Setting Up

Using apt	apt <COMMAND> <PACKAGE>
Firefox Extensions	Wappalyzer, Foxyproxy, HacKontent, Vulners
Note-Taking	Obsidian, Pwndocs

Pwndocs This is a professional Penetration Testing report generator available Here

System Updates You can add custom commands to your `~/.bashrc` file to run things like system updates without having to type the whole apt command

```
echo " alias sysupd ate ='sudo apt-get update -y && sudo apt-get upgrade -y'” >> ~/. bashrc
```

To run this command, start a new terminal and type `sysupdate`

Information Gathering

nslookup	
Query All	nslookup -query=all <URL>
Name Server	nslookup -type=ns <URL>
Zone Transfer	Link
Nmap	
Check Open Ports	nmap -n -Pn -vvv <IP>
Scan w/Common Scripts	nmap -sSCV -Pn -A -vvv -p=<PORTS> <IP> --min-rate=5000
Output Scan to Files	<nmap command> -oA filename
Change XML to HTML	xlstproc filename.xml -o filename.html
Whois	whois <URL>
Dnsenum	dnsenum <URL>
Cyberchef	Link

Replace <> with the respective info.

Exploitation

Metasploit	metasploit -q
Update	metasploit update
Documentation	Link
Multihandler	Link
Searchsploit	
Vulnerability Search	searchsploit <APPLICATION>
download module	searchsploit -m <MODULE NUM>
Reverse Shell Generator	Revshells
Netcat	
Reverse Shell (Connect)	nc -lvnp <PORT>
Bind Shell (Connect)	nc <IP> <PORT>
rlwrap	`rlwrap nc <..>` - Gives you more control
Pwncat - Python Netcat C2	Link

Bruteforce Attacks

Hashcat	Full Cheatsheet
Find encoding/encryption in help	hashcat -h | grep <ENC>
JohnTheRipper	Full Cheatsheet
Crackstation - Rainbow Table	Link
CrackMapExec	Link

Bruteforce Attacks (cont)

WPScan	Link

Hashcat
hashcat -h | grep md5

CrackMapExec (CME)
Comprehensive Guide

Wi-Fi Cracking

Airmon-ng - Monitor	
Start listener on interface	airmon-ng start wlan0
Airodump-ng - Dump	
Select Interface	airodump-ng wlan0
Dump Hashes	airodump-ng -w <WORDLIST> -c 1 --bssid <MAC> wlan0
	airodump-ng -w Attack1 -c 1 --bssid E6:6F:14:31:63:1C wlan0
Aircrack-ng - Crack	
Crack Captured MAC	aircrack-ng -a2 -b <MAC> -w <WORDLIST> </path/to/capture>

Sponsored by **Readable.com**
Measure your website readability!
https://readable.com

Wi-Fi Cracking (cont)

	aircrack-ng -a2 -b E6:6F:14:31:63:1C -w /root/Desktop/wordlist.txt /root/Desktop/Attack1-01.cap
Documentation	Link

Sponsored by **Readable.com**
Measure your website readability!
https://readable.com