YAYASAN PRAWITAMA
SMK WIKRAMA BOGOR
Jl. Raya Wangun Kel. Sindangsari Kota Bogor
Telp. 0251-8242411, email: prohumasi@smkwikrama.net, website : www.smkwikrama.net

LK Linux 2 – SSH KeyBased

Lembar Kerja Peserta Didik

Nama : Muhamad Dzakwan Ar Efendi
Nis : 12209161
Kelas : TJKT XI-1
Judul Materi : SSH Key-Based Authentication

NILAI

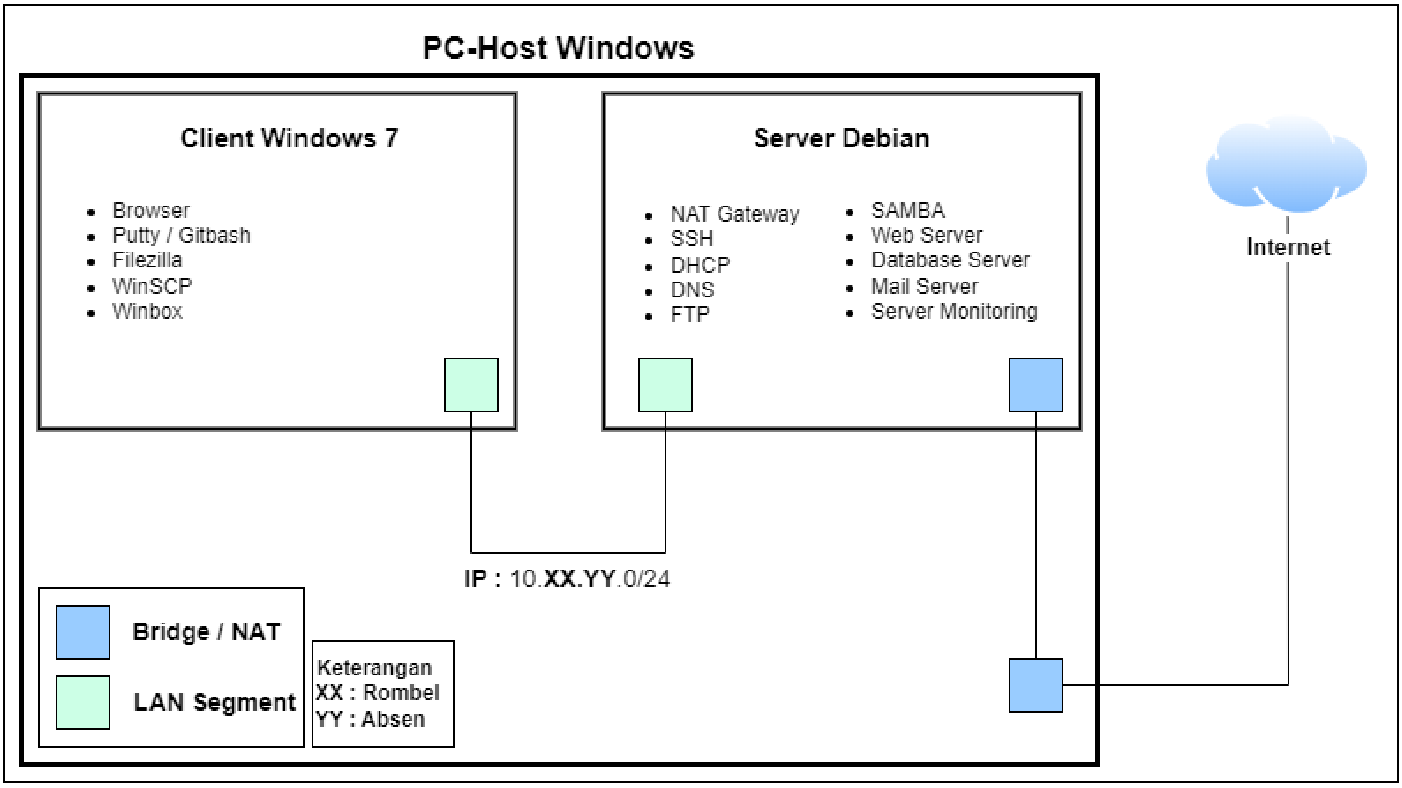
Kegiatan 1 :

a) Petunjuk Kerja :

- Menyiapkan Software aplikasi pendukung
- Menyiapkan Laptop / PC
- Menyiapkan Koneksi Internet
- Menyiapkan peralatan Praktek
- Menyiapkan Modul Panduan kerja Jobsheet Konfigurasi SSH Key-Based Authentication

https://dulcent.blogspot.com/2023/11/konfigurasi-ssh-key-based-authentication.html

b) Topologi



Buatlah Konfigurasi Web Server

Pra-Install

Berdasarkan topologi diatas terdiri dari 1 PC Server Linux dan 1 PC/Laptop CLient yang sudah terinstal pada aplikasi virtualbox atau vmware workstation

1. Create VM

VM Name	: Server_Nama Siswa
Memory	: 512 MB
Sistem Operasi	: Linux – Debian 11 (Virtual)
Net Adapter	: - Bridge/NAT - LAN Segment
IP Address	: 10.xx.yy.1/ 24
Domain	: srvnamaXY.net

Keterangan

xx : Nomor Rombel

yy : Nomor Absen

namaXY : Nama masing-masing dan 2 digit terakhir NIS

2. PC/Laptop (VM-Windows)

IP Address	: DHCP-Client
HDD/RAM	: 20GB/1GB
Sistem Operasi	**:** Windows
Net Adapter	: LAN Segmet

