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. `Sshuttle` can be extremely useful for automating the execution of iptables and adding pivot rules for the remote host. We can configure the Ubuntu server as a pivot point and route all of Nmap's network traffic with sshuttle using the example later in this section.

One interesting usage of sshuttle is that we don't need to use proxychains to connect to the remote hosts. Let's install sshuttle via our Ubuntu pivot host and configure it to connect to the Windows host via RDP.

Installing sshuttle

```
ipp@htb[/htb]$ sudo apt-get install sshuttle

Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  alsa-tools golang-1.15 golang-1.15-doc golang-1.15-go golang-1.15-src
  golang-1.16-src libcmis-0.5-5v5 libqt4 libqvm2b liblibreoffice-java
  libmotif-common libqrcodegencpp1 libunoloader-java libxm4
  linux-headers-5.10.0-6parrot1-common python-babel-localedata
  python3-aiofiles python3-babel python3-fastapi python3-pydantic
  python3-slowapi python3-starlette python3-uvicorn sqsh ure-java
Use 'sudo apt autoremove' to remove them.
Suggested packages:
  autossh
The following NEW packages will be installed:
  sshuttle
0 upgraded, 1 newly installed, 0 to remove and 4 not upgraded.
Need to get 91.8 kB of archives.
After this operation, 508 kB of additional disk space will be used.
Get:1 https://ftp-stud.hs-esslingen.de/Mirrors/archive.parrotsec.org rolling/main amd64 sshu
Fetched 91.8 kB in 2s (52.1 kB/s)
Selecting previously unselected package sshuttle.
(Reading database ... 468019 files and directories currently installed.)
Preparing to unpack .../sshuttle_1.0.5-1_all.deb ...
Unpacking sshuttle (1.0.5-1) ...
Setting up sshuttle (1.0.5-1) ...
Processing triggers for man-db (2.9.4-2) ...
Processing triggers for doc-base (0.11.1) ...
Processing 1 added doc-base file...
Scanning application launchers
Removing duplicate launchers or broken launchers
Launchers are updated
```

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.

Running sshuttle

Running sshuttle

```
ipp@htb[/htb]$ sudo sshuttle -r ubuntu@10.129.202.64 172.16.5.0 -v

Starting sshuttle proxy (version 1.1.0).
c : Starting firewall manager with command: ['/usr/bin/python3', '/usr/local/lib/python3.9/d
fw: Starting firewall with Python version 3.9.2
fw: ready method name nat.
c : IPv6 enabled: Using default IPv6 listen address ::1
c : Method: nat
c : IPv4: on
c : IPv6: on
c : UDP : off (not available with nat method)
c : DNS : off (available)
c : User: off (available)
c : Subnets to forward through remote host (type, IP, cidr mask width, startPort, endPort):
c :   (<AddressFamily.AF_INET: 2>, '172.16.5.0', 32, 0, 0)
c : Subnets to exclude from forwarding:
c :   (<AddressFamily.AF_INET: 2>, '127.0.0.1', 32, 0, 0)
c :   (<AddressFamily.AF_INET6: 10>, '::1', 128, 0, 0)
c : TCP redirector listening on ('::1', 12300, 0, 0).
c : TCP redirector listening on ('127.0.0.1', 12300).
c : Starting client with Python version 3.9.2
c : Connecting to server...
ubuntu@10.129.202.64's password:
 s: Running server on remote host with /usr/bin/python3 (version 3.8.10)
 s: latency control setting = True
 s: auto-nets:False
c : Connected to server.
fw: setting up.
fw: ip6tables -w -t nat -N sshuttle-12300
fw: ip6tables -w -t nat -F sshuttle-12300
fw: ip6tables -w -t nat -I OUTPUT 1 -j sshuttle-12300
fw: ip6tables -w -t nat -I PREROUTING 1 -j sshuttle-12300
fw: ip6tables -w -t nat -A sshuttle-12300 -j RETURN -m addrtype --dst-type LOCAL
fw: ip6tables -w -t nat -A sshuttle-12300 -j RETURN --dest ::1/128 -p tcp
fw: iptables -w -t nat -N sshuttle-12300
fw: iptables -w -t nat -F sshuttle-12300
fw: iptables -w -t nat -I OUTPUT 1 -j sshuttle-12300
fw: iptables -w -t nat -I PREROUTING 1 -j sshuttle-12300
fw: iptables -w -t nat -A sshuttle-12300 -j RETURN -m addrtype --dst-type LOCAL
fw: iptables -w -t nat -A sshuttle-12300 -j RETURN --dest 127.0.0.1/32 -p tcp
fw: iptables -w -t nat -A sshuttle-12300 -j REDIRECT --dest 172.16.5.0/32 -p tcp --to-ports
```

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.

Traffic Routing through iptables Routes

Traffic Routing through iptables Routes

```
ipp@htb[/htb]$ nmap -v -sV -p3389 172.16.5.19 -A -Pn

Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slowe
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-08 11:16 EST
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 11:16
Completed NSE at 11:16, 0.00s elapsed
Initiating NSE at 11:16
Completed NSE at 11:16, 0.00s elapsed
Initiating NSE at 11:16
Completed NSE at 11:16, 0.00s elapsed
Initiating Parallel DNS resolution of 1 host. at 11:16
Completed Parallel DNS resolution of 1 host. at 11:16, 0.15s elapsed
Initiating Connect Scan at 11:16
Scanning 172.16.5.19 [1 port]
Completed Connect Scan at 11:16, 2.00s elapsed (1 total ports)
Initiating Service scan at 11:16
NSE: Script scanning 172.16.5.19.
Initiating NSE at 11:16
Completed NSE at 11:16, 0.00s elapsed
Initiating NSE at 11:16
Completed NSE at 11:16, 0.00s elapsed
Initiating NSE at 11:16
Completed NSE at 11:16, 0.00s elapsed
Nmap scan report for 172.16.5.19
Host is up.

PORT     STATE    SERVICE       VERSION
3389/tcp filtered ms-wbt-server

NSE: Script Post-scanning.
Initiating NSE at 11:16
Completed NSE at 11:16, 0.00s elapsed
Initiating NSE at 11:16
Completed NSE at 11:16, 0.00s elapsed
Initiating NSE at 11:16
Completed NSE at 11:16, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 4.07 seconds
```

We can now use any tool directly without using proxychains.

Note: When spawning your target, we ask you to wait for 3 - 5 minutes until the whole lab with all the configurations is set up so that the connection to your target works flawlessly.

Start Instance

∞ / 1 spawns left

Waiting to start...

Optional Exercises

Challenge your understanding of the Module content and answer the optional question(s) below. These are considered supplementary content and are not required to complete the Module. You can reveal the answer at any time to check your work.

Target: Click here to spawn the target system!

Try using sshuttle to connect via RDP to the Windows target (172.16.5.19) on the internal network. Once completed type: "I tried sshuttle" as the answer.

Submit your answer here...

Submit

Reveal Answer

Previous Next

Mark Complete & Next

My Workstation

OFFLINE

Start Instance

∞ / 1 spawns left