

T.C.
BAHCESEHIR UNIVERSITY
GRADUATE SCHOOL OF EDUCATION
THE DEPARTMENT OF CYBER SECURITY

**RATIONALIZATION AND PENETRATION TESTING
OUTCOME ON IOT DEVICES (APS) USING THE “ETSI EN 303
645” STANDARD**

MASTER’S THESIS

YASSINE BOUMIZA

THESIS ADVISOR
Assoc. Prof. Okan Yaşar

ISTANBUL 2023

T.C.

BAHÇEŞEHİR UNIVERSITY

GRADUATE SCHOOL

...../...../.....

MASTER THESIS APPROVAL FORM

Program Name:	CYBER SECURITY (ENGLISH, THESIS)
Student's Name and Surname:	Yassine BOUMIZA
Name of The Thesis:	RATIONALIZATION AND PENETRATION TESTING OUTCOME ON IOT DEVICES (APS) USING THE “ETSI EN 303 645” STANDARD
Thesis Defense Date	14/06/2023

This thesis has been approved by the Graduate School which has fulfilled the necessary conditions as Master thesis.

.....

Institute Director

This thesis was read by us, quality and content as a master's thesis has been seen and accepted as sufficient.

	Title, Name	Signature
Thesis Advisor:	Mr. Okan Yaşar	
2. Member:	Mrs. Burcak VATANSEVER	
3. Member:	Mr. Mustafa Sundu	



I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Name, Surname: BOUMIZA Yassine

Signature :

ABSTRACT

RATIONALIZATION AND PENETRATION TESTING OUTCOME ON IOT DEVICES (APS) USING THE “ETSI EN 303 645” STANDARD

BOUMIZA Yassine

Cyber Security Master’s program

Thesis Advisor: Assoc. Prof. Okan Yaşar

June 2023, 82 pages

More and more devices in homes are connected to the internet, the cyber security of the IOT becomes more important and raises more concerns. People entrust their personal data to an increasing number of online devices and services. Products have traditionally been offline are now connected and need to be protected from cyber threats. With these aspects in mind, in the last year there was an intense focus on developing efficient standards aimed at addressing the security of consumer IOT products.

For that, a security assessment is required to acquire and overview of one’s security and identify major gaps.

The aim of this thesis is to evaluate the security level of an APS device (Advanced people sensor device) by performing penetration tests which will result in knowing what are the major gaps that the developers skipped that are mentioned in the standard then suggesting what should be changed in the device to abide by the minimum-security requirements of the mentioned standard. And finally Proposing an upgrade for the standard making it more up to date with the current most used vulnerabilities.

Keywords: IOT, Cybersecurity, Penetration testing, security

My academic journey has been made possible by the unwavering support and encouragement of my parents ABDELAZIZ Boumiza and Dalila Souilm, and for this, I am truly grateful. Their love, guidance, and sacrifices have been the cornerstone of my success. Additionally, I wish to express my appreciation to my family members for their continuous encouragement and support.

I also owe a debt of gratitude to my teachers and supervisors whose invaluable guidance, mentorship, and patience have been instrumental in the completion of this thesis. Without their expertise and encouragement, this accomplishment would not have been possible.

Finally, I want to thank my friends whose constant support, understanding, and motivation have been a source of strength and inspiration throughout this journey. I am fortunate to have such a wonderful group of people in my life, and I am grateful for their unwavering friendship and camaraderie.

ACKNOWLEDGMENTS

I wish to express my deepest gratitude to my supervisor Assoc. Prof. Okan Yaşar for his guidance, advice, criticism, encouragements, and insight throughout the research.

I would also like to thank my parents again, ABDELAZIZ BOUMIZA and Dalila SOUILEM, for their great support throughout their life. Without their understanding, and continuous support, I could have never been able to aspire for this level of education and complete this study.



Table of Contents

ETHICAL CONDUCT	iii
ABSTRACT	iv
ACKNOWLEDGMENTS.....	vi
LIST OF TABLES.....	ix
List of Figures.....	x
Introduction	1
1.1 Necessity Of Security for IOT Devices:.....	3
1.2 Objectives :	4
1.3 Scope And Limitations :	4
1.4 Work Methodology	4
2 Literature Review	6
2.1 What are the security issues in IOT devices:	7
2.2 Security analysis for industrial and consumer IOT devices	9
2.3 IOT security techniques using machine learning :	10
2.4 Automation of Penetration testing on IOT devices:.....	12
2.5 Penetration testing tool PENTOS	14
2.6 Example penetration test on intrusion detection system :	16
3. Internet Of Things (IOT)	20
3.1 What Is IOT:	20
3.2 Previous Issues With IOT :	21
3.3 IOT OWASP Top 10 :	22
3.4 Standard Life Cycle :	24
3.5 Types Of Standards :	26
3.6 ETSI EN 303 365 Standard :	28
3.7 Technical Security Requirments:	30
3.8 Activity Diagrams For ETSI EN 303 365:	32
3.8.1 standard activity diagram.	33
3.8.2 attack surfaces.	35
3.8.3 software integrity.	36
3.8.4 personal data security.....	37
3.8.5 valid input.....	39
3.8.6 conclusion.....	40
4 : Penetration Testing Methodology	41
4.1 Types Of Penetration Testing	41

4.2	Penetration Testing Phases	43
5:	APS penetration testing and ETSI EN 303 645 implementation	46
5.1	What Advanced People Sensor Device We Are Testing On :	46
5.2	APS Penetration Testing :	46
5.2.1	information gathering.....	46
	VPN.	47
5.2.1.1	website technologies, version and flaws.....	47
5.2.1.2	APS device client side web interface.	48
5.2.2	Burpsuite target discovering.....	54
5.2.3	nmap scan.	54
5.2.4	XSS vulnerability testing.	56
5.2.5	enumeration results.	57
5.3	Exploitation.....	58
5.3.1	Bruteforcing.....	58
5.3.2	cross site scripting vulnerability (XSS).	61
5.3.3	DDOS attacks.	62
5.4	Implementation of ETSI EN 303 645 standard	64
5.4.1	evaluation of the APS according to the standard.....	64
5.4.2	result.....	70
5.4.3	Recommendation for enhancement of the APS device according to the ETSI EN 303 645.	71
5.4.4	conclusion.....	73
5.5	Enhancement of ETSI EN 303 645 standard	73
	6: Conclusion and recommendations	76
	7: References	79
	8: Webography	82

LIST OF TABLES

Table 1 : Table of implementation of the standard.....	70
Table 2 : Device enhancement using the standard.....	72



List of Figures

Figure 1 : IOT top 10 risks pie chart.....	24
Figure 2 : Standard life cycle graph.....	25
Figure 3 : Chronological order of user standards for IOT	28
Figure 4 : Activity diagram example	32
Figure 5 : ETSI EN 303 645 Activity Diagram standard.....	33
Figure 6 : Attack surfaces diagram.....	35
Figure 7 : Software integrity diagram.....	36
Figure 8 : Personal data security diagram	37
Figure 9 : valid input diagram	39
Figure 10 : Percentage of use of penetration testing methods pie chart	42
Figure 11 . APS counting device HELLA Aglaia	46
Figure 12 : How a VPN works	47
Figure 13 : Technology used to create the APS interface Website	48
Figure 14 : Login Page.....	48
Figure 15 : Web interface menu	49
Figure 16 : Home page / 1st page.....	49
Figure 17 : Camera positioning menu.....	50
Figure 18 : Counting menu.....	50
Figure 19 : Zone Ocuupancy Setup menu.....	51
Figure 20 : Data recording menu	51
Figure 21 : Network communication settings menu	51
Figure 22 : System settings menu.....	52
Figure 23 : Service Tools menu.....	52
Figure 24 : Diagnostics and Test images menu.....	52
Figure 25 : About menu	53
Figure 26 : User management menu	53
Figure 27 : Burpsuite	54
Figure 28 : Using Nmap on Kali terminal.....	55
Figure 29 : Result / Open ports found.....	55
Figure 30 : Looking for possible vulnerabilities.	55
Figure 31 : Result of the vulnerability scan.	56
Figure 32 : Request interception.....	56

Figure 33 : XSS payload injection.....	57
Figure 34 : Verification for the request acceptance.....	57
Figure 35 : Selecting payload and attack type.....	58
Figure 36 : Choosing the username word list.....	59
Figure 37 : Chossing the password word list	59
Figure 38 : Attack results	60
Figure 39 : XSS alert.....	61
Figure 40 : Finding the XSS script	61
Figure 41 : Alert pops-up	62
Figure 42 : DDOS attack command.....	62
Figure 43 : Starting the DDOS attack.....	63
Figure 44 : DDOS attack result	63

Introduction

Cybersecurity is a critical aspect of our digital lives, and with the rapid growth of the Internet of Things (IoT), it has become even more vital. IoT refers to the interconnectivity of physical devices, vehicles, buildings, and other objects that are equipped with sensors and internet connectivity. These connected devices have the potential to collect and exchange data, creating new opportunities for innovation and efficiency in our daily lives, from smart homes to healthcare and transportation. However, the increasing interconnectivity of these devices also presents new security risks that must be addressed.

IoT devices are often vulnerable to hacking, malware, and other cyber-attacks due to their limited processing power and memory. This makes it challenging to implement strong security measures on these devices, which creates a large attack surface for potential security breaches. As a result, sensitive data and personal information can be compromised, posing a threat to the safety and privacy of individuals.

