Assignment-4 (50 Marks)

Tasks

We intercepted a sketchy router labeled **“FREE WIFI HERE”** in the wild. Our gut says it’s a trap for unsuspecting users. Crack the case by reverse engineering its firmware (cloned onto your spi flashes) and help us idenitfy the nature of this device.

Answer the following questions to prove that you are a true reversing pro:

- While we were trying to understand what was present on the flash, we extracted and read the contents of the flash into a binary blob with sha256sum `7d530283029f273601b89e4fb2b92f3c078d90a2d3c127f10b8a6e480a74a310`. Check if you read it correctly? **(5 marks)**
- We used our handy tool `binwalk` to find that there were **two files** in the extracted binary blob. But we were unable to use binwalk on those files directly, help us go further in our analysis.
- Report the SHA-256 checksum for the correctly processed firmware based on the `init` code. **(10 marks)**
- Now that you have the correct firmware, what is the CPU **architecture** and **endianness** that the device runs on? **(5 marks)**
- During our testing phase the router gave us a warning that said “the root password was changed”, we are wondering what that could be? Can you help identify what the password for the user **root** was changed to? Clearly explain your approach in the report. **(10 marks)**
- We noticed some malicious activity on the network, find and report the **IP addresses** of these devices along wih their **malicious activity**. **(5 marks)**
- There is a specific device which is trying to gain a remote shell access. Can you identify the **IP address** and **program** that it is trying to execute and the **port number** that it is trying to open? **(5 marks)**
- What actually happens when the malicious user sends these malicious commands, can you trace down the steps of their **execution** and find the **flag** that they might have left behind? **(10 marks)**

General Guidelines

- Please be very careful and accountable of the hardware that has been lent to you for the assignment.
- After reading the contents from the SPI-flash you can set the hardware aside safely or give other teammates a chance to do the same.
- The aim of this assignment is to give students an insight on how embedded devices function, how we can interface with and eventually reverse-engineer them.

Submission Guidelines

In this assignment we expect the following to be submitted :

- A single report that describes your approach for having found the clues with supporting screenshots.
- Mention the name of the team that you shared the hardware with.

Provided Hardware

- CH341A Pro (Image with its pinout)

- SOP8 Connector Clips

- SPI Flash Datasheet

Important Tools

- Binwalk Link
- Flashrom Link
- Other tools installed in the VM