Grenze International Journal of Engineering and Technology, June Issue

A Comprehensive Survey on IoT Infrastructure Vulnerability Analysis

Nikhil S Damle[1], Avantika V. Rewtani[2], Sanskruti A. Zade[3] and Gauri Damle[4]
[1-3]Department of Electronics Engineering, Shri Ramdeobaba College of Engineering and Management, Nagpur, Maharashtra India
Email: {rewtaniav, zadesa}@rknec.edu, nikhil.csio22a@ascir.res.in
[4]Ph-D Scholar CSIR-CSIO, Chandigarh India
Email: damlens@rknec.edu

***Abstract*— The Internet of Things (IoT) is notable and well-liked in human life due to the quick development and alterations of current technology and superior study. Due to the vast network of "Things," several technical and application obstacles are having trouble interacting with one another. In order to accomplish certain goals, the IoT network consists of items that are combined with hardware, software, sensors, networking, and other devices. Maintaining data security on the shared information is a crucial issue that cannot be disregarded given that the shared information comprises a significant amount of private information. Security is essential for the functioning of IoT, which is essential for the success of IoT, for both physical devices and service applications. This essay explores the issues of Television security from a certain angle**

***Index Terms*— Security, Internet of Things (IoT), Network, Testing, Exploitation**

I. INTRODUCTION

We are requesting that you follow these guidelines as closely as possible. We live in an era where various things around the world are connected to the Internet. These objects are uniquely identifiable and can be sensed, manipulated, and communicated without human intervention. IoT security is protection applied or provided to IoT devices. This security is active protection of the network to which the sensors, actuators or devices are connected. Vulnerability management describes the ongoing process of identifying, classifying, and eliminating security gaps. Each step in this process is part of an ongoing cycle focused on improving the security of your computer, network, or communications infrastructure. When the term "Internet of Things" was first introduced, the first question was what is a "thing"? Until the last few years, research groups and organizations have tried to clarify his definition of IoT. In IoT, "things" can be defined to refer to physical or virtual objects that are connected to the Internet and can communicate with human users or other objects.[1] Along with the development of IoT, while existing problems have become more serious, new security problems have arisen.

The main reason is the heterogeneity and extent of the objects. Influencing factors can be further divided into two categories:

Diversity of things and communication of things. Since each category presents different security issues, they are divided into two categories. First, security problems in things are caused by vulnerabilities created by careless program design. This creates an opportunity for malware and backdoors to be installed. Due to the heterogeneity

Grenze ID: 01.GIJET.10.2.217_1

and scale of things in IoT, such security issues are more complex than the ones we face today.

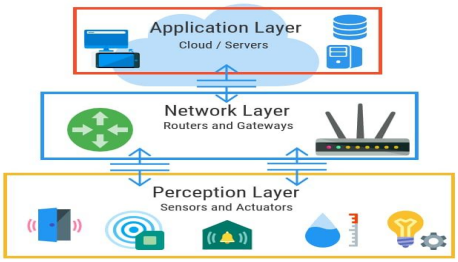

Fig. 1 Layers in IoT Infrastructure

All challenges to IoT systems should be safe, controllable, and confidential to smart users only if they are built securely. The general architecture of IoT systems is divided into three layers 1.) Physical Layer, also called Perception Layer, 2.) Network Layer, 3.) Application Layer. Various technologies are involved in the development process, and the smart and intelligent application of IoT connected devices contributes both personal and economic benefits to society. This document described the different layers of an IoT system and the IoT system's protocol stack, security challenges, and vulnerabilities of various underlying technologies. It further discusses IoT security issues and challenges, and also explores different types of attacks on IoT system models that pose privacy concerns in the infrastructure.