To mitigate these security risks, it is necessary to implement safety measures to secure IoT devices. This includes using secure protocols for communication, updating software and firmware regularly, using strong passwords, and ensuring that devices are properly configured. Companies producing IoT devices must also adopt security by design principles and embed security features into their products from the outset. This will not only enhance the security of IoT devices but also increase consumer confidence in the technology and encourage wider adoption.

In addition to these measures, it is essential to establish a standard that serves as a baseline for security in the IoT ecosystem. This standard should provide guidelines for the design, development, and deployment of secure IoT devices, as well as a framework for testing and evaluating the security of these devices. The standard should be developed by a consortium of stakeholders, including IoT device manufacturers, security experts, and government agencies, to ensure that it is comprehensive and relevant.

A standard for IoT security would not only help to address the security risks of IoT devices but also create a more secure and trustworthy IoT ecosystem. This, in turn,

will increase consumer confidence in the technology and encourage wider adoption of IoT devices, driving innovation and economic growth.

In conclusion, cybersecurity is a critical aspect of our digital lives, and with the rapid growth of the IoT, it is more important than ever to address the security risks associated with these connected devices. By implementing safety measures, adopting security by design principles, and establishing a standard for IoT security, we can enhance the security of IoT devices, create a more secure and trustworthy IoT ecosystem, and realize the full potential of this technology.



Responding to threats and vulnerabilities is crucial to any system and any IT project, creating a vulnerability management program that blends data science and advanced technology to predict vulnerabilities before it's in the company field and preventing exploitation of existing vulnerabilities is necessary. IOT devices are increasing at a very fast rate and becoming more and more complicated and more importantly more dependent on the network they are in, which in return makes any slight vulnerability a danger to everything connected to the IOT device. It is true that these devices make our life easier and sometimes we they are needed but without the proper care and security, the threat can far surpass the positives of having an IOT device at home or anywhere.

That is why in this project, the main goal is to apply the "ETSI EN 303 645" which is a globally applicable standard for consumer IOT cyber security on an advanced people sensor device to show an example of what should be done to ensure the security of an IOT device.

1.1 Necessity Of Security for IOT Devices:

The world is becoming more and more connected as a result of IOT becoming needed in every aspect of life. The combination of "smart" devices (mobile phones, web application, cloud servers, ...) makes the world feel like a central hub that keeps everything connected to it in the same place.

As more devices are connected to home and work internet, the cyber security is becoming more concerning.

People entrust their personal information and data to different services and devices everyday and products that have traditionally been offline are now connected to the internet and should be able to defend against cyber threats. Last year alone had an intense focus on developing efficient standards that aim to address the security of consumer IOT products.

A security assessment is a measurement of a system, facility, or organization's security apparatus (technology, procedure and people), in other words, the evaluation looks at how security is conceived and implemented and detects flaws and vulnerabilities.

1.2 Objectives :

The objective of this thesis is to find a minimum base security for IOT devices because of the continuous rise of exploits and vulnerabilities abused by hackers. It is necessary to make a standard and make it mandatory for IOT device companies and developers to use because any vulnerability that is common can lead to serious data leak and information theft. In this thesis report we will go over the main aspects of IOT and then introducing a standard called ETSI EN 303 654 to use it to penetrate the vulnerabilities found in this standard on a device as a test then as a future work creating a better standard that complies with the current vulnerabilities and providing a better baseline security for devices.

Method: The method that will be used is performing a penetration test on a specific device chosen then comparing the results found to the standard we chose to see what the developers did right and wrong. After creating the table that will show us the results, we can further improve the standard with the current wave of vulnerabilities and exploits used by cyber criminals.

1.3 Scope And Limitations :

Like mentioned before, the main target of this thesis is to reach a standard that includes all the main and common vulnerabilities used by hackers and attackers to steal data from IOT devices and intrude the networks of victims and keeping it up to date with the new exploits found because there is always the limitation of new and more lethal vulnerabilities found every period of time. The new standard is the baseline aka the minimum of security necessary which is much better than practically no security in the current state of IOT device.

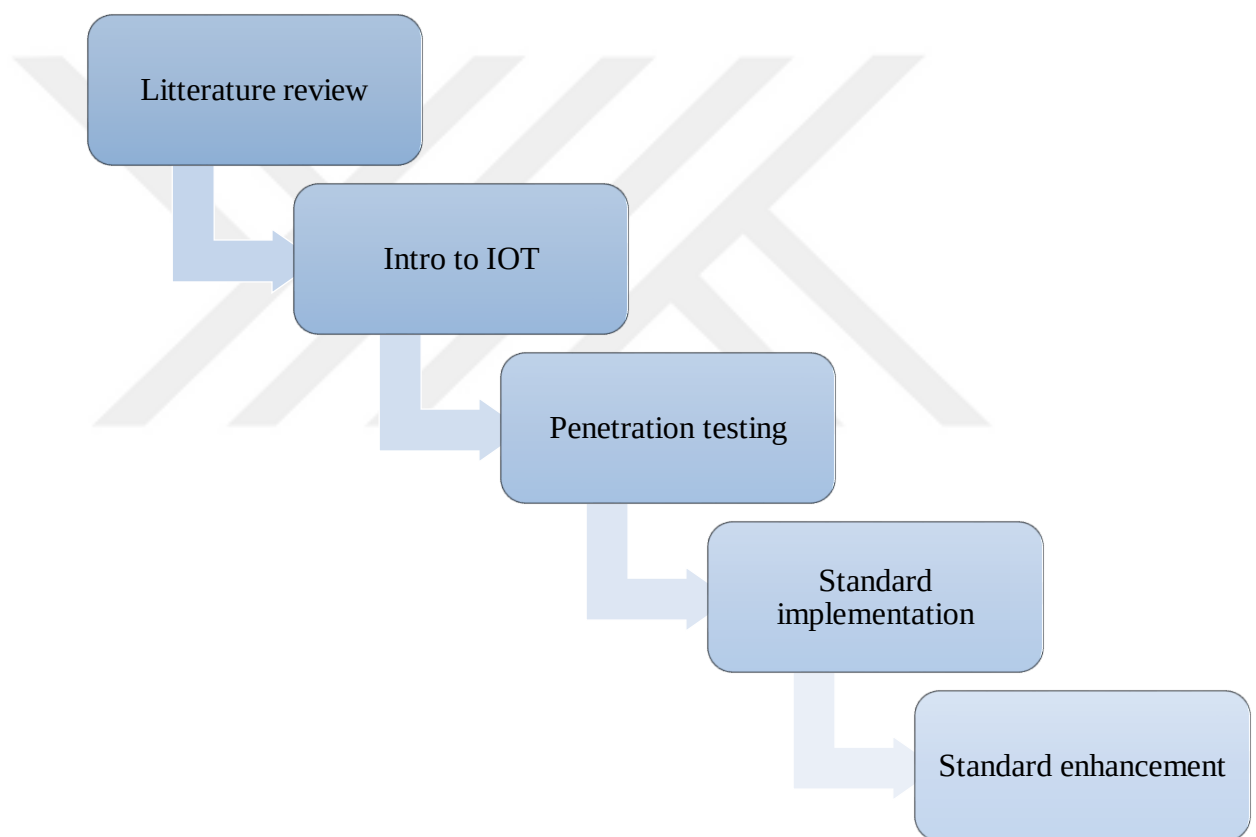
1.4 Work Methodology

For the work methodology, we decided to use the commonly used Waterfall methodology. It is a widely used project management method with a linear approach.

In Waterfall, each stage of the workflow needs to be completed before moving on to the next step. While there are various types of project management methodologies, Waterfall is well suited for projects where the objectives are clearly outlined from the beginning.

This methodology follows a strict linear order where if followed correctly will ensure that anyone using the steps chosen will understand how the project works, and

the order that should be followed. For the first step, we will go over the previous work of authors in the field so we can understand what previous research said about the subject and review previous published works in the field. Second step we will explain in detail what IOT is to further explain any misconception and definitions and to set the stage to the next part where we will introduce the device that we will in step three apply the necessary penetration testing to showcase that IOT devices are vulnerable to attacks and can be exploited. For the fourth step we will compare the device to the standard we chose (ETSI EN 303 645) and then in the fifth and final step we will try and improve the standard to further enhance it and make it up to date.



2 Literature Review

Ever since we started with the IOT era, many companies started developing new and innovative ways of making and creating small devices that have the purpose of making your life easier by doing tasks and giving data directly to the user. Internet of things the collective network of connected devices that facilitates communication between the devices themselves and more importantly the communication of data between the device and the end user. Nowadays we find these devices everywhere, smart homes, smart factories, smart companies and even smart cities. But with this upgrade in technology comes a risk, Hackers and attackers found that IOT devices if not secure well enough provide a unguarded door to your network which they use to access your data and steal all your private and valuable information.

To demonstrate how crucial, it is to secure IOT devices from unwanted attention, we need to look at many aspects of security like the issues and how to deal with them and take a look at some examples of tools and methods used by hackers to see how we can defend against them.

In this review we will be taking a look first at the major security issues in IOT devices to try and locate the main problem with the development of these small machines shown by the two professors from Erbil Polytechnic University Kurdistan Ali and Shavan Askar, and then look at the bigger scope of the problem which is how big these devices have been implemented in household homes and industries using the collective effort of many German researchers mentioning Jacob Wurm, Khoa Haoang, Orlando Arias and many more from the Technical university Darmstadt in Germany. Then we will be looking at ways to fortify the security of the devices using normal methods then machine learning using the articles of Chinese researchers Xiaozhen Lu, Yanyong Zhang and Di Wu which takes us to the final part of this review which is seeing what methods attackers use to bypass the security by taking an examples tool used to pen test called PENTOS and looking at an example of pen testing on an intrusion detection system.

