

LAPORAN

REMOTE ACCESS MENGGUNAKAN OS UBUNTU DAN WINDOWS.



Kelompok 2 :

Dede Jaenudin	(2142412)
Defa Mulya Pratama	(2142417)
Dimas Fathan Habibi	(2142423)
Lukman Maulana	(2142422)
Luthfi Nur Ramadhan	(2142430)

PROGRAM STUDI TEKNIK INFORMATIKA

STMIK “AMIK BANDUNG”

2023

BAB I

Pendahuluan

SSH (Secure Shell) adalah protokol jaringan yang digunakan untuk mengamankan komunikasi antara dua perangkat yang terhubung ke jaringan. SSH memungkinkan Anda untuk mengakses komputer jarak jauh dengan aman dan mengirimkan data melalui saluran terenkripsi. SSH juga memungkinkan pengguna untuk menjalankan perintah dan mengelola sistem jarak jauh dengan aman.

Remote access atau akses jarak jauh mengacu pada kemampuan untuk mengakses komputer atau jaringan dari lokasi jauh melalui jaringan. Dalam beberapa kasus, remote access memungkinkan pengguna untuk mengakses dan mengontrol komputer jarak jauh seolah-olah mereka sedang duduk di depannya. Remote access umumnya digunakan oleh para pekerja yang ingin bekerja dari rumah atau tempat lain yang jauh dari kantor mereka, atau oleh administrator sistem yang ingin mengelola server dari lokasi jauh.

SSH adalah salah satu protokol yang digunakan untuk remote access, karena memungkinkan pengguna untuk mengakses komputer jarak jauh dengan aman dan mengirimkan data melalui saluran terenkripsi. Namun, ada juga protokol remote access lainnya seperti RDP (Remote Desktop Protocol) dan VNC (Virtual Network Computing) yang digunakan untuk tujuan yang sama.

Ubuntu merupakan salah satu sistem operasi berbasis Linux yang umum digunakan. Ubuntu memiliki fitur bawaan SSH yang dapat digunakan untuk melakukan remote access ke komputer atau server. Sistem operasi Windows juga mendukung SSH, namun tidak memiliki fitur bawaan seperti pada Ubuntu. Untuk menggunakan SSH pada Windows, pengguna perlu menginstal software seperti PuTTY.

BAB II

Perangkat yang digunakan

Untuk melakukan SSH dan remote access, ada beberapa perangkat yang dapat digunakan, baik dalam bentuk software atau spesifikasi laptop/komputer, antara lain:

- SSH software: ada beberapa SSH software yang dapat digunakan, di antaranya OpenSSH, PuTTY, SecureCRT, dan lain-lain.
- Remote access software: ada beberapa remote access software yang dapat digunakan, seperti TeamViewer, AnyDesk, Remote Desktop Connection, dan lain-lain.
- OS dengan fitur bawaan SSH dan remote access: beberapa sistem operasi seperti Linux, MacOS, dan Windows 10 memiliki fitur bawaan untuk SSH dan remote access. Sebagai contoh, pada Windows 10, pengguna dapat menggunakan fitur Remote Desktop Connection untuk melakukan remote access ke komputer lain.
- Laptop/komputer dengan spesifikasi yang memadai: untuk melakukan remote access dengan lancar, dibutuhkan laptop/komputer dengan spesifikasi yang memadai, seperti CPU yang cukup cepat, RAM yang cukup besar, dan koneksi internet yang stabil.
- Perangkat jaringan: selain perangkat di atas, pengguna juga memerlukan perangkat jaringan yang memadai, seperti router atau switch yang mendukung protokol SSH dan remote access.

Perangkat yang digunakan untuk SSH dan remote access harus dipilih dengan hati-hati agar dapat berfungsi dengan lancar dan aman. Selalu pastikan untuk menginstal perangkat lunak yang terbaru dan memilih perangkat dengan spesifikasi yang memadai.

