LAPORAN RESMI PROYEK KEAMANAN JARINGAN KOMPUTER

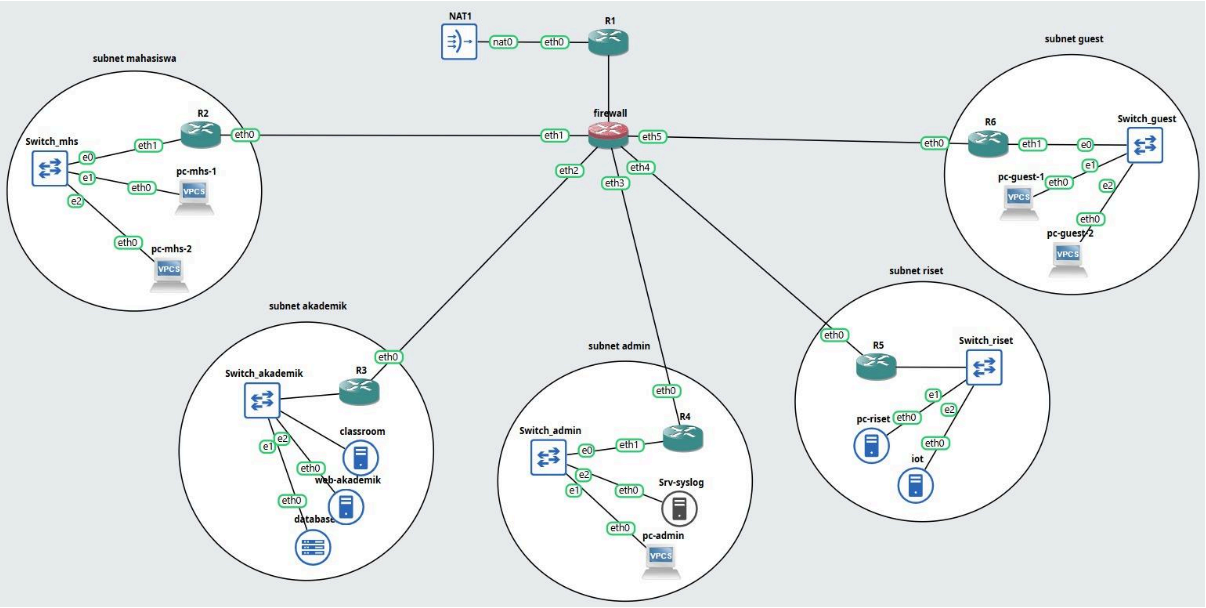
Analisis dan Implementasi Filtrasi Multi-Segment FP-KJK-B-05

ITS Secure Network Challenge (Week 10-11)

Anggota kelompok:

1. Rizqi Akbar Sukirman Putra (5027241044)
2. Oscaryavat Viryavan (5027241053)
3. Nisrina Bilqis (5027241054)
4. Ica Zika Hamizah (5027241058)

TOPOLOGI GNS



I. FILOSOFI DAN KEBIJAKAN KEAMANAN

1. Prinsip Dasar: Zero Trust Intranet

Filosofi yang digunakan adalah **"Zero Trust Intranet"**, yang berarti tidak ada subnet internal yang dipercaya secara otomatis. Kebijakan ini mewajibkan penerapan **Prinsip Hak Akses Minimum (*Least Privilege*)**, di mana komunikasi antar-subnet **secara *default* diblokir** dan hanya diizinkan melalui aturan eksplisit (*ALLOW*) pada protokol dan *port* yang spesifik.

2. Desain Topologi Final

Topologi ini mengadopsi arsitektur *Firewall Terpusat* dengan **enam Zona Keamanan** yang diisolasi secara fisik melalui *interface* yang berbeda pada perangkat firewall. Perangkat firewall bertindak sebagai *Gateway* L3, DHCP Server, dan *Stateful Firewall* utama.

Interface Firewall	Zona Keamanan	Subnet Klien	Fungsi Perangkat Terkait
eth1 (R1)	**WAN/Internet**	192.168.1.0/24 (NAT)	Koneksi ke Internet.
eth2 (R2)	**Mahasiswa**	10.20.10.0/24	Menghubungkan PC_mhs-1 & 2.
eth3 (R3)	**Akademik**	10.20.20.0/24	Menghubungkan Server Web, DB, dan Classroom.
eth4 (R4)	**Admin**	10.20.40.0/24	Menghubungkan PC_admin dan Srv_syslog.
eth5 (R5)	**Riset/IoT**	10.20.30.0/24	Menghubungkan PC_riset dan Server Log.
eth6 (R6)	**Guest**	10.20.50.0/24	Menghubungkan PC_guest.

3. Matriks Kebijakan Firewall (Disesuaikan dengan Topologi Final)

Matriks ini merepresentasikan kebijakan **Zero Trust** yang akan diterjemahkan menjadi *Firewall Filter Rules* pada perangkat firewall.

Aksi	Dari (Source IP / Interface)	Ke (Destination IP / Interface)	Port/Protokol	Catatan (Filosofi)
ALLOW	STATEFUL	ANY	ANY	**Stateful Inspection. Wajib untuk mengizinkan paket balasan (Reply) dari semua koneksi yang sah.**
ALLOW	**Admin** (`10.20.40.0/24` / `eth3`)	ANY	ANY	**Full Access.** Administrator dipercaya penuh untuk manajemen.
BLOCK	**Guest** (`10.20.50.0/24` / `eth5`)	SEMUA JARINGAN INTERNAL (10.20.x.x selain Internet)	ANY	**Isolasi Total.** Tamu tidak boleh melihat zona lain.
ALLOW	**Guest** (`10.20.50.0/24` / `eth5`)	**Web Akademik** (`10.20.20.100`)	TCP/80, 443	**Akses Publik Terbatas.** Hanya info publik diizinkan.

ALLOW	**Guest** (`10.20.50.0/24` / `eth5`)	**Internet** (`eth0`)	ANY	**Akses Dasar.** Mengizinkan browsing ke luar.
BLOCK	**Mahasiswa** (`10.20.10.0/24` / `eth1`)	**Admin** (`10.20.40.0/24`)	ANY	**Kritis.** Mencegah Mahasiswa mengakses infrastruktur manajemen.
BLOCK	**Mahasiswa** (`10.20.10.0/24` / `eth1`)	**Database** (`10.20.20.200`)	ANY	**Pertahanan Data.** Melindungi data sensitif (dilapisi Host Firewall).
ALLOW	**Mahasiswa** (`10.20.10.0/24` / `eth1`)	Akademik (eth3)	TCP 3306 (MySQL)	**Kolaborasi**. IoT mengirim data sensor ke database akademik.
ALLOW	**Mahasiswa** (`10.20.10.0/24` / `eth1`)	**Web Akademik** (`10.20.20.100`)	TCP/80	**Fungsionalitas.** Akses ke situs informasi kampus.
ALLOW	**Mahasiswa** (`10.20.10.0/24` / `eth1`)	**Classroom** (`10.20.20.101`)	TCP/80, **TCP/22**	**Simulasi Login.** Mengizinkan akses untuk belajar.
ALLOW	**Mahasiswa** (`10.20.10.0/24` / `eth1`)	**Riset/IoT** (`10.20.30.0/24`)	TCP/22	**Akses Terbatas.** Mengizinkan kontrol jarak jauh (SSH) untuk praktikum.

