CREST CRT AMI

- AWS Configuration
- Connecting to the machine
  - Windows Terminal
  - PuTTY
  - VNC From Windows
  - Kali

AWS Configuration

If you do not already have an AWS account, you can create one by heading over to:
https://aws.amazon.com/account/sign-up

Open EC2 in Region: London (eu-west-2) https://eu-west-2.console.aws.amazon.com/ec2/home?region=eu-west-2

Launch instance

Launch instance

To get started, launch an Amazon EC2 instance, which is a virtual server in the cloud.

Launch instance ▼ | **Migrate a server** ↗

Note: Your instances will launch in the Europe (London) Region

Name your instance

Name and tags Info

Name

CRT Candidate

Add additional tags

Search for CREST CRT in Application and OS Images (Amazon Machine Image) search box

Select community amis

Community AMIs (1)

Published by anyone

Make sure the details match the details below

```
Owner: 126620636130
Publish date: 2023-11-07
```

and press select

Use instance type t2.micro if you are free tier eligible to host the machine for free

Create your keypair and give it a meanigful name

▼ **Key pair (login)** Info

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - *required*

| CREST CRT 1 | ▼ |

↻ Create new key pair

Create the ssh rule to allow ssh traffic from your IP

Firewall (security groups) Info
A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

| ● Create security group | ○ Select existing security group |

We'll create a new security group called '**launch-wizard-1**' with the following rules:

☑ Allow SSH traffic from
Helps you connect to your instance

| Anywhere 0.0.0.0/0 | ▲ |

Anywhere ✓
0.0.0.0/0

☐ Allow HTTPS traffic from the interne
To set up an endpoint, for example when ‹ 0.0.0.0/0

Custom

☐ Allow HTTP traffic from the internet
To set up an endpoint, for example when ‹ My IP

█████████ /32

⚠ Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting   ✕
security group rules to allow access from known IP addresses only.

Configure the storage (Storage has to be at least 50gb)

▼ **Configure storage** Info   Advanced

1x | 50 | GiB | gp2 | ▼ | Root volume (Not encrypted)

ⓘ Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage   ✕

| Add new volume |

0 x File systems   Edit

Launch the instance once the above steps are complete

Connecting to the machine

Windows Terminal

Open CMD on your machine and type in:

```
ssh -L 5901:127.0.0.1:5901 -C -N -l kali <your-server-ip>
```


password: kali

Once you have successfully connected, it **won't** give a connection succeeded message

Connect via VNC

PuTTY

Open the PuTTY gui

Type the server ip in `Host Name`
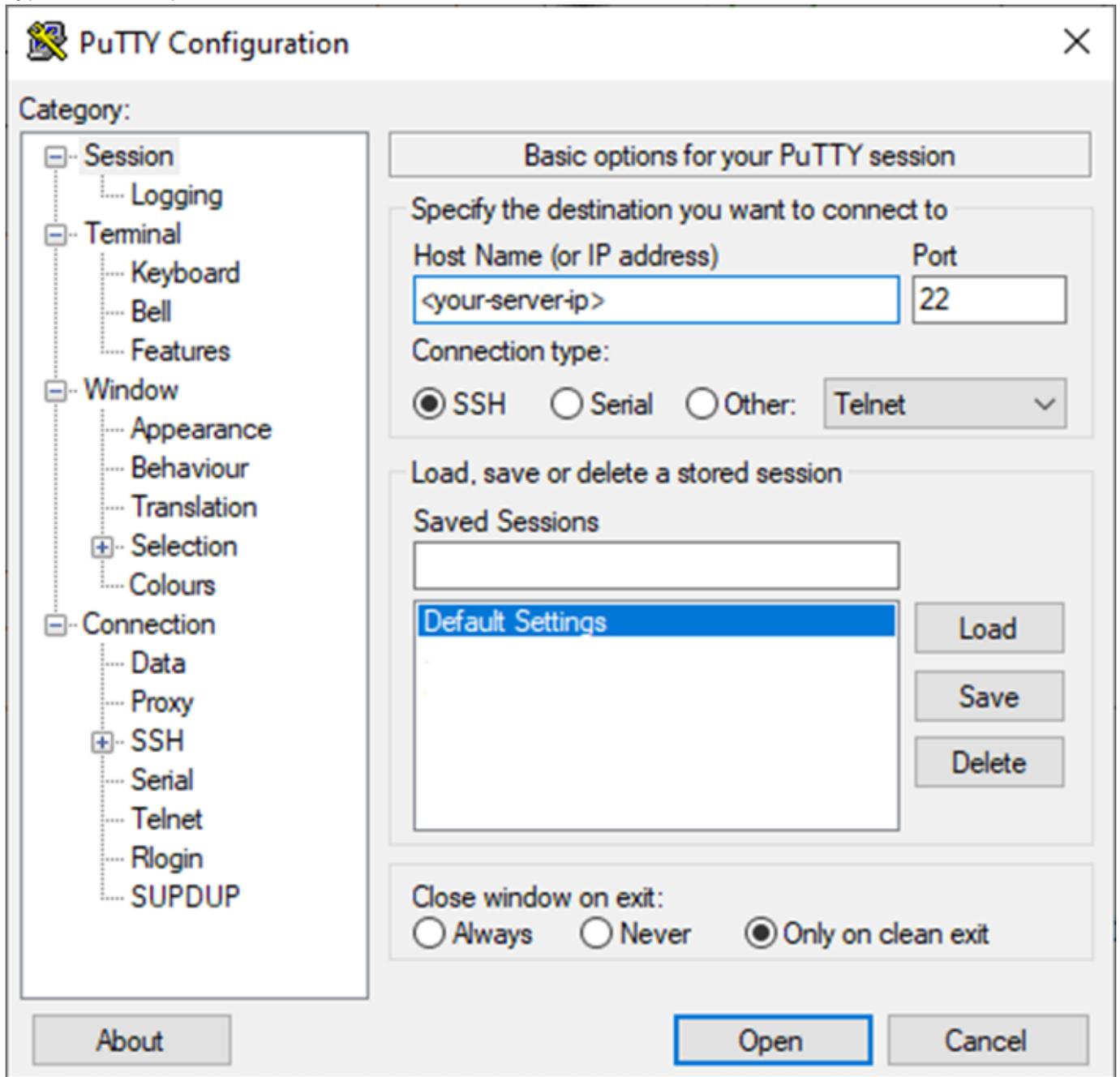
In the `Category` side tab, go to:

```
Connections > SSH > Tunnels
```

