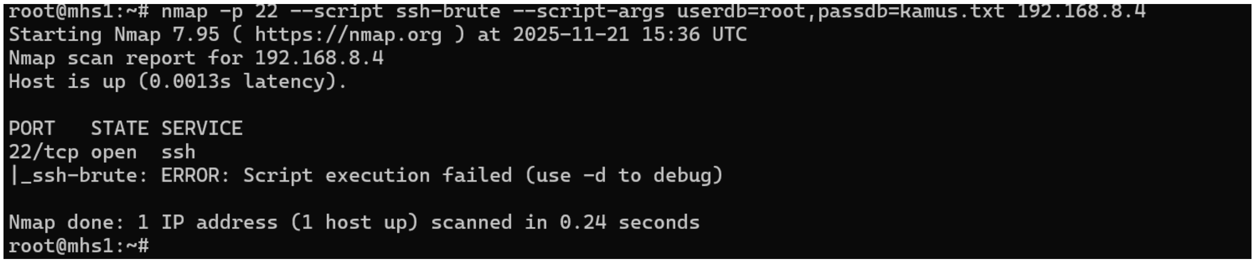
```
root@akademik1:~# ssh labber@192.168.8.4
The authenticity of host '192.168.8.4 (192.168.8.4)' can't be established.
ED25519 key fingerprint is SHA256:DIChjHFL/ycSLXUdk4gsITmCfZ+K+IRziOqQlyS5R7U.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.8.4' (ED25519) to the list of known hosts.
labber@192.168.8.4's password:
Linux Lab 6.8.0-87-generic #88-Ubuntu SMP PREEMPT_DYNAMIC Sat Oct 11 09:28:41 UTC 2025 x86_64

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

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Fri Nov 21 15:14:55 2025 from 192.168.2.2
Could not chdir to home directory /home/labber: No such file or directory
$ ls
bin  boot  dev  etc  gns3  gns3volumes  home  lib  lib64  media  mnt  opt  proc  root  run  sbin  srv  sys  tmp  usr  var
$ pwd
/
```

Pada node akademik,akademik dapat terkoneksi SSH ke node Lab sesuai dengan rule firewall.



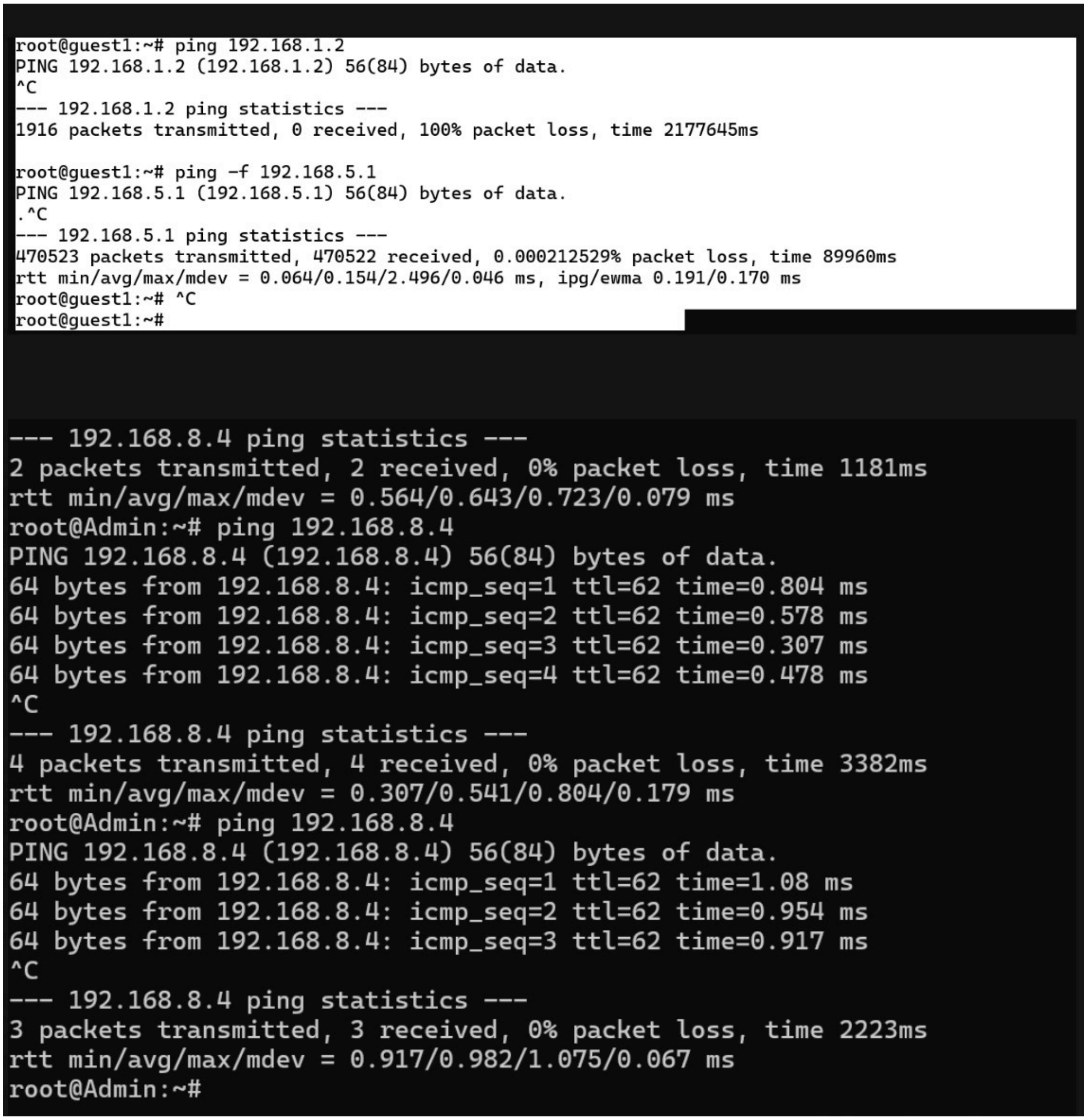
```
root@guest1:~# apt install nmap
nmap is already the newest version (7.95+dfsg-3).
Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 0
root@guest1:~# nmap -p 22 --script ssh-brute --script-args userdb=root,passdb=kamus.txt 192.168.8.4
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-21 15:36 UTC
Nmap scan report for 192.168.8.4
Host is up (0.00079s latency).

PORT   STATE  SERVICE
22/tcp closed ssh

Nmap done: 1 IP address (1 host up) scanned in 0.16 seconds
root@guest1:~#
```

