

Warmup:

bit.ly/LinuxBasicRvw



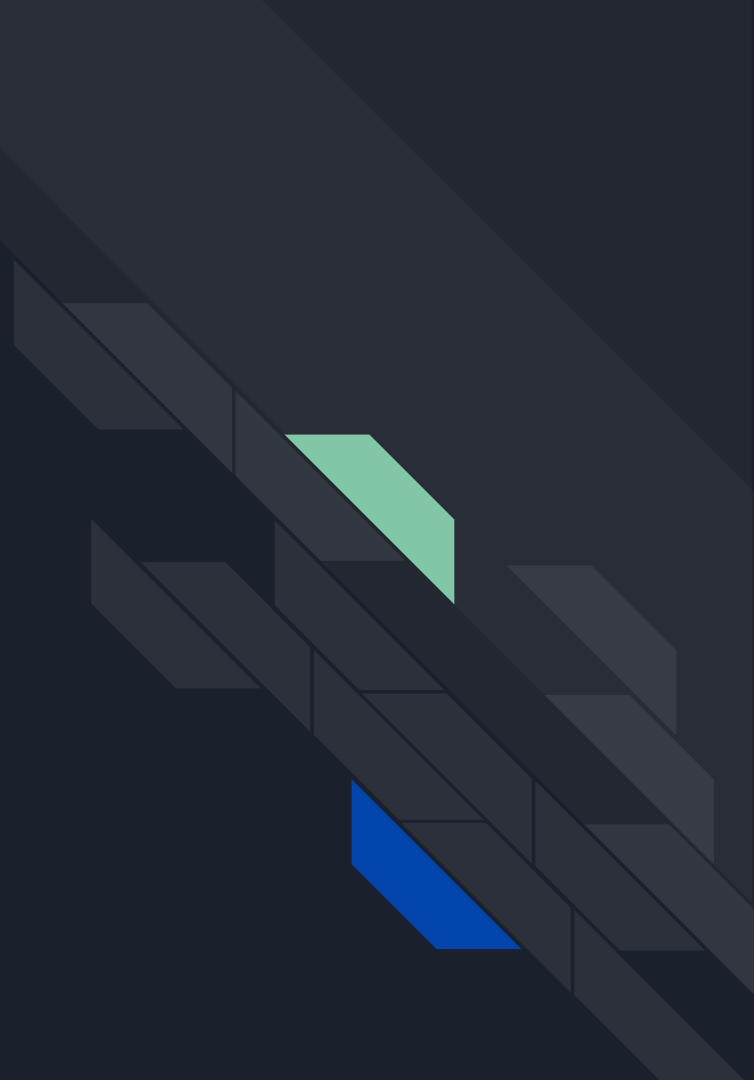


how 2 ssh for dummies

specifically you, dummy
linux baseq

WARNING

This is the first service we are configuring. Pay careful attention because lots of these concepts can be transferred to other services we'll be configuring later.



Q: What is SSH?



A: You say it when
people are being too
loud





SSH

SSH: Secure **S**hell

You get a secure, remote terminal connection to another person

What does that really mean though?

Basically...

Let's hack each other!!!