Fill in these details:
Source Port: `5901`

Destination: `127.0.0.1:5901`
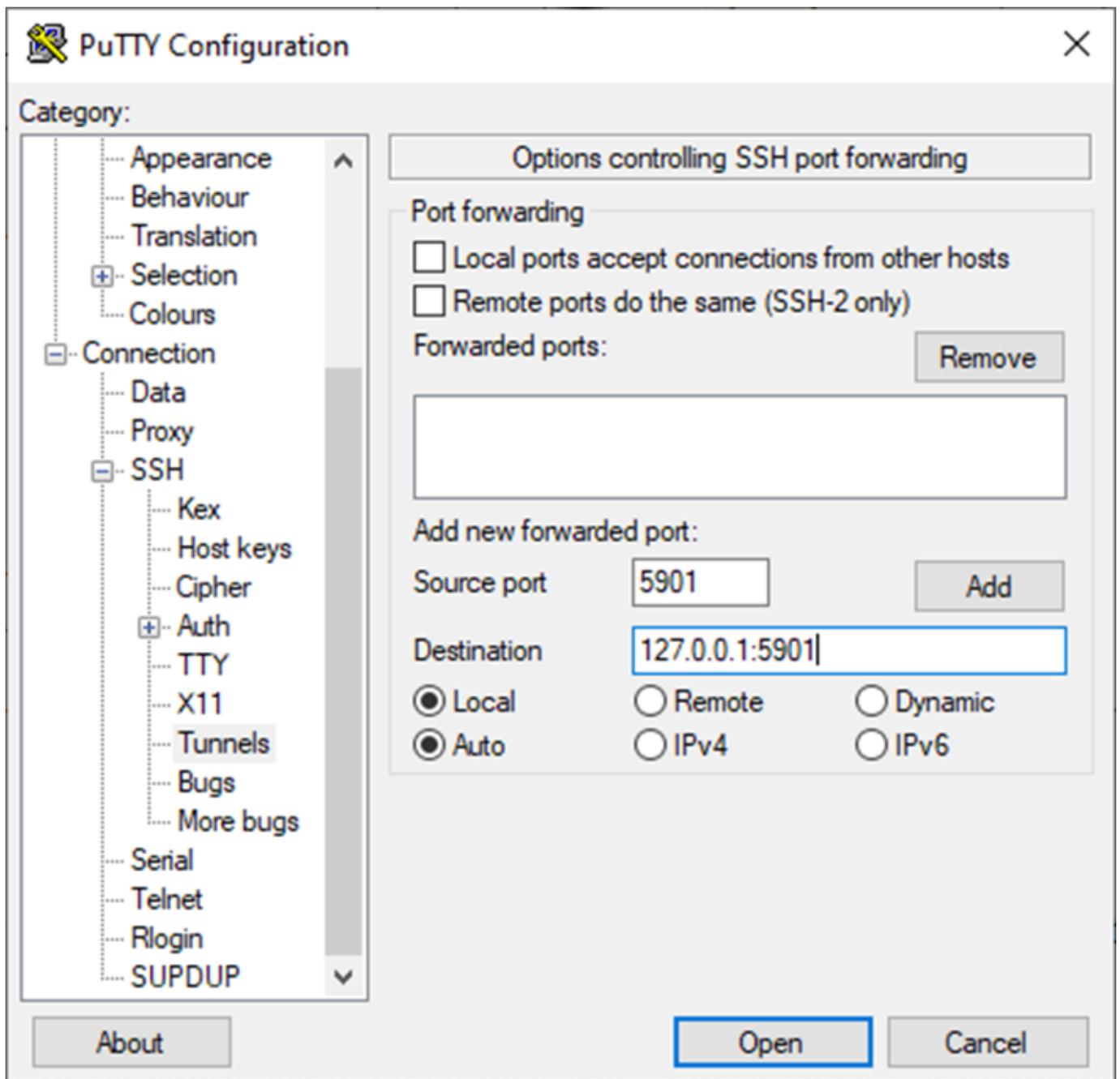
This step is **optional**