By reading this article we can see the level of protection the average IOT device use and how easy it is to penetrate and how easy your information can be stolen if you are not careful enough, and how necessary it is to use the ETSI EN 365 303 standard as a base line of defence from the device, then moving into suggesting changes to this

standard to keep it up to date with most used exploits and vulnerabilities to make sure the network connected to the device is secure enough. The references shown in this literature review are shown in the order of the review.

2.1 What are the security issues in IOT devices:

The Internet of Things is the most well-liked and useful internet system. It facilitates direct connection between people and objects by connecting to the Internet with various sensors and controls. IoT gadgets have similar architectural designs. Each layer (edge, middleware, and application) in this structure has a unique set of security concerns that must be considered. It is becoming the focus of cyberattacks as IoT devices gain popularity. And these assaults, both at home and abroad, delay operations, expose information, and cause financial harm, halting economic progress and jeopardizing the safety and security of daily activities. (Askar, 2017; Fizi & Askar, 2016; Askar, 2016; Ketu & Askar, 2015)

There is a need to introduce IOT security ideas as IOT-based systems expand. To accomplish this, we must understand the fundamentals of the Internet of Things (IoT) and how to apply it to existing networks (such as wireless sensors and node-based sensor networks). By using these systems, all security concerns and dangers associated with existing communication technologies are, by definition, transferred into the IoT system. (Andrea et al., 2015; Sulaiman & Askar, 2015; Fares & Askar, 2016). Security issues can be categorized into main parts mentioning, confidentiality, integrity, privacy, self-organization and access control.

First starting with confidentiality, Cryptographic algorithms can be used to maintain the confidentiality. Prior to implementation, current modulation methods should be assessed based on the operation, functionality, and criticality of the IoT system (Chowdhury, & Noll, 2011). It illustrates the calibre of study on secrecy and the important problems it raises. It also demonstrates the importance of authenticity and the dependability of the data's theoretical underpinnings (Suo, Wan, Zou, & Liu, 2012). As a hacker can only achieve the same values by placing a fake sensor next to the authorized one, the confidentiality required for sensors is not as crucial as reliability and authenticity (Mendez, Papapanagiotou, & Yang, 2017). However, the key areas where confidentiality is sensitive are contact, storage, identification, and authentication in the context of the IoT. The ability to ensure confidentiality for personal information by ensuring that only users with protected contacts are enabled

is necessary for maintaining confidentiality. Only a user with permission can access the data. A data encryption system can achieve confidentiality if each piece of information is transformed into cipher text and then subjected to a two-step authentication process. Components are only accessible if all required hardware and identity verification are successfully completed during the authentication process, which is immediately accessible to the user. (Swamy, Jadhav, & Kulkarni, 2017). Next aspect is integrity where (Fongen, 2012, Mendez et al 2017) said in the matter that Standard solutions include reading and writing protections as well as authentication techniques. Implementations of passwords that consider security issues, such as randomness and password length errors, frequently protect the data's integrity. Additionally, the resources employed in particular IoT systems do not support conventional cryptography techniques due to the restricted resources available. As for the privacy aspect, Data protection demands self-aware actions from linked machines, security, and resistance to variability, as well as secure cloud storage, management of data, and security standards (Roman, Najera, & Lopez, 2011). Then self-organization, Self-organization enables the IoT framework to carry out the specific function it is designed to perform while offering a framework for resource sharing in a way that can be advantageous to several vertical use cases (Hu & Zhu, 2012). Redundant devices can be simply incorporated into the IoT self-organization architecture to serve as a system crash in any unforeseen event. This will reassign a computer to a different task if one is losing. This self-organizing characteristic can result in the longevity and management of IoT items by enhancing their use, affordability, and capacities. The best network performance, scalable operations, service quality (QoS), scalability, reliable and reactive service delivery, and IoT devices can cooperate to share resources and encourage energy use. Consequently, there will be less of a need for data transfer (Athreya & Tague, 2013). And finally, we have the final aspect which is the major security issue and the most common, access control. In the event of an attack, access control means that the attacker has restricted access to all regions of the device. Computer-based access control structures and network-based access control plans like Microsoft Active Directory are similar. Access to the compromised data is restricted to areas of the network that are authorized by the corporate keys if someone manages to intercept corporate keys and get access to the network (Jurcut et al., 2020).

The term "internet of things" refers to a growing number of gadgets that use the internet. This covers everything from small appliances like lamps to massive gear used

in fields like robotics, sensors, smart traffic lights, and near-intelligent computers. The security of the devices and users is the primary challenge in this field, despite its rapid and extensive growth. This article examines the major problems and solutions in this area because the security flaws pose substantial risks to users' safety and property.

2.2 Security analysis for industrial and consumer IOT devices

IoT devices' fundamental function is to gather, process, and relay data through a communications channel, as well as occasionally control a much bigger machine. The information in question can include things like a person's heartbeat, room temperature, daily routines, and even their location. The ensuing privacy and security concerns that arise are known to manufacturers, however, security in IoT devices is either neglected or treated as an afterthought according to (Jacob Wurm, Khoa Hoang, Orlando Arias, Ahmad-Reza Sadeghi and Yier Jin from the university of central Florida and the university of Darmstadt Germany).

To understand their work better we need to look at the tests they ran on the limitation of IOT device design methodologies where they used attacks to hardware, software and network level of the two IOT devices case studies they used. First device they reviewed is the Hair Smartcare device, it is a device made to operate and read data from multiple sensors put across a user's home, including a smoke alarm, a water leakage sensor, a door-open/close sensor, and a remote power switch. The ZigBee protocol is used to connect these sensors.

The vulnerability study process they used started with a hardware platform investigation of the SmartCare components. A TI AM3352BZCZ60, which is a member of TI's Sitara range of processors, serves as the system's primary processing unit. The chip has an ARM Cortex A8 with NEON extensions as its processor. The CPU is also compatible with Android and Linux operating systems. they discovered traces for UART on the device by looking at the processor's info sheet.

They were able to read serial data from the device via the UART connection and see the SmartCare's boot procedure by configuring the terminal emulator's parameters correctly and attaching a serial-to-USB device. They were able to look through the binary and determine how it handles updates using binary analysis software. The MQTT protocol is used by the device to securely connect to the manufacturer's server over an encrypted channel. According to the

Publisher/Subscriber (P/S) model of the MQTT protocol, a broker receives data from publishers and pushes it to subscribers. With all this information in the hands of ((Jacob Wurm, Khoa Hoang, Orlando Arias, Ahmad-Reza Sadeghi and Yier Jin) they, can alter and manipulate the data they got. Next IOT device they ran tests on is the Itron Centron CL200 Smart Meter, this device's main role is to monitor a customer's energy use and transmit the data it gathers to a nearby meter reader or a nearby substation through an RF channel. The consumer is subsequently charged for the energy they consumed, and this data may also be used to compile statistics on the general energy use. Through their work, they concluded that poorly protected IoT devices are easily vulnerable to remote attacker compromise while being transported and deployed. Simple backdoors to complete device compromise are possible outcomes of these attacks. Industrial devices present a greater risk if they are compromised since important infrastructure may be harmed.

In their study, they were able to alter a smart meter's identity, broadcasting energy use while posing as a different gadget. An attacker has the ability to change how their power use is billed by carrying out this activity. Furthermore, the meter can be adjusted to indicate lower reads because it provides programming and debug interfaces.

They have shown through two case studies that IoT devices used in both commercial and industrial settings are susceptible to IoT-specific assaults. The fact that these devices offer only little security serves as a reminder that security should be taken into account while developing contemporary IoT devices. If we keep using the current IoT device design approach, the influx of IoT devices over the next ten years would result in significant security and privacy risks.

2.3 IOT security techniques using machine learning :

According to (Liang Xiao, Xiaoyue Wan, Xiaozhen Lu, Yanyong Zhang, and Di Wu from multiple Chinese universities) IoT devices typically lack the processing power, memory, radio bandwidth, and battery life necessary to complete computationally demanding and latency-sensitive security tasks, especially when dealing with huge data streams.

However, the majority of security solutions currently in use place a significant computational and communication burden on IoT devices, and outdoor IoT devices

like cheap sensors with weak security defences are typically more open to intrusion than computer systems. Figure 1 illustrates our investigation into safe offloading, malware detection, and IoT authentication and access control. According to the authors, In order to detect identity-based attacks like spoofing and Sybil attacks, traditional authentication approaches are not necessarily appropriate to IoT devices with limited CPU, battery, and memory capabilities. IoT devices can benefit from a minimal level of security protection from PHYlayer authentication techniques that take advantage of the spatial decorrelation of PHY-layer characteristics of radio channels and transmitters, such as the received signal strength indicators (RSSIs), received signal strength (RSS), channel impulse responses (CIRs) of the radio channels, channel state information (CSI), and the MAC address. The PHY-layer feature of the message under test is compared to the record of the claimed transmitter using PHY-layer authentication techniques like construct hypothesis testing. Their authentication accuracy is based on the hypothesis test's test threshold. Due to the radio environment and the unidentified spoofing model, it can be difficult for an IoT device to select an acceptable test level for authentication. The status of the learning is comprised of the false alarm and misdetection rate, according to the IoT device's estimation of the false alarm and misdetection rate of the spoofing detection at the most recent time slot. If the present state and test threshold are known, the future state observed by the IoT device is independent of the earlier states and activities. Therefore, a Markov decision process (MDP) with finite states can be used to represent the test threshold selection in the IoT authentication in the repeated game against spoofing assaults. In order to evaluate the runtime behaviour of the apps in malware detection, IoT devices can use supervised learning techniques.