Digital technology is widely used in home networks. Originally, home Internet connections were used only to access the World Wide Web. Later, the introduction of triple-play trading and the ability to watch TV and make phone calls over an internet connection provided users with even more services. Movement is intensifying. For example, kitchens will be equipped with smart refrigerators, hospital stays will be shortened with home medical devices, and a growing number of household chores will be supported by various smart automation systems. Many of these smart devices run operating systems and are connected to multiple networks so they can interact and be accessed remotely over the Internet.[2] As a result, the security of such devices has become a serious issue.

From a security perspective, there are two important aspects to consider. First, embedded operating systems, like any other embedded device, can contain vulnerabilities that can be exploited by attackers. Then you can connect your TV to multiple networks simultaneously, allowing an attacker to use your TV as a gateway between those networks. Smart TVs can clearly pose a real security threat to your home network. Therefore, it is important to analyze security and examine protection mechanisms to mitigate associated security risks.

Testing, a term that is defined as an ability to find faults or flaws that may exist in any system or on the system applications, whether mobile or web. Defects or errors that are detected can be recognized in terms of security or functionality. When the tester tests applications that search for exploitable vulnerabilities through cyberattacks on your system, that kind of testing is called Penetration Testing. Penetration testing attempts to breach the application security that developers cannot do.[3] It involves the process of recognizing vulnerabilities using Proprietary and Open-source tools which create a report with possible errors and flaws that can be the reason for vulnerabilities in the applications. The main purpose of Penetration Testing is finding vulnerabilities in an application if there are any, so that it can be shown as a risk that an attacker can perform to exploit and obtain unauthorized access to an application.

Penetration tests usually discover vulnerabilities, ensure your application is safe and error free. The different phases to go through when implementing a vulnerability Assessment and Penetration Tests include:

- Reconnaise
- Scanning
- Maintaining Access
- Analysis

Although sometimes used interchangeably, vulnerability assessment and penetration testing differ from one another in two possible ways.

1) Penetration testing tells or indicates the priority of that flaw, or, to put it another way, tells how big the bug is, whereas vulnerability assessment provides an indication of how big the vulnerability is.

2) Penetration testing is a manual procedure, whereas vulnerability assessment is automated. However, there are some tools that execute the test execution, provide analytical reports, and integrate the results to corroborate the vulnerability discovery. Some of these tools include:

- Nmap (For Vulnerability)
- Acunetix (For Vulnerability)
- Burp Suite (For Penetration Testing)
- Metasploit (For Penetration Testing)

The main purpose of this paper is to investigate experimentally possible attack vectors and identify exploitable vulnerabilities and attack scenarios in practice. The paper states the different types of security issues that can cause a huge problem to the user and also states the ways to check the number of ports that are open and are visible to the public for an application or website.

II. Related Work

According to the author [4] IoT is now a hard-core component of computing technology that connects numerous items, IoT-connected systems, gadgets, and ways of engaging with infrastructures, radio waves, and sensor network technology. IoT reduces the impact on the environment while also making our daily lives much easier and safer through command and control. In the age of smart technology, the majority of people have smartphones, and systems and internet connectivity are widely available, making it considerably simpler and less expensive to interfere with information.

In [5] authors had described the Internet of Things as the combination of two words, "first being internet and second being things," as there was no single definition of the IoT described by the community of users. The best definition of the Internet of Things that could be given is "An open and comprehensive network of intelligent objects that have the capacity to organize automatically, information sharing, data, and resources, reacting and acting in situations and changes within the environment" specific item, and given the size of IoT, the specific architectural design.

While defining some concepts, one must consider the architecture in order to understand how everything interacts to produce the term that is being defined. The European FP7 research project was one of the models that was released as a result of several studies, and it may be regarded as a primary model architecture. In addition, the Internet of Things (IoT) can leverage a variety of technologies, including IP, Wi-Fi, barcodes, and many others. These technologies were originally developed by RFID members. So, it is possible to draw the conclusion that IoT offers a variety of technologies that make today's society more intelligent and mobile. Yet, as IoT has grown in popularity, no specific definitions have been able to be made, no architecture has been defined, and IoT cannot be utilized for security testing or to identify any vulnerabilities. Researchers turned to the subject of penetration testing in order to produce vulnerable free software and get around the main limitation of IoT. The software life cycle model, which focuses on a specific aspect of penetration testing and aids the user in understanding how it works, must be understood by the user in order to fully comprehend the notion of penetration testing.is the product developed. SDLC contains the following parts described as: -

1) Requirements and use cases: The very first phase in the software development life cycle is to gather requirements and determine the use cases that must be addressed while developing a certain product. It is further categorized as

2) Abuse situations, which are unintended use cases or corner instances that must be taken into account when testing or building software.