BAB III

Langkah Pengerjaan

Berikut adalah langkah-langkah untuk melakukan SSH pada Ubuntu :

- Aktifkan SSH server pada komputer Ubuntu dengan menjalankan perintah berikut pada terminal:

```
defa@defa-VirtualBox: ~  
defa@defa-VirtualBox:~$ sudo apt-get install openssh-server
```

- Lalu kita harus mengetahui IP target yang akan kita remote :

```
defa@defaserver:~$ ifconfig  
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 192.168.43.91 netmask 255.255.255.0 broadcast 192.168.43.255  
    inet6 fe80::a00:27ff:fe45:b986 prefixlen 64 scopeid 0x20<link>  
    ether 08:00:27:45:b9:86 txqueuelen 1000 (Ethernet)  
    RX packets 422 bytes 266720 (266.7 KB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 328 bytes 29670 (29.6 KB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

- Setelah SSH server aktif, pengguna dapat melakukan remote access ke komputer Ubuntu dari komputer lain dengan menjalankan perintah berikut pada terminal, Kemudian masukkan password untuk masuk ke dalam komputer Ubuntu tersebut :

```
defa@defa-VirtualBox:~$ ssh 192.168.43.91  
defa@192.168.43.91's password:  
Welcome to Ubuntu 22.04.1 LTS (GNU/Linux 5.15.0-43-generic x86_64)  
  
 * Documentation:  https://help.ubuntu.com  
 * Management:    https://landscape.canonical.com  
 * Support:        https://ubuntu.com/advantage  
  
System information as of Sun Mar  5 07:59:32 AM UTC 2023  
  
System load:  0.0      Processes:            103  
Usage of /:   40.9% of 11.21GB   Users logged in:     1  
Memory usage: 12%      IPv4 address for enp0s3: 192.168.43.91  
Swap usage:   0%  
  
0 updates can be applied immediately.  
  
Last login: Sun Mar  5 07:35:21 2023  
defa@defaserver:~$
```

Berikut adalah langkah-langkah untuk melakukan remote access pada Ubuntu:

- Pastikan Remote Desktop Viewer sudah terinstal pada komputer Ubuntu.

```
defa@defa-VirtualBox: ~  
defa@defa-VirtualBox:~$ sudo apt install xrdp
```

- Aktifkan system XRDP nya

```
defa@defa-VirtualBox:~$ sudo systemctl enable --now xrdp  
sudo] password for defa:  
synchronizing state of xrdp.service with SysV service script with /lib/systemd/  
systemd-sysv-install.  
Executing: /lib/systemd/systemd-sysv-install enable xrdp  
defa@defa-VirtualBox:~$
```

- Mengizinkan port untuk terbuka

```
defa@defa-VirtualBox:~$ sudo ufw allow from any to any port 3389 proto tcp  
Rules updated  
Rules updated (v6)  
defa@defa-VirtualBox:~$
```

- Cek IP yang akan diremote

```
enp0s8: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
inet 192.168.43.141 netmask 255.255.255.0 broadcast 192.168.43.255  
inet6 fe80::b491:abf7:d7c:3603 prefixlen 64 scopeid 0x20<link>  
ether 08:00:27:9b:99:06 txqueuelen 1000 (Ethernet)  
RX packets 69 bytes 7549 (7.5 KB)  
RX errors 0 dropped 0 overruns 0 frame 0  
TX packets 132 bytes 13591 (13.5 KB)  
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

- Membuat user baru

```
defa@defa-VirtualBox:~$ sudo adduser kelompok2  
Adding user `kelompok2' ...  
Adding new group `kelompok2' (1001) ...  
Adding new user `kelompok2' (1001) with group `kelompok2' ...  
Creating home directory `/home/kelompok2' ...  
Copying files from `/etc/skel' ...  
New password:  
BAD PASSWORD: The password contains the user name in some form  
Retype new password:  
passwd: password updated successfully  
Changing the user information for kelompok2  
Enter the new value, or press ENTER for the default  
Full Name []:  
Room Number []:  
Work Phone []:  
Home Phone []:  
Other []:  
Is the information correct? [Y/n] y
```