Pastikan Pada Sisi Client mendapatkan Ip dari DHCP Server

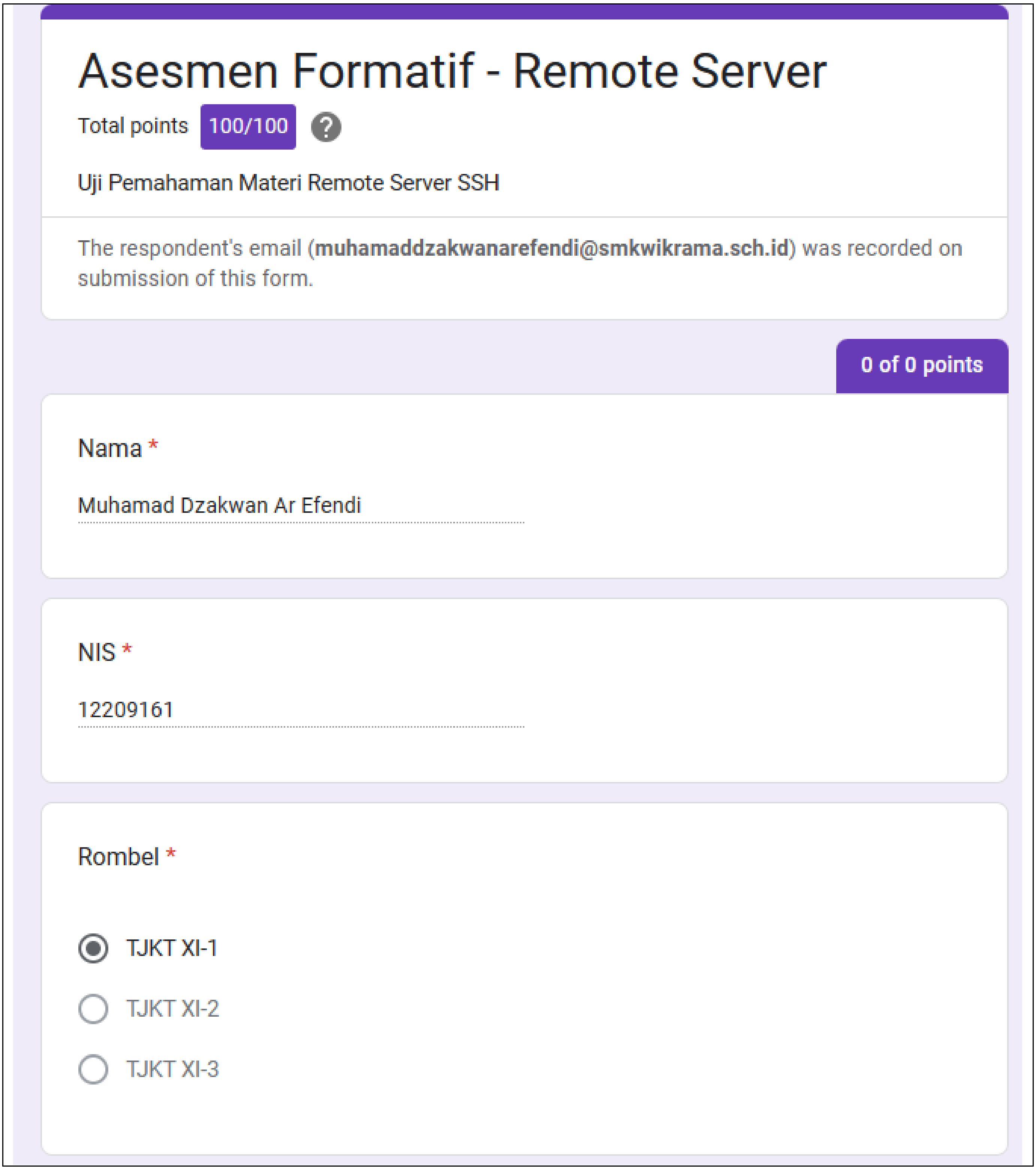
Pemahaman Materi

Silahkan kerjakan uji pemahaman materi Remote Server SSH pada link berikut ini :

https://forms.gle/8GXGV2wBNbUWZNzV8

Kerjakan ulang hingga mendapatkan nilai diatas KKM (>75). Jika belum bisa di kerjakan ulang.

Screenshot Hasil/Nilai Mengerjakan Uji Pemahaman



Asesmen Formatif - Remote Server

Total points 100/100

Uji Pemahaman Materi Remote Server SSH

The respondent's email (**muhamaddzakwanarefendi@smkwikrama.sch.id**) was recorded on submission of this form.

