21

Your team has informed you that Throwback Hacks has taken on some proper security practices and are properly segmenting their network resources. Now that you have a couple of footholds onto the network, you can utilize them as a proxy server to pivot and access internal resources.

Pivoting Overview

In a good network, often referred to as a “Segmented Network” there are certain rules in place preventing users from accessing certain parts of the Internal LAN (ex. The Workstation Subnet should not be able to access the Server Subnet). This can be a headache for Pentesters on occasion as most networks are not segmented, these networks are referred to as “Flat Networks”. To make Segmented Networks more like flat networks there are a proxying tools such as Proxychains or SSHuttle which make it incredibly easy to pivot from one subnet in a LAN to another. Metasploit offers a Proxy server as part of its Post Exploitation tool suite which will be covered below.

Introduction to Pivoting with proxychains

Auto-Routing our Traffic

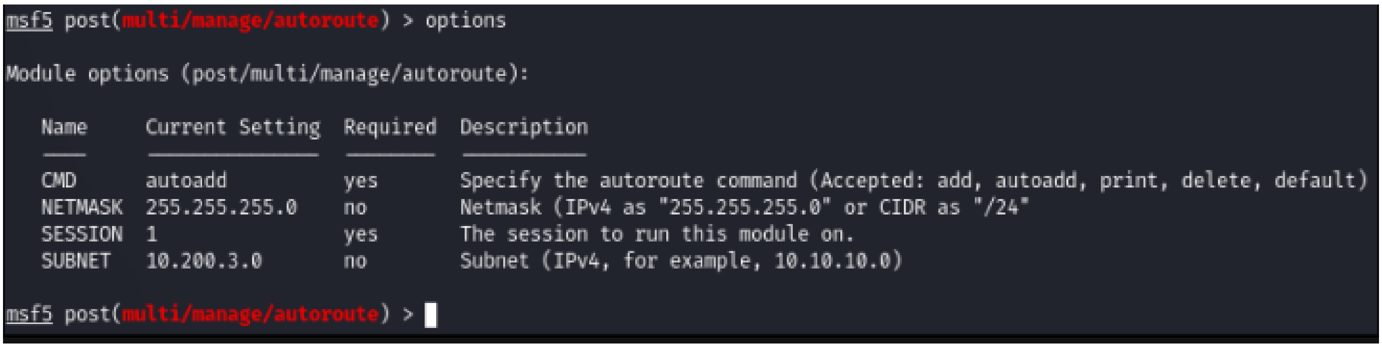
To setup a proxy server you will need a meterpreter session or a reverse shell open in metasploit before hand. You can easily get a meterpreter shell by uploading a payload to the machine and executing it.

1.) background

2.) use post/multi/manage/autoroute

3.) set SESSION 1

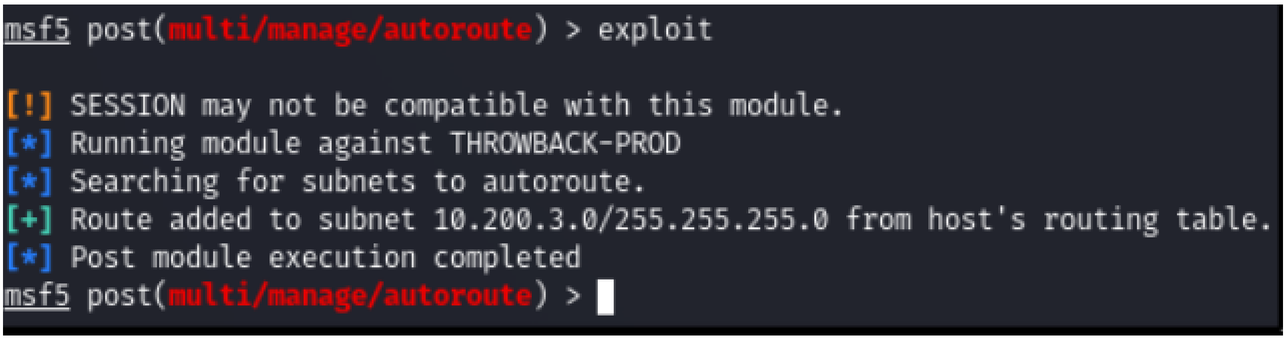
4.) set SUBNET 10.200.x.0



```
msf5 post(multi/manage/autoroute) > options

Module options (post/multi/manage/autoroute):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CMD      autoadd          yes       Specify the autoroute command (Accepted: add, autoadd, print, delete, default)
   NETMASK  255.255.255.0    no        Netmask (IPv4 as "255.255.255.0" or CIDR as "/24"
   SESSION  1                yes       The session to run this module on.
   SUBNET   10.200.3.0       no        Subnet (IPv4, for example, 10.10.10.0)

msf5 post(multi/manage/autoroute) >
```