- Memberikan izin pada user yang telah dibuat

```

defa@defa-VirtualBox: ~
GNU nano 6.2 /etc/sudoers.tmp
#Defaults:%sudo env_keep += "SSH_AGENT_PID SSH_AUTH_SOCK"

# Ditto for GPG agent
#Defaults:%sudo env_keep += "GPG_AGENT_INFO"

# Host alias specification

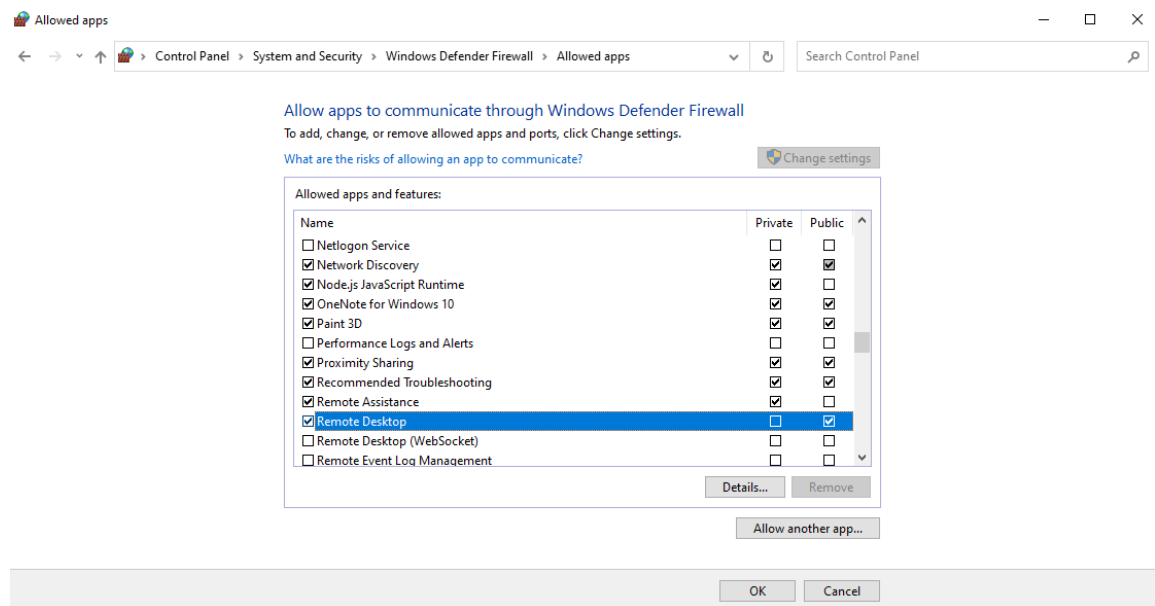
# User alias specification

# Cmnd alias specification

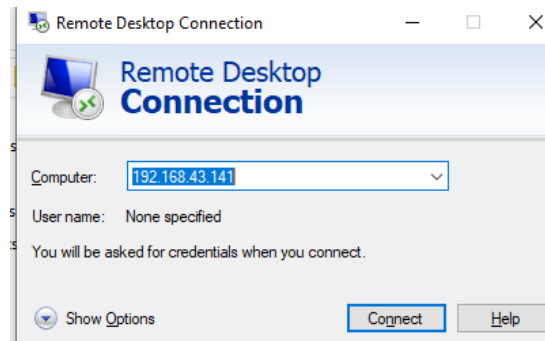
# User privilege specification
root    ALL=(ALL:ALL) ALL
defa    ALL=(ALL:ALL) ALL
kelompok2 ALL=(ALL:ALL) ALL
# Members of the admin group may gain root privileges

