Mirai demonstrates one of the fastest-growing attack vectors in modern times; improperly configured IoT devices. This attack vector is constantly on the rise as more and more IoT devices are being created and deployed around the globe, and is actively being exploited by a wide variety of botnets. Internal IoT devices are also being used for long-term persistence by malicious actors.

Starting with Nmap -sC -Sv 10.10.10.48

A screenshot of a computer program

AI-generated content may be incorrect.

We notice a few open ports but we start with the http one which is completely blank.

I captured the request and response for the website and I found a strange header

A screenshot of a computer program

AI-generated content may be incorrect.

Upon searching the X-pi-hole I found that is a header for pi devices.

I started ferox and searched for directories which led me to the /admin page.

A screenshot of a computer screen

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

Searching for default credential gave me an username and password (pi:rasppberry) which let me login via ssh and find the user flag.

A screenshot of a computer screen

AI-generated content may be incorrect.

For the root flag I’ve first used sudo -l to see what can I run ( I could just sudo su and gain root access).

The root flag wasn’t in it’s usual spot, instead I got a message:

A screenshot of a computer

AI-generated content may be incorrect.

The usb’s are located in /media/ but no luck, someone deleted the root.txt

A screen shot of a computer

AI-generated content may be incorrect.

Usually, the deleted files and such aren’t erased from memory so I could use “mount” to see the path for the raw usb media which in our case is /dev/sdb.

A screen shot of a computer screen

AI-generated content may be incorrect.

I’ve then grepped the “sdb” file and got the flag.

A screenshot of a computer

AI-generated content may be incorrect.