It basically involves a system and one or more actors interacting completely. The cases must be taken into account in order to prevent complaints or unfavourable reviews from end users.

3) Security requirements: As the title of the topic implies, penetration testing is the form of testing used to identify security flaws in the software; thus, security requirements are the functional security needs of the software that can be directly tested and observed.

4) Design: After the use cases and requirements are decided and the coding process has to start, the software needs to be properly designed. This is mostly done to ensure that the project will proceed with proper flow.

It also defines the order in which a project's risk management, planning, risk analysis, identification, and control processes occur.

5) Test Results: The test plan that was developed before the coding portion is now being conducted, and the outcome is recorded as PASS or FAIL for a specific test case.

6) End user feedback: After testing, if the release is PASSED, it is sent to the end user, whose feedback is eagerly anticipated and valued.[6]

End users typically view penetration testing as the final step in the approval process once application development is complete.

Penetration testing was referred to as the fundamental security act for maintaining the software's security by authors in. [7]
The [8] authors conducted research on the attack net penetration testing method, where penetration uses the attack tree and flaw hypothesis approaches. Today, penetration testing is crucial to the security of web applications since websites are so important to our daily lives that they must be secure and free of flaws. As meeting deadlines is their first goal, developers cannot consider use cases related to security while working on a project. When it comes to security, testers step in and test the program in a way that regular developers can't. The main function of a penetration tester is to advise developers on how to fix vulnerabilities. These flaws can be found using various security testing tools, such as Burp Suite [22], Selenium [24], and many others, which produce a pen testing report after running the application with the severity of each flaw stated with it. The developer then uses this report to fix the flaws. These tests scan the code for weaknesses such as those caused by XSS injection, HTML code, injection-based issues, and cryptographic injections.

III. METHODOLOGY

We are surrounded by many updated machines, various systems with grand and newly evolving technologies. They provide various facilities, services or any kind of upgradation in our day-to-day life. There are different types of technologies used to develop such systems of a number of different domains. One of those is Internet of Things i.e. IoT. We are nowadays using IoT devices very frequently on a large scale. A lot of highly sensitive information is floated on IoT devices. We can also see that IoT has occupied the space of manual working at most of the places. But, are they secure enough? Are they trustworthy enough to transfer and analyse the information or data? Moreover, IoT devices bring an additional level of complexity to the whole information system. So, are these complex systems able to maintain the originality and authenticity of data as it is? Most of the systems consist of a multitude of devices and endpoints. In most of the cases, traditional cyber security methods are applied to base levels. Are those methods reliable enough to keep the data protected?
To find answers to these questions, we have implemented a three-stage methodology. The three stages include the complete study and analysis regarding the three important and basic layers of IoT infrastructure. Whichever the model and protocols may be, the IoT infrastructure is bound to be based on these three layers. These are the main three layers of IoT infrastructure known as Application layer, Network layer and Perception layer. The study is completely divided into these three layers because whatever issues or vulnerabilities detected are going to belong to one of these layers for sure.
Application Layer: The application layer basically states all the applications that use IoT technology or in which IoT has been deployed. It is accountable for giving the applications the services. Because services are dependent on the data gathered by sensors, they may differ for each application. Security is one of several challenges at the application layer, where it is crucial. IoT, in particular, offers numerous hazards and weaknesses from both the inside and the outside when used to create a smart house. One of the key challenges in implementing robust security in an IoT-based smart house is that the gadgets used in smart homes have poor computing power and a low memory capacity. low amount of storage. The major issues found in this layer can be predicted as related to key agreement or privacy protection issues.
Network Layer: This particular layer can also be termed as Transmission layer. It serves as a link between the application layer and the perception layer. Via sensors, it transports and transmits the data gathered from real objects. Both wireless and wired technologies can be used as the transmission medium. It also assumes responsibilities for interconnecting networks, network devices, and smart things. Hence, there are very high chances that attackers can easily attack it as it is sensitive to attackers. It has prominent security issues regarding integrity and authentication of information that is being transported in the network. The major issues regarding this layer are found related to identity authentication and encryption mechanisms.
Perception Layer: It is also known as a sensor layer. It has the responsibility to identify things and collect information from them. The sensors are selected based on the needs of the applications. These sensors can gather data regarding position, changes in the atmosphere, the environment, motion, vibration, etc. But attackers who want to use them to replace the sensor with their own are primarily after them. So therefore, we can conclude that sensors are the main source of the major threats. Protection of sensor data concerns are closely related to this layer of the IoT.
Penetration Testing Tool are used as a part of a penetration test to automate certain tasks, improve efficiency and discover issues that might be difficult to find using manual analysis techniques alone. Different approaches can be taken when choosing what tool sets can be used for performing individual phases of the penetration test. There are