```

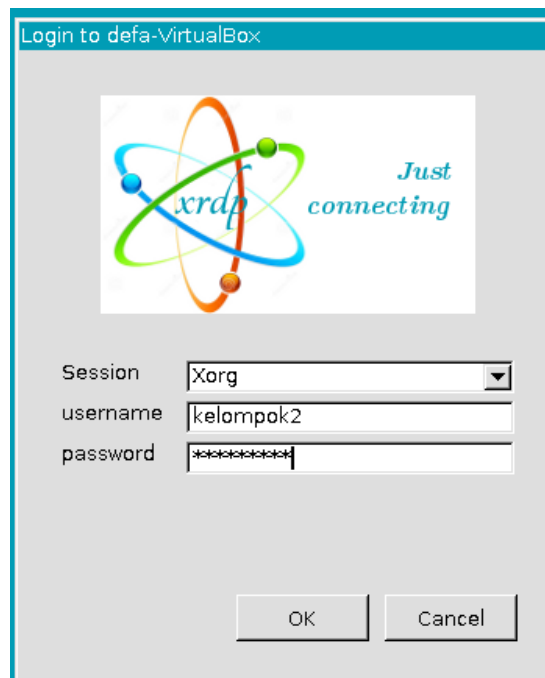
- Mengizinkan firewall agar dapat melakukan remote desktop



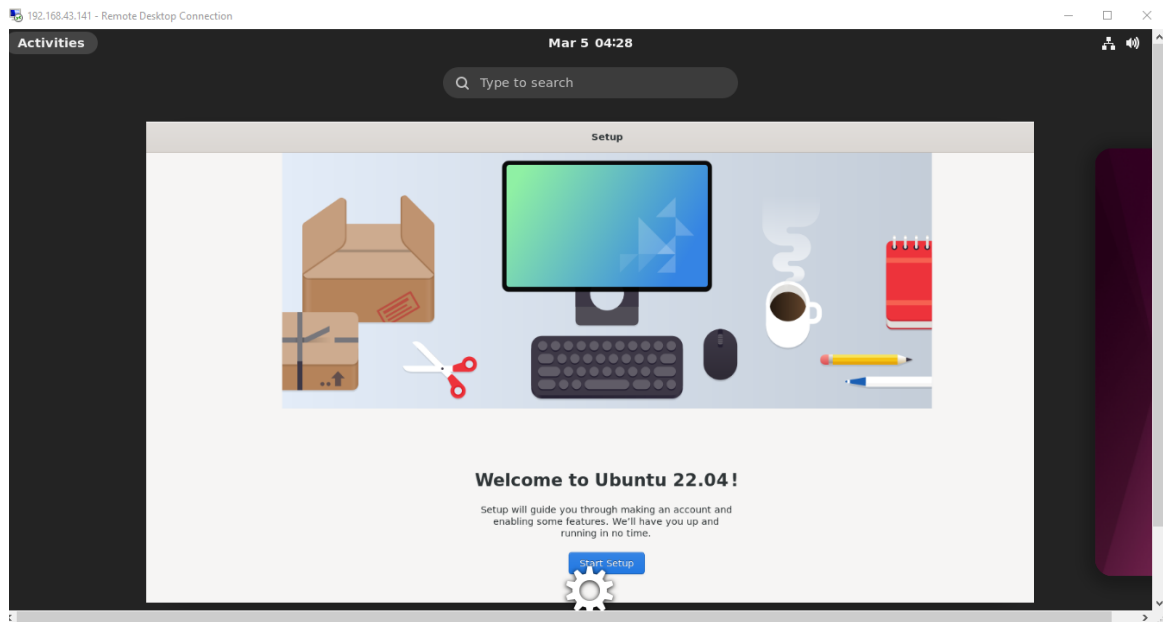
- Buka aplikasi Remote Desktop Viewer dan Masukkan alamat IP komputer tujuan yang ingin diakses.