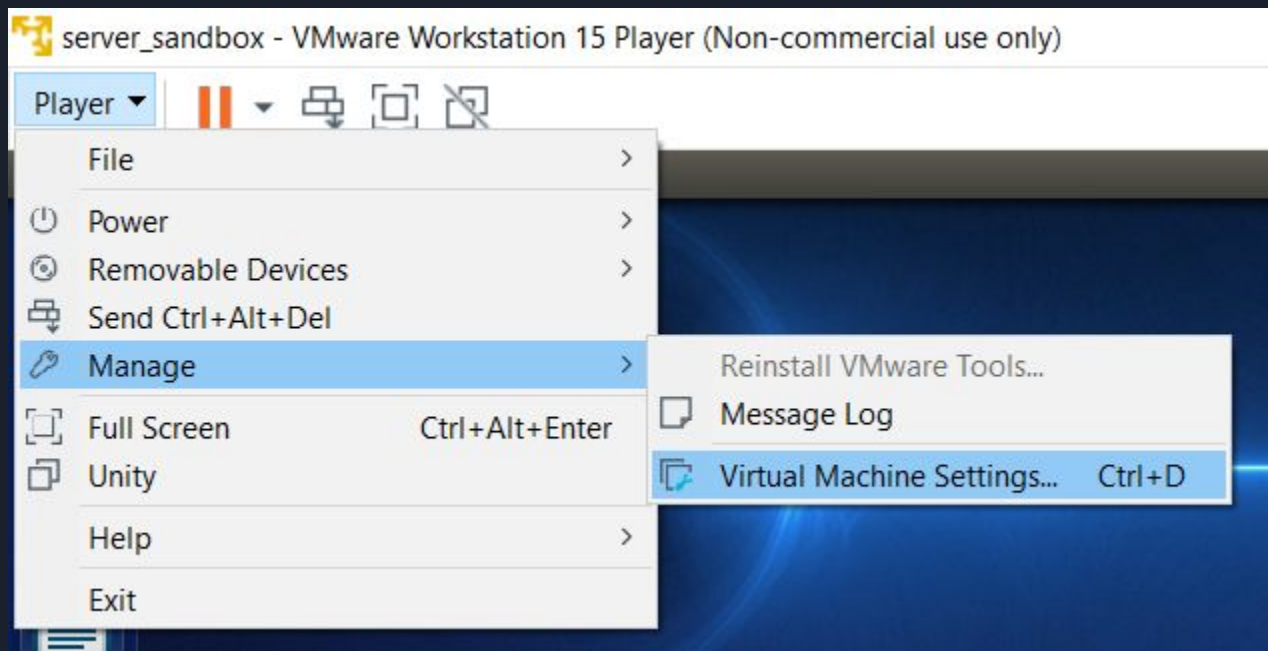
might so download these

```
apt-get install openssh-server
```