ALLOW	**Mahasiswa** (`10.20.10.0/24` / `eth1`)	**Internet (`eth0`)**	ANY	**Akses ke luar jaringan via NAT.**
IMPLICIT	**ANY**	**ANY**	ANY	**Default Policy: DROP. Semua yang tidak diizinkan di atas akan diblokir.**

II. ANALISIS HASIL PENGUJIAN (SEBELUM DAN SETELAH FIREWALL)

Bagian ini membandingkan status jaringan *default* (tidak aman) dengan kondisi jaringan *Zero Trust* setelah kebijakan *firewall* diterapkan.

1. Kondisi Jaringan Default (Sebelum Firewall)

Filosofi: ALLOW ALL (Tidak Ada Isolasi)

Sebelum firewall diaktifkan, traffic antar-segmen diizinkan secara default karena perangkat firewall bertindak sebagai router tanpa kebijakan keamanan.

A. Uji Celah Keamanan (Serangan Berhasil)

Sumber	Tujuan & Port	Hasil Pengujian (Bukti)	Implikasi Keamanan
Mahasiswa	Database (ICMP/Ping)	**BERHASIL**	*Lateral Movement* (ICMP) terbuka.
Mahasiswa	Database (SSH)	**BERHASIL** (Akses *root* - *HACK*)	**Kegagalan Kritis:** Mahasiswa dapat mengambil data sensitif.
Mahasiswa	PC Admin (ICMP/Ping)	**BERHASIL**	Administrasi (*Control Plane*) rentan terhadap *scanning* Mahasiswa.
Guest	Database (SSH)	**BERHASIL** (Akses *root* - *HACK*)	**Kegagalan Kritis:** Tamu dapat meretas Server Database.
Guest	PC Admin (ICMP/Ping)	**BERHASIL**	Jaringan Tamu tidak terisolasi dari infrastruktur manajemen.

B. Uji Fungsionalitas (Akses Diizinkan)

Sumber	Tujuan	Hasil Pengujian	Implikasi
Mahasiswa	Web Akademik	**BERHASIL** (Akses Web)	Akses esensial web sudah berfungsi.
Guest	Web Akademik	**BERHASIL** (Akses Web)	Akses web tamu sudah berfungsi.

Kesimpulan Kondisi Default: Jaringan berada dalam kondisi **sangat rentan** karena *default policy* **ALLOW ALL**. Setiap *host* internal, termasuk Tamu dan Mahasiswa, memiliki akses penuh (*ping, ssh*) ke Server Database dan infrastruktur manajemen.

2. Kondisi Jaringan Zero Trust (Setelah Firewall)

Filosofi: DENY ALL, diikuti oleh aturan **ALLOW** spesifik.

Setelah aturan firewall diimplementasikan, seluruh traffic antar-segmen diblokir secara default, dan hanya akses yang didefinisikan secara eksplisit yang diizinkan (Skenario Least Privilege).

A. Uji Keberhasilan Mitigasi (Serangan Gagal)

Sumber	Tujuan & Port	Hasil Pengujian (Bukti)	Justifikasi Keamanan
Mahasiswa	Database (ICMP/Ping)	**GAGAL** (100% *packet loss*)	**BLOCK** ICMP default berhasil, melindungi *database* dari *scanning* ICMP.
Mahasiswa	Database (SSH)	**GAGAL** (*Stuck / Connection timed out*)	**BLOCK Kritis** berhasil, mencegah upaya *hacking* SSH ke Database.

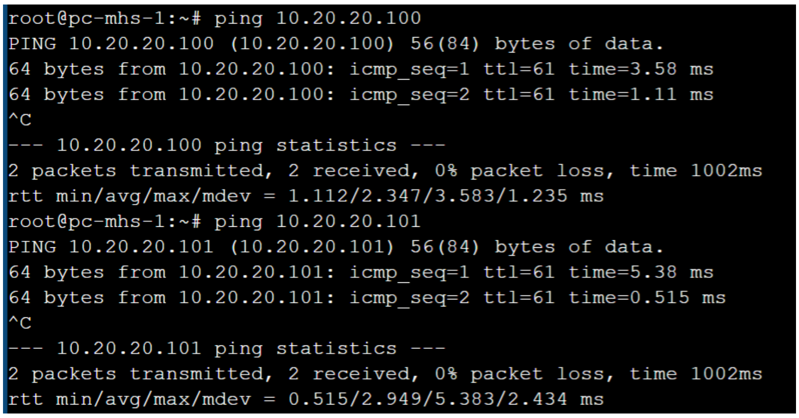
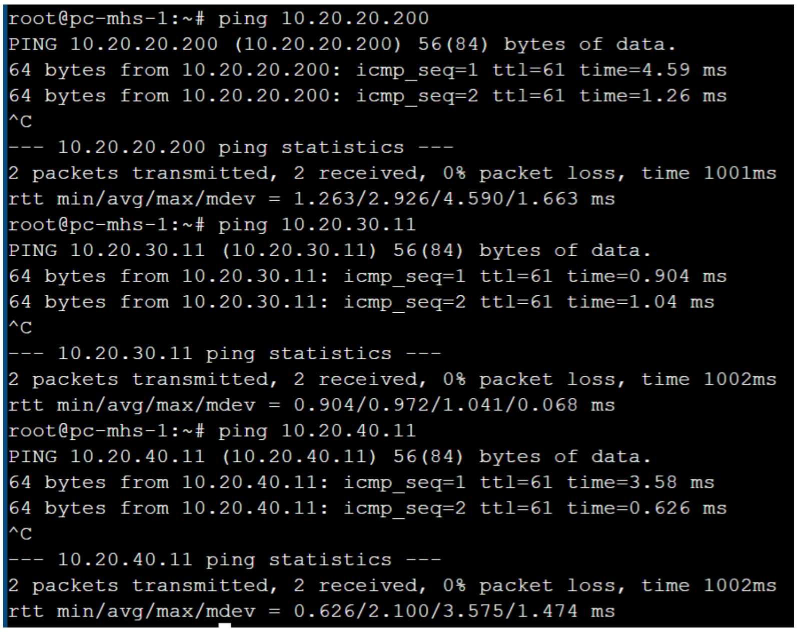
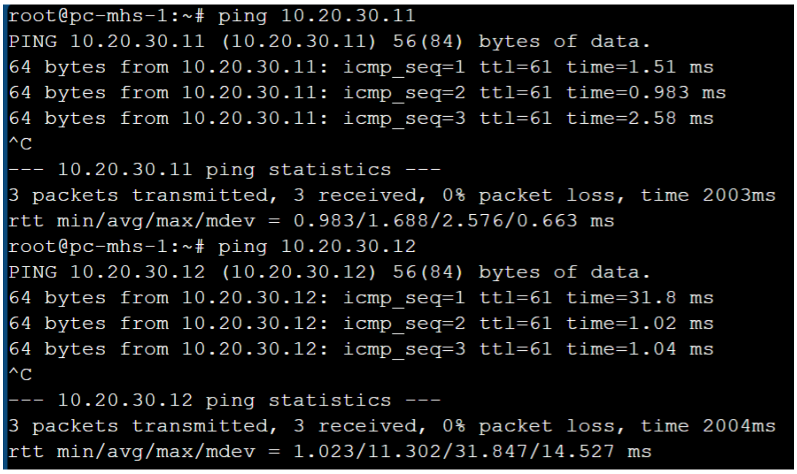
Mahasiswa	PC Admin (ICMP/Ping)	**GAGAL** (100% *packet loss*)	**BLOCK Kritis** berhasil, mengisolasi Jaringan Admin dari Mahasiswa.
Guest	Database (SSH)	**GAGAL** (*Stuck* / *Connection timed out*)	**ISOLASI TOTAL** berhasil, mencegah tamu meretas Database.
Guest	PC Admin (ICMP/Ping)	**GAGAL** (100% *packet loss*)	**ISOLASI TOTAL** berhasil, Tamu tidak dapat *ping* infrastruktur manajemen.
Guest	Classroom (SSH)	**GAGAL** (*Stuck*)	**BLOCK Kritis** berhasil, tamu hanya boleh akses web.

