

3.4.2.8

“no matter where you are, everyone is always connected”

11B

SSH with Beginner Config

Recall

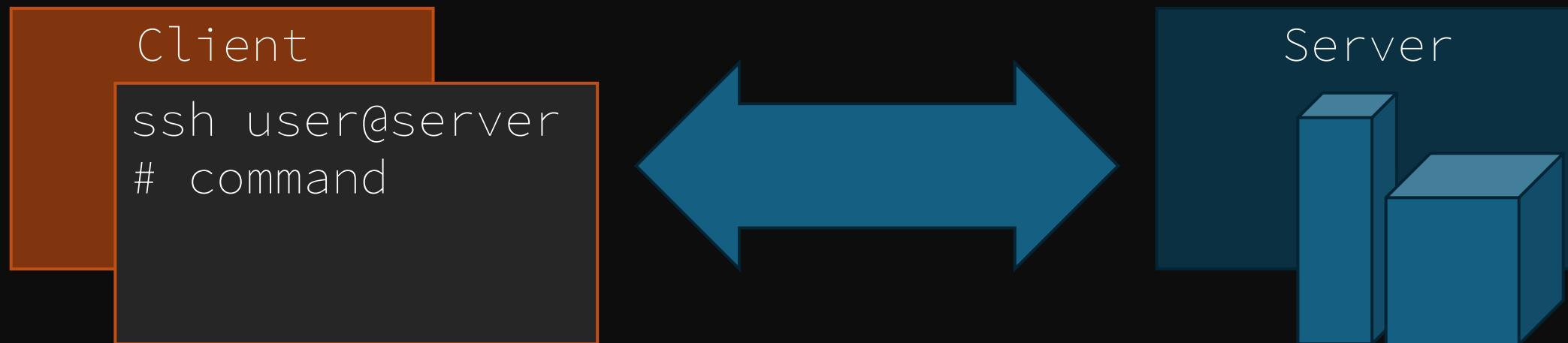
- In Round 1, `sshd` was considered a critical service.
- One of the possible points was:
 - 18 SSH root login has been disabled

What is SSH?

How can we secure it?

What is SSH?