If you want to save this configuration, head back to the `Session` category, type in a name in `Saved Sessions`

and press Save
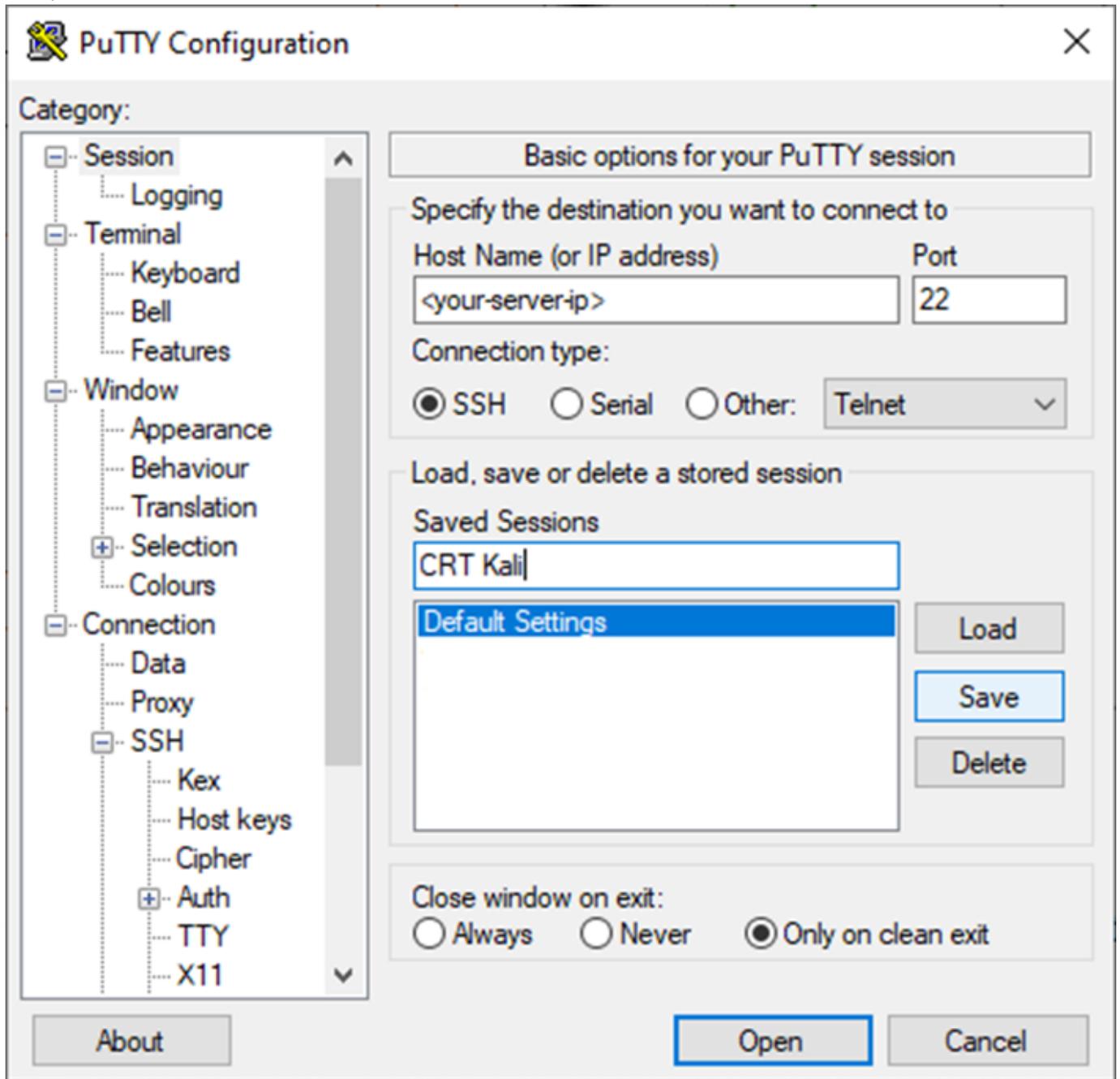
Press Open
username: kali