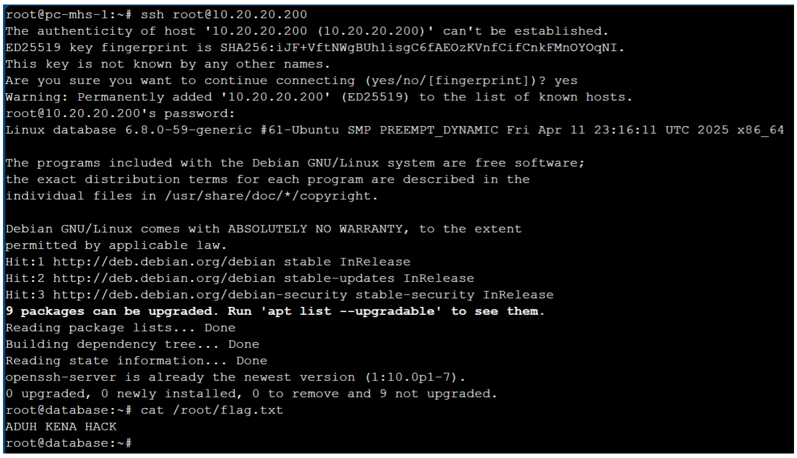
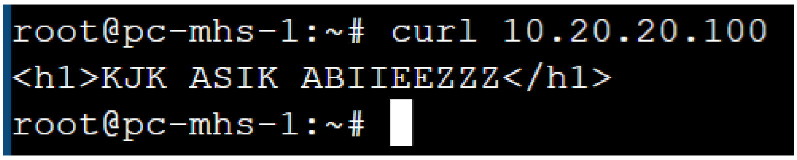
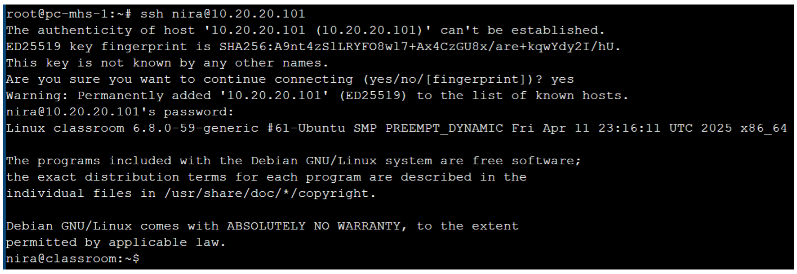
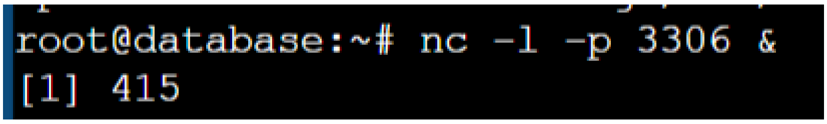
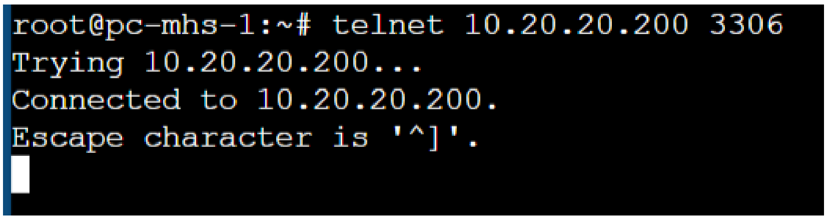
B. Uji Keberhasilan *Least Privilege* (Akses Diizinkan Terbatas)

Sumber	**Tujuan & Port**	**Hasil Pengujian (Bukti)**	**Justifikasi Keamanan (Aturan ALLOW)**
Mahasiswa	Web Akademik	**BERHASIL** (Akses Web - Curl)	**ALLOW** TCP 80/443 (HTTP/S) eksplisit berhasil, mendukung fungsionalitas esensial.
Mahasiswa	PC Riset/IoT (SSH)	**BERHASIL** (Akses di Port 22 saja)	**Pengecualian** dibuat untuk *troubleshooting* pada Port 22. Jika *ping* diblokir, ini membuktikan *Least Privilege* diterapkan (hanya SSH yang lolos, bukan ICMP).
Guest	Web Akademik	**BERHASIL** (Akses Web - Curl)	**ALLOW** TCP 80/443 eksplisit berhasil, sesuai kebijakan *browsing* tamu.