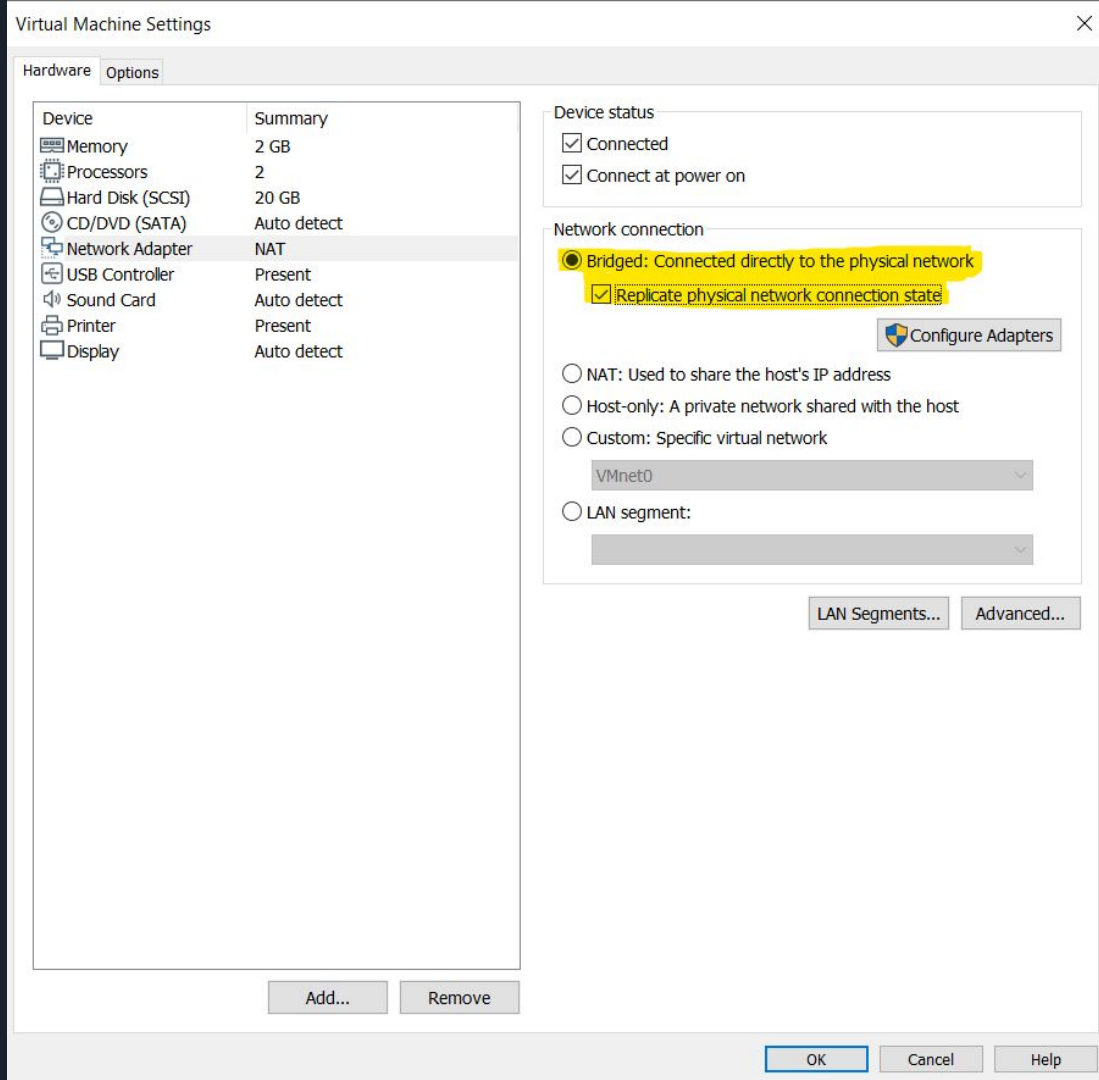
```
apt-get install openssh-client
```

The first one is the server and the second one is the client.

and partner up and do this



and this





Okay, so what did we just do?

Setting the bridged connection allows us to remotely connect to other people's VMs. If we didn't set it, you wouldn't be able to connect to anyone besides your local computer :(

openssh-server allows people to connect to you

openssh-client allows you to connect to other people

partnering up made you come to terms with the fact that you have no friends :'(



person getting hacked:

ifconfig

i blurred mine out bc i dont want you hacking me :)

let's just pretend it's 8.8.8.8

```
serveruser@ubuntu:~$ ifconfig
ens33      Link encap:Ethernet  HWaddr [REDACTED]
           inet addr: [REDACTED] Bcast: [REDACTED] Mask: [REDACTED]
           Scope:Link
           UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
           RX packets:11298 errors:0 dropped:0 overruns:0 frame:0
           TX packets:5471 errors:0 dropped:0 overruns:0 carrier:0
           collisions:0 txqueuelen:1000
           RX bytes:14755237 (14.7 MB)  TX bytes:356630 (356.6 KB)
```

person hacking:

ssh user@ipaddress

eg: ssh serveruser@172.31.12.27

are you impressed?

no?

it looks the same?

have the person not connected through ssh close their terminal

Me: *logs into server*

Server: There were 103840 failed login attempts since last successful login.

Me:





here's the spooky part


```
cd ~/Desktop
```

```
touch file
```

it showed up on their desktop o_O

Now restart their computer lmao





Cool, so now we know how it works, but how secure?

start editing fam

All configurations are stored
in one file

/etc/ssh/sshd_config

```
serveruser@ubuntu: /etc/ssh
GNU nano 2.5.3      File: sshd_config

# Package generated configuration file
# See the sshd_config(5) manpage for details

# What ports, IPs and protocols we listen for
Port 22
# Use these options to restrict which interfaces/protocols sshd will bind to
#ListenAddress ::
#ListenAddress 0.0.0.0
Protocol 2
# HostKeys for protocol version 2
HostKey /etc/ssh/ssh_host_rsa_key
HostKey /etc/ssh/ssh_host_dsa_key
HostKey /etc/ssh/ssh_host_ecdsa_key
HostKey /etc/ssh/ssh_host_ed25519_key
#Privilege Separation is turned on for security
UsePrivilegeSeparation yes

# Lifetime and size of ephemeral version 1 server key
KeyRegenerationInterval 3600
ServerKeyBits 1024

# Logging
SyslogFacility AUTH
LogLevel INFO

# Authentication:
[ Read 88 lines (Warning: No write permission) ]
^G Get Help  ^O Write Out  ^W Where Is  ^K Cut Text  ^J Justify  ^C Cur Pos
^X Exit      ^R Read File  ^\ Replace   ^U Uncut Text ^T To Spell  ^_ Go To Line
```