K-NNs and random forest classifiers are used by an IoT device to generate the malware-detection model in the malware detection strategy developed in [14]. The Internet of Things device filters TCP packets, chooses features from a range of network features, such as frame number and duration, assigns labels to them, and saves these features in a database.

The K-NN-based malware detection classifies network traffic according to the K-NN with the most objects. To differentiate malware, the random forest classifier creates decision trees using tagged network traffic. The authors claim that using the

MalGenome data set and the K-NN-based malware detection and random forest-based schemes, the true positive rates are, respectively, 99.7% and 99.9%.

Assaults including jamming, rogue edge devices, rogue IoT devices, eavesdropping, man-in-the-middle attacks, and clever attacks must be addressed by IoT offloading because they originate from the PHY- or MAC-layer. As a model-free RL technique, Q-learning is simple to use and has low computational complexity. IoT devices, for instance, can choose their offloading data rates to protect themselves from jamming and spoofing assaults by using the Q-learning-based offloading. The Internet of Things device calculates the utility in this time period by analysing the signal-to-interference-plus-noise ratio (SINR) of the received signals, secrecy capacity, offloading latency, and energy consumption of the offloading operation.

IoT authentication, access control, virus detection, and secure offloading are just a few of the learning based IoT security solutions that have been recognized by the article's writers as being particularly effective at protecting the IoT. The implementation of learning-based security solutions in real-world IoT systems faces a number of difficulties.

2.4 Automation of Penetration testing on IOT devices:

In the article made by (Ge Chu and Aexei Lisitia from the university of Liverpool UK) we explore the growing number of attacks received to the IOT device and look at the different layers that need to be secure, mentioning Network layer, Application layer and perception layer, explaining each one and securing them then looking at how they automated this work using the BDI model to achieve it.

First is the network layer, The network layer is used to convey information between the application layer and the perception layer. The network layer integrates a variety of many different types of networks, including the internet, mobile networks, satellites, GSM, GPRS, 3G, 4G, Wi-Fi, and others. These networks are vulnerable to signal interference attacks, DDOS assaults, sniffer attacks, data manipulation attacks, and attacks on data integrity and have similar security flaws to conventional networks. Additionally, mixing different network topologies creates new security issues. Then we have the Application layer where Users can access a wide range of services, including smart grid, intelligent traffic, smart cities, smart homes, intelligent healthcare, and smart buildings, among others. Through a variety of applications on

various technological platforms, such as computers, mobile devices, or smart hardware devices, users can access and administer IoT. Similar to previous layers, the application layer's key security risk is its susceptibility to various types of attacks depending on the IoT scenario, such as buffer overflow, SQL injection, XSS, password assault, and social engineering attack. And finally, the perception layer where these 2 article authors explain it by saying using hardware like RFID, sensors, GPS, and other devices, the perception layer, often referred to as the recognition layer or physical layer, collects data from the physical environment and integrates it into the digital world. The nodes at the perception layer are typically unmanned, light, low power, and have limited computation and storage capabilities. Therefore, standard information security measures are not applied at the perception layer. The attack surfaces and vulnerabilities from the perception network to the nodes increase due to certain security issues. Nodes are vulnerable to attacks like jamming, shielding, cloning, eavesdropping, skimming, and spoofing, for instance.

And then they talked about the main part of their article which is the automation part of the penetration testing. An established set of objectives and strategies are necessary for penetration testing success. The capacity of the BDI agent to automate processes makes it the ideal model for this issue. to interact with the target during penetration testing through perception and action. This section looks at how the BDI paradigm can be used to simulate penetration testing for IoT. The method by which an agent can decide on actions in connection to the target information during penetration testing is described by the BDI model. Three logical elements—belief, desire, and intention—define the BDI. Our model adopts the Jason Interpreter's conventions, which are based on the Procedural Reasoning System (PRS). The BDI agent is defined with the following structure $\langle Ag, B, D, I, P, A, S \rangle$, where:

- Ag is the name of the agent.
- B is the belief set, which represents the target's information and will be updated after actions are taken.
- D is the desire set, which represents all of the agent's options or potential candidate plans for penetration testing; and I is the intention set, which represents the agent's objectives or the plan the agent chooses to execute.
- P stands for a plan set, which consists of accessible plans that each provide details on how to accomplish the objectives.

- A is a collection of activities that the agent is capable of taking.
- S is a set of perceptions that contains information about the environment.

The original purpose of the BDI agent is root privilege in the application layer or controls the IoT, and the default value of privilege is none. Based on the penetration testing for IoT that was discussed in the previous part, they pre-define plans to probe information and launch attacks on three tiers of agents. For instance, the BDI agent can perform password attacks, sniffer attacks, replay attacks, and buffer overflow attacks on three tiers in addition to probing the OS type, port, service, vulnerability information, and network type. The internal askAll and tell actions of Jason enable the simulation experiment. The Jason code is the following:

```
+!probe information: true<-send(agent name, askAll, information type(value)).
+!attack action: true<-send(agent name, tell, attack action).
```

As a summary for their paper, they originally discussed the Internet of Things (IoT) and penetration testing in this paper. Second, they talked about the IoT's security and outlined its security aspects. Thirdly, they presented specific tools and a methodology for conducting penetration tests for the Internet of Things. Then, in order to increase efficiency, they automate it using the BDI model. Finally, they test their work using a simulated experiment in Jason.

2.5 Penetration testing tool PENTOS

Despite the abundance of online penetration testing tools, most of them are difficult for individuals who are not security specialists to use. In this study, they create the PENTOS (Penetration Testing Tool for Internet of Things Devices) penetration testing tool, which gathers the necessary penetration tools for IoT devices. The major goals of PENTOS are to give inexperienced users an automated, simple, step-by-step tutorial on how to do penetration testing and to raise their level of security awareness when deploying IoT devices.

These are the contributions that this work makes. They (Vasaka Visoottiviseth, Phuripat Akarasiriwong, Siravitch Chaiyasart, Siravit Chotivatunyu from Faculty of Information and Communication Technology Mahidol University, Nakhonpathom, Thailand) start by developing a one-stop service for conducting penetration testing that will cover the exploitation of weaknesses in IoT devices in order to come up with a

better solution. The user can check for new vulnerabilities published on the Internet by using their program, which can also automatically retrieve the most recent CVEs and CPEs from the web repositories. Second, based on the Top 10 IoT Vulnerabilities from OWASP, they also offer a function to briefly educate users on how to fix current vulnerabilities and develop security awareness practices for users.

Following the result of their pen testing tool, anyone who has access to this software can use its different modules for information gathering, password attacks, wi-fi attacks, Bluetooth analysis, web scanning and attacking and finally making summarized result for their penetration testing. We will go over them explaining each functionality of them. First, we will be starting by information gathering. This module looks up the IP addresses of all the devices connected to the same WLAN as the PENTOS-running PC. PENTOS will collect the primary data of the chosen device, such as the operating system, its version, services that are running on each port, type, and the CPE version of the device, after our target Raspberry Pi that connects to the same WLAN is chosen. Next is password attacks, The target device's running services are analyzed by this module's process, and then a password attack is launched against these service ports. The information gathering process revealed the target device's opening ports. PENTOS offers SSH/SSH2 attack, FTP assault, Telnet attack, RSH attack, SNMP attack, rexec attack, and rlogin attack for password attacks.

The Information Gathering module learned from the experiment they conducted for the article that the target Raspberry Pi has port number 22 open. The user then launched an SSH assault on the Raspberry Pi. The SSH password, as well as the Raspberry Pi's default username and password, were successfully broken by PENTOS as a result of the experiment.

Third is Wi-Fi attack, this module scans the Wi-Fi that the target IoT device is connected with and analyzes the encryption type of the Wi-Fi whether it uses WEP, WPA or WPA2. This attack has an algorithm to crack the username and password the target access point. We performed an experiment with the target Raspberry Pi that is connected into the same WLAN as PENTOS the screen output of PENTOS is shown in the experiment which found the SSID name “dlink”, the password “012345678” and the “WEP” as the encryption type.

Fourth is Bluetooth analyses, this module checks every Bluetooth version installed on the target IoT device for vulnerabilities in its pairing procedures. PENTOS first establishes a connection with the target IoT device by sniffing its Secure Simple Pairing (SSP) PIN. Next, it searches for the target device's MAC address to determine its Bluetooth version. The system will check the target IoT device's Bluetooth version against the publication "Guide to Bluetooth Security" (NIST SP-800-121), which is advised by the National Institute of Standard and Technology or NIST and display any vulnerabilities.

Fifth is web scanning and attacking where the target Raspberry Pi runs the WordPress CMS as a web server, according to the experiment's findings. PENTOS discovered complete information about WordPress, including plug-in, theme, module, and all user accounts used on the website, after conducting the online attack with CMSscan.

And finally, the reporting feature where the tools creates a reporting menu that can be explained with the following explanation, The findings of the user's penetration testing are summarized on the upper screen. The user did not launch the Wi-Fi assault in the example they used in their experiment. While the web attack was unsuccessful, PENTOS was able to crack the password and attack the Bluetooth connectivity. The user can click on any category to view more information. It analysed the findings and found that the target device is dangerous near the bottom of the main window. PENTOS also examined each category's weaknesses, and users can download all penetration testing findings and suggestions as a PDF file by selecting the button in the bottom right corner.

