HACKTHEBOX

WI-FI PENETRATION TESTING BASICS

CHEAT SHEET

Interfaces and Interface Modes

Command	Description
`sudo iw reg set US`	Set Region for the Interface.

`sudo ifconfig wlan0 down`
`sudo iwconfig wlan0 txpower 30`
`sudo ifconfig wlan0 up`
	Change the Interface Strength.

`iwlist wlan0 scan | grep 'Cell\\|Quality\\|ESSID\\|IEEE'`	Scan Available WiFi Networks.

`sudo ifconfig wlan0 down`
`sudo iwconfig wlan0 channel 64`
`sudo ifconfig wlan0 up`
	Change the Interface Channel.

`sudo ifconfig wlan0 down`
`sudo iwconfig wlan0 freq "5.52G"`
`sudo ifconfig wlan0 up`
	Change the Interface Frequency.

`sudo ifconfig wlan0 down`
`sudo iwconfig wlan0 mode managed`
`sudo ifconfig wlan0 up`
	Set the Interface to Managed Mode.

`sudo iwconfig wlan0 mode ad-hoc`
`sudo iwconfig wlan0 essid HTB-Mesh`
	Set the Interface to Ad-hoc Mode.

`sudo iw dev wlan0 set type mesh`	Set the Interface to Mesh Mode.