password: kali
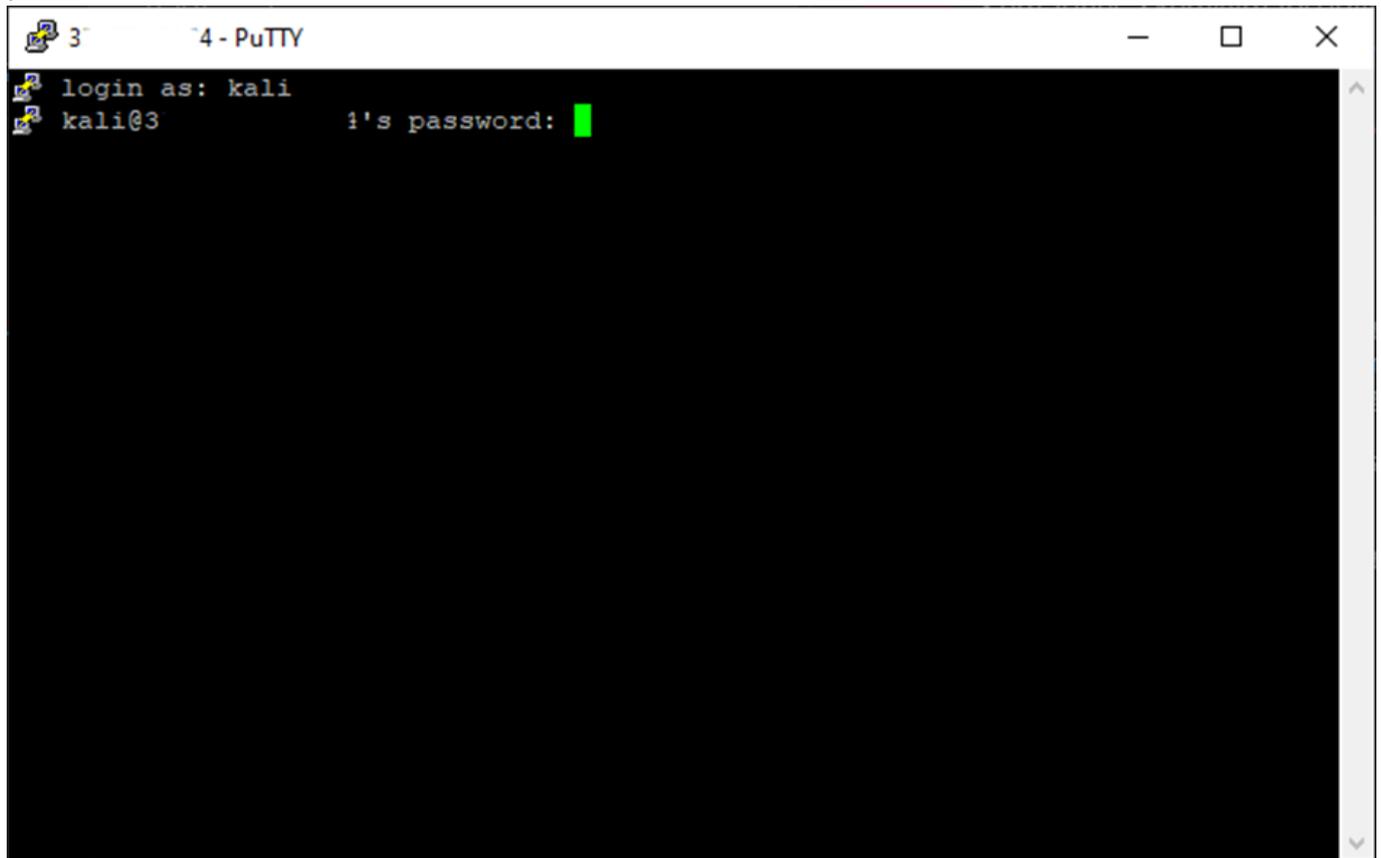
Once you have logged in successfully, the terminal should look like this:
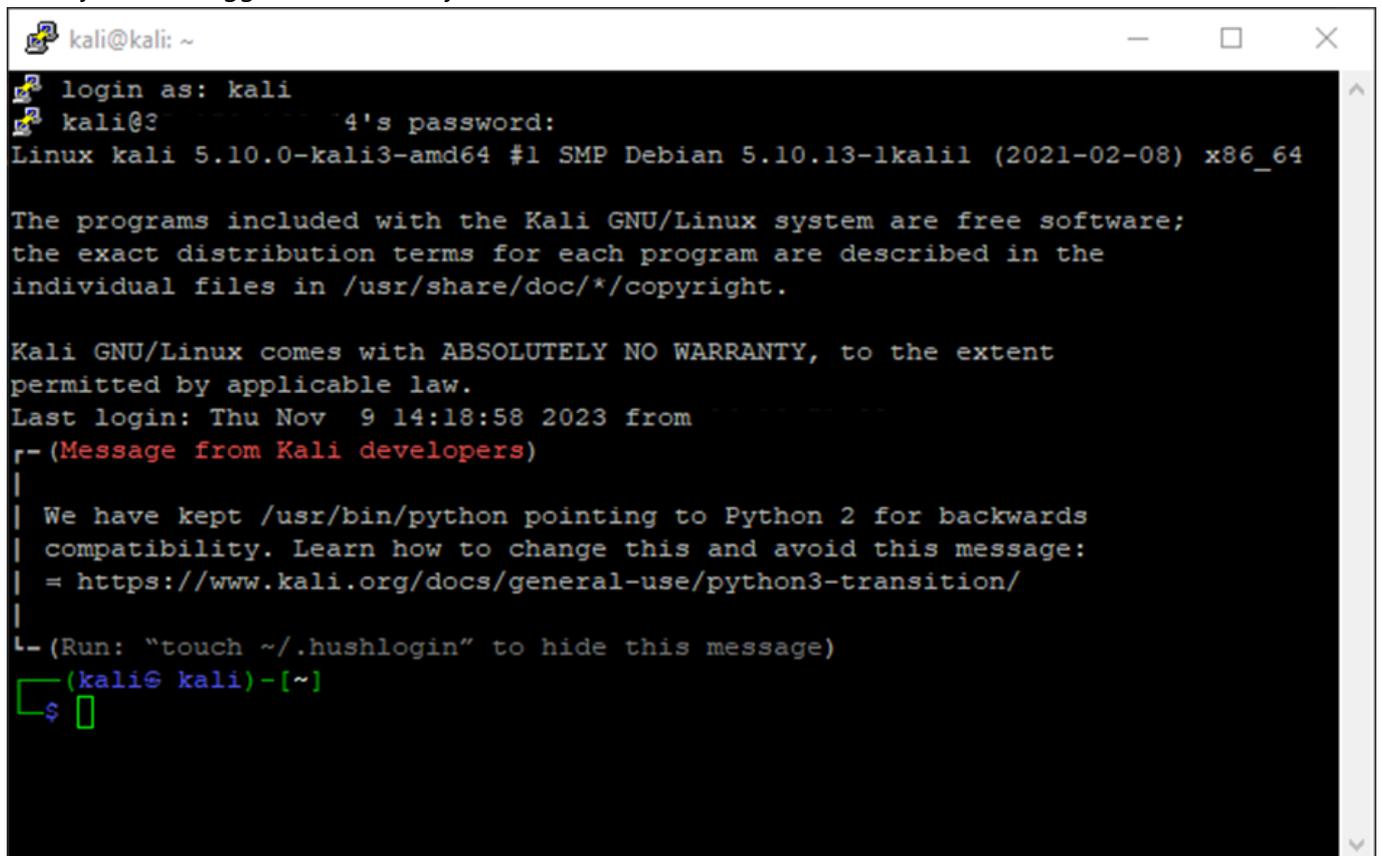
Connect via VNC