PENTOS, or Penetration Testing Tools for Internet of Things Devices, attempts to assist users in identifying the weaknesses and potential threats of their IoT devices. The system is created by fusing many technologies, including Linux APIs for penetration testing and Kali Linux. The OWASP Top 10 vulnerabilities of the Internet of Things served as a guide for the development of the tool.

2.6 Example penetration test on intrusion detection system :

The two types of IDS/IPS tools are anomaly-based and signature-based. Anomaly-based techniques compare network traffic behaviour and data deviations to the profile or condition of a statistically normal network. This method has the benefit

of allowing for the detection of previously unidentified attacks. Tools that use signatures can identify and differentiate between typical system states and databases of known traces and patterns that could indicate a penetration attempt. Low error rates are a benefit of signature-based detection, but it is unable to identify attacks of an unknown type. In addition, systems can be categorized as Network Based IDS and Host Based IDS (Host Based IDS) (NIDS). The main objective of this paper is running some tests on the intrusion detection system which is protected by the mentioned IDS/IPS tools to see the level of security provided by this defence system. The writers of this article (Vasaka Visoottiviseth, Phuripat Akarasiriwong, Siravitch Chaiyasart, Siravit Chotivatunyu from Mahidol university, Thailand) will be taking a look at network security, vulnerability scanning tools, penetration testing tools, network attacks and probing attacks.

First is testing the network security, IDS/IPS testing rates to the process of evaluating the effectiveness of the system and its security guidelines. The vulnerability scanning tools and the penetration testing tools are the two categories of security tools for system security verification. toolkits for penetration testing. The tools for vulnerability scanning are designed to find weaknesses in systems and applications and then produce reports on potential dangers. These vulnerabilities are used by the penetration testing tools to break into the network. The techniques should work in concert for the greatest possible IDS/IPS functioning verification.

Next is the vulnerability scanning tools, Tools for vulnerability scanning find possible weaknesses in network devices such as firewalls, routers, switches, servers, and applications. Tools check the information that has been identified against a database of known vulnerabilities. Vulnerability scans can be carried out using this automated method on an unlimited number of devices. There are numerous tools available, including OpenVAS and Nmap. The free source utility Nmap (Network Manager) finds all the devices and services in the network. It works for testing individual devices and is intended for quick scanning of large networks. Nmap is compatible with Windows, Linux, and Mac OS. It supports the terminal, the Zenmap GUI (Graphical User Interface), and the Ncat debugging tool. A tool that uses terminal is called Hping3. The protocols TCP, UDP, ICMP, RAW-IP, and traceroute mode are supported. It is utilized for OS fingerprinting, firewall and network testing, and port scanning.

Second is the penetration testing tools used, according to the writers a technique for assessing the security of gadgets, systems, and apps is penetration testing. For analysis, breaching security, and penetration, various tools are employed [11]. The entire procedure is quite expensive and not automated. Typically done once a year, vulnerability scanning is concentrated on vulnerabilities with the highest priority. One penetration testing tool is the open source Metasploit penetration framework, which is developed for exploitation and the creation of security remedies.

Third and lastly is the network attacks, depending on how the data is acquired, the network attack might either be active or passive. If the attacker intercepts data being transmitted over the network, it can be said that the attack is passive. If the attacker tries to prevent the network from operating normally, that is considered an active network attack [19]. The following are the network attacks employed in Suricata's penetration testing, as stated in the chapter that follows:

- Attacks known as Denial of Service (DoS) occur when a system is overloaded, and attempts are made to stop servers connected to the Internet from functioning. When a significant number of dispersed computers are utilized, an assault may be categorized as a DDoS (Distributed DoS). Smurf, Neptune, Ping of Death, ICMP flood, SYN flood, and UDP flood are a few examples of DoS attacks.
- Attacks that take place when the system is searched for weaknesses are known as probing or reconnaissance attacks. As examples of these assaults, ipsweep, mscan, nmap, and portsweep might be listed.

After applying these types of attacks on the device Suricata I mentioned, the result is as follows, Testing of probing attacks demonstrates that Suricata IPS is capable of spotting assaults that use the NMAP tool to scan ports in normal, sly, and paranoid modes. The port scanning was stopped by the Suricata IPS with success. Despite being regarded as easily detectable, Suricata IPS was unable to pick up the XMas Tree assault. That's why it was introduced as a rule that Suricata might recognize the assault. The rule examines inbound traffic for TCP packets with the Fin, PSH, and URG flags. Suricata correctly recognizes the assault using a supplied activated rule. The effective identification of network traffic with more than 1000 packets per second is the outcome of this rule being triggered. The drop rule can be added in IPS Suricata mode, which means that the alert action in the presented rule is changed to the drop action, which then blocks network traffic. The eth0 interface sent the ICMP Flood

attack to the victim's IP address. Suricata failed to recognize the attack. The Suricata IPS was able to prevent an ICMP Flood attack by switching the alert action for the drop action. Suricata penetration tests reveal that the open version of the emerging threats ruleset is not capable of thwarting every kind of assault. Tests of the pro version of the emerging threats rule-set and other rulesets will be the focus of future development.

This study demonstrates a technique for IDS/IPS tool Suricata penetration testing on the Raspberry Pi 3, a low-performance embedded IoT device. Network assaults, penetration testing tools, and vulnerability scanning tools are covered. The primary contribution of our work is a comparison between various tools and types of network attacks and the Suricata IPS response as implemented on the Raspberry Pi 3. Suricata comes pre-configured with a standard set of rules. In order to prevent the XMas Tree attack, the ICMP flood assault, and the SYN flood attack, these rules were tested, and new rules were introduced. Because IPS frequently analyzes a huge amount of data, which is particularly demanding for these platforms, experimental use of the IDS on an embedded platform is not typically deployed in real network.

3. Internet Of Things (IOT)

3.1 What Is IOT:

The Internet of Things (IoT) is a system where various physical devices such as vehicles, buildings, and other objects are embedded with software, sensors, and connectivity, which enables them to connect and exchange data according to the definition of techtarget.com. According to Wikipedia, This technology has the potential to revolutionize the way we live and work by providing an efficient, cost-effective, and safe way of collecting and analyzing data. IoT devices can range from small sensors in appliances to large commercial airplanes, and they connect to the internet through various means such as Wi-Fi, Bluetooth, or cellular connections. The data collected by these devices is then sent to a central location for analysis and decision-making. The real-time monitoring of devices, equipment, and systems, automation of processes, improvement of safety, and enhancement of customer experience are some of the advantages IoT offers. As more and more devices become connected to the internet, the potential for IoT is limitless.

According to Alexander Roznovsky the technical writer for light it global, the most significant benefits of IoT is the ability to gather data in real-time. This allows for real-time monitoring of devices, equipment, and systems, which can improve efficiency and prevent downtime. For example, a manufacturing plant may use IoT sensors to monitor the temperature and humidity of the factory. If the sensors detect an abnormal temperature or humidity level, the system can alert the operator, allowing them to take corrective action before a problem occurs.

Another benefit of IoT is the ability to automate processes. IoT devices can be programmed to take actions based on the data they collect. For example, a smart thermostat can be programmed to adjust the temperature in a room based on the time of day or the presence of people. Similarly, a smart irrigation system can be programmed to turn on and off based on the weather forecast, saving water and energy. But all of this comes with the cost of putting your network at risk of exposure, typically IOT devices are not very secure and any intruder with malicious intent can access the network and steal all personal information all through the IOT device, so what are the previous issues encountered with IOT devices.

3.2 Previous Issues With IOT :

There have been several notable IoT cybersecurity incidents in the real world, we can mention the following:

- Mirai botnet : In 2016, a botnet made up of compromised IoT devices, primarily routers and security cameras, was used to launch a massive DDoS attack that caused widespread internet disruption. The attackers used default login credentials and easily guessed passwords to gain control of the devices.
- Vulnerabilities in smart home devices : In 2018, researchers discovered that several popular smart home devices, including security cameras and thermostats, had vulnerabilities that could allow attackers to gain access to the devices and potentially control them remotely.
- Security camera hacks: In recent years, there have been several reported incidents of hackers gaining access to security camera systems and using them to spy on individuals or steal personal information.
- Insecure medical devices: In 2017, the US Food and Drug Administration issued a warning about the potential cybersecurity risks associated with certain medical devices, including insulin pumps and pacemakers. These devices can be vulnerable to hacking, which could potentially harm patients.
- Vulnerabilities in industrial control systems: In 2017, the US Department of Homeland Security warned about vulnerabilities in industrial control systems that could allow attackers to disrupt operations at critical infrastructure facilities, such as power plants and water treatment facilities.

All these examples show that IoT devices are often not properly secured and can be easily hacked, leading to serious consequences such as data breaches, loss of privacy, and physical harm.

3.3 IOT OWASP Top 10 :

The OWASP Internet of Things (IoT) Top 10 Project is an effort to raise awareness about IoT security and provide a set of guidelines for securing IoT devices and systems. The project aims to identify the top 10 most critical IoT security risks and provide guidance on how to mitigate them. The OWASP IoT Top 10 is based on the OWASP Top 10, a widely recognized framework for web application security risks.

