**Walkthrough: Mirai HTB Machine**

This report details the penetration test of the "Mirai" machine, which demonstrates the security risks associated with improperly configured IoT devices. This attack vector is increasingly common due to the proliferation of IoT devices.

**1. Initial Reconnaissance and Service Enumeration**

An Nmap scan was performed on the target IP address, 10.10.10.48. Several open ports were noted, with the HTTP port (likely 80) being the initial point of investigation. The website itself was blank. Capturing the HTTP request and response revealed a peculiar header: X-pi-hole.

A screenshot of a computer program

AI-generated content may be incorrect.

A screenshot of a computer program

AI-generated content may be incorrect.

**2. Gaining a Foothold - Pi-hole and Default Credentials**

Researching the X-pi-hole header indicated its association with Pi-hole devices. feroxbuster was then used to discover directories on the web server, which led to the /admin page.

A search for default Pi-hole credentials yielded pi:raspberry. These credentials allowed successful SSH login to the target machine as the pi user, and the user flag was subsequently found.

A screenshot of a computer screen

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer screen

AI-generated content may be incorrect.

**3. Privilege Escalation - sudo and Deleted File Recovery**

To obtain the root flag, sudo -l was executed to check sudo privileges. It was discovered that the pi user could execute sudo su, effectively granting root access.

However, the root flag was not in its usual location. A message indicated that it might be on a USB drive. The /media/ directory, where USBs are typically mounted, was checked, but the root.txt file was not present, suggesting it had been deleted.

Knowing that deleted files often persist in memory, the mount command was used to identify the raw path of the USB media, which was /dev/sdb. Finally, the sdb file was grepped to recover the contents of the root flag.

A screenshot of a computer

AI-generated content may be incorrect.

A screen shot of a computer

AI-generated content may be incorrect.

A screen shot of a computer screen

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.