III. BUKTI VISUAL PENGUJIAN

1. Bukti Kondisi Default (Sebelum Firewall)

Keterangan	Bukti Screenshot
Mahasiswa dapat melakukan ping terhadap web-akademik dan classroom	 root@pc-mhs-1:~# ping 10.20.20.100 PING 10.20.20.100 (10.20.20.100) 56(84) bytes of data. 64 bytes from 10.20.20.100: icmp_seq=1 ttl=61 time=3.58 ms 64 bytes from 10.20.20.100: icmp_seq=2 ttl=61 time=1.11 ms ^C --- 10.20.20.100 ping statistics --- 2 packets transmitted, 2 received, 0% packet loss, time 1002ms rtt min/avg/max/mdev = 1.112/2.347/3.583/1.235 ms root@pc-mhs-1:~# ping 10.20.20.101 PING 10.20.20.101 (10.20.20.101) 56(84) bytes of data. 64 bytes from 10.20.20.101: icmp_seq=1 ttl=61 time=5.38 ms 64 bytes from 10.20.20.101: icmp_seq=2 ttl=61 time=0.515 ms ^C --- 10.20.20.101 ping statistics --- 2 packets transmitted, 2 received, 0% packet loss, time 1002ms rtt min/avg/max/mdev = 0.515/2.949/5.383/2.434 ms
Mahasiswa dapat melakukan ping terhadap database, pc riset, dan pc admin.	 root@pc-mhs-1:~# ping 10.20.20.200 PING 10.20.20.200 (10.20.20.200) 56(84) bytes of data. 64 bytes from 10.20.20.200: icmp_seq=1 ttl=61 time=4.59 ms 64 bytes from 10.20.20.200: icmp_seq=2 ttl=61 time=1.26 ms ^C --- 10.20.20.200 ping statistics --- 2 packets transmitted, 2 received, 0% packet loss, time 1001ms rtt min/avg/max/mdev = 1.263/2.926/4.590/1.663 ms root@pc-mhs-1:~# ping 10.20.30.11 PING 10.20.30.11 (10.20.30.11) 56(84) bytes of data. 64 bytes from 10.20.30.11: icmp_seq=1 ttl=61 time=0.904 ms 64 bytes from 10.20.30.11: icmp_seq=2 ttl=61 time=1.04 ms ^C --- 10.20.30.11 ping statistics --- 2 packets transmitted, 2 received, 0% packet loss, time 1002ms rtt min/avg/max/mdev = 0.904/0.972/1.041/0.068 ms root@pc-mhs-1:~# ping 10.20.40.11 PING 10.20.40.11 (10.20.40.11) 56(84) bytes of data. 64 bytes from 10.20.40.11: icmp_seq=1 ttl=61 time=3.58 ms 64 bytes from 10.20.40.11: icmp_seq=2 ttl=61 time=0.626 ms ^C --- 10.20.40.11 ping statistics --- 2 packets transmitted, 2 received, 0% packet loss, time 1002ms rtt min/avg/max/mdev = 0.626/2.100/3.575/1.474 ms
Mahasiswa dapat melakukan ping terhadap iot dan pc riset.	 root@pc-mhs-1:~# ping 10.20.30.11 PING 10.20.30.11 (10.20.30.11) 56(84) bytes of data. 64 bytes from 10.20.30.11: icmp_seq=1 ttl=61 time=1.51 ms 64 bytes from 10.20.30.11: icmp_seq=2 ttl=61 time=0.983 ms 64 bytes from 10.20.30.11: icmp_seq=3 ttl=61 time=2.58 ms ^C --- 10.20.30.11 ping statistics --- 3 packets transmitted, 3 received, 0% packet loss, time 2003ms rtt min/avg/max/mdev = 0.983/1.688/2.576/0.663 ms root@pc-mhs-1:~# ping 10.20.30.12 PING 10.20.30.12 (10.20.30.12) 56(84) bytes of data. 64 bytes from 10.20.30.12: icmp_seq=1 ttl=61 time=31.8 ms 64 bytes from 10.20.30.12: icmp_seq=2 ttl=61 time=1.02 ms 64 bytes from 10.20.30.12: icmp_seq=3 ttl=61 time=1.04 ms ^C --- 10.20.30.12 ping statistics --- 3 packets transmitted, 3 received, 0% packet loss, time 2004ms rtt min/avg/max/mdev = 1.023/11.302/31.847/14.527 ms

Mahasiswa dapat masuk ke dalam ssh database (hack).	
Mahasiswa mendapatkan akses menuju web akademik.	
Mahasiswa dapat masuk ke dalam classroom.	
Mahasiswa dapat mengakses TCP 3306 pada database	 

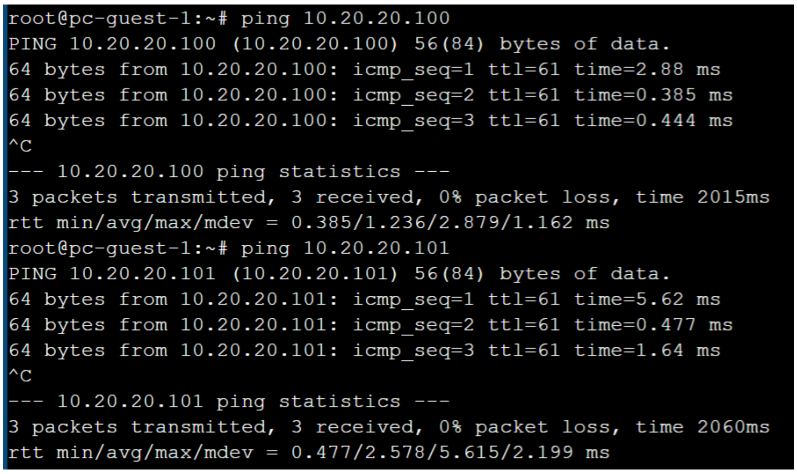
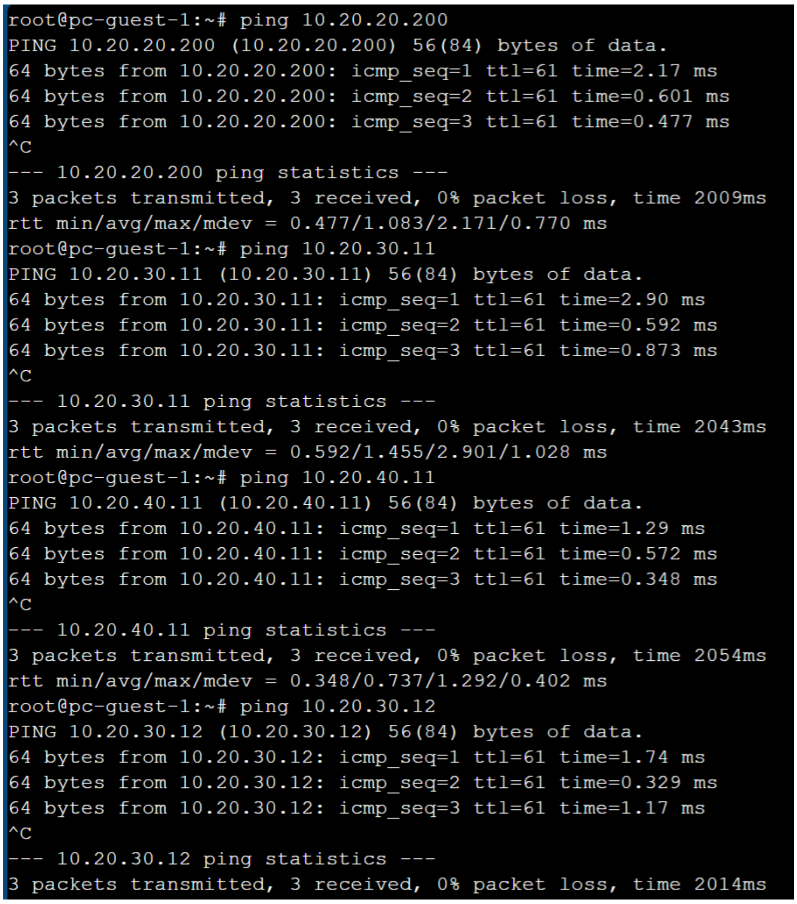
```
root@pc-mhs-1:~# ssh root@10.20.20.200
The authenticity of host '10.20.20.200 (10.20.20.200)' can't be established.
ED25519 key fingerprint is SHA256:iJF+VftNWgBUhlisgC6fAEOzKVnfCifCnkFMnOYOqNI.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.20.20.200' (ED25519) to the list of known hosts.
root@10.20.20.200's password:
Linux database 6.8.0-59-generic #61-Ubuntu SMP PREEMPT_DYNAMIC Fri Apr 11 23:16:11 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.
Hit:1 http://deb.debian.org/debian stable InRelease
Hit:2 http://deb.debian.org/debian stable-updates InRelease
Hit:3 http://deb.debian.org/debian-security stable-security InRelease
9 packages can be upgraded. Run 'apt list --upgradable' to see them.
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
openssh-server is already the newest version (1:10.0p1-7).
0 upgraded, 0 newly installed, 0 to remove and 9 not upgraded.
root@database:~# cat /root/flag.txt
ADUH KENA HACK
root@database:~#
```