0 of 0 points

Nama *

Muhamad Dzakwan Ar Efendi

NIS *

12209161

Rombel *

● TJKT XI-1

○ TJKT XI-2

○ TJKT XI-3

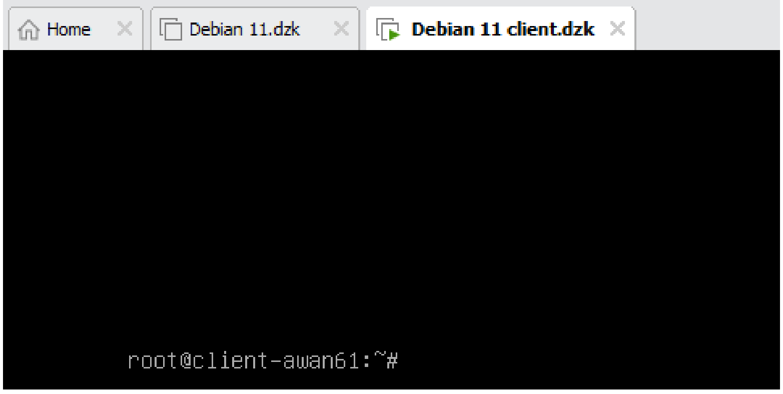
Langkah Kerja

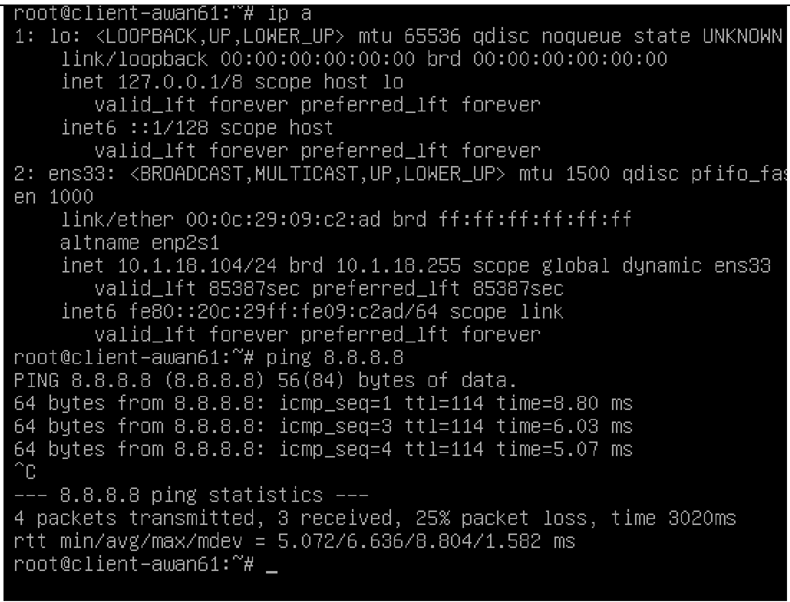
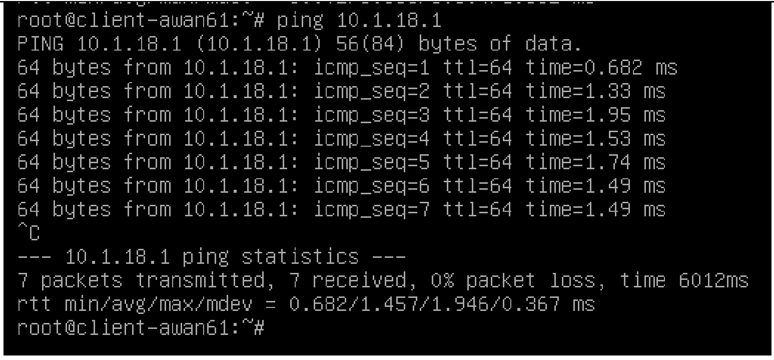
Pada LK ini silahkan teman-teman praktikan konfigurasi autentikasi SSH berbasis kunci, dengan 3 skenario yaitu :

- Remote ssh key-based dari Linux,
- Remote ssh key-based dari Windows CMD, dan
- Remote ssh key-based menggunakan Putty.

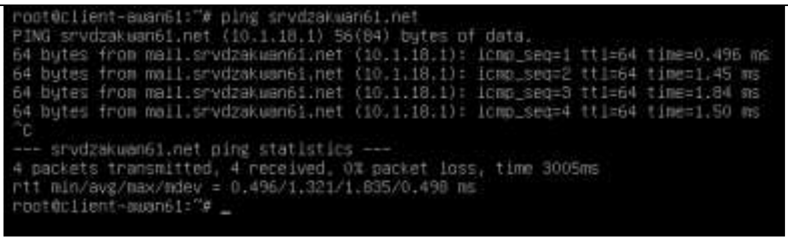
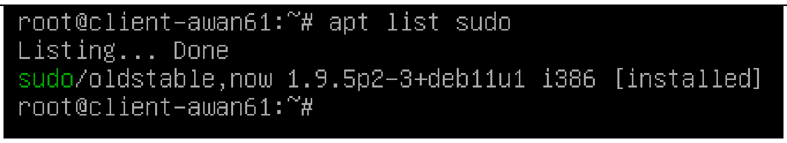
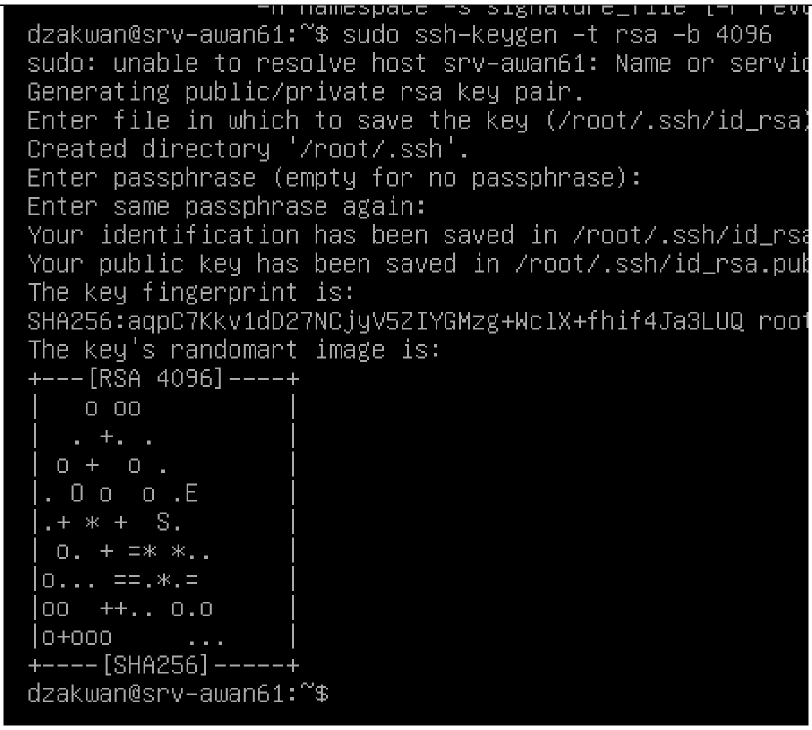
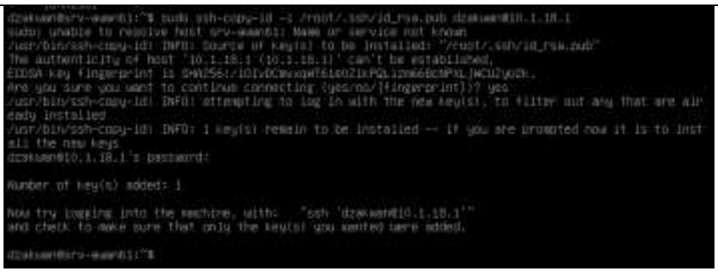
Untuk kelancaran konfigurasi dipastikan sudah menginstall openssh, menginstall sudo dan menambahkan user kedalam sudoers di Debian Server dan Client.