- Masukkan username dan password untuk masuk ke dalam komputer tersebut.



- Klik ok

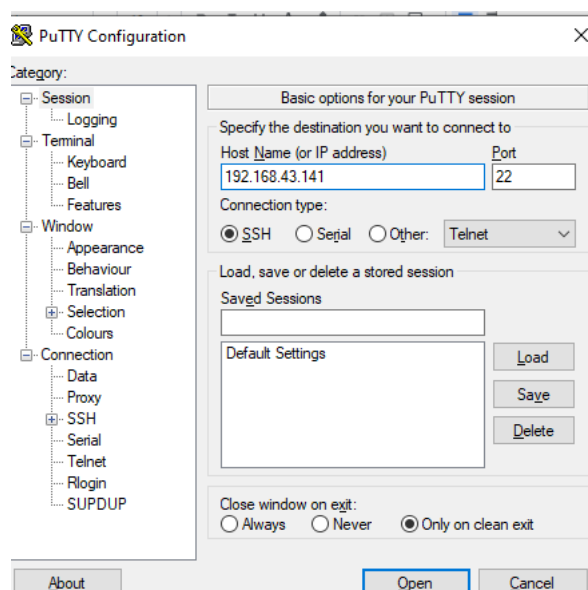


Berikut adalah langkah-langkah untuk melakukan SSH pada Windows:

