Cheat Sheet

Virtual Machine Creation

`https://www.youtube.com/watch?v=MzUwi4yqxYI`
Takes you through installing windows 10 using fusion. Similar process for any linux distribution

FTP

10.10.10.23: an example IP Address
PORT: port number (LPORT is local and RPORT is remote)
comma separated commands

`connect`	ftp 10.10.10.23 or on a web browser ftp://10.10.10.23
`remote directory`	cd, ls, pwd, dir
`local traversal`	lcd, lpwd, !ls, !dir
`download to local`	get filename (use mget for many files)
`upload to remote`	put filename (use mput for many files)
`delete`	del filename (use mdel for many files)
`create directory`	mkdir name (use rmdir to remove)
`end connection`	bye (or quit)

If you need help while in ftp, type help or ?

SSH

10.10.10.23: an example IP Address
PORT: port number (LPORT is local and RPORT is remote)

`connect`	ssh -p PORT username@10.10.10.23
`connect with key`	ssh -i path_to_key username@10.10.10.23
`reverse ssh`	ssh -fN -R RPORT:localhost:LPORT username@10.10.10.23
`generate keys`	ssh-keygen -t rsa
`upload keys`	ssh-copy-id -p PORT -i path_to_key username@10.10.10.23

If you need help, man ssh. If troubleshooting add verbose mode with -v

SCP

10.10.10.23: an example IP Address
PORT: port number
The -P is capitalized!
. means here/this directory
is shorthand for this user's directory

`push`	scp -P PORT -i path_to_key file1.ext file2.ext username@10.10.10.23:~/documents/hello.txt
`pull`	scp -P PORT -i path_to_key username@10.10.10.23:~/documents/hello.txt .

If you need help, man scp. If troubleshooting add verbose mode with -v. If copying directories add a -r

NMAP

192.168.1.23: an example target IP
Run an arp-scan -l or fping or netdiscover to discover notation

`scan`	nmap -Pn -n -v -sV 192.168.1.23/24 -oA scan
`full scan`	nmap -Pn -n -A 192.168.1.23 -p- -oA scan
`script`	nmap –script="smb-vuln-ms17-010" 192.168.1.23

All nmap scripts can be found in /usr/share/nmap/scripts/ If you need help, man nmap.

Hail Hydra

10.10.10.21: an example target IP Address
deez: username we are attacking
ssh: You can target other services like ftp,http,https,smb
is shorthand for this user's directory
Here is a simple dictionary attack with hydra
`hydra -l deez -P rockyou.txt 10.10.10.21 ssh`
if you need to specify a port add a -s with a port number
`hydra -l deez -P rockyou.txt 10.10.10.21 ssh -s PORT`
you can save to a file via `-o hydra_passwords.txt`
If there are multiple users, add each all names to a file and use -L
`hydra -L usernames.txt -P rockyou.txt 10.10.10.21 ssh -s PORT`
Speed up hydra by adding more threads via the -t option
`hydra -l usernames.txt -P rockyou.txt -t 6 10.10.10.21 ssh -s PORT`
For lots of target machines, add them all to file and use -M option
`hydra -l usernames.txt -P rockyou.txt -t 6 -M hosts.txt ssh -s PORT`

hashcat

Lets crack some passwords
You can use hashid or hash-identifier on your hash to identify type
`hashid some_hash` or `hash-identifier some_hash`
After you get the hash, use `hashcat –help |grep type` to find its number. That goes infront of -m. specify hash type with -m, attack type -a, output file -o.
Cracking an md5 hash(0) with straight mode(0)
`hashcat -m 0 -a 0 hash hak5.txt -o cracked.txt`
Cracking a similar hash using md5 with combination mode(1)
`hashcat -m 0 -a 1 hash hak5.txt hak5.txt -o cracked.txt`
add special rules to each dictionary prior to combining them like so The j adds - after a word in left, k adds ! to the end of other word prior to combining them
`hashcat -m 0 -a 1 hash hak5.txt -j '$-' hak5.txt -k '$!'`
Brute force attack mode with -a 3 followed by hash and mask. The mask here is seven characters long of lower case letters(look up built in charsets via man)
`hashcat -m 0 -a 3 hash ?l?l?l?l?l?l?l`
You can specify your own charset to use via -1, -2, -3, -4
`hashcat -m 0 -a 3 -1 abcdef1234% hash ?1?1?1?l`
We can use append mode(-a 6) or prepend mode(-a 7) to add words. Here we append
four special characters to words in hak5 prior to cracking
`hashcat -m 100 -a 6 hash hak5.txt ?s?s?s?s`
We can use rules on word list. You must be in attack mode (0)
`hashcat -m 0 -a 0 hash -r /usr/share/hashcat/rules/leetspeak.rule hak5.txt`
We can create our own wordlists via –stdout option
`hashcat –stdout -a0 -r incisiverule rockyou.txt >>incisive_rockyou.txt`
Crunch may be used for simple wordlist generation
`crunch 10 10 -t "hello^dog%" -o wordlist.txt`
Will generate 10 letter words marching a pattern after the t and store it in wordlist.txt
if your hash or hash file has a username use `–username`, if you need to find cracked passwords use `–show` or look at the pot file `~/.local/share/hashcat/hashcat.potfile`