Uji serangan dengan melakukan finding password dan username pada DB root dengna menggunakan NMAP hasilnya ialah pada node atau daerah yang di REJECT oleh firewall maka status port akan closed berbeda halnya dengan yang sudah diizinkan oleh firewall contoh mhs1 :



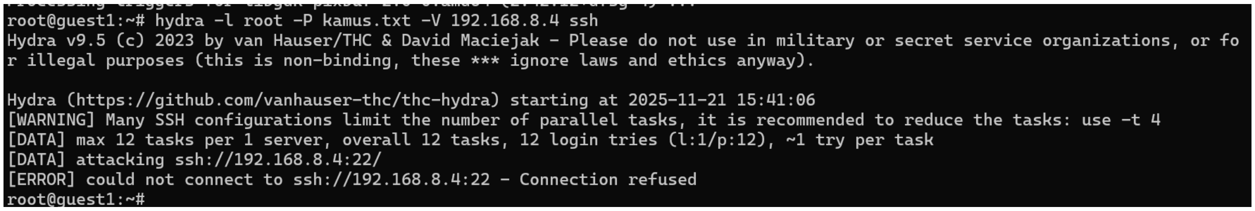
```
root@mhs1:~# nmap -p 22 --script ssh-brute --script-args userdb=root,passdb=kamus.txt 192.168.8.4
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-21 15:36 UTC
Nmap scan report for 192.168.8.4
Host is up (0.0013s latency).

PORT   STATE SERVICE
22/tcp open  ssh
|_ssh-brute: ERROR: Script execution failed (use -d to debug)

Nmap done: 1 IP address (1 host up) scanned in 0.24 seconds
root@mhs1:~#
```

Karena mhs1 diizinkan akses ke lab maka status port akan open.



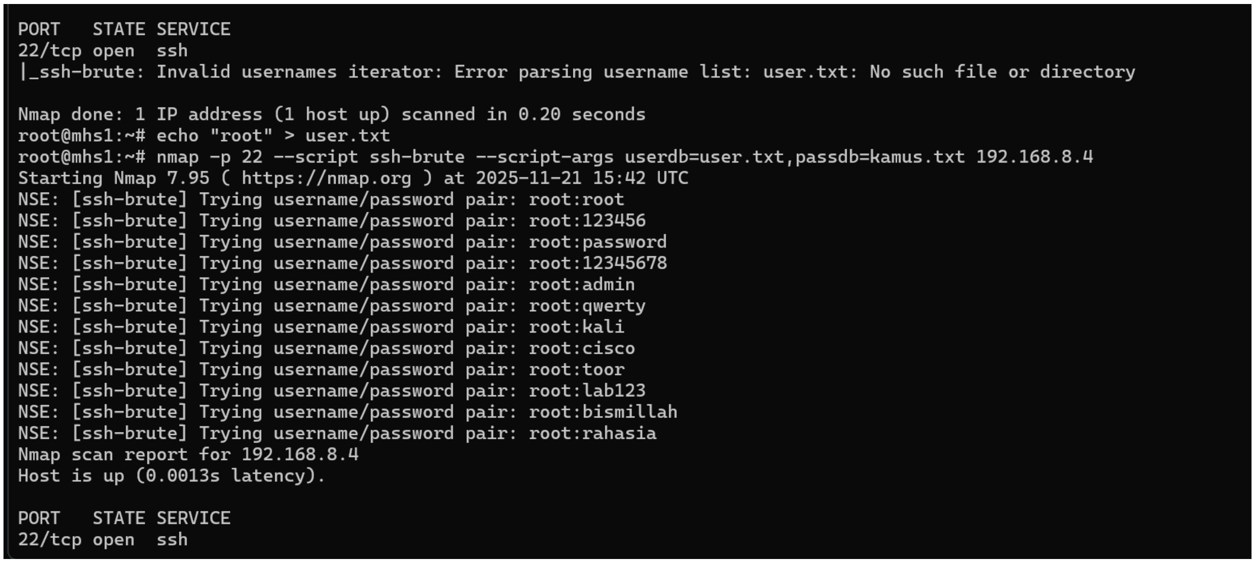
```
root@guest1:~# ping 192.168.1.2
PING 192.168.1.2 (192.168.1.2) 56(84) bytes of data.
^C
--- 192.168.1.2 ping statistics ---
1916 packets transmitted, 0 received, 100% packet loss, time 2177645ms

root@guest1:~# ping -f 192.168.5.1
PING 192.168.5.1 (192.168.5.1) 56(84) bytes of data.
.^C
--- 192.168.5.1 ping statistics ---
470523 packets transmitted, 470522 received, 0.000212529% packet loss, time 89960ms
rtt min/avg/max/mdev = 0.064/0.154/2.496/0.046 ms, ipg/ewma 0.191/0.170 ms
root@guest1:~# ^C
root@guest1:~#
```

```
--- 192.168.8.4 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1181ms
rtt min/avg/max/mdev = 0.564/0.643/0.723/0.079 ms
root@Admin:~# ping 192.168.8.4
PING 192.168.8.4 (192.168.8.4) 56(84) bytes of data.
64 bytes from 192.168.8.4: icmp_seq=1 ttl=62 time=0.804 ms
64 bytes from 192.168.8.4: icmp_seq=2 ttl=62 time=0.578 ms
64 bytes from 192.168.8.4: icmp_seq=3 ttl=62 time=0.307 ms
64 bytes from 192.168.8.4: icmp_seq=4 ttl=62 time=0.478 ms
^C
--- 192.168.8.4 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3382ms
rtt min/avg/max/mdev = 0.307/0.541/0.804/0.179 ms
root@Admin:~# ping 192.168.8.4
PING 192.168.8.4 (192.168.8.4) 56(84) bytes of data.
64 bytes from 192.168.8.4: icmp_seq=1 ttl=62 time=1.08 ms
64 bytes from 192.168.8.4: icmp_seq=2 ttl=62 time=0.954 ms
64 bytes from 192.168.8.4: icmp_seq=3 ttl=62 time=0.917 ms
^C
--- 192.168.8.4 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2223ms
rtt min/avg/max/mdev = 0.917/0.982/1.075/0.067 ms
root@Admin:~#
```



```
root@guest1:~# hydra -l root -P kamus.txt -V 192.168.8.4 ssh
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or fo
r illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-11-21 15:41:06
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 12 tasks per 1 server, overall 12 tasks, 12 login tries (l:1/p:12), ~1 try per task
[DATA] attacking ssh://192.168.8.4:22/
[ERROR] could not connect to ssh://192.168.8.4:22 - Connection refused
root@guest1:~#
```