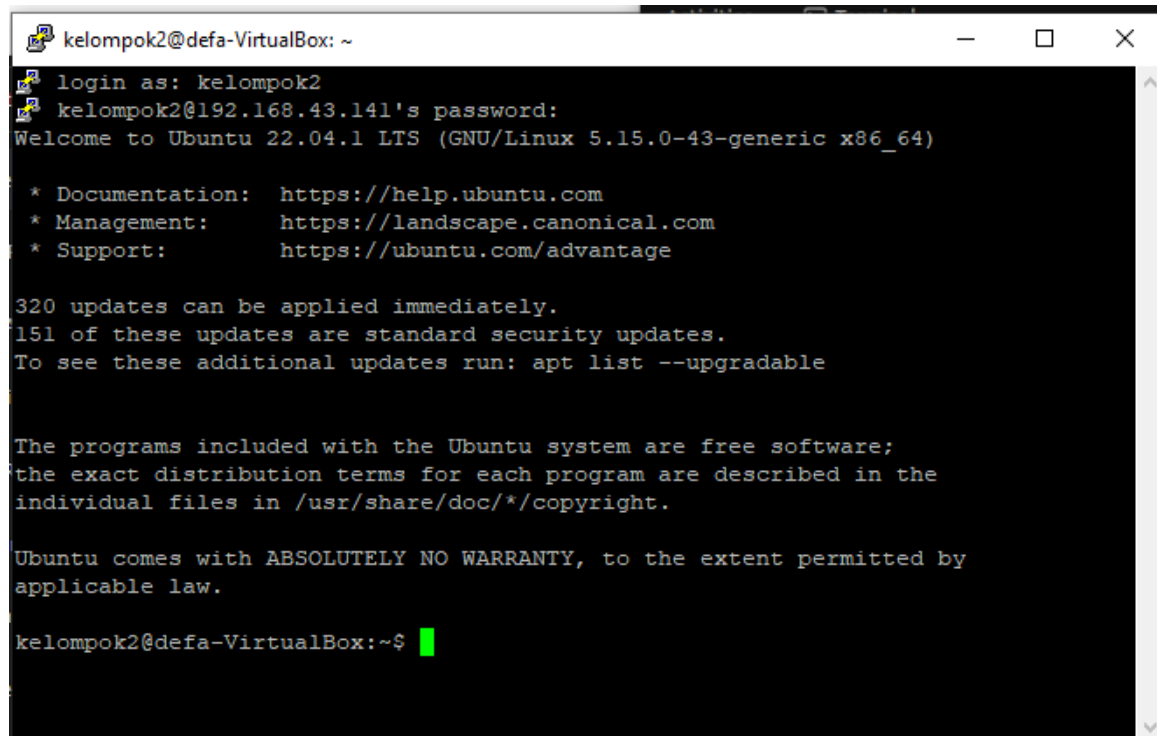
- Mengetahui ip yang target

```
enp0s8: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.43.141 netmask 255.255.255.0 broadcast 192.168.43.255
    inet6 fe80::b491:abf7:d7c:3603 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:9b:99:06 txqueuelen 1000 (Ethernet)
    RX packets 69 bytes 7549 (7.5 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 132 bytes 