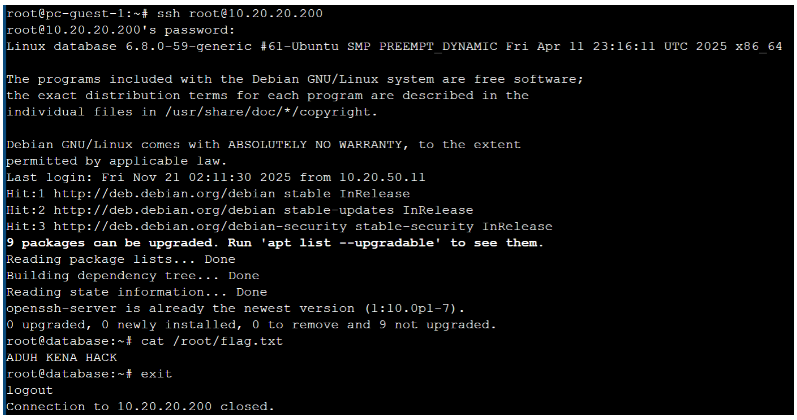
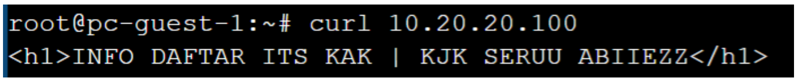
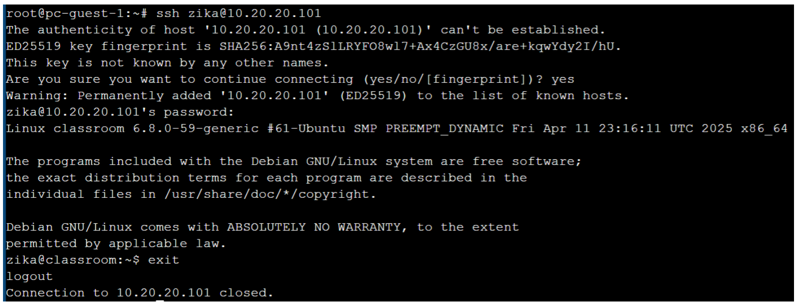
```
root@pc-mhs-1:~# curl 10.20.20.100
<h1>KJK ASIK ABIIEEZZZ</h1>
root@pc-mhs-1:~# █
```

```
root@pc-mhs-1:~# ssh nira@10.20.20.101
The authenticity of host '10.20.20.101 (10.20.20.101)' can't be established.
ED25519 key fingerprint is SHA256:A9nt4zSlLRYFO8wl7+Ax4CzGU8x/are+kqwYdy2I/hU.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.20.20.101' (ED25519) to the list of known hosts.
nira@10.20.20.101's password:
Linux classroom 6.8.0-59-generic #61-Ubuntu SMP PREEMPT_DYNAMIC Fri Apr 11 23:16:11 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.
nira@classroom:~$
```

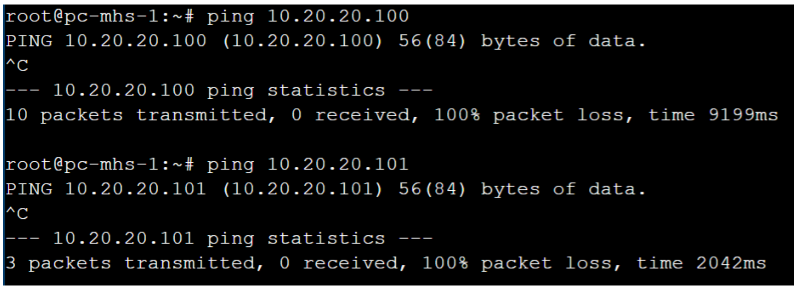
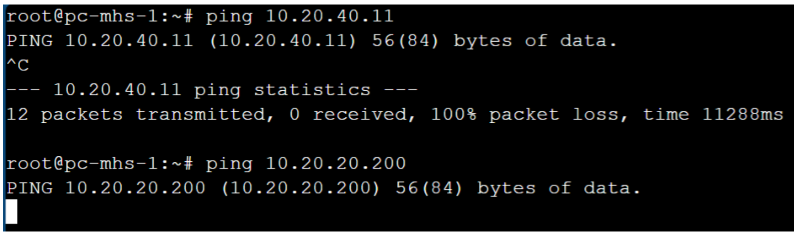
```
root@database:~# nc -l -p 3306 &
[1] 415
```

```
root@pc-mhs-1:~# telnet 10.20.20.200 3306
Trying 10.20.20.200...
Connected to 10.20.20.200.
Escape character is '^]'.
█
```