plenty of tools and toolsets for penetration testing and can be used for testing various types of products and conducting diverse types of attacks [9]. These tools are connected together under various categories that are based on the function which they perform. A method in which a machine is scanned for open ports that are Transmission Control Protocol (TCP)/Universal Datagram Protocol (UDP) ports is known as Port Scanning.
The practice of locating system vulnerabilities before they may be exploited by someone else trying to harm the network is known as vulnerability analysis. This is a proactive method in which the vulnerability is identified and addressed appropriately before anyone is made aware of it [10].
Vulnerability Exploitation is something that requires special skills and techniques to launch an attack on a target system. Experienced penetration testers can use their skills to launch attacks on the system [11]. Generally, machines are connected to a network and run many services that use TCP or UDP ports for communication with each other. The total number of defined ports on a computer are 65536 ports. These ports are categorized into three large ranges:

- Well known ports (0–1023)
- Registered ports (1024–49 151)
- Dynamic and/or private ports (49 152–65 535)

There are five main reasons why there is a need for penetration testing tools. Those are stated below:

- It saves time and effort
- Gives accurate results
- Has advanced analysis
- It is capable of gathering bulk data
- Automate manual tasks

Fig. 2 Penetration Testing Tool

Each module in Penetration Testing has a different Processing time. The table for the same is shown below:

TABLE NO. I AVERAGE PROCESSING TIME FOR EACH MODULE

Penetration Testing Module	Average Processing Time (seconds)
Information Gathering	132.25
Password Attacking	390.82
Wi-Fi Attacking	45.26
Bluetooth Analyzing	16.56
Web Scanning	389.20
Web Attacking	34.99
Total Processing Time	**1099.08**

NMAP - Port Scanning Tool Overview

A free and open-source tool for network exploration and security audits is called Nmap ("Network Mapper"). It is useful for duties like managing service, upgrading schedules, inventory of the network, and uptime of the host or service, according to several systems and network managers. To identify which hosts are present on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, which packet filters/firewalls are in use, and a large number of other characteristics, Nmap employs novel techniques that use raw IP packets. It works well against single hosts but was made to quickly scan vast networks[12]. Nmap is available in console and graphical forms, and it runs on all popular computer operating systems.
Eight criteria were used to evaluate the four tools. The criteria are listed in section A. The actual assessment is presented in Section B utilizing tables and graphs.

A. Evaluation Criteria

Number of ports scanned: This option indicates how many of the tool's 65535 ports were really examined.