VNC From Windows

Open VNC Software (TightVNC) and connect using Remote Host: 127.0.0.1:5901
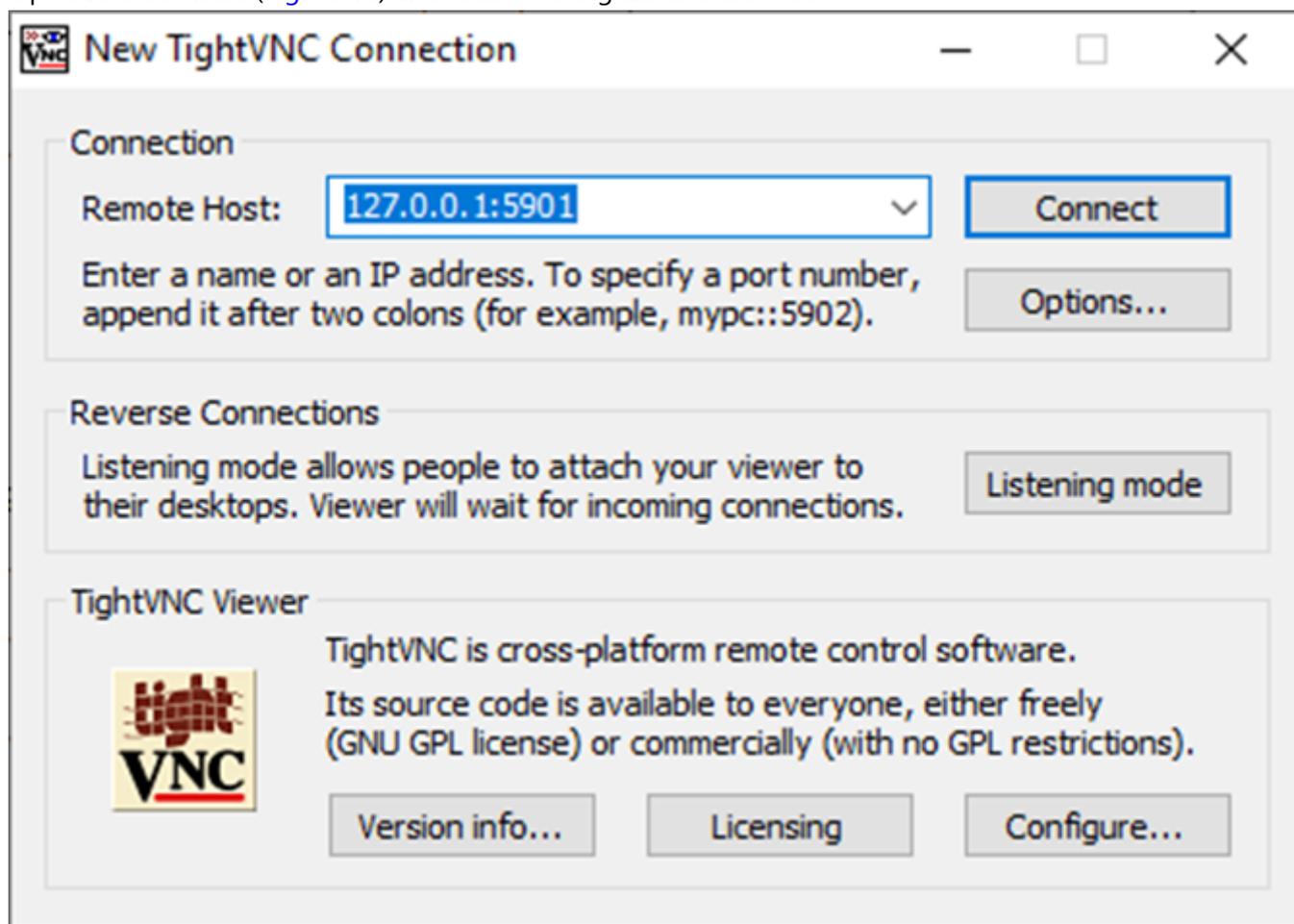