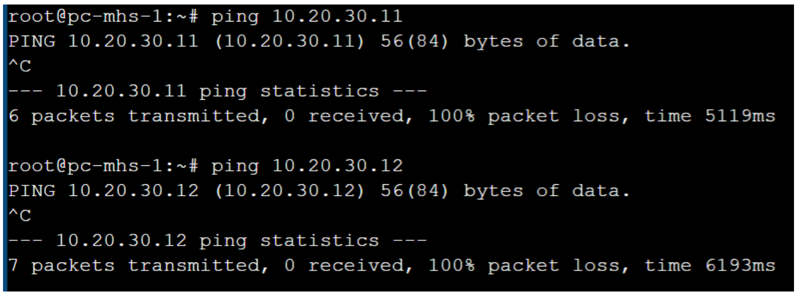
Guest dapat melakukan ping terhadap web akademik dan classroom.	 root@pc-guest-1:~# ping 10.20.20.100 PING 10.20.20.100 (10.20.20.100) 56(84) bytes of data. 64 bytes from 10.20.20.100: icmp_seq=1 ttl=61 time=2.88 ms 64 bytes from 10.20.20.100: icmp_seq=2 ttl=61 time=0.385 ms 64 bytes from 10.20.20.100: icmp_seq=3 ttl=61 time=0.444 ms ^C --- 10.20.20.100 ping statistics --- 3 packets transmitted, 3 received, 0% packet loss, time 2015ms rtt min/avg/max/mdev = 0.385/1.236/2.879/1.162 ms root@pc-guest-1:~# ping 10.20.20.101 PING 10.20.20.101 (10.20.20.101) 56(84) bytes of data. 64 bytes from 10.20.20.101: icmp_seq=1 ttl=61 time=5.62 ms 64 bytes from 10.20.20.101: icmp_seq=2 ttl=61 time=0.477 ms 64 bytes from 10.20.20.101: icmp_seq=3 ttl=61 time=1.64 ms ^C --- 10.20.20.101 ping statistics --- 3 packets transmitted, 3 received, 0% packet loss, time 2060ms rtt min/avg/max/mdev = 0.477/2.578/5.615/2.199 ms
Guest dapat melakukan ping terhadap database, pc riset, dan pc admin, iot.	 root@pc-guest-1:~# ping 10.20.20.200 PING 10.20.20.200 (10.20.20.200) 56(84) bytes of data. 64 bytes from 10.20.20.200: icmp_seq=1 ttl=61 time=2.17 ms 64 bytes from 10.20.20.200: icmp_seq=2 ttl=61 time=0.601 ms 64 bytes from 10.20.20.200: icmp_seq=3 ttl=61 time=0.477 ms ^C --- 10.20.20.200 ping statistics --- 3 packets transmitted, 3 received, 0% packet loss, time 2009ms rtt min/avg/max/mdev = 0.477/1.083/2.171/0.770 ms root@pc-guest-1:~# ping 10.20.30.11 PING 10.20.30.11 (10.20.30.11) 56(84) bytes of data. 64 bytes from 10.20.30.11: icmp_seq=1 ttl=61 time=2.90 ms 64 bytes from 10.20.30.11: icmp_seq=2 ttl=61 time=0.592 ms 64 bytes from 10.20.30.11: icmp_seq=3 ttl=61 time=0.873 ms ^C --- 10.20.30.11 ping statistics --- 3 packets transmitted, 3 received, 0% packet loss, time 2043ms rtt min/avg/max/mdev = 0.592/1.455/2.901/1.028 ms root@pc-guest-1:~# ping 10.20.40.11 PING 10.20.40.11 (10.20.40.11) 56(84) bytes of data. 64 bytes from 10.20.40.11: icmp_seq=1 ttl=61 time=1.29 ms 64 bytes from 10.20.40.11: icmp_seq=2 ttl=61 time=0.572 ms 64 bytes from 10.20.40.11: icmp_seq=3 ttl=61 time=0.348 ms ^C --- 10.20.40.11 ping statistics --- 3 packets transmitted, 3 received, 0% packet loss, time 2054ms rtt min/avg/max/mdev = 0.348/0.737/1.292/0.402 ms root@pc-guest-1:~# ping 10.20.30.12 PING 10.20.30.12 (10.20.30.12) 56(84) bytes of data. 64 bytes from 10.20.30.12: icmp_seq=1 ttl=61 time=1.74 ms 64 bytes from 10.20.30.12: icmp_seq=2 ttl=61 time=0.329 ms 64 bytes from 10.20.30.12: icmp_seq=3 ttl=61 time=1.17 ms ^C --- 10.20.30.12 ping statistics --- 3 packets transmitted, 3 received, 0% packet loss, time 2014ms

Guest dapat masuk ke dalam ssh database (hack).	 root@pc-guest-1:~# ssh root@10.20.20.200 root@10.20.20.200's password: Linux database 6.8.0-59-generic #61-Ubuntu SMP PREEMPT_DYNAMIC Fri Apr 11 23:16:11 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 02:11:30 2025 from 10.20.50.11 Hit:1 http://deb.debian.org/debian stable InRelease Hit:2 http://deb.debian.org/debian stable-updates InRelease Hit:3 http://deb.debian.org/debian-security stable-security InRelease 9 packages can be upgraded. Run 'apt list --upgradable' to see them. Reading package lists... Done Building dependency tree... Done Reading state information... Done openssh-server is already the newest version (1:10.0p1-7). 0 upgraded, 0 newly installed, 0 to remove and 9 not upgraded. root@database:~# cat /root/flag.txt ADUH KENA HACK root@database:~# exit logout Connection to 10.20.20.200 closed.
Guest dapat mengakses web akademik.	 root@pc-guest-1:~# curl 10.20.20.100 <h1>INFO DAFTAR ITS KAK | KJK SERUU ABIIEZZ</h1>
Guest dapat masuk classroom.	 root@pc-guest-1:~# ssh zika@10.20.20.101 The authenticity of host '10.20.20.101 (10.20.20.101)' can't be established. ED25519 key fingerprint is SHA256:A9nt4zSlLRYFO8wl7+Ax4CzGU8x/are+kqwYdy2I/hU. This key is not known by any other names. Are you sure you want to continue connecting (yes/no/[fingerprint])? yes Warning: Permanently added '10.20.20.101' (ED25519) to the list of known hosts. zika@10.20.20.101's password: Linux classroom 6.8.0-59-generic #61-Ubuntu SMP PREEMPT_DYNAMIC Fri Apr 11 23:16:11 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. zika@classroom:~$ exit logout Connection to 10.20.20.101 closed.

2. Bukti Kondisi Zero Trust (Setelah Firewall)

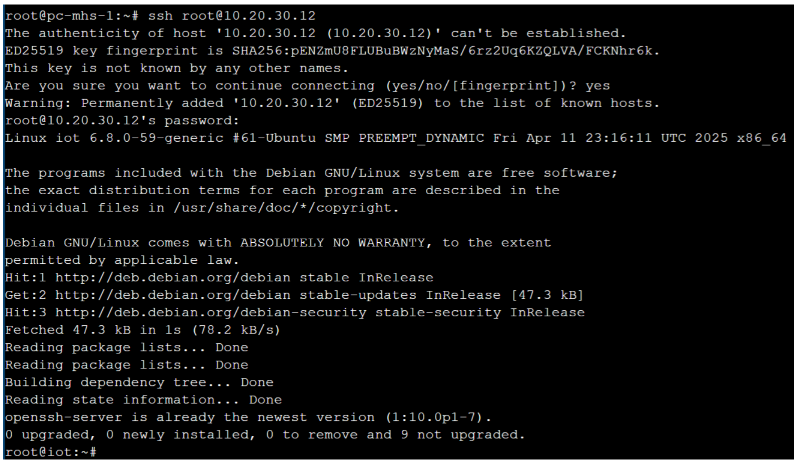
Keterangan	Bukti Screenshot
Mahasiswa tidak dapat melakukan ping web akademik dan classroom.	 root@pc-mhs-1:~# ping 10.20.20.100 PING 10.20.20.100 (10.20.20.100) 56(84) bytes of data. ^C --- 10.20.20.100 ping statistics --- 10 packets transmitted, 0 received, 100% packet loss, time 9199ms root@pc-mhs-1:~# ping 10.20.20.101 PING 10.20.20.101 (10.20.20.101) 56(84) bytes of data. ^C --- 10.20.20.101 ping statistics --- 3 packets transmitted, 0 received, 100% packet loss, time 2042ms
Mahasiswa tidak dapat melakukan ping database dan pc admin.	 root@pc-mhs-1:~# ping 10.20.40.11 PING 10.20.40.11 (10.20.40.11) 56(84) bytes of data. ^C --- 10.20.40.11 ping statistics --- 12 packets transmitted, 0 received, 100% packet loss, time 11288ms root@pc-mhs-1:~# ping 10.20.20.200 PING 10.20.20.200 (10.20.20.200) 56(84) bytes of data.