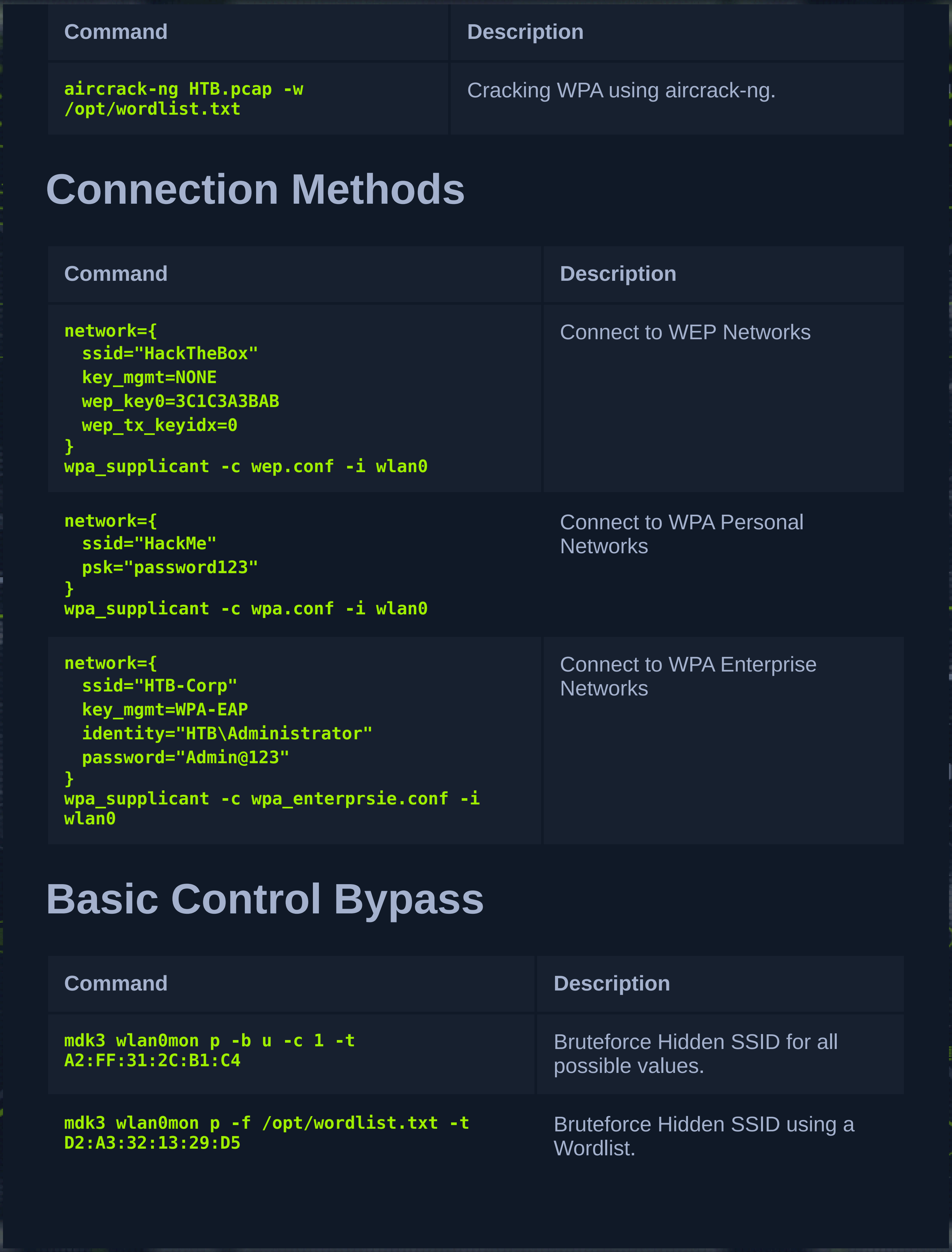
HTB ACADEMY CHEATSHEET

Command	Description

`sudo ifconfig wlan0 down`
`sudo iw wlan0 set monitor control`
`sudo ifconfig wlan0 up`
	Set the Interface to Monitor Mode.

Aircrack-ng Essentials

Command	Description
`sudo airmon-ng start wlan0`	Start Monitor mode using airmon-ng.
`sudo airmon-ng start wlan0 11`	Start Monitor mode using airmon-ng on specific channel.
`sudo airodump-ng wlan0mon`	Scan Available WiFi Networks using airodump-ng.
`sudo airodump-ng -c 11 wlan0mon`	Scan Available WiFi Networks using airodump-ng on Specific Channels or a Single Channel.
`sudo airodump-ng wlan0mon --band a`	Scan 5 GHz Wi-Fi bands.
`sudo airodump-ng wlan0mon -w HTB`	Save the airodump-ng output to a file.
`airgraph-ng -i HTB-01.csv -g CAPR -o HTB_CAPR.png`	Clients to AP Relationship Graph.
`airgraph-ng -i HTB-01.csv -g CPG -o HTB_CPG.png`	Common Probe Graph.
`sudo aireplay-ng --test wlan0mon`	Test for Packet Injection.
`aireplay-ng -0 5 -a 00:14:6C:7A:41:81 -c 00:0F:B5:32:31:31 wlan0mon`	Perform Deauthentication using Aireplay-ng
`airdecap-ng -w 1234567890ABCDEF HTB-01.cap`	Decrypt WEP-encrypted captures.
`aircrack-ng -K HTB.ivs`	Cracking WEP using aircrack-ng.



Command	Description
`aircrack-ng HTB.pcap -w /opt/wordlist.txt`	Cracking WPA using aircrack-ng.

Connection Methods

Command	Description

`network={`
`  ssid="HackTheBox"`
`  key_mgmt=NONE`
`  wep_key0=3C1C3A3BAB`
`  wep_tx_keyidx=0`
`}`
`wpa_supplicant -c wep.conf -i wlan0`
	Connect to WEP Networks

`network={`
`  ssid="HackMe"`
`  psk="password123"`
`}`
`wpa_supplicant -c wpa.conf -i wlan0`
	Connect to WPA Personal Networks

`network={`
`  ssid="HTB-Corp"`
`  key_mgmt=WPA-EAP`
`  identity="HTB\Administrator"`
`  password="Admin@123"`
`}`
`wpa_supplicant -c wpa_enterprsie.conf -i wlan0`
	Connect to WPA Enterprise Networks

Basic Control Bypass

Command	Description
`mdk3 wlan0mon p -b u -c 1 -t A2:FF:31:2C:B1:C4`	Bruteforce Hidden SSID for all possible values.
`mdk3 wlan0mon p -f /opt/wordlist.txt -t D2:A3:32:13:29:D5`	Bruteforce Hidden SSID using a Wordlist.

Command	Description

`airmon-ng stop wlan0mon`
`sudo macchanger wlan0 -m 3E:48:72:B7:62:2A`
`sudo ifconfig wlan0 up`
	Change the MAC address of the interface.