Listing the configured options for autoroute

5.) exploit



```
msf5 post(multi/manage/autoroute) > exploit

[!] SESSION may not be compatible with this module.
[*] Running module against THROWBACK-PROD
[*] Searching for subnets to autoroute.
[+] Route added to subnet 10.200.3.0/255.255.255.0 from host's routing table.
[*] Post module execution completed
msf5 post(multi/manage/autoroute) >
```

Launching our new autoroute

Setting up our Proxy with Metasploit

1.) use auxiliary/server/socks4a

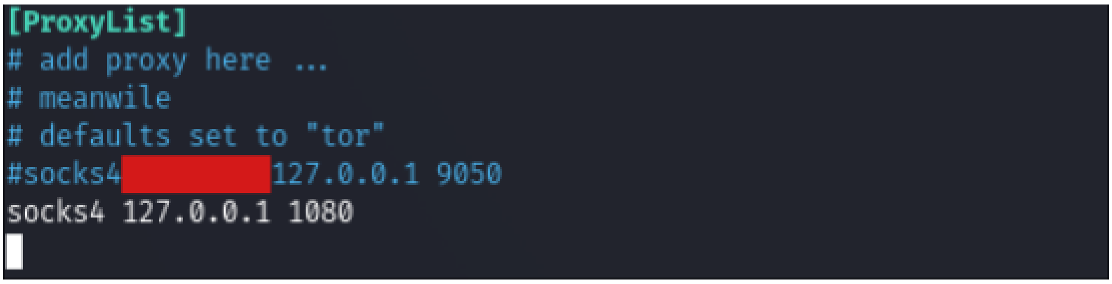
2.) (optional) Change you port, you can either keep the default 1080 port or change it to an open port of your choice.

Note: Depending on what version of Metasploit you are using, the Proxy Server module will be different. MSF5 and lower will have auxiliary/server/socks4a or socks5, MSF6 and newer will have socks/auxiliary/socks_proxy. With MSF6, you will need to specify if you want to use SOCKS4(a) or SOCKS5.

Configuring and Using the Proxy Chain

1.) sudo nano /etc/proxychains.conf

You will need to comment out the socks4 proxy on 9050 which is a default proxy for tor and add the proxy chain we just created with the port that you gave when creating the proxies.

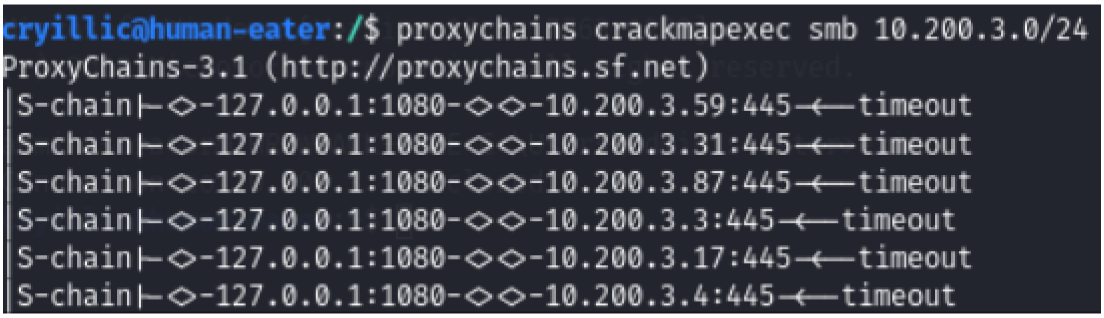


```
[ProxyList]
# add proxy here ...
# meanwile
# defaults set to "tor"
#socks4[redacted]127.0.0.1 9050
socks4 127.0.0.1 1080
```

