

Penetration Testing On Consumers Internet of Things (IoT) Devices

Andom Fekadu Alemayo
P151438
andomina70@gmail.com

1. Introduction

Nowadays, the IoT devices became an integral part of almost every aspect of our modern life including, health, business, education, industries and so on. The type of IoT devices commonly used in our homes are known as consumers IoT devices. However, many scholar believe that these gadgets are not secure and just like the low hanging fruit, the number and type of cyber attacks towards these devices are constantly rising. Based on the report released in 2020, 57% of IoT devices are susceptible to cyber attacks[1] [2].

This research focuses on investigating the security flaws on consumers IoT devices through the penetration testing methods.

2. Aim & Objectives

Aim:

To Perform Penetration testing on Consumers Internet of Things (IoT) devices.

Objectives:

- I. To conduct background research and literature reviews in the subject area.
- II. Adopt the necessary penetration testing steps.
- III. To Ethically attempt to penetrate the security system of the devices under study.
- IV. To Make use of open sources penetration testing tools such as Kali Linux.
- V. To analyse and evaluate the experimental results, compare the obtained results with result from another studies .

3. Methodology

- Research Philosophy – **Positivism**
- Research Approach – **Deductive**
- Research Strategy – **Experiment**
- Time Horizon – **Cross-Sectional**
- Data Collection – **Observational**

4.Design and Implementation

The network topology below was designed to mimic the real-world household IoT network ecosystem . During setup of the test, all the smart gadgets were connected to the Access Point (AP). The wireless AP is a network devices that connects all the IoT devices together to create a wireless network. The wireless communication between the devices was facilitated through the Wi-Fi communication protocol which implements the Wi-Fi Protected Access (WPA) security protocol. The following IoT devices were used during the implementation

- Access Point device branded as (WAVLIN).
- TCP Smart Light Bulb.
- S8 Android phone.
- Indoor IP Camera branded as (GENBOLT).
- Galaxy Tablet A .
- Laptop device.

The Kali Linux platform was installed in a virtual box on the tester’s machine, and it was connected to the same network as the victim’s devices using the USB wireless network adapter.

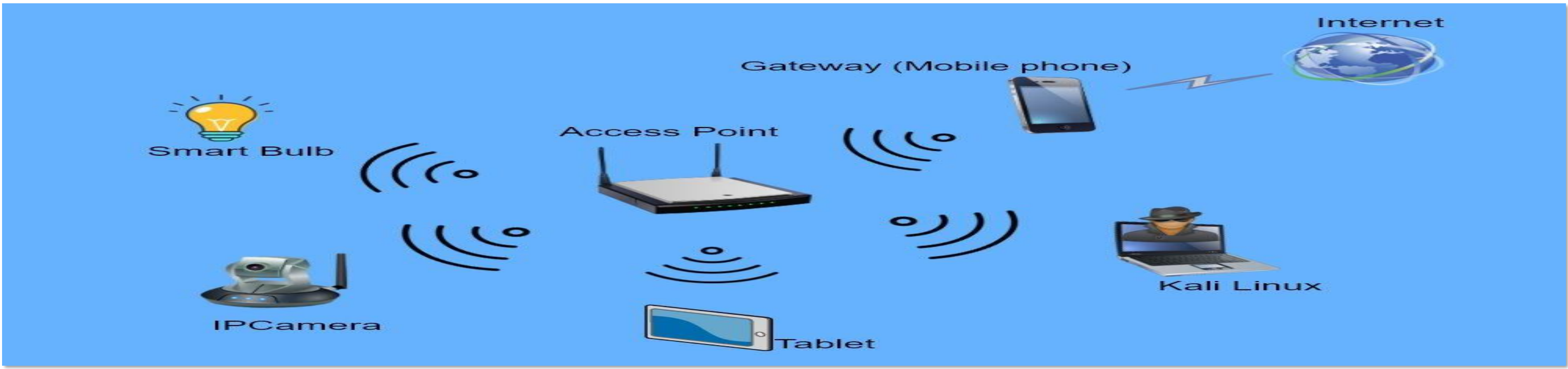


Figure1: IoT Network Topology

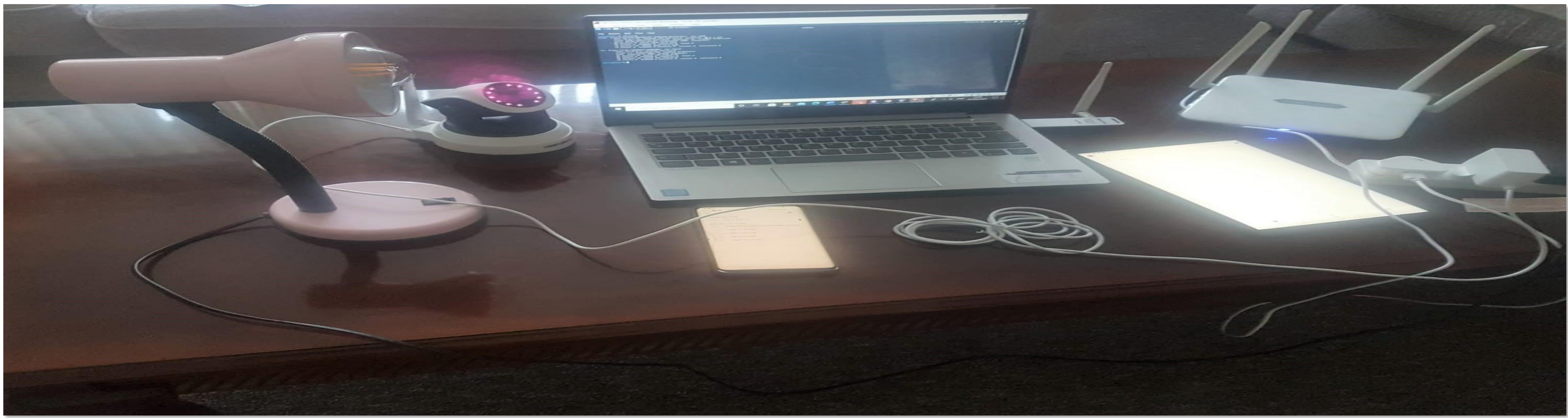


Figure :2 Actual Design Implementation

5. Testing

The testing process was performed on the bases of the relevant penetration testing method such as planning, information gathering, discovery and attacking .

Planning: Provides insight about the scope, resources and approach to be used.

Information gathering : Conducted through Nmap and Kismet tools.

Discovery: performed using Nmap Script Engine (NSE).

Attacking and gaining access: Through three types of attacks namely, Denial of Service (DoS), Man-In The Middle (MITM) and the Password cracking attack using Dictionary attack .

6. Results

The result obtained from the testing section of this project outlines the following vulnerabilities

- Open port (port80).
- Running outdated Operating system.
- Insecure communication services (HTTP).
- Use of common or easily guessable credentials.

7. Conclusion

Overall the project was successful all the objective of the project are met.

- The relevant penetration testing methodologies were adopted.
- The author ethically attempted to penetrate the security system of the consumers IoT devices.
- Relevant open-source tool are used.
- The conclusion and recommendations are drawn.
- Future work was Identified.

8. References

- [1] J. S. Kumar and D. R. Patel, “A Survey on Internet of Things: Security and Privacy Issues,” 2014.
- [2] “IoT devices more at risk of cyber attack than ever - report,” 17-Mar-2020. [Online]. Available: <https://securitybrief.com.au/story/iot-devices-more-at-risk-of-cyber-attack-than-ever-report>. [Accessed: 04-May-2021].