Ssh
-L local bind
-R Reverse proxy
-D bind
Ssh

-f? -f includes -n
-N?

Exercise commands:

Set up nc listener on port 80 on your windows machines
Turn on ssh on your kali box
Run ifconfig on both boxes. Find your vmnet ip address for both.
Test ping from host machine to VM
-nc 10.11.11.156 80 #this ip is your remote windows Offsec machine. Should not work
-ping 10.11.11.156 #also will not work
-ping 172.16.14.163
-ssh archang31@172.16.14.163
-ssh 172.16.14.163 -L 8080:10.11.11.156:80 #this might not work if user names do not match.
#Show how to specify user names
-ssh archang31@172.16.14.163 -L 8080:10.11.11.156:80
#Try to close ssh without losing nc first. Show it does not work
ask how to keep nc open after closing connect? -L (no -l) on windows, -k (extra option) on linux

#So that is great, but what port are we communicating with Kali on? (22). How do I change this port? (with the -p 53 option) like:
-ssh archang31@172.16.14.163 -p 53 -L 8080:10.11.11.156:80
#this command will not work. Why? Not listening in Kali on port 53. Can I do that?
-locate sshd_config
#point out the :usr: symbolic link
-Sudo vi /etc/ssh/sshd_config ##add Port 53
-sudo service restart ssh

#now the previous ssh command will work
-ssh archang31@172.16.14.163 -p 53 -L 8080:10.11.11.156:80

#show you can fork into background
ssh archang31@172.16.14.163 -p 53 -L 8080:10.11.11.156:80 -f -N

#find with ps aux | grep ssh
-kill <pid>

Now let's do a reverse proxy. I am going to set up a listener that the remote machine is going to connect to. When then connect to their own port via the port I specify, they will have access to the port I specify on my machine
-sudo nc -nlv 53 on my outside host (Mac VM). this is to simulate the service I want to give access too
-ssh archang31@172.16.14.163 -R 6000:127.0.0.1:53
#the end is my local port and the

Question: if I wanted to have the same functionality as the first example, how would I run this command

- D (bind proxy)
  -D [bind_address:]port
  Example: Ssh -D <local proxy port> -p <remote port><target>
  Example: ssh -D 8080 -p 2222 a.b.c.d
 (this command is run on the attacker machine. This allows anything connecting to the attack machine on port 8080 to be ssh tunneled to the

What is SOCKS?
http://www.youngzsoft.net/ccproxy/difference-between-socks4-and-socks5.htm
SOCKet Secure (SOCKS) is an Internet protocol that routes network packets between a client and server through a proxy server. SOCKS5 additionally provides authentication so only authorized users may access a server. Practically, a SOCKS server proxies TCP connections to an arbitrary IP address, and provides a means for UDP packets to be forwarded.SOCKS performs at Layer 5 of the OSI model (the session layer, an intermediate layer between the presentation layer and the transport layer).

What is the difference between 4/5?
SOCKS4 and SOCKS5 both belong to SOCKS protocol. It is the concrete supportive application that distinguishes them.**SOCKS4 only supports TCP application, while SOCKS5 supports TCP and UDP applications**. However, because of the fact that SOCKS5 also supports various authentication mechanisms and domain name resolution (DNS), which does not go with SOCKS4, the outgoing SOCKS proxy is normally SOCKS4 proxy. As a result, UDP applications are not supported normally. That is to say, SOCKS5 could support anything that SOCKS4 supports, but it is not the same with SOCKS4.

Talk about HTTP Tunneling. What is the HTTP Connect method? How does this HTTP tunnel via a Proxy work? Why does HTTP Connect exist?
Definition: HTTP CONNECT method for establishing end-to-end tunnels across HTTP proxies

#Try this command
-ssh -D 127.0.0.1:8080 -p 53 archang31@172.16.14.163

What does this do? Is sends anything connected on the port 8080 on the host machine through the ssh tunnel to 172.16.14.163 on port 53. The traffic in then routed via the routing table on 163.

How do I run a command using this proxy? Like I want to run nmap but if I nmap 10.11.1.0/24, I will currently do it from my host computer
#use proxy chains!

-sudo proxychains #see that it is currently using port 9050.