The IoT Top 10 Risks are:

- Injection (SQL, NoSQL, OS, etc.) - 15.3%: Injection vulnerabilities occur when untrusted data is sent to an interpreter as part of a command or query, which can allow attackers to execute unauthorized actions. Examples include SQL injection, NoSQL injection, and OS command injection.
- Broken Authentication and Session Management - 15.1%: Authentication and session management vulnerabilities occur when attackers can bypass or exploit the mechanisms used to identify and track users on a web application. This can allow attackers to impersonate legitimate users and gain unauthorized access to sensitive data or functionality.
- Cross-Site Scripting (XSS) - 7.9%: XSS vulnerabilities occur when an attacker is able to inject malicious scripts into a web page viewed by other users, which can allow the attacker to steal sensitive information or perform unauthorized actions on behalf of the victim.
- Broken Access Control - 7.6%: Access control vulnerabilities occur when attackers are able to bypass or exploit the mechanisms used to restrict access to certain resources or functionality within a web application. This can allow attackers to gain unauthorized access to sensitive data or functionality.
- Security Misconfiguration - 6.6%: Security misconfiguration vulnerabilities occur when systems or applications are not configured securely or have unnecessary services or features enabled, which can allow attackers to exploit weaknesses in the configuration to gain unauthorized access or perform other attacks.
- Insecure Cryptographic Storage - 5.6%: Insecure cryptographic storage vulnerabilities occur when sensitive data is not stored securely, such as using weak encryption or storing data in plain text. This can allow attackers to steal sensitive data, such as passwords or credit card numbers.

- Insufficient Transport Layer Protection - 5.2%: Transport layer protection vulnerabilities occur when data is transmitted over insecure channels or with weak encryption, which can allow attackers to intercept and steal sensitive data in transit.
- Injection (XML, SSI, LDAP, etc.) - 4.5%: Similar to injection vulnerabilities in the top spot, these refer to attacks that target various data parsing and handling methods, such as XML, Server Side Includes (SSI), and Lightweight Directory Access Protocol (LDAP).
- Using Components with Known Vulnerabilities - 4.1%: This refers to vulnerabilities that exist within third-party components (such as libraries, frameworks, or plugins) that are used in web applications. If these components contain known vulnerabilities, attackers can exploit them to gain unauthorized access or perform other attacks.
- Insufficient Logging and Monitoring - 3.9%: This refers to the lack of proper logging and monitoring capabilities within web applications, which can make it difficult to detect and respond to attacks in a timely manner.

These risks illustrate that IoT devices are often connected to the internet with weak security, and vulnerable to hacking, which can lead to serious consequences such as data breaches, loss of privacy, and physical harm. To mitigate these risks, it is important to ensure that IoT devices are properly secured and that organizations have policies and procedures in place to manage and secure these devices. This includes implementing secure development practices, performing security testing, and monitoring for security incidents. It is also important for organizations to stay informed about new IoT security risks and to be prepared to respond quickly to security incidents.

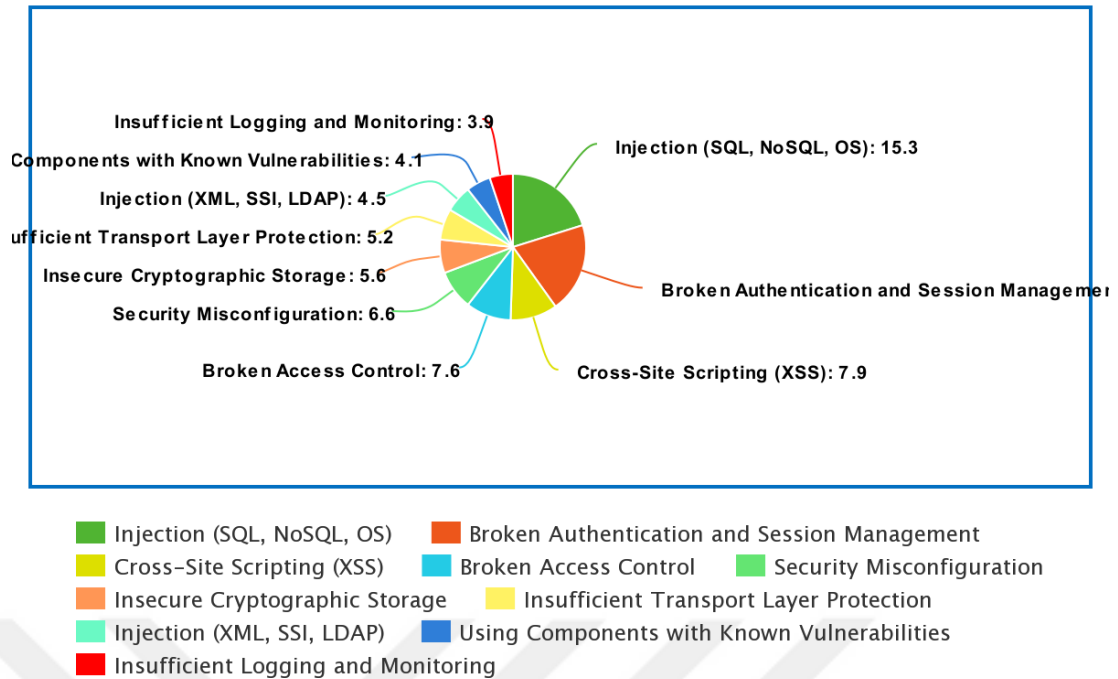


Figure 1 : IOT top 10 risks pie chart made with Meta-chart

It should be emphasized that the percentages provided indicate the occurrence rate of these vulnerabilities in actual web applications, based on OWASP's studies in the sources mentioned in the end of this report. Nevertheless, it is worth noting that the precise percentages may differ depending on the particular application and setting under review.

3.4 Standard Life Cycle :

A security standard life cycle refers to the process of creating, maintaining, and updating a security standard. This cycle typically includes the following stages :

- **Development:** This is the first stage of the security life cycle where the organization conducts an assessment to identify its assets, vulnerabilities, and risks. This stage may include performing a security audit, a vulnerability assessment, or a risk analysis. For example, an organization might conduct a vulnerability assessment of its network to identify potential security weaknesses that could be exploited by attackers.
- **Planning:** The planning stage involves creating a security plan that outlines how the organization will address the identified vulnerabilities and risks. This stage may include developing policies and procedures, setting security objectives and metrics, and defining roles and responsibilities. For example, a security plan for an

organization might include implementing a firewall, intrusion detection system, and antivirus software to protect the network.

- **Implementation:** The implementation stage involves putting the security plan into action by installing hardware and software security controls, implementing security policies and procedures, and training employees on security best practices. For example, an organization might install firewalls, set up access controls, and implement multi-factor authentication to protect its network.
- **Maintenance:** The maintenance stage involves ongoing monitoring and maintenance of the security measures to ensure they remain effective. This stage may include updating security controls, conducting regular security audits, and responding to security incidents. For example, an organization might update its antivirus software to protect against new malware threats or conduct regular penetration testing to identify new vulnerabilities in its network.
- **Retirement:** After a period of time, the standard may become obsolete and be retired. This can occur if the standard is no longer relevant or if a new standard has been developed to replace it.

The security standard life cycle is an important process that ensures that security standards remain relevant and effective in addressing current and emerging security threats. Regular review and updating of security standards help organizations to maintain a strong security posture and protect against cyber-attacks.

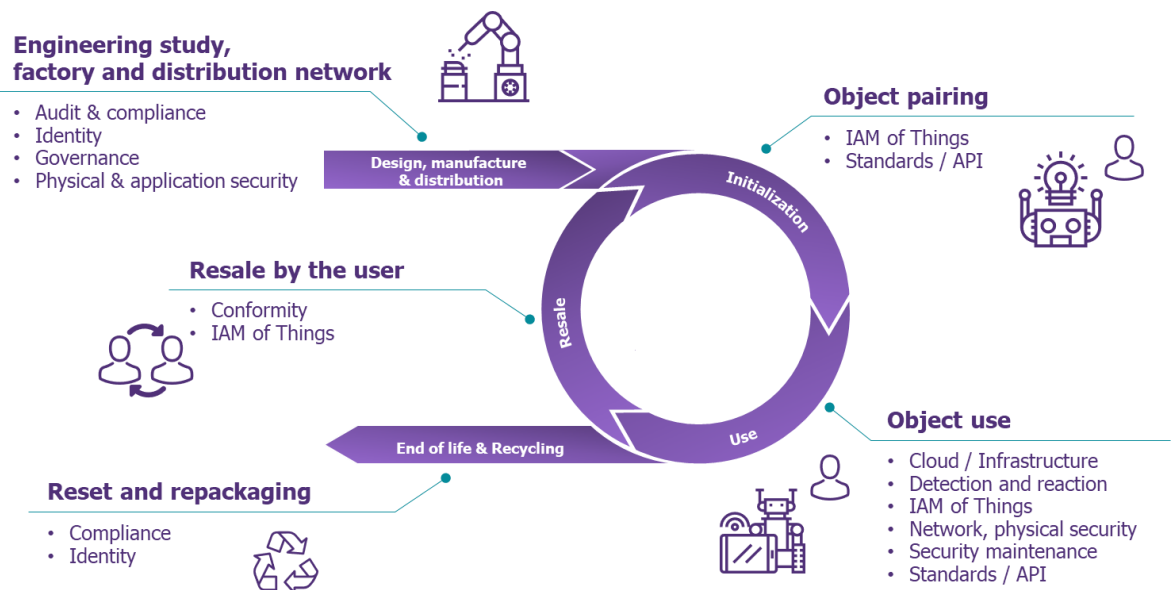


Figure 2 : Standard life cycle graph

3.5 Types Of Standards :

The following are some of the key standards for IoT security, along with a brief overview of each in chronological order:

OWASP IoT Top 10 (2014): This is a list of the top ten IoT security risks published by the Open Web Application Security Project (OWASP) in 2014. The list includes common vulnerabilities such as weak authentication and authorization, insecure communication, and lack of encryption. This standard is used to guide IoT security assessments and help organizations prioritize their security efforts.