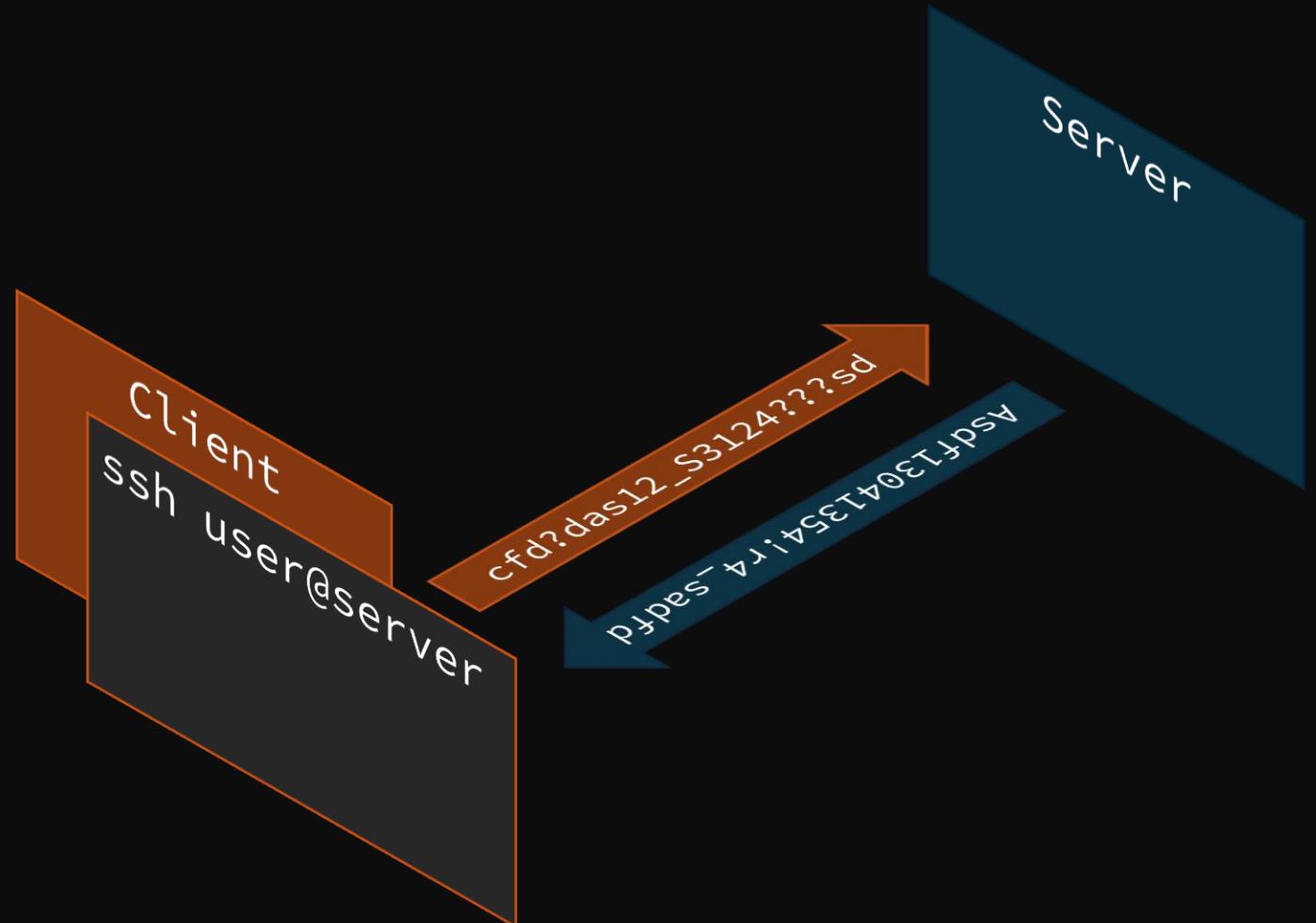
SSH stands for Secure Shell. It is a service that lets us connect to another computer's terminal remotely.



How So?

SSH uses encryption to ensure that anything sent between systems cannot be easily seen across the network or Internet.

When a user connects to a server using SSH, encryption is set up upon connection.



Connecting via SSH

in terminal

```
# ssh sebastian@10.0.0.1  
    user to      server  
    log in as    address
```

sebastian@10.0.0.1's password:

.
. .

Connection to 10.0.0.1 closed.

One can install an SSH client to be able to connect to a server via SSH.

In Linux, you can begin an SSH session by running the SSH command.

Try It

Log in via ssh to sebastian@10.4.2.32

The password is tR@!n!Ng1234

Find the README file. What does the README say?

The SSH Server

sshd is the SSH Daemon. This is the program that runs an SSH server and accepts remote connections.

This is the program that you will be configuring. We will now look at some secure configuration values for *sshd*.

Configuration

in file `/etc/ssh/sshd_config`

Protocol 2

Port 22

PermitRootLogin no

UsePAM Yes

MaxAuthTries 2

MaxSessions 2

UseDNS no

Banner none

StrictModes yes

X11Forwarding no

X11DisplayOffset 10

Find, replace, or add
the following lines
in

`/etc/ssh/sshd_config`

Configuration

in file `/etc/ssh/sshd_config`

```
ClientAliveCountMax 0
ClientAliveInterval 300
PrintMotd no
Compression no
LoginGraceTime 30
PrintLastLog no
LogLevel INFO
TCPKeepAlive no
```

Find, replace, or add
the following lines
in

`/etc/ssh/sshd_config`

Test Your Configuration

in terminal

```
# sshd -T
```

The following command checks to see if your configuration is valid. If it is invalid, *sshd* will not run properly (and may lose you points)