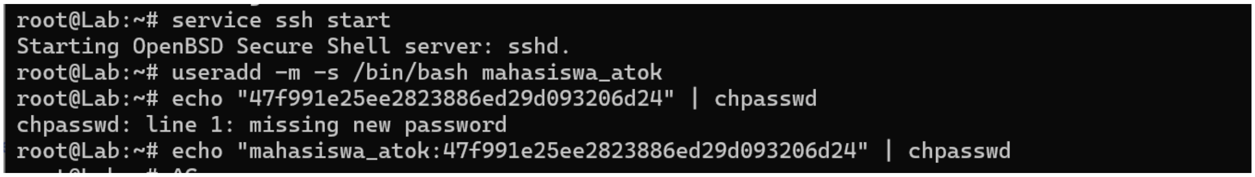
Uji coba **bruteforcing SSH** dengan menggunakan tools **hydra** gagal karena memang sudah diatur pada firewall untuk rulesnya Guest tidak bisa akses ke internal.



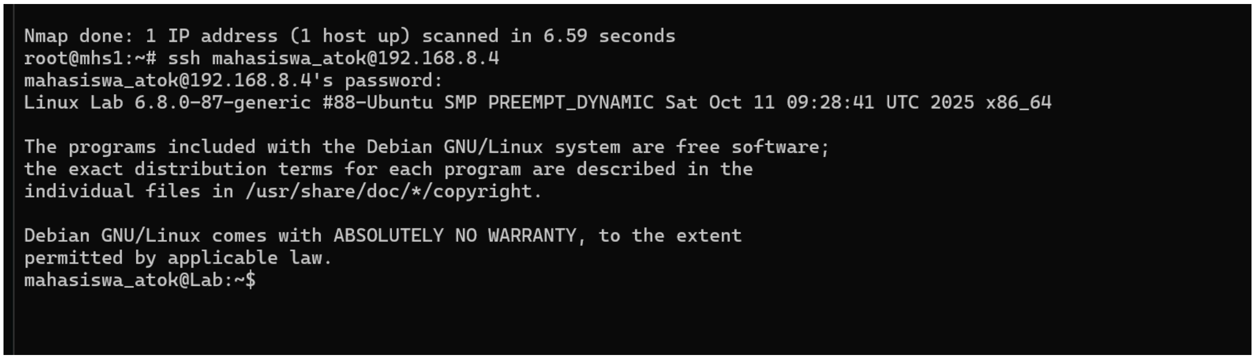
```
PORT   STATE SERVICE
22/tcp open  ssh
|_ssh-brute: Invalid usernames iterator: Error parsing username list: user.txt: No such file or directory

Nmap done: 1 IP address (1 host up) scanned in 0.20 seconds
root@mhs1:~# echo "root" > user.txt
root@mhs1:~# nmap -p 22 --script ssh-brute --script-args userdb=user.txt,passdb=kamus.txt 192.168.8.4
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-21 15:42 UTC
NSE: [ssh-brute] Trying username/password pair: root:root
NSE: [ssh-brute] Trying username/password pair: root:123456
NSE: [ssh-brute] Trying username/password pair: root:password
NSE: [ssh-brute] Trying username/password pair: root:12345678
NSE: [ssh-brute] Trying username/password pair: root:admin
NSE: [ssh-brute] Trying username/password pair: root:qwerty
NSE: [ssh-brute] Trying username/password pair: root:kali
NSE: [ssh-brute] Trying username/password pair: root:cisco
NSE: [ssh-brute] Trying username/password pair: root:toor
NSE: [ssh-brute] Trying username/password pair: root:lab123
NSE: [ssh-brute] Trying username/password pair: root:bismillah
NSE: [ssh-brute] Trying username/password pair: root:rahasia
Nmap scan report for 192.168.8.4
Host is up (0.0013s latency).

PORT   STATE SERVICE
22/tcp open  ssh
```

Jika kasusnya ialah pada mhs1 maka akan bisa untuk login dan melakukan bruteforcing namun seharusnya upaya ini akan dilaporkan pada logging sehingga akan tercatat jikalau adanya upaya peretasan,juga sebenarnya pada bruteforcing tergantung seberapa banyak wordlists yang ada semakin besar wordlist maka semakin mudah untuk proses bruteforcing user & password, best practicenya ialah untuk tiap tiap mahasiswa diberikan username dan password masing masing pada Lab dengan mungkin bisa menggunakan metode Multi-layer encryption, juga dibuatkan folder sendiri sendiri sehingga jika nantinya mahasiswa mencoba akses ke yang lainnya otomatis akan ditolak dan tidak bisa, atau semisal ingin melakukan akses ke illgeal pada milik mahasiswa lainnya juga akan ditolak.