Adding our Socks4a server to the proxychains configuration file

2.) proxychains

You can now run any normal commands or tools that you want and it will be forwarded through the proxy chain if you append your tool or command with “proxychains”.



```
cryillic@human-eater:/$ proxychains crackmapexec smb 10.200.3.0/24
ProxyChains-3.1 (http://proxychains.sf.net)
|S-chain|-<>-127.0.0.1:1080-<><>-10.200.3.59:445-<--timeout
|S-chain|-<>-127.0.0.1:1080-<><>-10.200.3.31:445-<--timeout
|S-chain|-<>-127.0.0.1:1080-<><>-10.200.3.87:445-<--timeout
|S-chain|-<>-127.0.0.1:1080-<><>-10.200.3.3:445-<--timeout
|S-chain|-<>-127.0.0.1:1080-<><>-10.200.3.17:445-<--timeout
|S-chain|-<>-127.0.0.1:1080-<><>-10.200.3.4:445-<--timeout
```

An example of running a command through proxy chains

Pivoting with proxychains

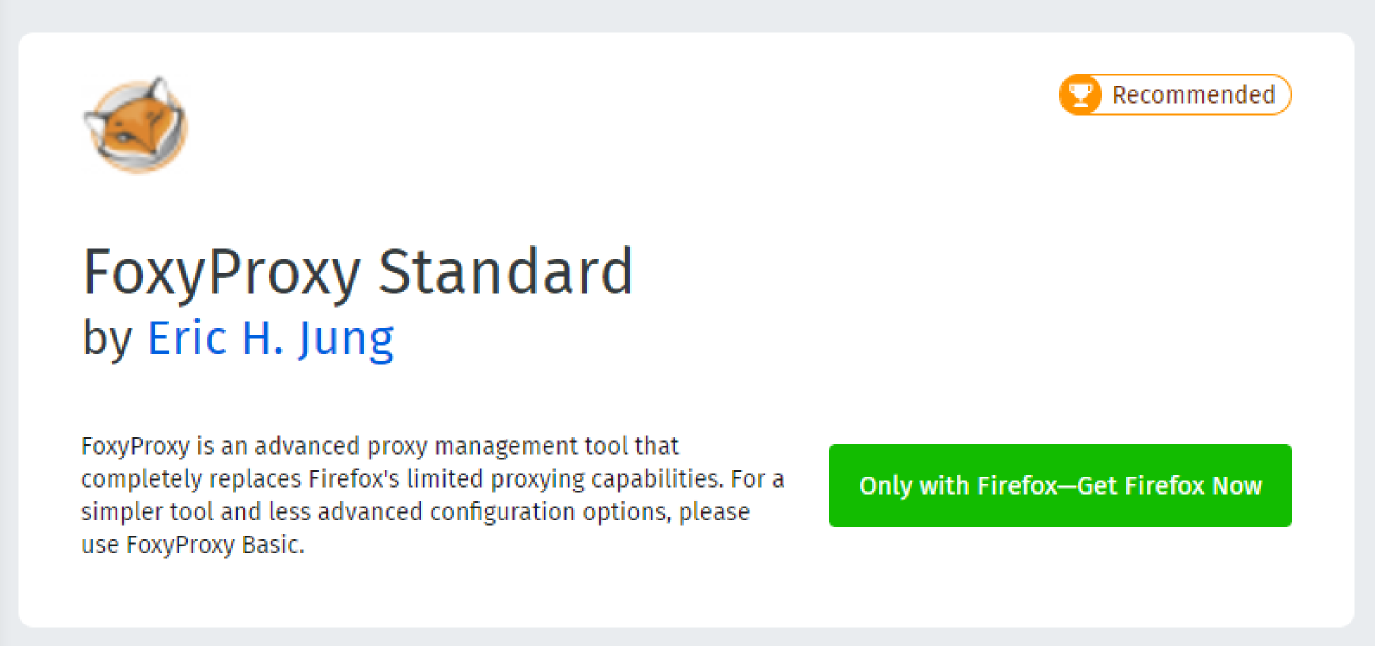
Pivoting may seem like a very big and scary thing but it is actually fairly simple after you have your proxy server set up. After setting up the proxy server you can pivot to any machines or resources that the proxy server has access to. For example if you had a proxy server on example-ws01 and example-ws02 was segmented by a security groups that made it so only example-ws01 had access you could use your proxy server on example-ws01 to access example-ws02. You can use any way of accessing the machine that you would usually like ssh, rdp, win-rm, psexec you just have to prepend the command with proxychains.