1. Remote SSH Key-Based dari client Linux.

<table>
<tr><th>No</th><th>Konfigurasi</th><th>Hasil (Gambar)</th><th>Keterangan</th></tr>
<tr><td>1</td><td>Membuat VM Debian 11 baru</td><td>

<pre>root@client-awan61:~#</pre></td><td>Disini saya clone dari debian server saya, namun semua konfigurasi yang ada pada debian server saya hilangkan dengan menggunakan perintah: <b>Apt purge (nama software).</b></td></tr>
<tr><td>2</td><td>Konfigurasikan agar Debian client mendapatkan IP DHCP dari Debian-Server.</td><td>
<pre>
root@client-awan61:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fas
en 1000
    link/ether 00:0c:29:09:c2:ad brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 10.1.18.104/24 brd 10.1.18.255 scope global dynamic ens33
       valid_lft 85387sec preferred_lft 85387sec
    inet6 fe80::20c:29ff:fe09:c2ad/64 scope link
       valid_lft forever preferred_lft forever
root@client-awan61:~# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=114 time=8.80 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=114 time=6.03 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=114 time=5.07 ms
^C
--- 8.8.8.8 ping statistics ---
4 packets transmitted, 3 received, 25% packet loss, time 3020ms
rtt min/avg/max/mdev = 5.072/6.636/8.804/1.582 ms
root@client-awan61:~# _
</pre></td><td>Disini saya memakai adapter LAN segment yang tehubung pada debian 11 server, dan semua konfigurasi DHCP dan NAT gateway telah berhasil masuk kedalam debian client dan bekerja dengan baik.</td></tr>
<tr><td>3</td><td>Ping debian-client ke Debian-Server</td><td>
<pre>
root@client-awan61:~# ping 10.1.18.1
PING 10.1.18.1 (10.1.18.1) 56(84) bytes of data.
64 bytes from 10.1.18.1: icmp_seq=1 ttl=64 time=0.682 ms
64 bytes from 10.1.18.1: icmp_seq=2 ttl=64 time=1.33 ms
64 bytes from 10.1.18.1: icmp_seq=3 ttl=64 time=1.95 ms
64 bytes from 10.1.18.1: icmp_seq=4 ttl=64 time=1.53 ms
64 bytes from 10.1.18.1: icmp_seq=5 ttl=64 time=1.74 ms
64 bytes from 10.1.18.1: icmp_seq=6 ttl=64 time=1.49 ms
64 bytes from 10.1.18.1: icmp_seq=7 ttl=64 time=1.49 ms
^C
--- 10.1.18.1 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6012ms
rtt min/avg/max/mdev = 0.682/1.457/1.946/0.367 ms
root@client-awan61:~#
</pre></td><td>Debian client saya telah berhasil terhubung ke debian 11 server.

Disini saya juga meng-test apakah ping menggunakan</td></tr>
</table>

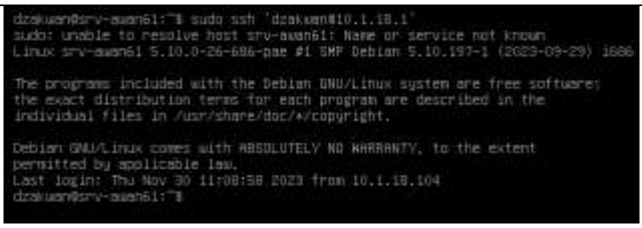
			dns berhasil atau tidak, dan ternyata berhasil. (selalu perhatikan /etc/resolv.conf)
4	Konfigurasi Sudoers. Install sudo, menambahkan user kedalam group sudo, dan login kedalam user tersebut.		Dikarenakan saya akan konfigurasi menggunakan user biasa, jadi saya membutuhkan sudo agar user biasa sayang sudah di daftarkan pada grup sudo akan bisa edit file/directory.
5	Generate key-pair, gunakan algortima rsa dengan ukuran 4096 bit.		Disini saya generate key-pair untuk di copy kedalam server agar bisa remote tidak perlu menggunakan password. (untuk bit itu di gunakan sesuai dengan kebutuhan kita, janga sampai asal menggunakan bit rsa. Gunakan sebaik mungkin).
6	Copy public key ke remote host (debian-server)		Disini saya copy kode public key yang berasal dari debian client dipindahkan ke debian server dengan menggunakan command

```
root@client-awan61:~# ping srvdzakuan61.net
PING srvdzakuan61.net (10.1.18.1) 56(84) bytes of data.
64 bytes from mail.srvdzakuan61.net (10.1.18.1): icmp_seq=1 ttl=64 time=0.496 ms
64 bytes from mail.srvdzakuan61.net (10.1.18.1): icmp_seq=2 ttl=64 time=1.45 ms
64 bytes from mail.srvdzakuan61.net (10.1.18.1): icmp_seq=3 ttl=64 time=1.84 ms
64 bytes from mail.srvdzakuan61.net (10.1.18.1): icmp_seq=4 ttl=64 time=1.50 ms
^C
--- srvdzakuan61.net ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 0.496/1.321/1.835/0.490 ms
root@client-awan61:~# _
```