<table>
<tr>
<td>Mahasiswa tidak dapat melakukan ping iot dan pc riset.</td>
<td>



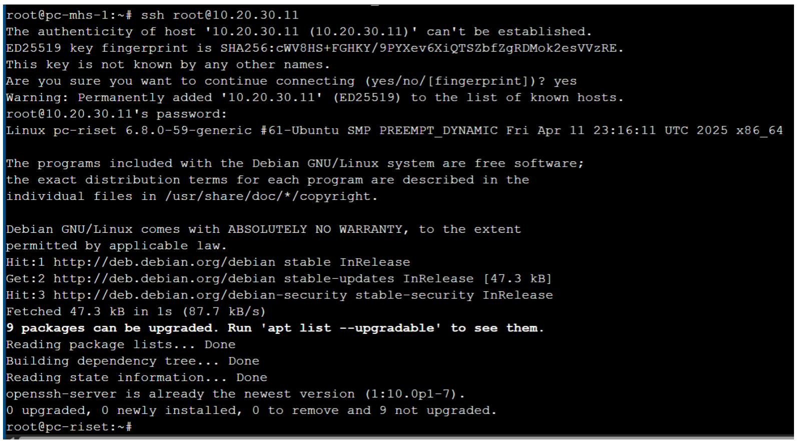
```
root@pc-mhs-1:~# ping 10.20.30.11
PING 10.20.30.11 (10.20.30.11) 56(84) bytes of data.
^C
--- 10.20.30.11 ping statistics ---
6 packets transmitted, 0 received, 100% packet loss, time 5119ms

root@pc-mhs-1:~# ping 10.20.30.12
PING 10.20.30.12 (10.20.30.12) 56(84) bytes of data.
^C
--- 10.20.30.12 ping statistics ---
7 packets transmitted, 0 received, 100% packet loss, time 6193ms
```

</td>
</tr>
<tr>
<td>Mahasiswa dapat masuk ke iot di port 22 saja.</td>
<td>



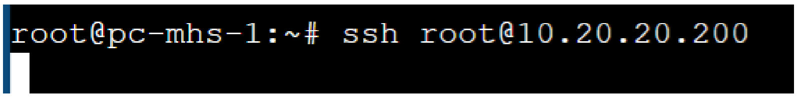
```
root@pc-mhs-1:~# ssh root@10.20.30.12
The authenticity of host '10.20.30.12 (10.20.30.12)' can't be established.
ED25519 key fingerprint is SHA256:pENZmU8FLUBuBWzNyMaS/6rz2Uq6KZQLVA/FCKNhr6k.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.20.30.12' (ED25519) to the list of known hosts.
root@10.20.30.12's password:
Linux iot 6.8.0-59-generic #61-Ubuntu SMP PREEMPT_DYNAMIC Fri Apr 11 23:16:11 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.
Hit:1 http://deb.debian.org/debian stable InRelease
Get:2 http://deb.debian.org/debian stable-updates InRelease [47.3 kB]
Hit:3 http://deb.debian.org/debian-security stable-security InRelease
Fetched 47.3 kB in 1s (78.2 kB/s)
Reading package lists... Done
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
openssh-server is already the newest version (1:10.0p1-7).
0 upgraded, 0 newly installed, 0 to remove and 9 not upgraded.
root@iot:~#
```

</td>
</tr>
<tr>
<td>Mahasiswa dapat masuk ke pc riset di port 22 saja.</td>
<td>



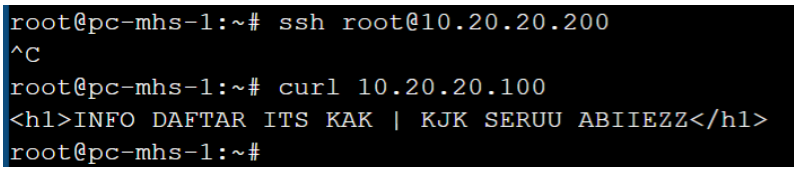
```
root@pc-mhs-1:~# ssh root@10.20.30.11
The authenticity of host '10.20.30.11 (10.20.30.11)' can't be established.
ED25519 key fingerprint is SHA256:cWV8HS+FGHKY/9PYXev6XiQTSZbfZgRDMok2esVVzRE.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.20.30.11' (ED25519) to the list of known hosts.
root@10.20.30.11's password:
Linux pc-riset 6.8.0-59-generic #61-Ubuntu SMP PREEMPT_DYNAMIC Fri Apr 11 23:16:11 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.
Hit:1 http://deb.debian.org/debian stable InRelease
Get:2 http://deb.debian.org/debian stable-updates InRelease [47.3 kB]
Hit:3 http://deb.debian.org/debian-security stable-security InRelease
Fetched 47.3 kB in 1s (87.7 kB/s)
9 packages can be upgraded. Run 'apt list --upgradable' to see them.
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
openssh-server is already the newest version (1:10.0p1-7).
0 upgraded, 0 newly installed, 0 to remove and 9 not upgraded.
root@pc-riset:~#
```

</td>
</tr>
<tr>
<td>Mahasiswa tidak dapat memasuki ke ssh database (hack) - stuck.</td>
<td>



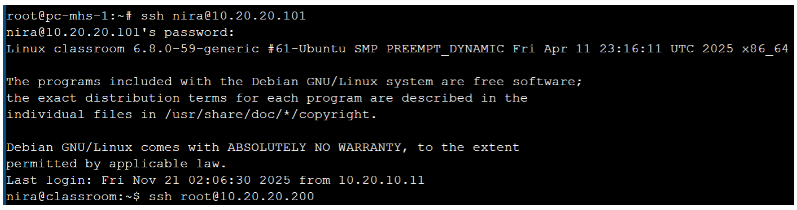
```
root@pc-mhs-1:~# ssh root@10.20.20.200
```

</td>
</tr>
<tr>
<td>Mahasiswa dapat mengakses web akademik.</td>
<td>

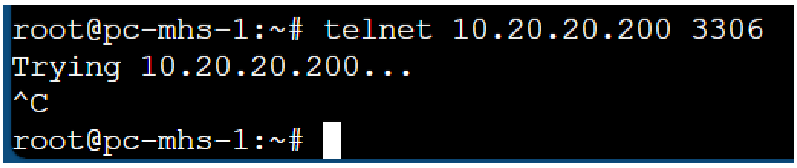
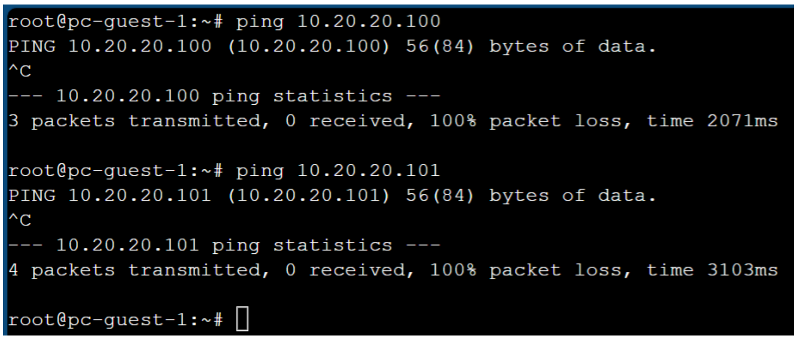


```
root@pc-mhs-1:~# ssh root@10.20.20.200
^C
root@pc-mhs-1:~# curl 10.20.20.100
<h1>INFO DAFTAR ITS KAK | KJK SERUU ABIIEZZ</h1>
root@pc-mhs-1:~#
```