Configs - General

You MAY want to change it from Port 22 to a different port
probably don't though

Make sure that you're using Protocol 2

Protocol 1 is very bad

```
# What ports, IPs and protocols we listen for
Port 22
# Use these options to restrict which interfaces/protocols sshd will bind to
#ListenAddress ::
#ListenAddress 0.0.0.0
Protocol 2
```





Configs - Passwords/Login

```
# To enable empty passwords, change to yes (NOT RECOMMENDED)
PermitEmptyPasswords no
```

Don't let them enter empty passwords
That's silly

```
# Authentication:
LoginGraceTime 120
PermitRootLogin no
StrictModes yes
```

Don't let them log in as root
That's also silly

Avoiding getting hacked

```
RSAAuthentication yes
PubkeyAuthentication yes
#AuthorizedKeysFile      %h/.ssh/authorized_keys
# similar for protocol version 2
HostbasedAuthentication no
# Change to no to disable tunnelled clear text passwords
PasswordAuthentication no
```

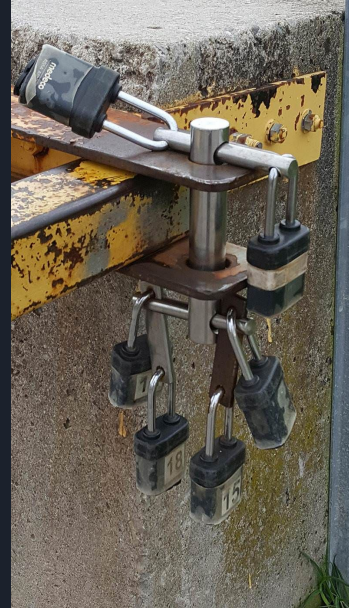
ssh is secure because it can use pubkey encryption

It can authenticate and encrypt messages using pre-generated keys on other machines

This way, only certain machines with the correct keys can connect to you, instead of anyone that knows the password

We don't want people being able to log in with the password because that's another weakpoint

Generating/setting up keys is beyond the scope of this lesson, figure it out yourself if you want to lmao





Minor Stuff

```
X11Forwarding no
X11DisplayOffset 10
PrintMotd no
PrintLastLog yes
TCPKeepAlive yes
#UseLogin no
#MaxStartups 10:30:60
Banner /etc/issue.net
```

These are pretty minor but still a generally good to edit

Mostly X11Forwarding and PrintMotd

Disabling X11Forwarding means they can't get your GUI info

vv example motd vv

```
This network device is for authorized use only. Unauthorized or improper use
of this system may result in you hearing very bad music. If you do not consent
to these terms, LOG OFF IMMEDIATELY.
```

```
Ha, only joking. Now you have logged in feel free to change your root password
using the 'passwd' command. You can safely modify any of the files on this
system. A factory reset (press and hold add on power on) will remove all your
modifications and revert to the installed firmware.
```

```
Enjoy!
```

```
#
```

There's like a billion more things we don't have time to show you, like white/blacklists and chroot jailing

Make sure to do your own research too!

Also restart ssh after you make changes thx

`sudo service sshd restart`

Checklist+prep for practice round

- pick day and time WITH YOUR TEAM (duh 4head)
- what to do
- when to do it
- organize your notes
- figure out seat assignments (you should have a row for 5 peoples so plan for that)
- REsEarch?
- how to restart if your system has gone to toilet land
 - ask these questions:
 - do you know how you got your points?
 - do you have time to get the points?
 - does your team agree?
 - suspend
 - delete that folder
 - empty recycling bin
 - re-extract
 - start again!