Safeguarding Data

file.txt: a random file with contents we care about
uwotm8.png: an random image file encode file.txt into hex or base64 via xxd or base64
`xxd file.txt >file.encoded` or `base64 file.txt >file.encoded`
Decode them back
`xxd -p -r file.encoded >file.decoded` or `base64 –decode file.encoded >file.decoded`
Encrypt encoded files using openssl using a specific encoding like aes-256-cbc
`openssl enc -aes-256-cbc -e -in file.encoded -out file.encrypted`
Decrypt the file similary with -d option
`openssl enc -aes-256-cbc -d -in file.encrypted -out file.decrypted`
Add our encrypted file to a compressed zip archive via 7z available from p7zip-full
`7z a -mhe=on archive.7z file.encrypted`
To extract the zip archive just do
`7z e archive.7z`
We can embed a file into an image with steghide like so
`steghide embed -ef archive.7z -cf uwotm8.png -sf suspicious.png`
We can extract the file from the image via steghide as well
`steghide extract -sf suspicious.png`
Verify hashes on any file via the utility md5sum,sha1sum, sha256su or sha512sum
`md5sum file.txt >file.md5`
compare the hash to what is known to be right

wpa supplicant

wlan0: interface we identified using `ip a` or `iwconfig`.
If interface is down, bring it up and set it in managed mode
`sudo ifconfig wlan0 up` then `sudo airmon-ng stop wlan0`
Grab the ssid, psk of the network you intend to connect via airodump for example
Place the information in
`/etc/wpa_supplicant/wpa_supplicant.conf`

Place ctrl_interface=/var/run/wpa_supplicant at the top of the file then

```
network = {
    ssid="l33t"
    psk="yourmama" }
```

To connect to a hidden wpa network add the scan_ssid=1 option

```
network = {
    ssid="l33t"
    psk="yourmama"
    scan_ssid=1}
```

To connect to an open network aka no password/psk needed

```
network= {
    ssid="l33t"
    key_mgmt=NONE
    priority=100 }
```

To connect to a WEP network with a simple key "12345"

```
network = {
    ssid="l33t"
    key_mgmt=NONE
    wep_key0="12345"
    wep_tx_keyidx=0}
```

After updating wpa_supplicant.conf, you can run it with

```
sudo wpa_supplicant -c
/etc/wpa_supplicant/wpa_supplicant.conf -i wlan0 -d
```

This runs and tests the connection in the foreground. If all is good run it the background

```
sudo wpa_supplicant -B -c
/etc/wpa_supplicant/wpa_supplicant.conf -i wlan0
```

In case of connection issues kill all running wpa_supplicant processes and start over

```
sudo killall -HUP wpa_supplicant
```

Cracking WPA/WEP

Its proven science by this point. Plenty of good ones out there. Here's an excellent one

`https://github.com/V0lk3n/WirelessPentesting-CheatSheet`

Metasploit

Another excellent cheat sheet. No use reinventing the wheel Sometimes just using the exploit as provided by findsploit or searchsploit is enough

`https://github.com/coreb1t/awesome-pentest-cheat-sheets/blob/master/docs/Metasploit-CheatSheet.pdf`

Active Directory traversal

```
net users /domain
net groups /domain
net group "Domain Admins" /domain
```

Use kiwi while on windows machine using meterpreter to access creds

```
load kiwi
creds_dwdigets or creds_all
```

kismet

Running kismet is straight forward.

```
sudo kismet
```

If you are having issues with gps as is common. Kill all gpsd processes

Check /etc/kismet/kismet.conf and make sure the following line is present

```
sudo gpsd -n -N -D 2 /dev/ttyUSB0
```

Verify you can receive gps

```
cgps -s
```

then run it. You can add -c to specify interface

```
sudo kismet -c wlan0
```

Use kismetdb_to_kml or kismetdb_to_cap as needed to convert between formats

Create the image via gpsprune XXXXXXXX.kml file

Happy Hacking from dungeon_master_us_tz