password: kali1234

Once you have connected succesfully it will look like this:
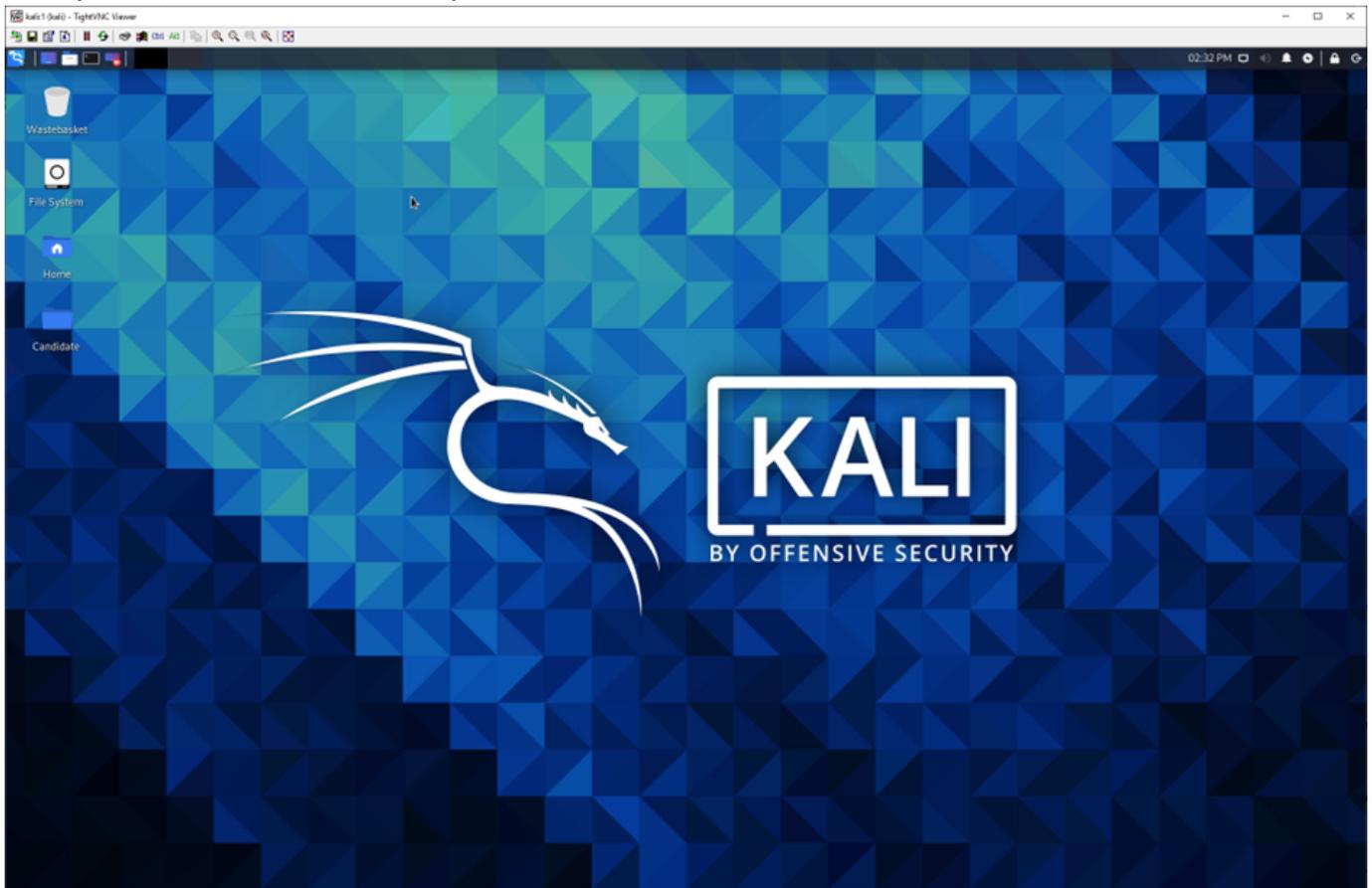
Kali