- Quantity of open ports discovered – This option lists the quantity of open ports that the utility has discovered.
- Available scan types - This option lists the several types of scans that are available:
- 1) TCP SYN scan,
- 2) UDP scan.
- Scan time: The seconds needed for the tool to complete the scan are listed in this parameter.
- OS and service version detection – This parameter indicates whether the scanner can identify the operating system version of the host(s) under scan.
- Type of interface – This option lists the various interface types that the tool offers.

Platform support is a parameter that specifies the platforms on which the tools can be used.

B. Evaluation Procedure

The four tools in question are contrasted using the aforementioned standards. When new tools are added, the same strategy will be applied. Each table had four criteria, and the criteria were split across the two tables. Some cells offer yes/no answers, while others contain values based on the criteria used.

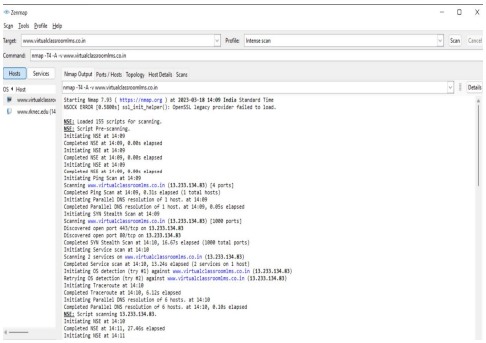

Fig. 3 Configuration on Nmap

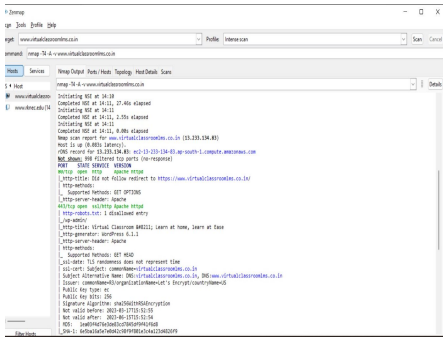

Fig. 4 Configuration on Nmap

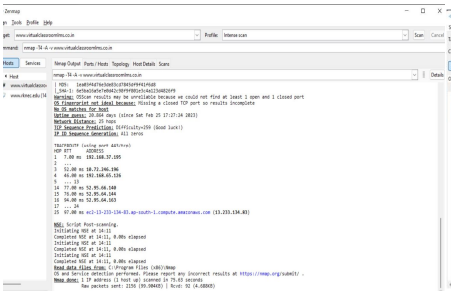

Fig. 5 Configuration on Nmap

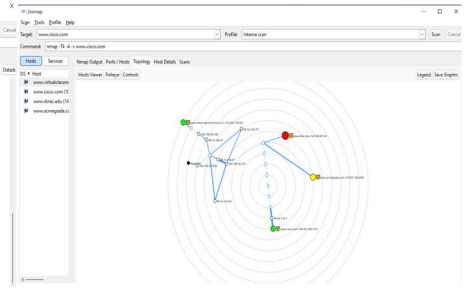

Fig. 6 Demonstration on nmap

IV. CONCLUSION

This appears to be the first attempt of its sort in gathering and combining data on penetration testing in the IoT space. As an extension of current work, in the future, the work for how the open ports is exploited and how this kind of exploitation can be ended will be carried out. Different Penetration Testing tools will be used to check the flaws and errors in an application or software so that the vulnerability issues in that application or software can be reduced.

REFERENCES

[1] R. Johari, I. Kaur, R. Tripathi and K. Gupta, "Penetration Testing in IoT Network," 2020 5th International Conference on Computing, Communication and Security (ICCCS), Patna, India, 2021, pp. 1-7, doi: 10.1109/ICCCS49678.2020 .9276853

[2] Madakam, S., Ramaswamy, R. and Tripathi, S. Internet of Things (IoT): A literature review. Journal of Computer and Communications 3(05), p.164., 2020

[3] McDermott, J.P. Attack net penetration testing. In NSPW (pp. 15-21)., September 2020