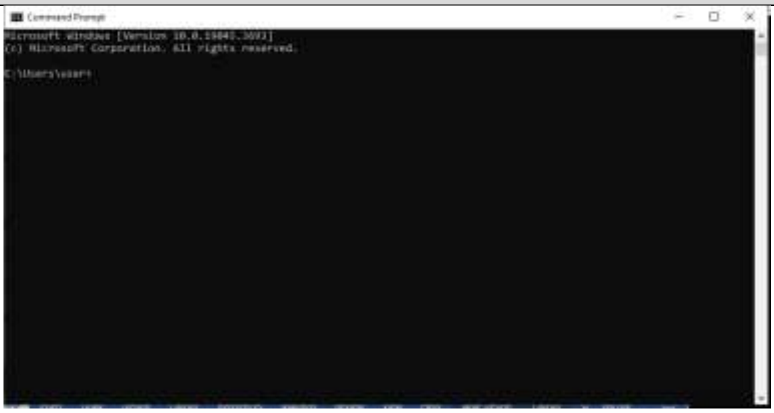
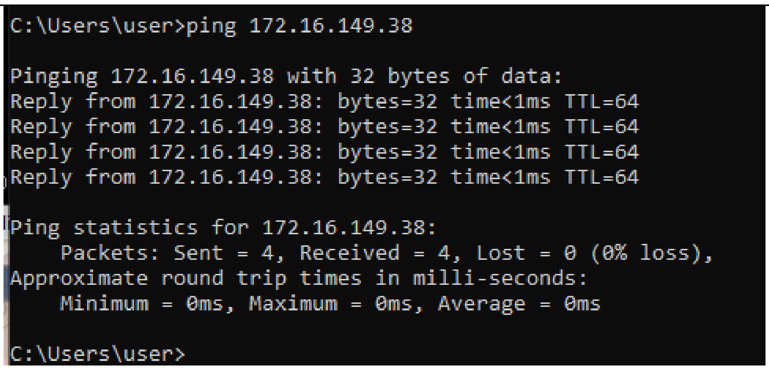
```
root@client-awan61:~# apt list sudo
Listing... Done
sudo/oldstable,now 1.9.5p2-3+deb11u1 i386 [installed]
root@client-awan61:~#
```

```
          -n namespace -s signature_file [-r revo
dzakwan@srv-awan61:~$ sudo ssh-keygen -t rsa -b 4096
sudo: unable to resolve host srv-awan61: Name or servic
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa)
Created directory '/root/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa
Your public key has been saved in /root/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:aqpC7Kkv1dD27NCjyV5ZIYGMzg+Wc1X+fhif4Ja3LUQ root
The key's randomart image is:
+---[RSA 4096]----+
|    o oo         |
|   . +. .        |
| o +  o .        |
|. O o  o .E      |
|.+ * +  S.       |
| o. + =* *..     |
|o... ==.*.=      |
|oo  ++.. o.o     |
|o+ooo     ...    |
+----[SHA256]-----+
dzakwan@srv-awan61:~$
```

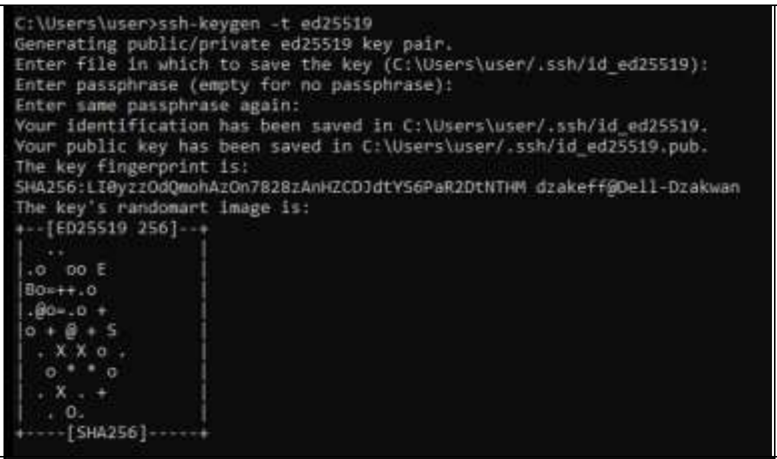
```
dzakwan@srv-awan61:~$ sudo ssh-copy-id -i /root/.ssh/id_rsa.pub dzakwan@10.1.18.1
sudo: unable to resolve host srv-awan61: Name or service not known
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/root/.ssh/id_rsa.pub"
The authenticity of host '10.1.18.1 (10.1.18.1)' can't be established.
ECDSA key fingerprint is SHA256:[illegible].
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are alr
eady installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now it is to inst
all the new keys
dzakwan@10.1.18.1's password:

Number of key(s) added: 1

Now try logging into the machine, with:   "ssh 'dzakwan@10.1.18.1'"
and check to make sure that only the key(s) you wanted were added.

dzakwan@srv-awan61:~$
```

			ssh_copy_id (alamat direktory) (sekaligus pengetesan ssh kepada user@ip-server).
7	Uji-Coba Remote SSH ke debian-server. Pastikan login tanpa memasukan password !!!	 dzakuan@srv-auan61:~$ sudo ssh 'dzakuan@10.1.18.1' sudo: unable to resolve host srv-auan61: Name or service not known Linux srv-auan61 5.10.0-26-686-pae #1 SMP Debian 5.10.197-1 (2023-09-29) i686 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: Thu Nov 30 11:08:58 2023 from 10.1.18.104 dzakuan@srv-auan61:~$	Disini saya berhasil remote ssh tanpa menggunakan password dan berjalan dengan baik.

2. Remote SSH Key-Based dari Windows (CMD).

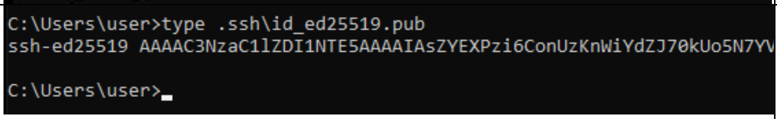
No	Konfigurasi	Hasil (Gambar)	Keterangan
1	Buka Windows CMD	 Command Prompt Microsoft Windows [Version 10.0.19045.3693] (c) Microsoft Corporation. All rights reserved. C:\Users\user>	Nah, sekarang kita akan melakukan ssh mengunakan cmd windows. Disini saya menggunaka windows host dan ip debian server yang akan dipanggil, adalah ip yang berasal dari server sekolah saya.
2	Ping windows-host ke remote server (Debian)	 C:\Users\user>ping 172.16.149.38 Pinging 172.16.149.38 with 32 bytes of data: Reply from 172.16.149.38: bytes=32 time<1ms TTL=64 Reply from 172.16.149.38: bytes=32 time<1ms TTL=64 Reply from 172.16.149.38: bytes=32 time<1ms TTL=64 Reply from 172.16.149.38: bytes=32 time<1ms TTL=64 Ping statistics for 172.16.149.38: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 0ms, Average = 0ms C:\Users\user>	Disini saya ping ip bridge milik debian server, dan berasil terhubung.