Comtoh implementasi

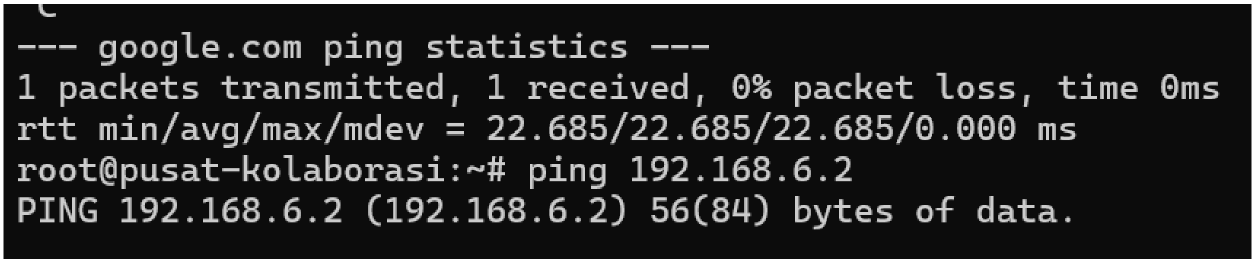


```
root@Lab:~# service ssh start
Starting OpenBSD Secure Shell server: sshd.
root@Lab:~# useradd -m -s /bin/bash mahasiswa_atok
root@Lab:~# echo "47f991e25ee2823886ed29d093206d24" | chpasswd
chpasswd: line 1: missing new password
root@Lab:~# echo "mahasiswa_atok:47f991e25ee2823886ed29d093206d24" | chpasswd
```

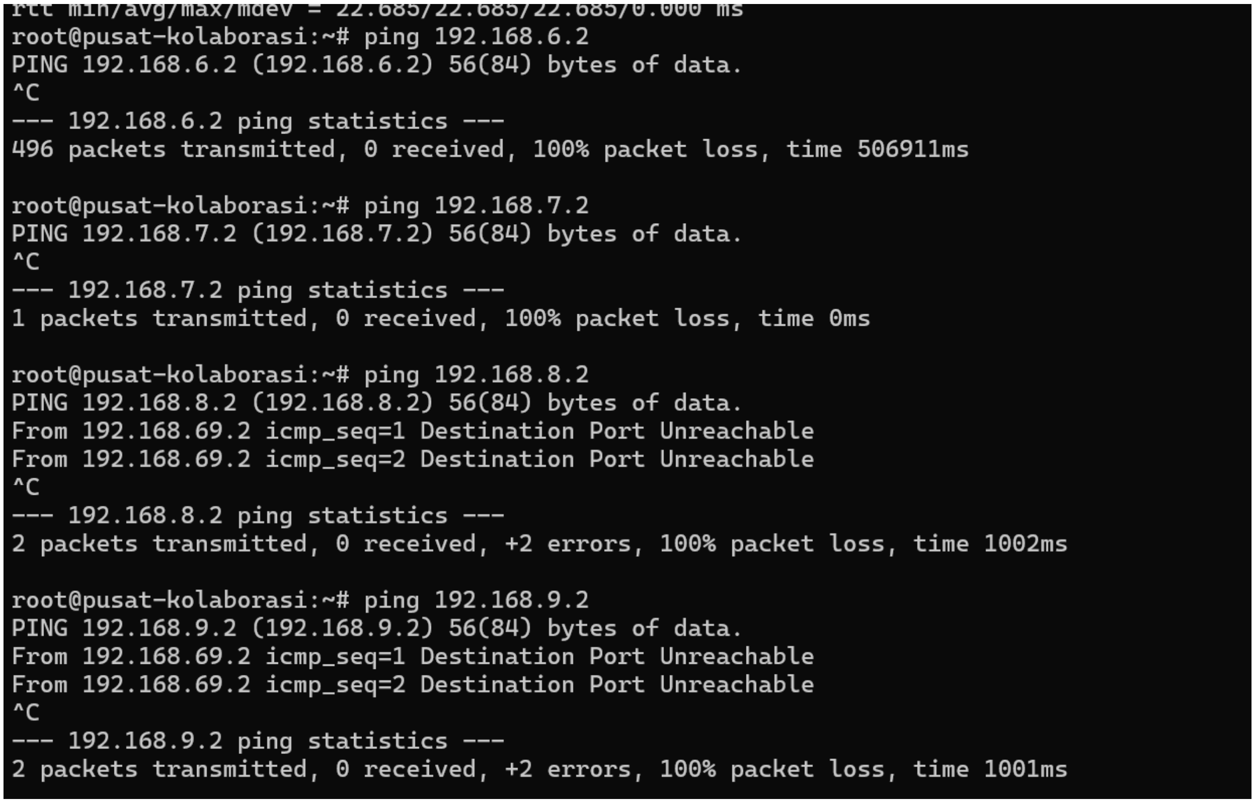


```
Nmap done: 1 IP address (1 host up) scanned in 6.59 seconds
root@mhs1:~# ssh mahasiswa_atok@192.168.8.4
mahasiswa_atok@192.168.8.4's password:
Linux Lab 6.8.0-87-generic #88-Ubuntu SMP PREEMPT_DYNAMIC Sat Oct 11 09:28:41 UTC 2025 x86_64

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

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
mahasiswa_atok@Lab:~$
```

