Getting Kali and Metasploit Up and Running

```
# msfupdate

# service postgresql start       //verify port 5432

# msfdb init

#service apache2 start           //local webserver started up

# msfconsole

msf> db_status

msf> workspace

                                  //update-rc.d "service" defaults if
                                  you want to add startup persistence
```

To change to a static IP address for eth0 edit /etc/network/interfaces

```
auto eth0

iface eth0 inet static

address 192.168.0.x

netmask 255.255.255.0

broadcast 192.168.0.255

gateway xxx.xxx.xxx.xxx
```

For DHCP on eth0, comment out the lines above except (auto eth0) and add (iface eth0 inet dhcp)

You may have to change nameserver in /etc/resolv.conf

```
domain localdomain

search localdomain

nameserver 192.168.195.2    //your nameserver of choice
```

```
service networking restart       //may need to restart the services
above
```

Once you are on TGT, think about what you want from the box:

getuid	//to get current privilege and user level you are running under
migrate or getsystem	//to run under different process
clearev probably do a last step	//clear logs in app, system, security;
hashdump	//pulls SAM database
ipconfig	
idletime	//since last user logged in
ps	//current processes running on tgt
upload	//what to full/path/to/destination
download	//remember to use escape/ in full pathname
webcam_snap	
screenshot	
search -f	//search for files
persistence?	
Pivoting by adding routes	
Putting tools up on target with nc if possible	

More in Metasploit, The Penetration Tester's Guide , Annex B

Create OP Notes to keep track of what, where, how, and when you do something on Targets

192.168.0.13 (Kali)

--> 172.16.32.1 (Windows XP sp3) TGT 1

--> 172.16.32.4 (Metasploitable Linux 2.6.3) TGT 2

----> 10.10.0.2 (Windows 7 sp0) TGT 3

8:31 AM 2/20/2017: On TGT 1 with MS08_067

8:33 AM 2/20/2017: Got System

8:33 AM 2/20/2017: Uptime: 3 day, 12 hours, 47 min

8:34 AM 2/20/2017: Grabbed screenshot, no one on box

8:35 AM 2/20/2017: Hashdump complete, got user jpecos

8:37 AM 2/20/2017: Searched for plans.*

8:37 AM 2/20/2017: Downloaded plans.jpg and plans.pdf

8:39 AM 2/20/2017: Cleared Logs; off TGT 1

8:40 AM 2/20/2017: On TGT 2 with DRuby

8:40 AM 2/20/2017: Got Root

8:41 AM 2/20/2017: Uptime: 303 days, 17 hours, 31 min

8:45 AM 2/20/2017: Set up Pivot to TGT 3

8:51 AM 2/20/2017: On TGT 3 with Passed Hash user jpecos

8:52 AM 2/20/2017: Got System

8:52 AM 2/20/2017: Uptime: 1 day, 1 hour, 53 min

8:55 AM 2/20/2017: Installed persistence

8:57 AM 2/20/2017: Cleaned logs; Off TGT 3

9:01 AM 2/20/2017: Off TGT 2

End notes

Malware Analysis Quick Methodology

Static Analysis:

MD5Sum and/or SHA1Sum the file against VirusTotal or other places

PEView to see any export/import tables

- Dlls that might characterize the malware

DIE to look for and ID packing

- Is an unpacker needed?

Strings the file with SysInt Strings or other program

OllyBdg or IDAPro

Dynamic and Behavior Analysis (need FakeDNS and INetSim Webserver):

Autoruns save before kicking off malware

TShark to start packet capture

RegShot and save to know what the registry was like before

PROCMON and pause/clear the capture before kicking off malware

- Filter for the malware
- Handles and processes kicked off

TCPView to look for connections from the malware

ProcessHacker

Run the Malware and let it go for a while

Pause PROCMON and filter any new spawned processes

RegShot, save, and compare looking for persistence

Stop TShark and look for suspicious network traffic

Check FakeDNS and Webserver logs

Write a Triage Malware Report

Metadata including original file name, type, size, dates, hashes

Overall Summary

FileSystem and Registry Changes

Network Activity (IPs, URLs requested, clear, encrypted comms)

Strings of Interest

Mutexes Created

Process Activity (created, terminated)