<table>
<tr>
<td>3</td>
<td>Generate Key-Pair menggunakan algoritma ed25519.</td>
<td>



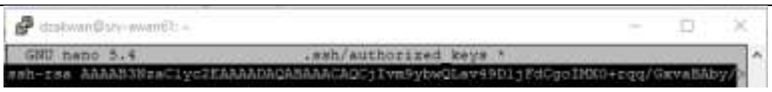
```
C:\Users\user>ssh-keygen -t ed25519
Generating public/private ed25519 key pair.
Enter file in which to save the key (C:\Users\user/.ssh/id_ed25519):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in C:\Users\user/.ssh/id_ed25519.
Your public key has been saved in C:\Users\user/.ssh/id_ed25519.pub.
The key fingerprint is:
SHA256:LI0yzzOdQmohAzOn7828zAnHZCDJdtYS6PaR2DtNTHM dzakeff@Dell-Dzakwan
The key's randomart image is:
+--[ED25519 256]--+
|   ..            |
|.o  oo E         |
|Bo=++.o          |
|.@o=.o +         |
|o + @ + S        |
| . X X o .       |
|  o * * o        |
| . X . +         |
|  . O.           |
+----[SHA256]-----+
```

</td>
<td>Disini sama seperti pada debian client namun yang berbeda adalah algoritmanya.
Disini menggunakan ed22519 sedangkan debian menggunakan rsa 4096 bit.
(sesuaikan algoritma sesuai dengan kebutuhan)</td>
</tr>
<tr>
<td>4</td>
<td>Tampilkan isi file public key.</td>
<td>



```
C:\Users\user>type .ssh\id_ed25519.pub
ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIAsZYEXPzi6ConUzKnWiYdZJ70kUo5N7YV

C:\Users\user>_
```

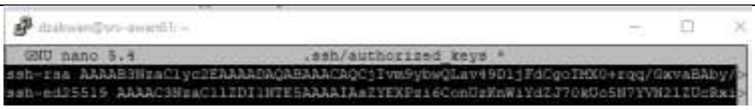
</td>
<td>Disini telah ada isi dari public key yang sudah ter generate.</td>
</tr>
<tr>
<td>5</td>
<td>SSH biasa ke dalam remote server (debian-server) kemudian buat direktori .ssh dan file authorized_keys untuk menyimpan public key.</td>
<td>



dzakwan@srv-awan61: ~

```
  GNU nano 5.4              .ssh/authorized_keys *
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAACAQCjIvm9ybwQLav49D1jFdCgoIMX0+rqq/GxvaBAby/
```

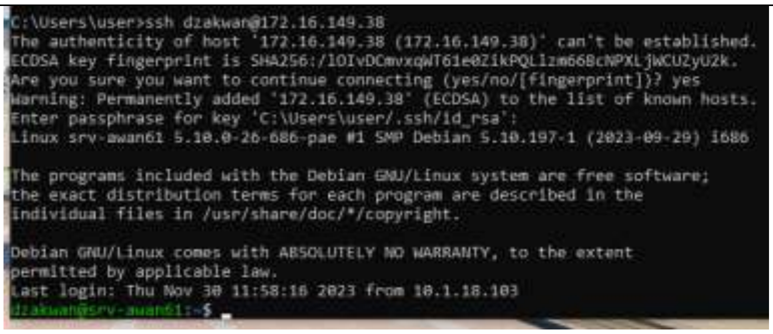
</td>
<td>Disini masuk kedalam file yang berisi dengan public-key yang ter generate oleh debian client. Kemudian saya akan masukan public yang di generate oleh CMD
(untuk pergi kedalam .ssh, login atau cd kedalam user yang akan di remote.
Contoh:
-dzakwan@srv-awan61$ <b>sudo nano .ssh/authorized_keys</b>
-root@srv-awan61# <b>nano /home/dzakwan/.ssh/authorized_keys</b></td>
</tr>
<tr>
<td>6</td>
<td>Paste public key ke file authorized_keys.</td>
<td>



dzakwan@srv-awan61: ~

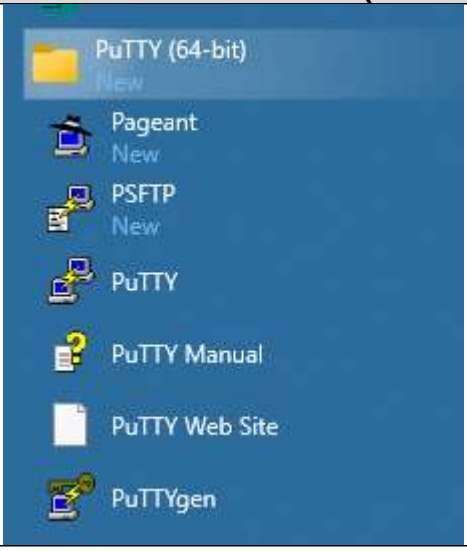
```
  GNU nano 5.4              .ssh/authorized_keys *
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAACAQCjIvm9ybwQLav49D1jFdCgoIMX0+rqq/GxvaBAby/
ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIAsZYEXPzi6ConUzKnWiYdZJ70kUo5N7YVN21ZUzRxi
```

