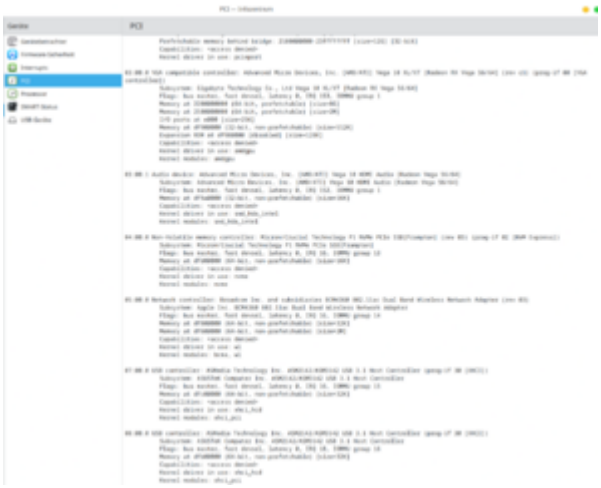
Es tut sich wieder was bei Broadcom WLAN

Beitrag von „DerBeste“ vom 23. Dezember 2025, 12:42

> Zitat von karacho
>
> DerBeste Die Firmware habe ich noch nirgends gefunden. Ich habe so eine PCIe Karte im Rechner. Ist es nicht möglich die Firmware auszulesen und als .bin zu speichern?



> Zitat von Azteca
>
> Würde gerne die Sachen liefern, jedoch hab keine Ahnung wie man das aus der Karte kopiert.

> Zitat von schrup21
>
> Es gibt keine Firmware für BCM4360.
>
> Diese Module werden in Linux mit der SMAC Firmware betankt.
>
> https://wireless.docs.kernel.o…rs/drivers/brcm80211.html

> Code
>
> 1. /lib/firmware/brcm/bcm43xx-0.fw
>
> Apple verwendet eine eigene, proprietäre Firmware, die ist in AirPort_BrcmNIC enthalten (auch die FW für die BCM943602 und BCM94350 ist da integriert).

Hier eine Anleitung wie ihr die Firmware-ROM eines Broadcom-WLAN-Chips mit Nexmon extrahiert

Beispielchip: BCM43602

Ziel: Erzeugung einer originalen "rom.bin" direkt aus dem WLAN-Chip

1. Voraussetzungen

Bevor ihr beginnt, müssen alle folgenden Bedingungen erfüllt sein:

- Betriebssystem: Linux (Ubuntu wird empfohlen)

- Rechte: Root-Zugriff (`sudo`)

- Hardware: Broadcom-WLAN-Chip, der von Nexmon unterstützt wird (z. B. BCM43602)

- Systemstatus: Der WLAN-Chip wird vom System korrekt erkannt

Ohne diese Voraussetzungen ist der Vorgang nicht erfolgreich durchführbar.

2. System vorbereiten

Öffne ein Terminal und aktualisiere dein System:

bash

sudo apt update

sudo apt upgrade -y

Installiere anschließend alle benötigten Werkzeuge:

bash

```
sudo apt install -y git build-essential make gcc bc python3
```

Diese Pakete sind notwendig, um Nexmon zu kompilieren und Patches zu bauen.

3. Nexmon herunterladen

Wechsle in dein Home-Verzeichnis:

bash

```
cd ~
```

Klone das offizielle Nexmon-Repository:

bash

```
git clone https://github.com/seemoo-lab/nexmon.git
```

Wechsle in das Nexmon-Verzeichnis:

bash

```
cd nexmon
```

4. Nexmon-Umgebung einrichten

Initialisiere die Nexmon-Umgebung:

bash

source setup_env.sh

Wichtig:

Dieser Schritt setzt notwendige Umgebungsvariablen. Ohne ihn schlagen alle weiteren Befehle fehl.

5. Passenden Chip auswählen

Navigiere in das Patch-Verzeichnis:

bash

cd patches

Suche den Ordner deines Chips, z. B.:

bash

bcm43602

Wechsle in das Nexmon-Unterverzeichnis des Chips:

bash

cd bcm43602/nexmon

6. ROM-Dump-Patch bauen

Baue das ROM-Dump-Patch:

bash

```
make dump-rom
```

Dabei wird ein kleines Patch-Programm erzeugt, das später den ROM-Inhalt des WLAN-Chips ausliest.

7. WLAN-Interface vorbereiten

Deaktiviere das WLAN-Interface, um Konflikte zu vermeiden:

bash

```
sudo ifconfig wlan0 down
```

Falls dein Interface anders heißt (zB. "wlp2s0"), passe den Namen entsprechend an.

8. ROM-Dump ausführen

Starte nun den ROM-Dump:

bash

sudo make run-dump-rom

Was dabei passiert:

- Der WLAN-Chip wird initialisiert
- Der ROM-Inhalt wird in den RAM gespiegelt
- Die Daten werden ausgelesen
- Der Dump wird in eine Datei geschrieben

Der Vorgang dauert nur wenige Sekunden.

9. Ergebnis prüfen

Nach erfolgreichem Abschluss findest du eine Datei wie:

bash

rom.bin

oder

bash

fw_rom.bin

Prüfe die Dateigröße:

bash

ls -lh rom.bin

Erwartet:

- Größe zwischen 500 KB und 1 MB

Fehlerfall:

- Datei ist leer oder 0 Byte → Dump fehlgeschlagen

10. ROM-Datei sichern

Kopiere die Datei auf den USB-Stick

bash

cp rom.bin ~/firmware_bcm43602_rom.bin

Diese Datei ist nun die Grundlage für die Analyse- oder Patch-Arbeiten.

11. ROM-Datei analysieren (optional)

Zur Analyse der Firmware kannst du "binwalk" verwenden:

bash

sudo apt install -y binwalk

binwalk firmware_bcm43602_rom.bin

Damit lassen sich Code-Bereiche und Strukturen identifizieren – insbesondere relevant für Reverse Engineering.

12. Rechtliche Hinweise

- Die Firmware ist proprietär
- Nutzung ausschließlich zu Forschungs- und privaten Zwecken
- Keine öffentliche Weiterverbreitung !
- Broadcom- und ggf. Apple-Lizenzen gelten weiterhin

Kurzfassung

- Linux vorbereiten
- Nexmon herunterladen und initialisieren
- Broadcom-Chip auswählen
- ROM-Dump-Patch bauen
- ROM aus dem WLAN-Chip auslesen
- "rom.bin" sichern und optional analysieren

Ergebnis:

Eine originale WLAN-Firmware direkt aus der Hardware.

Edit:

Lasst euch aber Zeit. Ich arbeite derzeit an einem anderen Projekt und kann mich erst dann darum kümmern, wenn ich das neue Projekt abgeschlossen habe.