Examples of pivoting

1.) proxychains ssh user@MACHINE_IP
2.) proxychains xfreerdp /u:user /p:password /v:MACHINE_IP
3.) proxychains evil-winrm -i MACHINE_IP -u user -p password

Setting up a Web Proxy with FoxyProxy

Now that we have a proxy setup to forward our traffic through we need a way to easily access the resources on the network. Let's add an extension to our web browser to allow us to easily route our traffic through it! For this room, we'll be using 'FoxyProxy Standard' on firefox. Navigate to the following link to install FoxyProxy Standard: Link

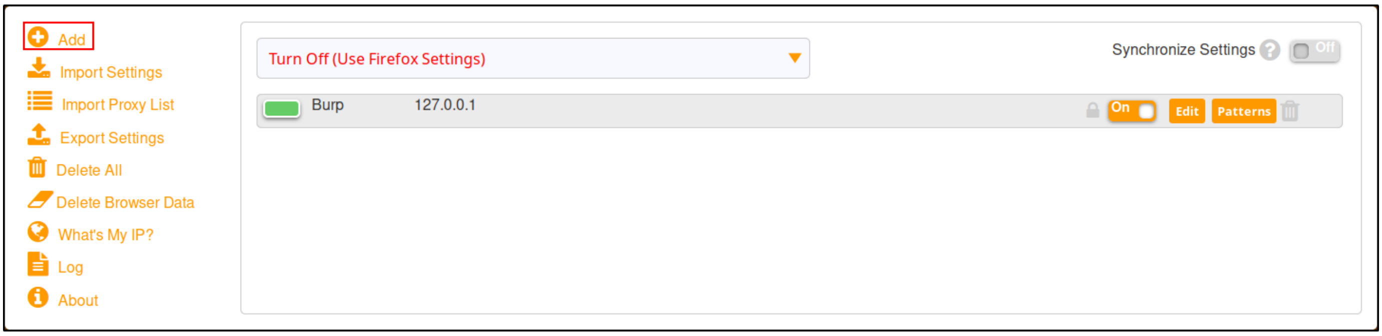


FoxyProxy Standard
by Eric H. Jung

FoxyProxy is an advanced proxy management tool that completely replaces Firefox's limited proxying capabilities. For a simpler tool and less advanced configuration options, please use FoxyProxy Basic.