Open the terminal (CTRL+ALT+T) and type in

```
ssh -L 5901:127.0.0.1:5901 -C -N -l kali <your-server-ip>
```

password: kali

Once you have successfully connected, it **won't** give a connection succeeded message
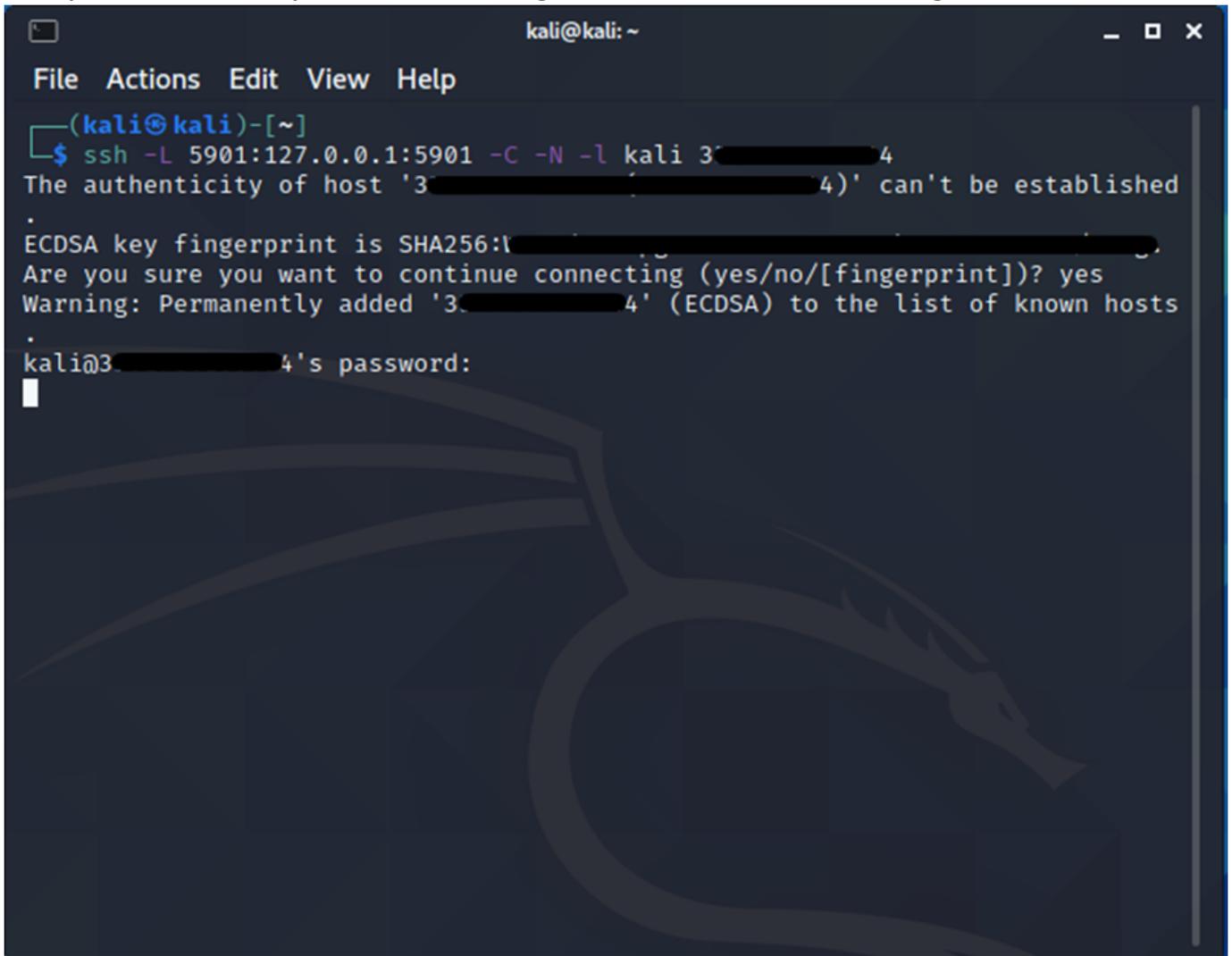
Open Remmina (built in RDP/VNC software)

