SSH Pivoting with sshuttle

w1j0y

SSH Pivoting with Sshuttle

Sshuttle is another tool written in Python which removes the need to configure proxychains. However, this tool only works for pivoting over SSH and does not provide other options for pivoting over TOR or HTTPS proxy servers

https://github.com/sshuttle/sshuttle

Installing sshuttle

```
sudo apt-get install sshuttle
```

To use sshuttle, we specify the option -r to connect to the remote machine with a username and password. Then we need to include the network or IP we want to route through the pivot host, in our case, is the network 172.16.5.0/23.

```
sudo sshuttle -r ubuntu@10.129.202.64 172.16.5.0/23 -v
```

With this command, sshuttle creates an entry in our iptables to redirect all traffic to the 172.16.5.0/23 network through the pivot host.

```
nmap -v -sV -p3389 172.16.5.19 -A -Pn
```