FoxyProxy Standard install card

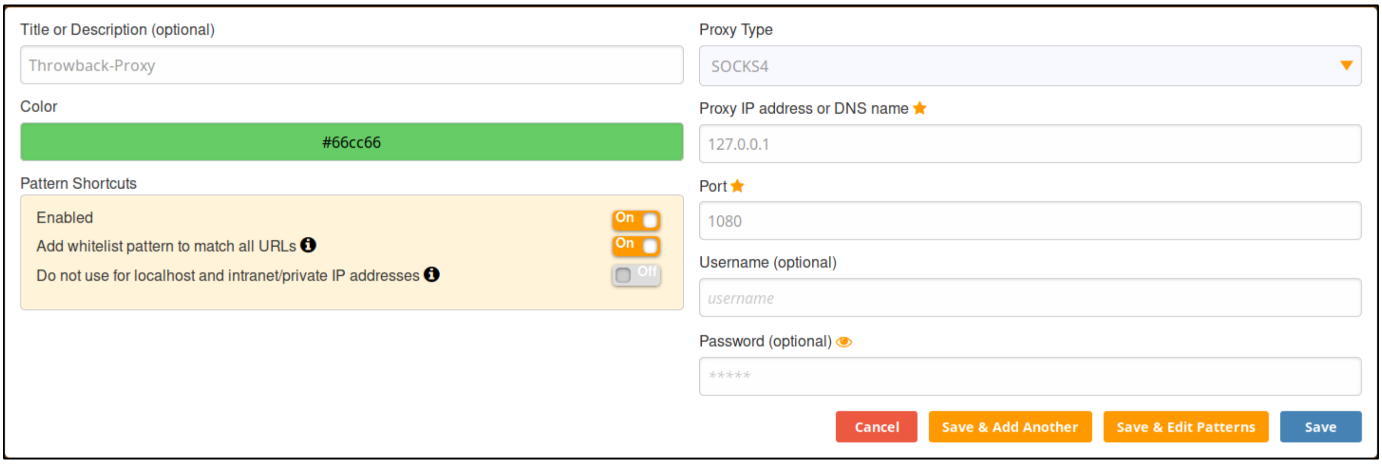
1.) Click on FoxyProxy among your extensions. After that, click on 'Options', Then click on 'Add'.



Burp 127.0.0.1

FoxyProxy Options Panel

2.) Enter in the following setting you will need to fill in the title, proxy type (SOCKS4), Proxy IP, and Port then click 'Save'.



Title or Description (optional): Throwback-Proxy

Color: #66cc66

Pattern Shortcuts
- Enabled: On
- Add whitelist pattern to match all URLs: On
- Do not use for localhost and intranet/private IP addresses: Off

Proxy Type: SOCKS4

Proxy IP address or DNS name ★: 127.0.0.1

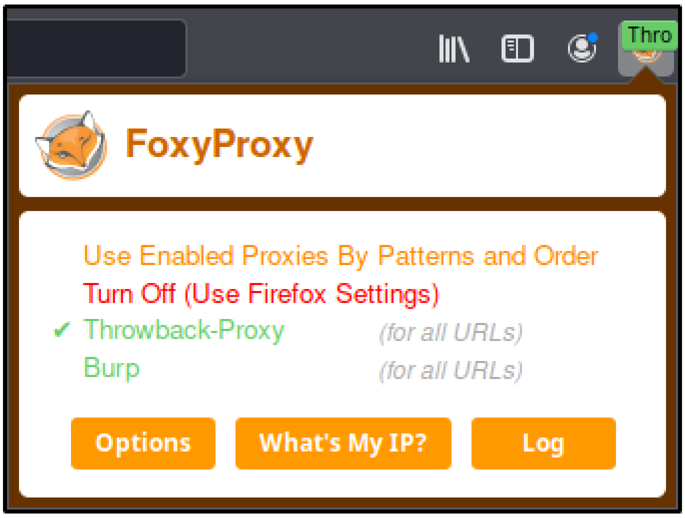
Port ★: 1080

Username (optional): username

Password (optional): *****

FoxyProxy add proxy menu

3.) Click on Foxy Proxy in your extensions and enable the web proxy.


Thro
FoxyProxy
Use Enabled Proxies By Patterns and Order
Turn Off (Use Firefox Settings)
✓ Throwback-Proxy (for all URLs)
Burp (for all URLs)
Options
What's My IP?
Log

FoxyProxy enable menu

You can now access internal resources and devices from within firefox.

Answer the questions below

Read the above and setup your proxy

Question Done