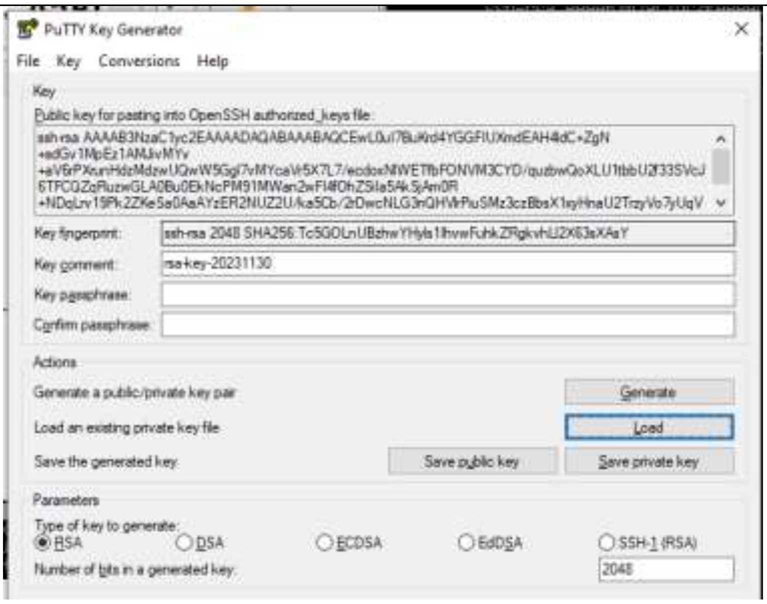
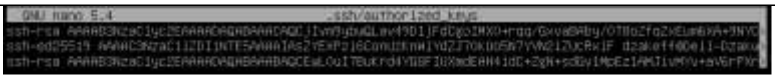
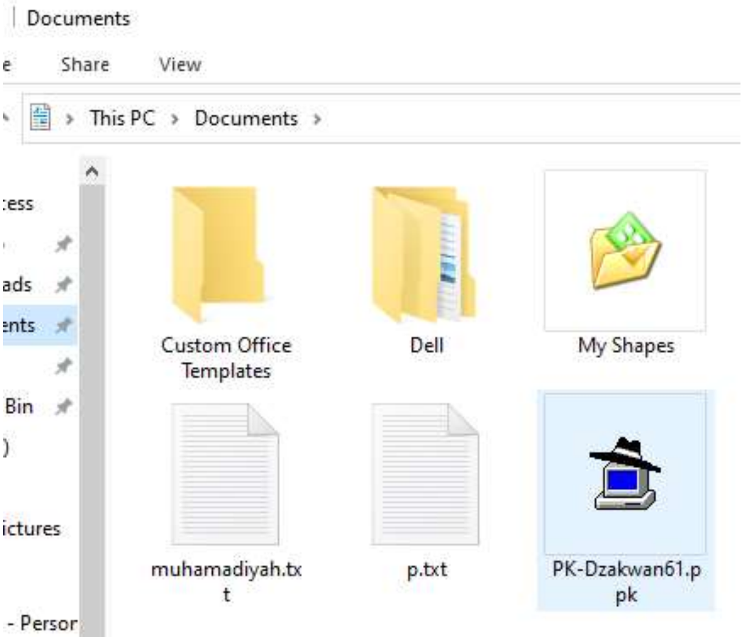
</td>
<td>Setelah muncul, copy kedalam file .shh di debian server. Disini bisa menggunakan putty atau bisa langsung copy melalui vmware.</td>
</tr>
</table>

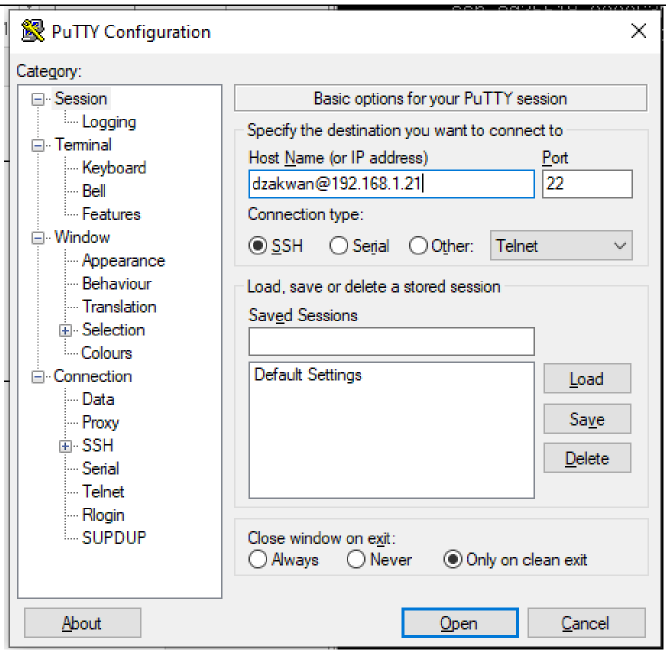
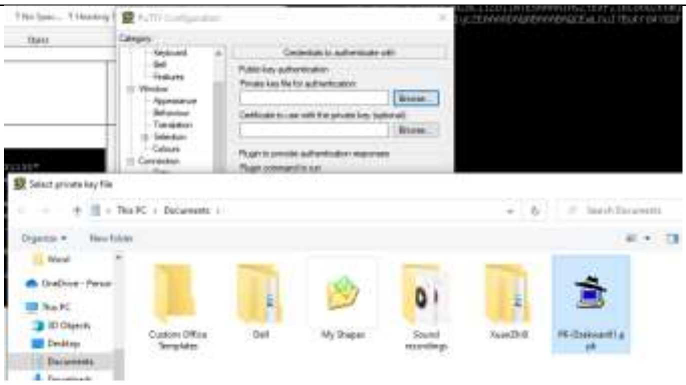
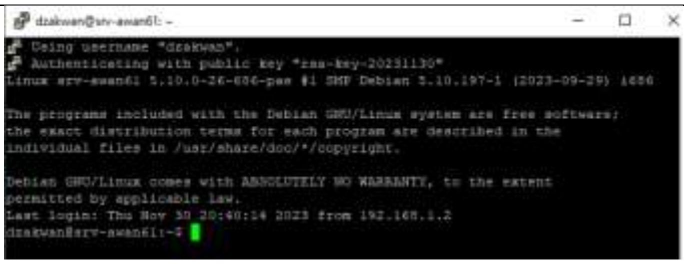
7	Uji-Coba Remote SSH ke remote host (Debian) Pastikan login tanpa memasukan password !!!		Kemudian, silahkan ujicoba panggil debian server secara remote melalui CMD. Dan debian server milik saya berhasil dipanggil tanpa menggunakan password.

```
C:\Users\user>ssh dzakwan@172.16.149.38
The authenticity of host '172.16.149.38 (172.16.149.38)' can't be established.
ECDSA key fingerprint is SHA256:/lOIvDCmvxqWT61e0ZikPQLlzm668cNPXLjWCUZyU2k.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '172.16.149.38' (ECDSA) to the list of known hosts.
Enter passphrase for key 'C:\Users\user/.ssh/id_rsa':
Linux srv-awan61 5.10.0-26-686-pae #1 SMP Debian 5.10.197-1 (2023-09-29) i686

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: Thu Nov 30 11:58:16 2023 from 10.1.18.103
dzakwan@srv-awan61:~$
```