13591 (13.5 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

- Memasukkan ip ke dalam putty



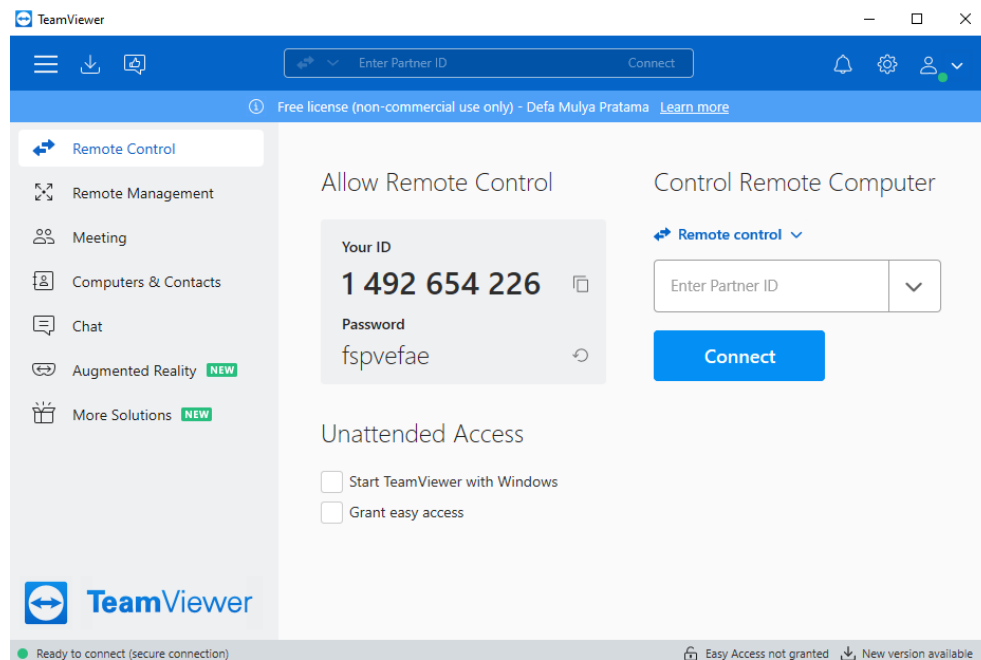
- klik Open dan masukkan username serta password nya



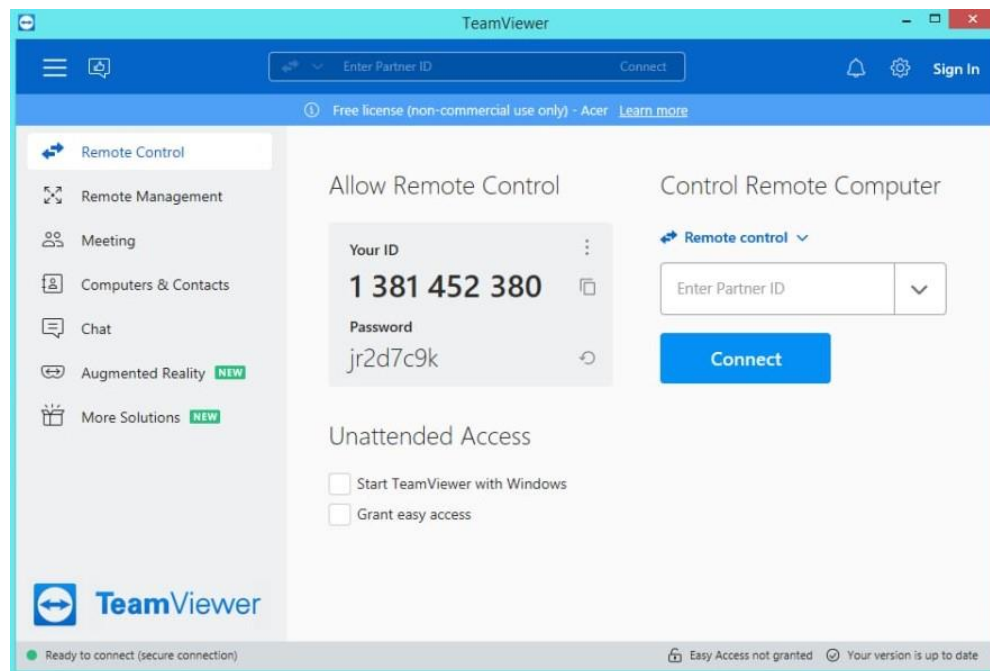
```
kelompok2@defa-VirtualBox: ~  
login as: kelompok2  
kelompok2@192.168.43.141's password:  
Welcome to Ubuntu 22.04.1 LTS (GNU/Linux 5.15.0-43-generic x86_64)  
  