Industrial Internet Security Framework (2015): This framework was developed by the Industrial Internet Consortium (IIC) to provide a comprehensive security architecture for industrial IoT systems. It includes guidance on secure hardware and software design, secure communication, and identity and access management. This standard is used to guide the development and implementation of secure industrial IoT systems.

NIST Cybersecurity Framework (2018): This framework was developed by the National Institute of Standards and Technology (NIST) to provide a common language for organizations to describe and manage cybersecurity risk. It includes five core functions: identify, protect, detect, respond, and recover. This standard is used to guide IoT security planning and risk management.

IoT Security Maturity Model (2020): This model was developed by the Industrial Internet Consortium (IIC) to provide a framework for evaluating the maturity of an organization's IoT security program. It includes five levels of maturity, from basic to optimized, and covers areas such as risk management, asset management, and incident response. This standard is used to assess an organization's IoT security program and identify areas for improvement.

ETSI EN 303 645 (2021): This is a standard developed by the European Telecommunications Standards Institute (ETSI) to provide a baseline for IoT security. It includes 13 provisions, such as ensuring software integrity, securing communication, and minimizing data exposure. This standard is used to guide the development and procurement of secure IoT devices.

Some Examples of implementation for these standards is the following:

- OWASP IoT Top 10: One of the top ten risks listed in this standard is "weak or guessable passwords," which can be exploited by attackers to gain unauthorized access to IoT devices. To address this risk, organizations can implement strong password policies that require the use of complex, unique passwords, and mandate periodic password changes. They can also consider implementing two-factor authentication or biometric authentication to further enhance access control.
- Industrial Internet Security Framework: One of the key recommendations in this framework is to implement secure communication protocols, such as Transport Layer Security (TLS), to protect data transmitted between IoT devices and servers. Organizations can also consider implementing secure boot processes and firmware updates to ensure the integrity of the IoT devices' software.
- NIST Cybersecurity Framework: The "detect" function in this framework emphasizes the importance of continuous monitoring and event detection to identify potential security incidents in a timely manner. To implement this function, organizations can implement security information and event management (SIEM) systems that can detect and alert security personnel to anomalous activity. They can also consider implementing intrusion detection and prevention systems (IDPS) to further enhance their detection capabilities.

Each of these IoT security standards offers a structure for managing and mitigating specific security issues in the IoT ecosystem. By adhering to these standards, organizations can enhance the security of their IoT systems, and safeguard the integrity of the data they collect and transmit.

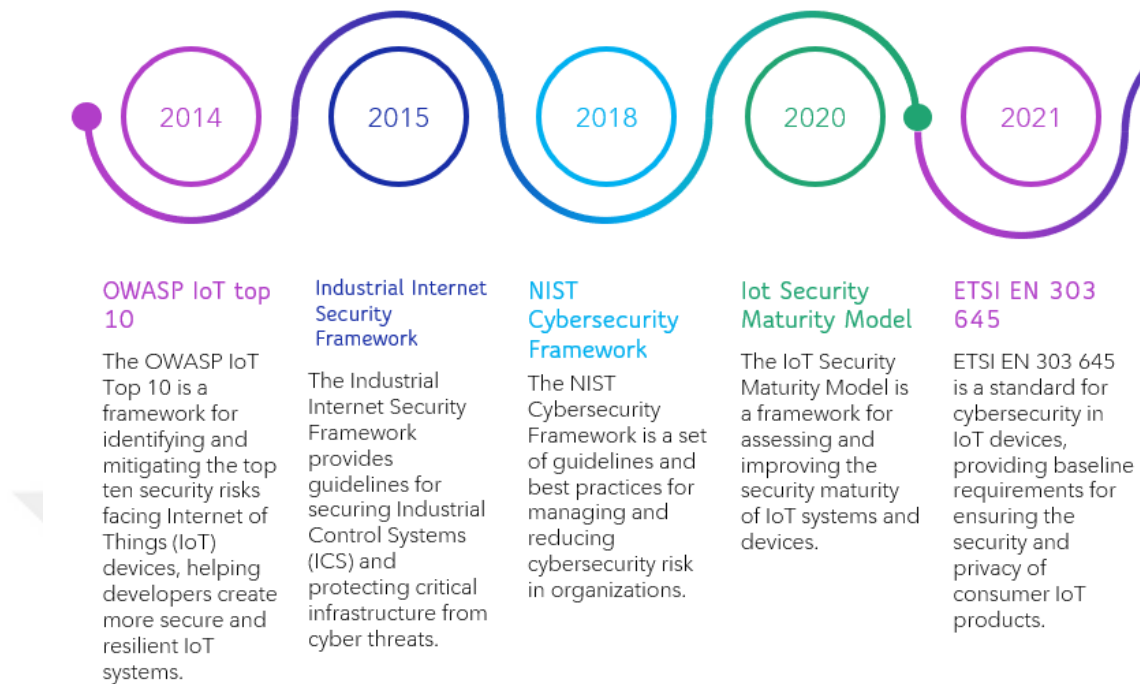


Figure 3 : Chronological order of user standards for IOT

3.6 ETSI EN 303 365 Standard :

The ETSI EN 303 365 standard, also known as the "Cyber Security for Internet of Things (IoT)," is a set of guidelines and specifications for securing Internet of Things (IoT) devices and systems. These guidelines were developed by the European Telecommunications Standards Institute (ETSI) to address the increasing security risks associated with the integration of IoT devices in various sectors.

The standard provides a comprehensive approach to IoT security, covering the full lifecycle of IoT devices, from design and development to deployment, operation, and retirement. It covers various aspects of IoT security, including secure communication, secure device management, secure software and firmware updates, and secure data storage and processing.

One of the key components of the standard is the requirement for secure communication between IoT devices. The standard specifies the use of secure protocols, such as Transport Layer Security (TLS) and Secure Sockets Layer (SSL), to protect against eavesdropping and tampering of communications. It also requires the use of secure keys and certificates for device authentication and encryption of communications.

The standard also addresses the issue of device management, which is critical for ensuring the security of IoT devices. It requires the use of secure methods for provisioning, configuring, and updating IoT devices. This includes the use of secure protocols for remote management and the use of secure methods for updating device software and firmware.

In addition, the standard addresses the issue of secure data storage and processing. It requires the use of secure methods for storing and processing data, such as encryption and secure key management. It also requires the use of secure methods for transmitting and receiving data, such as secure protocols and secure data transfer methods.

The standard also includes guidelines for incident management and incident response. It requires organizations to have incident management procedures in place and to be prepared to respond quickly to security incidents. The standard also requires organizations to report security incidents to the appropriate authorities and to take steps to prevent similar incidents from happening in the future.

The ETSI EN 303 365 standard is useful for organizations that are developing, deploying, and operating IoT devices and systems. It provides a set of guidelines and specifications that can be used to ensure the security of IoT devices and systems.

By following the guidelines and specifications outlined in the standard, organizations can reduce the risk of security incidents and protect against the unauthorized access, use, disclosure, disruption, modification, or destruction of sensitive information.

Moreover, the standard helps organizations to meet regulatory and compliance requirements. Many countries and regions have adopted or are in the process of adopting regulations that require organizations to secure IoT devices and systems. The ETSI EN 303 365 standard provides a set of guidelines and specifications that can be used to meet these regulatory and compliance requirements.

In summary, the ETSI EN 303 365 standard provides a comprehensive approach to IoT security and covers various aspects of IoT security, from design and development to deployment, operation, and retirement. It helps organizations to secure their IoT devices and systems and reduce the risk of security incidents. Additionally, it helps organizations to meet regulatory and compliance requirements for IoT security.

3.7 Technical Security Requirements:

Ensuring the security of IoT devices requires organizations to consider a range of technical requirements. These are the most notable ones:

Secure communication: IoT devices should use secure communication protocols to ensure the confidentiality, integrity, and authenticity of data transmitted over the network. This includes the use of secure transport protocols, such as Transport Layer Security (TLS), to encrypt data in transit and prevent eavesdropping and tampering. In addition, IoT devices should implement secure authentication mechanisms to ensure that only authorized devices can access the network. (Source: NISTIR 8228: Considerations for IoT Device Manufacturers)

Access control: Access control mechanisms such as authentication, authorization, and accountability should be implemented to ensure that only authorized users can access and manipulate IoT devices and data. This includes the use of strong passwords, multi-factor authentication, and role-based access control. In addition, access logs should be maintained to enable auditing and accountability. (Source: OWASP IoT Top 10)

Device identification and authentication: IoT devices should have unique identifiers and authentication mechanisms to prevent unauthorized access and ensure data privacy. This includes the use of unique device IDs, digital certificates, and secure boot mechanisms to verify the integrity of device software and firmware. (Source: NIST SP 800-183: Network of Things (NoT) Security).

Secure software and firmware updates: IoT devices should support secure software and firmware updates to address security vulnerabilities and improve the overall security posture of the device. This includes the use of secure update mechanisms, such as code signing and secure boot, to ensure that only authorized updates are installed. In addition, update procedures should be tested and validated to ensure they do not introduce new vulnerabilities. (Source: IIC Industrial Internet Security Framework).