Uji Koneksi Daerah External (Pusat Kolaborasi)



```
^C
--- google.com ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 22.685/22.685/22.685/0.000 ms
root@pusat-kolaborasi:~# ping 192.168.6.2
PING 192.168.6.2 (192.168.6.2) 56(84) bytes of data.
```



```
rtt min/avg/max/mdev = 22.685/22.685/22.685/0.000 ms
root@pusat-kolaborasi:~# ping 192.168.6.2
PING 192.168.6.2 (192.168.6.2) 56(84) bytes of data.
^C
--- 192.168.6.2 ping statistics ---
496 packets transmitted, 0 received, 100% packet loss, time 506911ms

root@pusat-kolaborasi:~# ping 192.168.7.2
PING 192.168.7.2 (192.168.7.2) 56(84) bytes of data.
^C
--- 192.168.7.2 ping statistics ---
1 packets transmitted, 0 received, 100% packet loss, time 0ms

root@pusat-kolaborasi:~# ping 192.168.8.2
PING 192.168.8.2 (192.168.8.2) 56(84) bytes of data.
From 192.168.69.2 icmp_seq=1 Destination Port Unreachable
From 192.168.69.2 icmp_seq=2 Destination Port Unreachable
^C
--- 192.168.8.2 ping statistics ---
2 packets transmitted, 0 received, +2 errors, 100% packet loss, time 1002ms

root@pusat-kolaborasi:~# ping 192.168.9.2
PING 192.168.9.2 (192.168.9.2) 56(84) bytes of data.
From 192.168.69.2 icmp_seq=1 Destination Port Unreachable
From 192.168.69.2 icmp_seq=2 Destination Port Unreachable
^C
--- 192.168.9.2 ping statistics ---
2 packets transmitted, 0 received, +2 errors, 100% packet loss, time 1001ms
```

Pusat kolaborasi tidak diperbolehjkan akses ke dalam daerah internal dengan alasan security. Berikut alasan mengapa paket dari pusat kolaborasi di DROP dan bukan di REJECT alasan berikut sekaligus menjadi alasan mengapa pada firewall other dilakukan setup dengan rules DROP dan bukan REJECT, dengan berbagai pertimbangan yakni sebagai berikut :

1. Security through Obscurity (Stealth Mode)

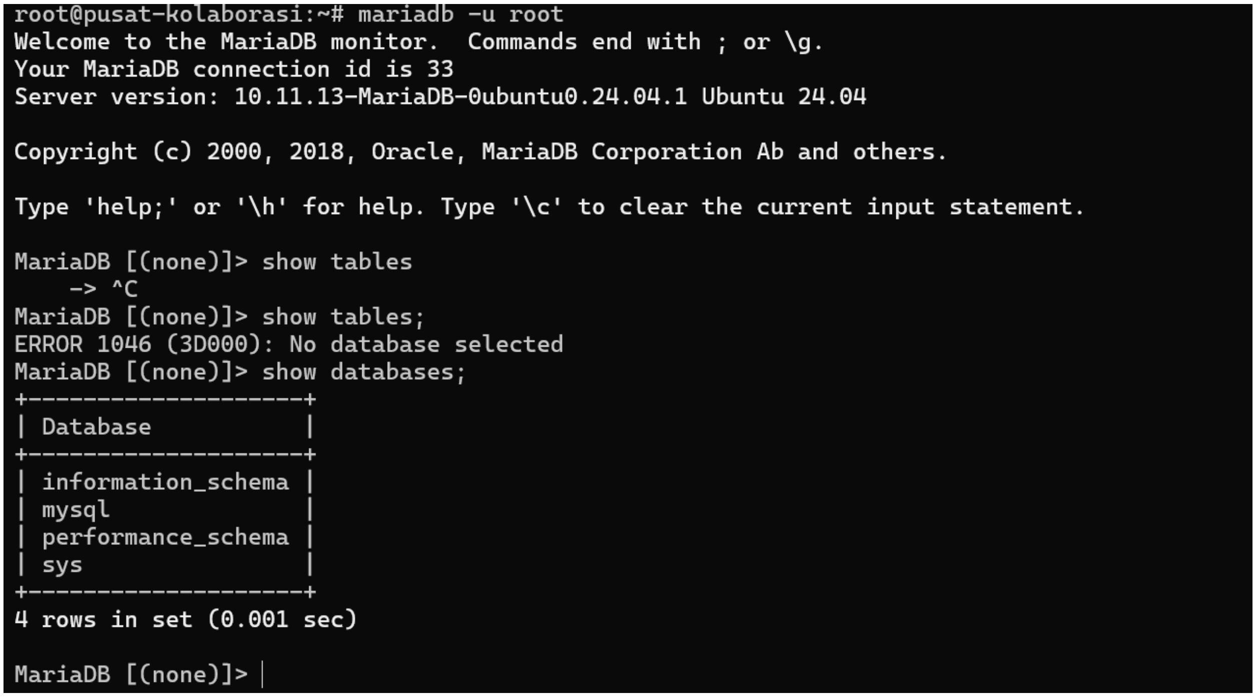
Jika Pusat Kolaborasi terkena retas (compromised), threat actor akan mencoba melakukan Scanning ke arah jaringan Internal Anda (192.168.10.x, 2.x, dll).
Jika menggunakan rules REJECT threat actor akan mengetahui bahwa ia diblokir namun IP hidup, threat actor berpotensi bisa memetakan topologi jaringan internal dengan cepat dan jika menggunakan rules DROP threat actor tidak mendapat balasan apa-apa, tools seperti scanner (Nmap) akan menunggu lama hingga terputus(Timeout). Ini memperlambat proses reconnaissance (pengumpulan info) mereka secara drastis.

2. Menghemat Resource Firewall

Menghasilkan paket balasan ICMP Destination Unreachable (REJECT) membutuhkan CPU.
Jika Pusat Kolaborasi mengirim serangan banjir paket (Flood/DDOS) ke arah Internal, dan Firewall akan melakukan returning dengan menolak sumber target , maka CPU Firewall berpotensi mengalami lonjakan resouce usage,dengan DROP, Firewall cukup membuang paketnya dan tidak meneruskannya sangat ringan dan efisien.