3. Remote SSH Key-Based menggunakan SSH Client PUTTY.

No	Konfigurasi	Hasil (Gambar)	Keterangan
1	Download Putty dan PuttyGen.		Disini saya download putty dengan mendownload package, jadi saya install semua software putty. *pastikan putty memiliki versi yang terbaru.

2	Generate Key-Pair menggunakan PuttyGen. Algoritma : RSA	 PuTTY Key Generator File Key Conversions Help Key Actions Parameters Public key for pasting into OpenSSH authorized_keys file: ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCEwL0uI7BuKrd4YGGFIUXmdEAH4idC+ZgN +sdGv1MpEz1AMJIvMYv +aV6rPXunHdzMdzwUQwW5Ggl7vMYcaVr5X7L7/ecdoxNWETfbFONVM3CYD/quzbwQoXLU1tbbU2f33SVcJ 6TPCQZqRuzwGLA0Bu0EkNcPM91MWan2wFI4fOhZSIa5Ak5jAm0R +NDqLrv19Pk2ZKe5a0AaAYzER2NUZ2U/ka5Cb/2rDwcNLG3nQHVrPuSMz3czBbsX1xyHnaU2TrzyVo7yUqV Key fingerprint: ssh-rsa 2048 SHA256:Tc5GOLnUBzhwYHyls1lhvwFuhkZRgkvhU2X63sXAaY Key comment: rsa-key-20231130 Key passphrase: Confirm passphrase: Generate a public/private key pair [Generate] Load an existing private key file [Load] Save the generated key [Save public key] [Save private key] Type of key to generate: ● RSA ○ DSA ○ ECDSA ○ EdDSA ○ SSH-1 (RSA) Number of bits in a generated key: 2048	Disini saya telah generate key-pair pada putty. Cara nya adalah -masuk ke puttygen -pilih algoritma dan bits yang akan digunakan -puttygen akan menyuruh kita untuk menggerakan cursor di blank area sampai proses generate selesai -save generated key sebagai private-key.
3	Copy Public key ke remote host (debian-server)	 GNU nano 5.4 .ssh/authorized_keys ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCjIvm9ybwQLav49D1jFdCgoIMXO+rqq/GxvaBAby/OTBoZfqZkEum6XA+JNYC ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIAs2YExPz16ConuIKnWlYdZJ70KU0EN7YVN2lZUcRx1F dzaketf@Dell-Dzaku ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCEwL0uI7BuKrd4YGGFIUXmdEAH4idC+ZgN+sdGv1MpEz1AMJIvMYv+aV6rPXr	Seperti pada generate CMD, copy key-pair yang sudah dibuat kedalam file authorized_keys pada debian server
4	Save private key. File name : PK-NamaXX XX – 2 digit terakhir NIS	 Documents e Share View This PC › Documents › :ess ads ents Bin) ictures - Persor Custom Office Templates Dell My Shapes muhamadiyah.txt p.txt PK-Dzakwan61.ppk	Agar key-pair yang telah dibuat tidak hilang, save key-pair untuk digunakan di putty.

5	Remote SSH ke debian-server menggunakan Putty.	 PuTTY Configuration Basic options for your PuTTY session Specify the destination you want to connect to Host Name (or IP address): dzakwan@192.168.1.21 Port: 22 Connection type: ● SSH ○ Serial ○ Other: Telnet Load, save or delete a stored session Saved Sessions: Default Settings Close window on exit: ○ Always ○ Never ● Only on clean exit Category: Session Logging Terminal Keyboard Bell Features Window Appearance Behaviour Translation Selection Colours Connection Data Proxy SSH Serial Telnet Rlogin SUPDUP Load Save Delete About Open Cancel	Disini masukan nama user dan ip bridge debian server.
6	Insert Private key ke Putty.	 PuTTY Configuration Credentials to authenticate with Public-key authentication Private key file for authentication: Certificate to use with the private key (optional) Plugin to provide authentication responses Plugin command to run Select private key file This PC › Documents Category Keyboard Bell Features Window Appearance Behaviour Translation Selection Colours Connection Browse... Browse... Search Documents Organize New folder OneDrive - Person This PC 3D Objects Desktop Documents Downloads Custom Office Templates Dell My Shapes Sound recordings XuanZhi8 PK-Dzakwan61.ppk	Pada menu category, pergi ke kategori SSH, kemudian klik auth lalu pilih private-key yang sudah kita save tadi.
7	Uji-Coba Screenshot hasil Remote SSH menggunakan Putty. Pastikan login tanpa memasukan password !!!	 dzakwan@srv-awan61: ~ Using username "dzakwan". Authenticating with public key "rsa-key-20231130" Linux srv-awan61 5.10.0-26-686-pae #1 SMP Debian 5.10.197-1 (2023-09-29) i686 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: Thu Nov 30 20:40:14 2023 from 192.168.1.2 dzakwan@srv-awan61:~$	Disini saya berhasil masuk kedalam debian server tanpa menggunakan password.

☺ Selamat Mengerjakan☺