Select VNC as the connection type
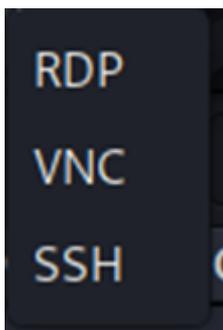
Connect to: 127.0.0.1:5901
password: kali1234
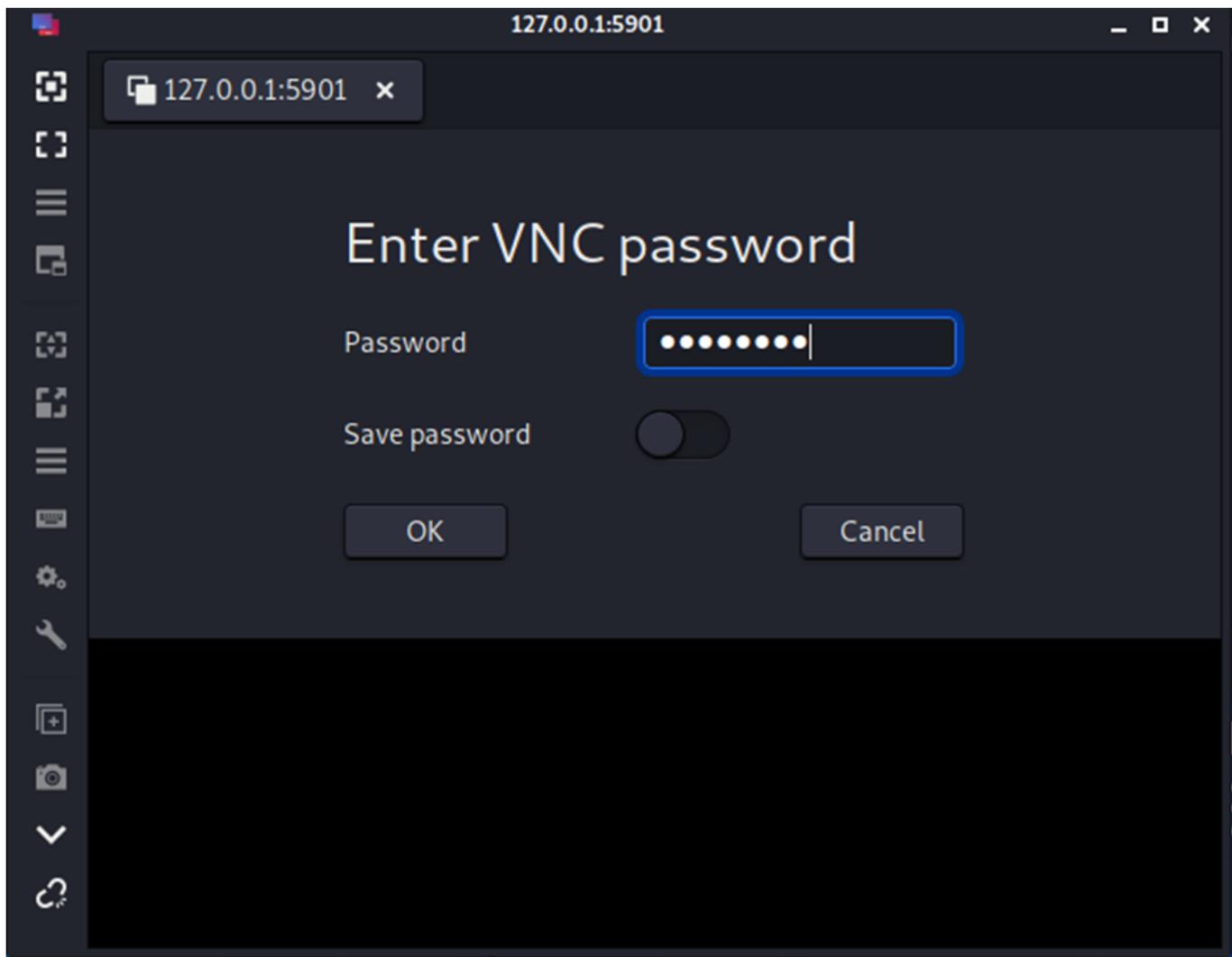
Once you have succesfully connected it will look like this: