

Forum:[Hack Forums](#)

Thread: [RTL8812AU on VMware: PMKID/WPS dead, Deauth blocked \(802.11w?\) Need modern attack p](#)

ggzz1 - August 11, 2026, 6:53 am

Kali Linux (VMware Workstation)

USB WiFi: RTL8812AU (monitor mode working)

Target: 2023+ home router, WPA2, likely PMF/802.11w enabled

What I've tried & failed:

PMKID: hcxdump tool captures nothing (--active-scan runs, but hcxpcapngtool output empty). Router probably has PMKID caching disabled.

WPS: reaver/bully stuck at handshake (Receive timeout, 0x02 errors). wash sees WPS 2.0, but never progresses past first PIN.

Deauth for handshake: aireplay-ng -0 returns [0|0 ACKs] – clients ignore deauth (PMF/802.11w likely active).

Questions for the pros:

What's the current go-to attack chain against PMF-protected WPA2 routers? Is Evil Twin the only reliable path now? Any tool better than airgeddon for this (e.g., bettercap, KTO, hostapd-mana)?

Is RTL8812AU fundamentally a bad choice in VMware? Should I move to bare-metal Kali or swap to AR9271? Or is there a driver/firmware tweak that actually stabilizes it for injection?

If you were facing this exact scenario, what would be your step-by-step modern approach? (Assume I have no prior credentials, just a monitor-mode interface.)

Looking for a battle-tested workflow, not theoretical.

Thanks in advance.

DramaKing - August 11, 2026, 7:31 am

Evil Twin. You can check for PMF, but it's unlikely on WPA2 for compatibility reasons.

ggzz1 - August 11, 2026, 1:36 pm

(Aug 11, 2026 07:31 AM)DramaKing Wrote: [\[CITE\]](#) Evil Twin. You can check for PMF, but it's unlikely on WPA2 for compatibility reasons.

Hey, following up on your previous reply.

We tried PMKID, WPS, and Deauth handshake capture – all failed. We want to confirm: are these failures due to our environment (VMware + RTL8812AU), or are these attack vectors actually dead against modern WPA2 routers? If they are dead, what do real pentesters use instead today?

Also, for Evil Twin – without Deauth, how do you actually get a user to connect to your fake AP? Is it just signal strength and patience, or is there a smarter way to nudge them?

We just want to know what someone who actually does this for a living would do in this situation. If Evil Twin is the only realistic path, we'll commit to it.

Pr0m3th3us - August 13, 2026, 11:00 am

(Aug 11, 2026 06:53 AM)ggzz1 Wrote: [\[CITE\]](#) Kali Linux (VMware Workstation)

USB WiFi: RTL8812AU (monitor mode working)

Target: 2023+ home router, WPA2, likely PMF/802.11w enabled

What I've tried & failed:

PMKID: hcxdump tool captures nothing (--active-scan runs, but hcxpcapng tool output empty). Router probably has PMKID caching disabled.

WPS: reaver/bully stuck at handshake (Receive timeout, 0x02 errors). wash sees WPS 2.0, but never progresses past first PIN.

Deauth for handshake: aireplay-ng -0 returns [0|0 ACKs] – clients ignore deauth (PMF/802.11w likely active).

Questions for the pros:

What's the current go-to attack chain against PMF-protected WPA2 routers? Is Evil Twin the only reliable path now? Any tool better than airgeddon for this (e.g., bettercap, KTO, hostapd-mana)?

Is RTL8812AU fundamentally a bad choice in VMware? Should I move to bare-metal Kali or swap to AR9271? Or is there a driver/firmware tweak that actually stabilizes it for injection?

If you were facing this exact scenario, what would be your step-by-step modern approach? (Assume I have no prior credentials, just a monitor-mode interface.)

Looking for a battle-tested workflow, not theoretical.

Thanks in advance.

I get handshakes all day on modern PMF routers. I use hcxdump tool. I think your issue may be your using a VM. I don't do that when I'm doing deauth attacks and grabbing handshakes. Also I use an Alfa AWUS036AXML. Which uses the MediaTek MT7921AUN. But your chipset is fine it does monitor and packet.

I think it's down to 2 main issues.

1. you're on a VM, and it's not setup correctly.
2. there are no devices to deauth and grab a handshake from connected to that network.

also are you rotating channels? or stuck on 1 channel...?

Code watch -n 1 'iw dev wlx00c0cab72e58 info | grep channel'

Try this script....

```
Code Code
#!/bin/bash
IFACE="wlx00c0cab72e58"

echo "[+] Resetting WiFi adapter..."
sudo pkill hcxdumptool 2>/dev/null
sudo pkill wpa_supplicant 2>/dev/null

sudo ip link set $IFACE down

echo "[+] Reloading mt7921u driver..."
sudo modprobe -r mt7921u
sleep 5
sudo modprobe mt7921u
sleep 8

echo "[+] Clearing rfkill..."
sudo rfkill unblock all
sleep 1

CAPTURE="capture_$(date +%Y%m%d_%H%M%S).pcapng"
echo
echo "[+] Starting hcxdumptool"
echo "[+] Saving to: $CAPTURE"
echo

sudo hcxdumptool \
-i $IFACE \
-w $CAPTURE \
--rds=1 \
-F
```

ggzz1 - September 17, 2026, 7:30 pm

(Aug 13, 2026 11:00 AM)Pr0m3th3us Wrote: [\[CITE\]](#) I get handshakes all day on modern PMF routers. I use hcxdumptool. I think your issue may be your using a VM. I dont do that when im doing deauth attacks and grabbing handshakes. Also i use an Alfa AWUS036AXML. Which uses the MediaTek MT7921AUN. But your chipset is fine it does monitor and packet.

I think its down to 2 main issues.

1. your on a vm, and its not setup correctly.
2. there are no devices to deauth and grab a handshake from connected to that network.

also are you rotating channels? or stuck on 1 channel...?

Code watch -n 1 'iw dev wlx00c0cab72e58 info | grep channel'

Try this script....

```
Code Code
#!/bin/bash
IFACE="wlx00c0cab72e58"
```

```
echo "[+] Resetting WiFi adapter..."
sudo pkill hcxdumptool 2>/dev/null
sudo pkill wpa_supplicant 2>/dev/null
```

```
sudo ip link set $IFACE down
```

```
echo "[+] Reloading mt7921u driver..."
sudo modprobe -r mt7921u
sleep 5
sudo modprobe mt7921u
sleep 8
```

```
echo "[+] Clearing rfkill..."
sudo rfkill unblock all
sleep 1
```

```
CAPTURE="capture_$(date +%Y%m%d_%H%M%S).pcapng"
echo
echo "[+] Starting hcxdumptool"
echo "[+] Saving to: $CAPTURE"
echo
```

```
sudo hcxdumptool \
-i $IFACE \
-w $CAPTURE \
--rds=1 \
-F
```

Thanks for the support, boss. I've already captured the hash using native Kali, but unfortunately the wordlists I have on hand are limited and the device's computing power is a bit old. Could I implore you to help me run a wordlist cracking job?