RDP Through SSH Tunnel

Author: Chris Morales

Summary: Having a direct route from the outside world into the private subnet is not a good idea unless you have top-tier security. One way to encourage this is through an SSH tunnel.

Procedure

Below is the procedure for creating an SSH tunnel that will be used for RDP connections.

Prior Information

You want to have the following information prior to deploying this:

1. Target IP (typically private) of the target Windows machine.
2. RDP port of the Windows machine (3389 by default).
3. Machine that you're going to use as a stepping stone to the Windows machine (one that has a route to it). You can make an alias (in a config file under your .ssh directory) or a direct user@IP connection.

Format of the command

This command will have to run on your local Windows machine that you will be trying to RDP into the remote server into.

```
    ssh -L <source port>:<dest IP>:<dest Port> -f -N <Intermediate Alias or
user@IP>
```

To explain the flags:

- -L: Start a listener on some interface and some port (by default, it's going to be localhost)
- -f: Run this process in the background.
- -N: You don't need to execute any commands on this SSH session.

Sample

For example, if we have the following information:

1. Client desired port: 9000
2. Target Windows Machine IP: X.X.X.X
3. Target Windows RDP Port: 3389
4. Intermediate User: test
5. Intermediate IP: Y.Y.Y.Y

The format of the command can be:

```
ssh -L 9000:X.X.X.X:3389 -f -N test@Y.Y.Y.Y
```

If I have an alias (ALIAS), then I can just update the command.

```
ssh -L 9000:X.X.X.X:3389 -f -N ALIAS
```

Next, all you need to do is simply open up RDC and then use localhost:9000 as the address.