[4] Mainka, C., Somorovsky, J. and Schwenk, J. Penetration testing tool for web services security. In 2012 IEEE Eighth World Congress on Services (pp. 163-170). IEEE.
[5] S. Karnouskos, P. J. Marrn, G. Fortino, L. Mottola, and J. R. Martinez de Dios, "Applications and Markets for Cooperating Objects. Springer Briefs in Electrical and Computer Engineering," Springer, 2020, pp. i-xiv, 1-120.
[6] Catarinucci, L., Donno, D. d., Mainetti, L., Palano, L., Pa trono, L., Stefanizzi, M. L., and Tarricone, L. (2021). An iot-aware architecture for smart healthcare systems.
[7] Tsiaras C, Hobi L, Hofstetter F, Liniger S, Stiller B. Park IT smart: Minimization of cruising for parking. 24th International Conference on Computer Communications and Networks (ICCCN); University of Zurich, Switzerland. 2021. p. 1-8.
[8] Nicola Dragoni, Alberto Giaretta, Manuel Mazzara, The Internet of Hackable Things, International Conference in Software Engineering for Defence Applications 2019.
[9] Xiao Nie, Xiong Zhong,Security In the Internet of Things Based on RFID: Issues and Current Countermeasures, Proceedings of the 2nd International Conference on Computer Science and Electronics Engineering (ICCSEE) , March 2019.
[10] Mishra D., Gunasekaran A., Childe S.J., Papadopoulos T., Dubey R., Wamba S. Vision, applications and future challenges of Internet of Things: A bibliometric study of recent literature. Ind. Manag.
[11] Islam S.R., Kwak D., Kabir M.H., Hossain M., Kwak K.S. The Internet of things for health care: A comprehensive survey. IEEE Access. 2015;3:678–708. doi: 10.1109/ACCESS.2015.2437951.
[12] 2020 Unit 42 IoT Threat Report
[13] Giuliano, R., Mazzenga, F., Neri, A., Vegni, A.M.: Security access protocols in iot capillary networks. Internet Things 4(3), 645–657
[14] https://www.opensourceforu.com/2019/06/ basics-vulnerability-assessment-penetration-testing/
[15] S. Haller, S. Karnouskos, and C. Schroth, "The Internet of Things in an Enterprise Context," in Future Internet – FIS 2020 Lecture Notes in Computer Science Vol. 5468, pp 14-28.
[16] Kaushik, M. and Ojha, G. Attack penetration system for SQL injection. International journal of advanced computer research, 4(2), p.724.
[17] Stiawan, D., Idris, M.Y., Abdullah, A.H., Aljaber, F. and Budiarto, R. Cyber-Attack Penetration Test and Vulnerability Analysis. International Journal of Online Engineering, 13(1)., 2020.
[18] Stiawan, D., Idris, M.Y.B., Abdullah, A.H., AlQurashi, M. and Budiarto, R. Penetration Testing and Mitigation of Windows Server Vulnerabilities. IJ Network Security, 18(3), pp.501-513., 2020.
[19] D. Stiawan, M. Y. Idris, and A. H. Abdullah Penetration testing and network auditing: Linux Journal of Information Processing Systems, vol. 11, pp. 104115
[20] Gigli, M. and Koo, S.G. Internet of Things: Services and Applications Categorization. Advances in Internet of Things, 1, 27-31.
[21] Fisher, D.K., Fletcher, R.S. and Anapalli, S.S. (2020) Evolving Open-Source Technologies Offer Options for Remote Sensing and Monitoring in Agriculture. Advances in Internet of Things, 10, 1-10.
[22] Evans, D. The Internet of Everything: How More Relevant and Valuable Connections Will Change the World. Cisco Internet Business Solutions Group (IBSG), Cisco Systems, Inc., San Jose, 1-9.
[23] Prehofer, C. and Chiarabini, L. From Internet of Things Mashups to Model-Based Development. 2015 IEEE 39th Annual Computer Software and Applications Conference, Vol. 3, 499-504.