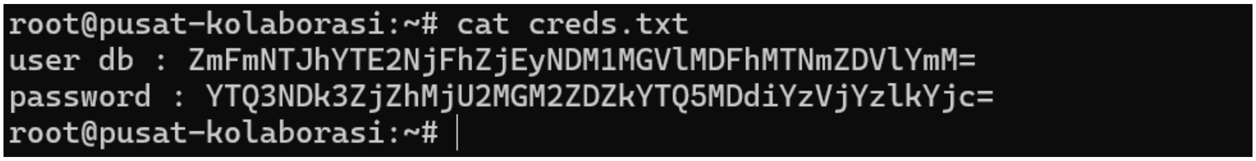
Adapun beberapa fasilitas yang disediakan pada pusta kolaborasi yakni :

1. Port 3306 (MySQL server/db)



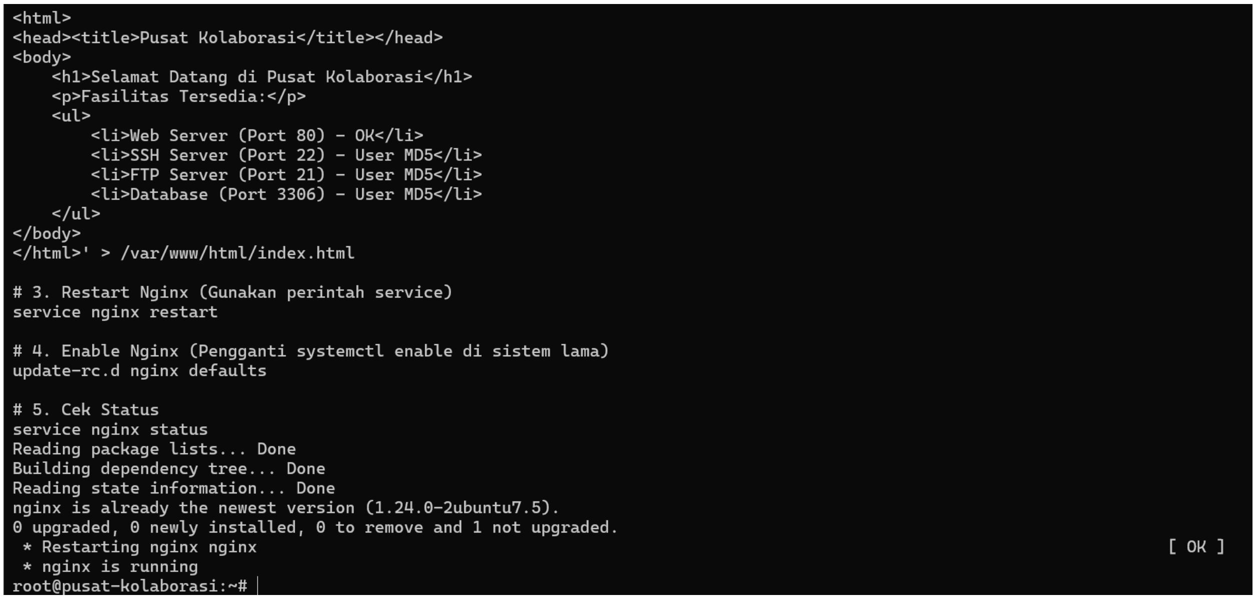
```
root@pusat-kolaborasi:~# mariadb -u root
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 33
Server version: 10.11.13-MariaDB-0ubuntu0.24.04.1 Ubuntu 24.04

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> show tables
    -> ^C
MariaDB [(none)]> show tables;
ERROR 1046 (3D000): No database selected
MariaDB [(none)]> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
| performance_schema |
| sys                |
+--------------------+
4 rows in set (0.001 sec)

MariaDB [(none)]> 
```

Dengan pengamanan ketat pada DB username dan password khusus pada sistem login mariadb yakni menerapkan keamanan **Multilayer-encrytpion** di mana layer pertama kami menggunakan algoritma hash **MD5(Message Diggest 5)** dan layer kedua menggunakan algoritma enkripsi **Base64**. Sehingga pada saat semisal pusat kolaboarsi berhasil di retas dan di **privilege-escalation (post exploitation)** oleh threat actor maka yang ada pada catatan creds.txt hanyalah algoritma Base64 sebagai berikut :



```
root@pusat-kolaborasi:~# cat creds.txt
user db : ZmFmNTJhYTE2NjFhZjEyNDM1MGVlMDFhMTNmZDVlYmM=
password : YTQ3NDk3ZjZhMjU2MGM2ZDZkYTQ5MDdiYzVjYzlkYjc=
root@pusat-kolaborasi:~#
```

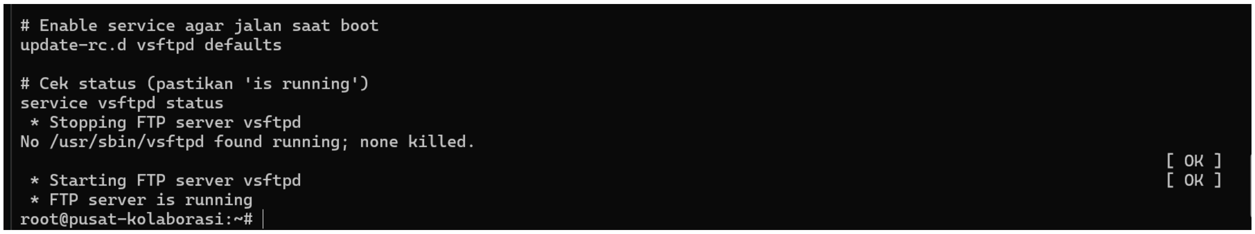
2. Nginx



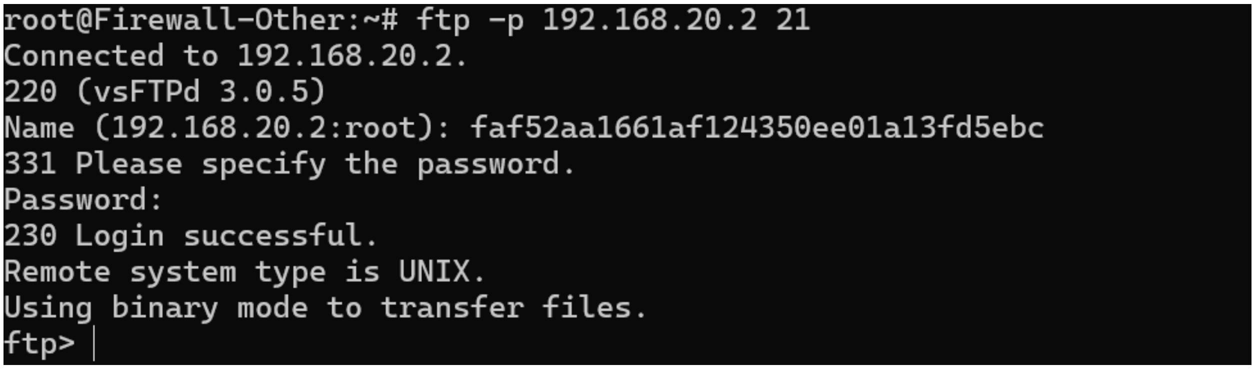
```
<html>
<head><title>Pusat Kolaborasi</title></head>
<body>
    <h1>Selamat Datang di Pusat Kolaborasi</h1>
    <p>Fasilitas Tersedia:</p>
    <ul>
        <li>Web Server (Port 80) - OK</li>
        <li>SSH Server (Port 22) - User MD5</li>
        <li>FTP Server (Port 21) - User MD5</li>
        <li>Database (Port 3306) - User MD5</li>
    </ul>
</body>
</html>' > /var/www/html/index.html

# 3. Restart Nginx (Gunakan perintah service)
service nginx restart

# 4. Enable Nginx (Pengganti systemctl enable di sistem lama)
update-rc.d nginx defaults

# 5. Cek Status
service nginx status
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
nginx is already the newest version (1.24.0-2ubuntu7.5).
0 upgraded, 0 newly installed, 0 to remove and 1 not upgraded.
 * Restarting nginx nginx                                                                                    [ OK ]
 * nginx is running
root@pusat-kolaborasi:~#
```

Sebagai fasilitas jika ingin melakukan deployment,hosting dll.

3. FTP Server (VSFTPD)



```
# Enable service agar jalan saat boot
update-rc.d vsftpd defaults

# Cek status (pastikan 'is running')
service vsftpd status
 * Stopping FTP server vsftpd
No /usr/sbin/vsftpd found running; none killed.
                                                                                                             [ OK ]
 * Starting FTP server vsftpd                                                                                [ OK ]
 * FTP server is running
root@pusat-kolaborasi:~#
```



```
root@Firewall-Other:~# ftp -p 192.168.20.2 21
Connected to 192.168.20.2.
220 (vsFTPd 3.0.5)
Name (192.168.20.2:root): faf52aa1661af124350ee01a13fd5ebc
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> |
```

4. Evaluasi efektivitas & efisiensi

Pada bagian ini dilakukan evaluasi terhadap efektivitas aturan firewall/ACL yang sudah diterapkan, serta seberapa efisien konfigurasi berjalan ketika diuji menggunakan beberapa skenario koneksi dan simulasi serangan.

1. Evaluasi Efektivitas

- Dari hasil pengujian koneksi dan simulasi, aturan yang diterapkan sudah berjalan sesuai dengan tujuan awal perancangan.
- Batasan akses antar-subnet bekerja sesuai kebutuhan.
  Mahasiswa tidak bisa mengakses subnet Akademik maupun subnet Riset, tapi tetap bisa mengakses Host Lab sesuai aturan. Ini menunjukkan bahwa filtering berdasarkan zona sudah efektif.
- Guest berhasil dibatasi secara ketat.
  Guest tidak bisa mengakses jaringan internal mana pun, tapi tetap bisa ping ke internet dan melakukan update. Artinya konfigurasi untuk zona guest sudah sesuai, yaitu isolasi total dari internal.
- Admin tetap bisa mengakses seluruh jaringan dan firewall.
  Aturan untuk subnet Admin sudah berjalan tanpa konflik dengan aturan lain, sehingga fungsi manajemen tetap terjaga.
- Aturan anti-spoofing terbukti berfungsi.
  Saat dilakukan uji source IP yang tidak sesuai subnet interface, paket langsung ditolak sesuai aturan.
- Serangan dasar (flooding) berhasil diblokir sepenuhnya.
  Pada saat pengujian IP flooding, seluruh paket mengalami packet loss 100%. Ini menunjukkan firewall mampu mencegah serangan berbasis request besar-besaran.
- Secara keseluruhan, dari sisi efektivitas, seluruh aturan inti (izinkan/blokir) sudah sesuai dengan rancangan awal dan tidak ditemukan akses yang lolos secara tidak sengaja.