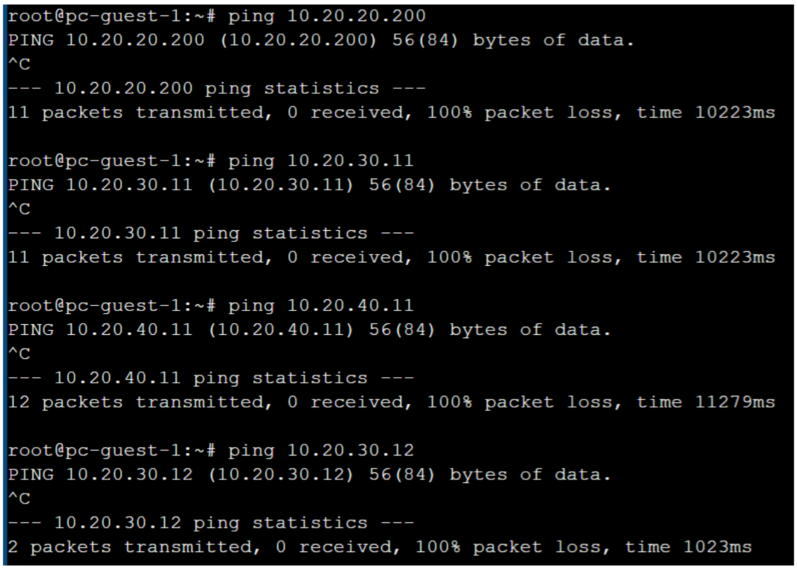
</td>
</tr>
</table>

<table>
<tr><td>Mahasiswa dapat masuk ke dalam classroom.</td><td>
root@pc-mhs-1:~# ssh nira@10.20.20.101
nira@10.20.20.101's password:
Linux classroom 6.8.0-59-generic #61-Ubuntu SMP PREEMPT_DYNAMIC Fri Apr 11 23:16:11 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.

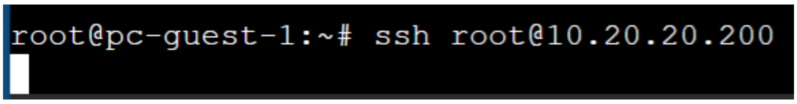
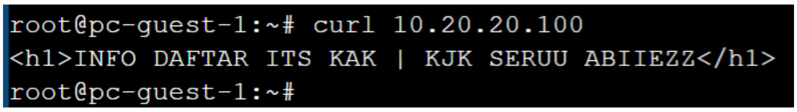
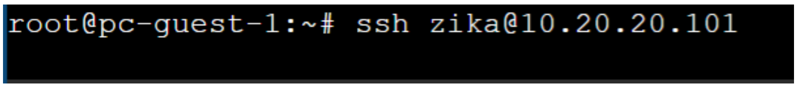
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Fri Nov 21 02:06:30 2025 from 10.20.10.11
nira@classroom:~$ ssh root@10.20.20.200</td></tr>
<tr><td>Mahasiswa tidak dapat mengakses TCP 3306 pada database - stuck</td><td>
root@pc-mhs-1:~# telnet 10.20.20.200 3306
Trying 10.20.20.200...
^C
root@pc-mhs-1:~#</td></tr>
<tr><td>Guest tidak dapat melakukan ping web akademik dan classroom.</td><td>
root@pc-guest-1:~# ping 10.20.20.100
PING 10.20.20.100 (10.20.20.100) 56(84) bytes of data.
^C
--- 10.20.20.100 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2071ms

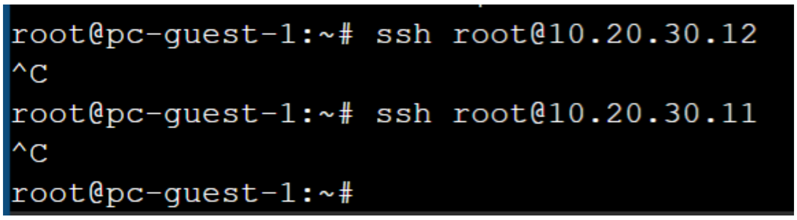
root@pc-guest-1:~# ping 10.20.20.101
PING 10.20.20.101 (10.20.20.101) 56(84) bytes of data.
^C
--- 10.20.20.101 ping statistics ---
4 packets transmitted, 0 received, 100% packet loss, time 3103ms

root@pc-guest-1:~#</td></tr>
<tr><td>Guest tidak dapat melakukan ping database, pc riset, dan pc admin, iot.</td><td>
root@pc-guest-1:~# ping 10.20.20.200
PING 10.20.20.200 (10.20.20.200) 56(84) bytes of data.
^C
--- 10.20.20.200 ping statistics ---
11 packets transmitted, 0 received, 100% packet loss, time 10223ms

root@pc-guest-1:~# ping 10.20.30.11
PING 10.20.30.11 (10.20.30.11) 56(84) bytes of data.
^C
--- 10.20.30.11 ping statistics ---
11 packets transmitted, 0 received, 100% packet loss, time 10223ms

root@pc-guest-1:~# ping 10.20.40.11
PING 10.20.40.11 (10.20.40.11) 56(84) bytes of data.
^C
--- 10.20.40.11 ping statistics ---
12 packets transmitted, 0 received, 100% packet loss, time 11279ms

root@pc-guest-1:~# ping 10.20.30.12
PING 10.20.30.12 (10.20.30.12) 56(84) bytes of data.
^C
--- 10.20.30.12 ping statistics ---
2 packets transmitted, 0 received, 100% packet loss, time 1023ms</td></tr>
<tr><td>Guest tidak bisa masuk ke dalam ssh database - stuck.</td><td>
root@pc-guest-1:~# ssh root@10.20.20.200</td></tr>
<tr><td>Guest dapat mengakses web akademik.</td><td>
root@pc-guest-1:~# curl 10.20.20.100
<h1>INFO DAFTAR ITS KAK | KJK SERUU ABIIEZZ</h1>
root@pc-guest-1:~#</td></tr>
<tr><td>Guest tidak dapat memasuki classroom - stuck.</td><td>
root@pc-guest-1:~# ssh zika@10.20.20.101</td></tr>
</table>

Guest tidak bisa masuk melalui server ssh ke dalam iot maupun pc riset.	
	`root@pc-guest-1:~# ssh root@10.20.30.12`
	`^C`
	`root@pc-guest-1:~# ssh root@10.20.30.11`
	`^C`
	`root@pc-guest-1:~#`

Logging setiap aktivitas yang melalui firewall	belum terealisasi

script bisa diakses di link berikut: script