* Documentation:  https://help.ubuntu.com  
* Management:    https://landscape.canonical.com  
* Support:        https://ubuntu.com/advantage  
  
320 updates can be applied immediately.  
151 of these updates are standard security updates.  
To see these additional updates run: apt list --upgradable  
  
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.  
  
kelompok2@defa-VirtualBox:~$
```

Berikut adalah langkah-langkah untuk melakukan remote access pada Windows:

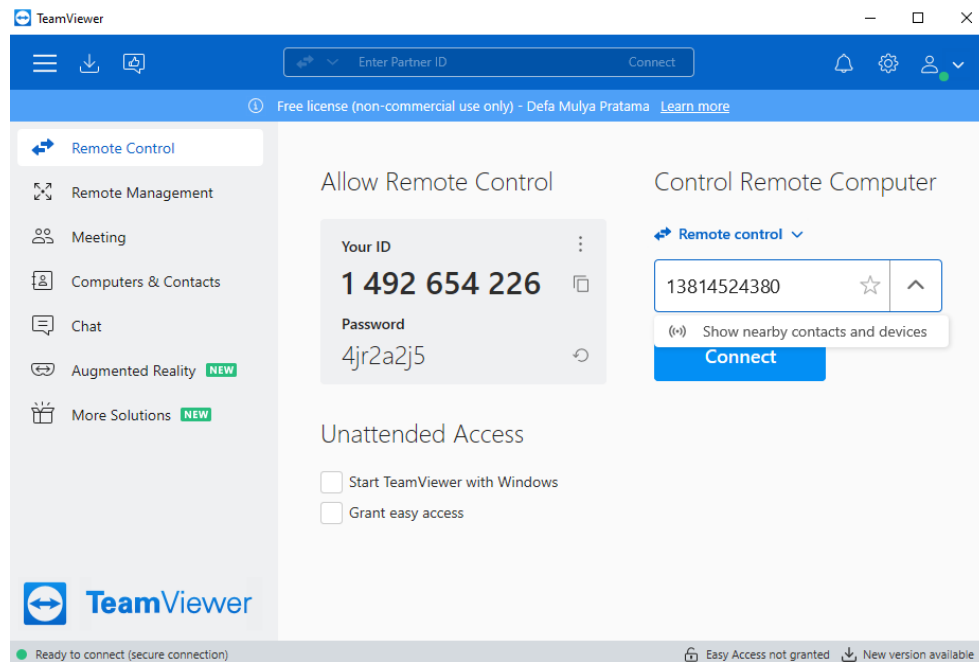
- Buka TeamViewer



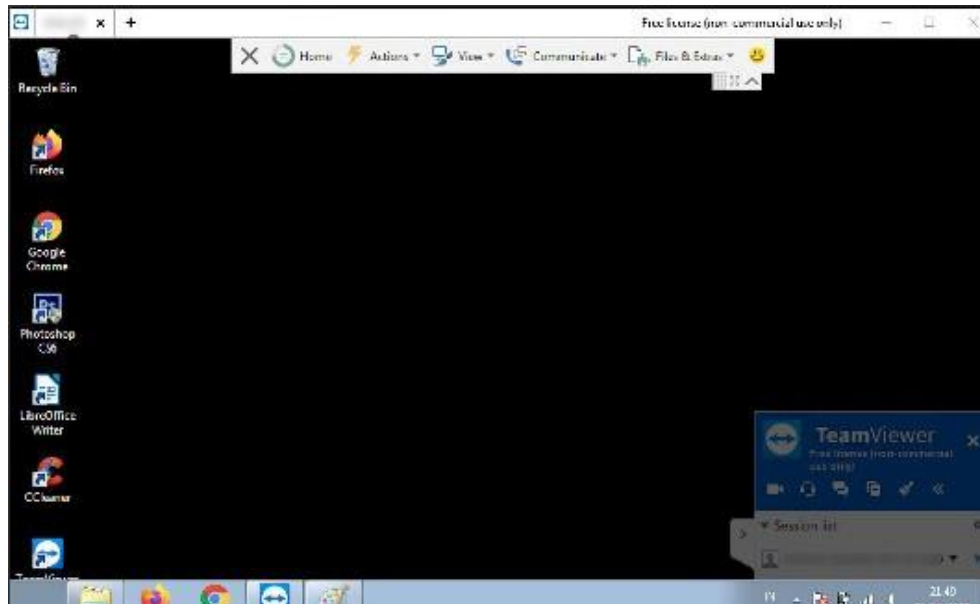
- Masukkan id yang akan di remote lalu klik connect



- Masukkan password target yang akan di remote



- klik remote



Catatan: Langkah-langkah di atas adalah langkah umum dan mungkin dapat berbeda tergantung pada jenis software atau sistem operasi yang digunakan. Selain itu, sebelum melakukan SSH atau remote access, pastikan untuk meminta izin dan akses yang sesuai dari administrator sistem atau pemilik komputer/server yang ingin diakses.

BAB IV

Kesimpulan

Melakukan SSH dan Remote Access dapat memberikan berbagai manfaat, antara lain:

- Akses jarak jauh: Dengan melakukan SSH dan remote access, pengguna dapat mengakses dan mengontrol komputer jarak jauh dengan mudah dan cepat, bahkan dari tempat yang berbeda.
- Kolaborasi: SSH dan remote access juga memungkinkan pengguna untuk berkolaborasi dengan tim atau rekan kerja di lokasi yang berbeda, sehingga memudahkan dalam mengelola proyek dan pekerjaan.
- Efisiensi: Dengan melakukan remote access, pengguna dapat mengakses komputer atau server jarak jauh tanpa harus pergi ke lokasi fisik, sehingga dapat menghemat waktu dan biaya transportasi.

Namun, penting untuk diingat bahwa pengguna harus berhati-hati dalam menggunakan SSH dan remote access, karena jika tidak digunakan dengan benar dapat membahayakan keamanan sistem dan data yang dikirimkan. Pastikan untuk selalu menggunakan protokol yang aman, seperti protokol enkripsi yang kuat, dan selalu meminta izin dan akses yang sesuai dari administrator sistem atau pemilik komputer/server yang ingin diakses.