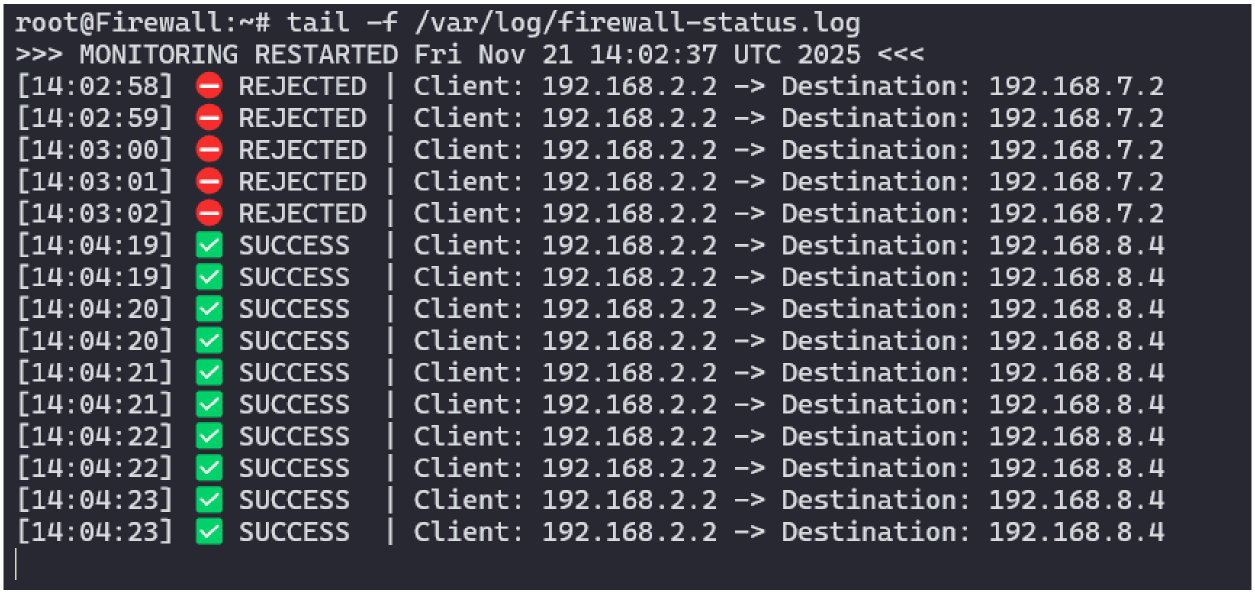
2. Evaluasi Efisiensi

Selain efektif, konfigurasi juga dievaluasi dari sisi efisiensi, terutama bagaimana aturan tersebut berjalan tanpa memberikan beban yang tidak perlu.

- Beberapa aturan masih ada yang tumpang tindih.
  Contohnya aturan Admin → Router sudah muncul dua kali (aturan umum + aturan khusus SSH). Ini tidak mengganggu sistem, tapi bisa dirapikan supaya lebih ringkas.
- Cleanup rule di akhir sudah bekerja, tapi bisa dioptimasi.
  Aturan DROP/REJECT terakhir membuat semua paket yang tidak cocok langsung ditolak. Namun jika ingin lebih detail, logging pada paket tertentu bisa ditambah supaya troubleshooting lebih mudah.
- Akses internet beberapa zona masih terlalu luas.
  Misalnya subnet Akademik diberi akses penuh ke internet tanpa pembatasan port. Untuk efisiensi dan keamanan, bisa dipersempit ke port yang benar-benar diperlukan.
- Tidak ada gejala lag atau bottleneck ketika firewall diberi beban.
  Pada saat simulasi flooding, firewall tetap bisa mempertahankan rule tanpa mengganggu koneksi subnet lain. Ini menunjukkan performa firewall cukup efisien untuk skala topologi yang digunakan.
- Struktur NAT sederhana dan mudah di-manage.
  NAT hanya berada pada satu titik, sehingga routing ke internet stabil. Namun pada implementasi nyata bisa dipertimbangkan failover NAT untuk menghindari single point of failure.

Logging into File

Agar memudahkan tracking traffic, log diperlukan untuk mencatat segala aktivitas lalu lintas yang terjadi.



```
root@Firewall:~# tail -f /var/log/firewall-status.log
>>> MONITORING RESTARTED Fri Nov 21 14:02:37 UTC 2025 <<<
[14:02:58] ⛔ REJECTED | Client: 192.168.2.2 -> Destination: 192.168.7.2
[14:02:59] ⛔ REJECTED | Client: 192.168.2.2 -> Destination: 192.168.7.2
[14:03:00] ⛔ REJECTED | Client: 192.168.2.2 -> Destination: 192.168.7.2
[14:03:01] ⛔ REJECTED | Client: 192.168.2.2 -> Destination: 192.168.7.2
[14:03:02] ⛔ REJECTED | Client: 192.168.2.2 -> Destination: 192.168.7.2
[14:04:19] ✅ SUCCESS  | Client: 192.168.2.2 -> Destination: 192.168.8.4
[14:04:19] ✅ SUCCESS  | Client: 192.168.2.2 -> Destination: 192.168.8.4
[14:04:20] ✅ SUCCESS  | Client: 192.168.2.2 -> Destination: 192.168.8.4
[14:04:20] ✅ SUCCESS  | Client: 192.168.2.2 -> Destination: 192.168.8.4
[14:04:21] ✅ SUCCESS  | Client: 192.168.2.2 -> Destination: 192.168.8.4
[14:04:21] ✅ SUCCESS  | Client: 192.168.2.2 -> Destination: 192.168.8.4
[14:04:22] ✅ SUCCESS  | Client: 192.168.2.2 -> Destination: 192.168.8.4
[14:04:22] ✅ SUCCESS  | Client: 192.168.2.2 -> Destination: 192.168.8.4
[14:04:23] ✅ SUCCESS  | Client: 192.168.2.2 -> Destination: 192.168.8.4
[14:04:23] ✅ SUCCESS  | Client: 192.168.2.2 -> Destination: 192.168.8.4
```

Pada gambar ini, terdapat beberapa informasi, yaitu berupa starting point log, waktu, status, client, destination beserta IPnya. Jika akses dari client ke destination berhasil, maka akan muncul status SUCCESS. Sebaliknya, jika aksesnya diblokir makan akan muncul status REJECTED.

Link docs : KJK_3_PBL

Link github : https://github.com/AtokTajuddin/kjk-kelompok03