Data protection: IoT devices should use encryption and other data protection mechanisms to safeguard sensitive information such as personally identifiable information (PII) and authentication credentials. This includes the use of strong encryption algorithms, such as Advanced Encryption Standard (AES), to protect data

at rest and in transit. In addition, data should be deleted securely to prevent data leakage. (Source: ISO/IEC 30141:2018 Information technology — Internet of Things (IoT) — Reference architecture)

Physical security: IoT devices should be physically secured to prevent unauthorized access and protect against tampering or theft. This includes the use of tamper-resistant enclosures, security seals, and anti-tamper mechanisms to detect and respond to physical attacks. In addition, the physical security of devices should be regularly audited and monitored. (Source: NISTIR 8228: Considerations for IoT Device Manufacturers).

Resilience to attacks: IoT devices should be designed to detect and respond to cyber-attacks in a timely and effective manner, such as by implementing intrusion detection systems or threat intelligence. This includes the use of anomaly detection algorithms, network segmentation, and incident response plans to mitigate the impact of attacks. In addition, devices should be designed with resilience and redundancy to maintain operation in the face of attacks. (Source: NIST SP 800-183: Network of Things (NoT) Security)

Privacy protection: IoT devices should be designed with privacy in mind, and privacy should be built into the device architecture and functionality. This includes the use of privacy-preserving technologies, such as differential privacy and data minimization, to reduce the collection and sharing of personal data. In addition, privacy policies should be transparent and easily accessible to users. (Source: ISO/IEC 30141:2018 Information technology — Internet of Things (IoT) — Reference architecture)

Compliance with regulations : IoT devices should comply with applicable laws and regulations governing data privacy, security, and consumer protection. This includes compliance with regulations such as the Genera

Regular security assessments: IoT devices should be regularly assessed for vulnerabilities and security patches and software updates should be applied as needed.

By following these technical security requirements, organizations can help ensure the security of their IoT devices and protect against unauthorized access, use, disclosure, disruption, modification or destruction of sensitive information. It is important to remember that security is a continuous process, and it is important to

regularly review and update the security measures in place to ensure that they are still effective in protecting your devices and data.

3.8 Activity Diagrams For ETSI EN 303 365:

Activity diagrams, also known as flowcharts or process diagrams, are graphical illustrations that demonstrate the flow of activities in a system. They are utilized to depict actions, decisions, and activities that are executed within a system to accomplish a specific objective. These diagrams give a straightforward and precise understanding of the interactions between elements in the system and the flow of control from one activity to another. They play a crucial role in modeling business processes, organizational structures, and software systems. Furthermore, they can be employed to show the control flow of data processing, event-driven processes, and workflows. The visual representation offered by activity diagrams helps stakeholders grasp complex processes effortlessly and intuitively. As a master's student, I consider activity diagrams to be a significant tool in business analysis and software development, as they provide a clear understanding of the system's operations and support identifying areas for improvement.

Activity diagrams use different but limited number of shapes connected using arrows, every shape has a different meaning, ellipses are actions, diamonds are decisions, black circle means the start and encircled black circle represents the end.

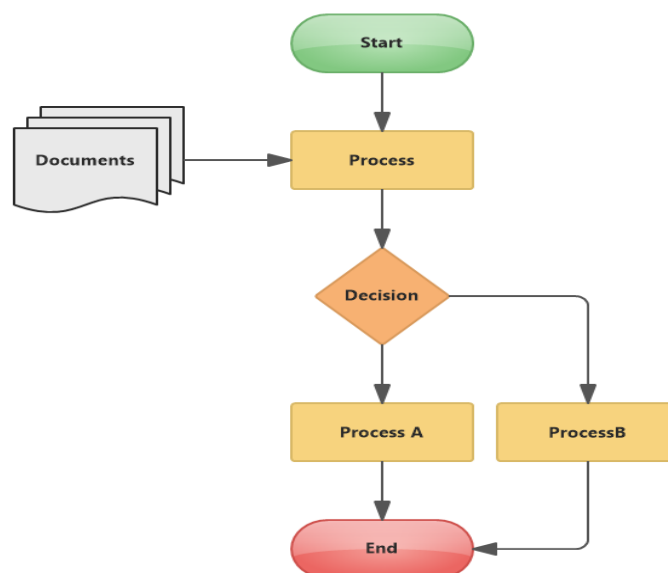


Figure 4 : Activity diagram example

3.8.1 standard activity diagram.

In this activity diagram we will be looking at which scenarios we will be using the “ETSI EN 303 645” standard and how deep do we need to use it to secure our IOT devices.

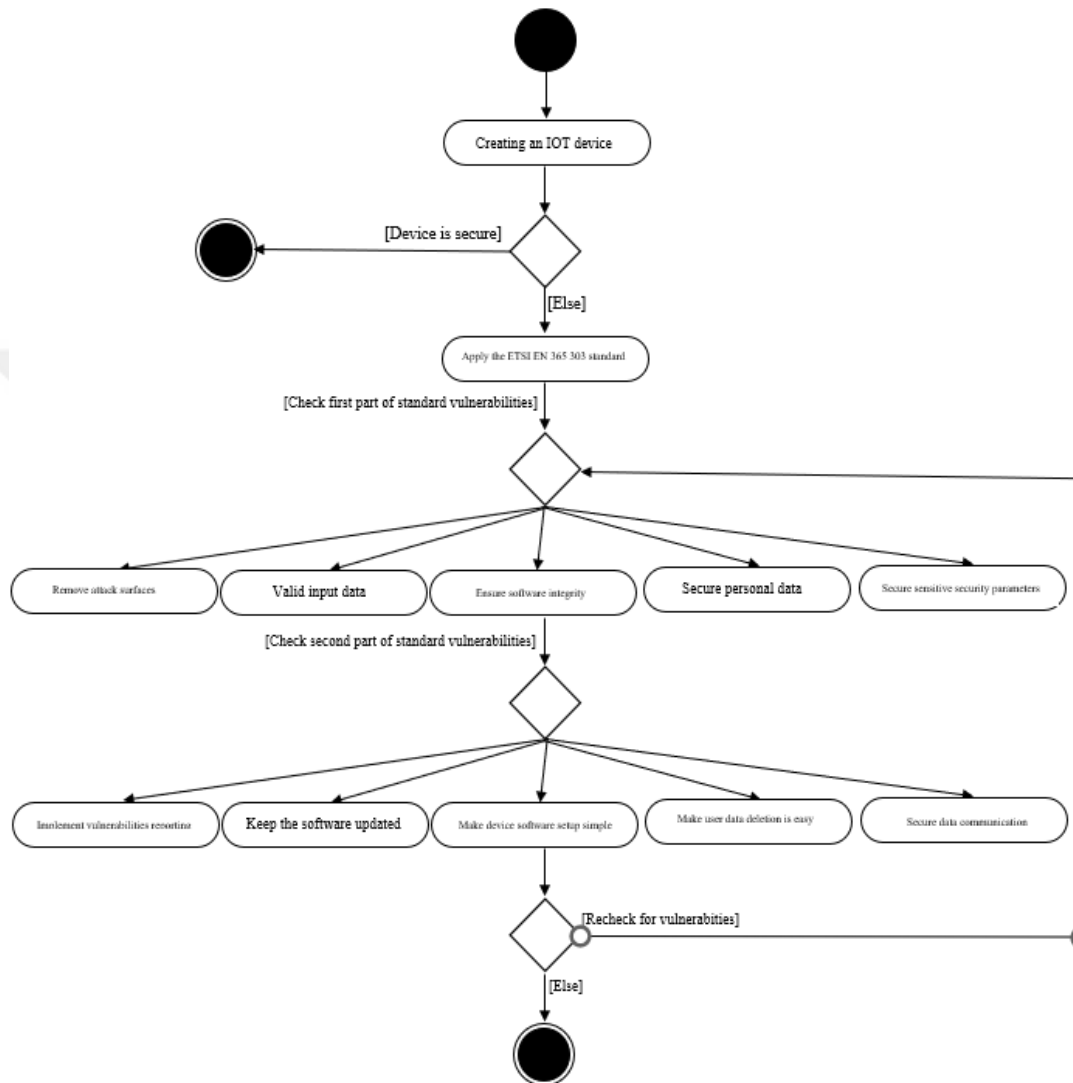


Figure 5 : ETSI EN 303 645 Activity Diagram standard

The first thing after finishing the creation of the IOT device and satisfying the customer needs, the IOT developer needs to take a good look at the security of his device, doing some penetration testing and general inspection of vulnerabilities that can be available on the device.

This is where the ETSI EN 365 303 standard comes in place and makes the job of securing the device much easier, in the general IOT security scenario the first thing

done by the developer is going over the major vulnerabilities mentioned in the standard one by one and seeing if the device is protected against the mentioned weaknesses or not. In this diagram, vulnerabilities are divided into 2 parts, first part includes: Removing attack surfaces, validating input data, ensuring software integrity, securing person data and securing sensitive security parameters. The developer needs to make a good inspection on these vulnerabilities and try to look if his system is vulnerable against it or not. After securing the first wave of vulnerabilities on the device, the developer can move into the second part of vulnerabilities which includes: Implementing vulnerabilities reporting, keeping the software updated, making the device software setup simple, making sure the data deletion is easy, and securing data communication. Again, after making sure every vulnerability is secured against, the last thing the developer should do according to the diagram is doing a 2nd recheck on the vulnerabilities mentioned. Sure, it can take him a bit more time but with this extra step the IOT device can be safe and when deployed into the market no complaints of weak security and no cases of attackers abusing that specific IOT device will be found. If this IOT device security diagram along with the ETSI EN 303 645 standard are combined and utilized in the creation of the IOT device, many issues can be avoided.

3.8.2 attack surfaces.

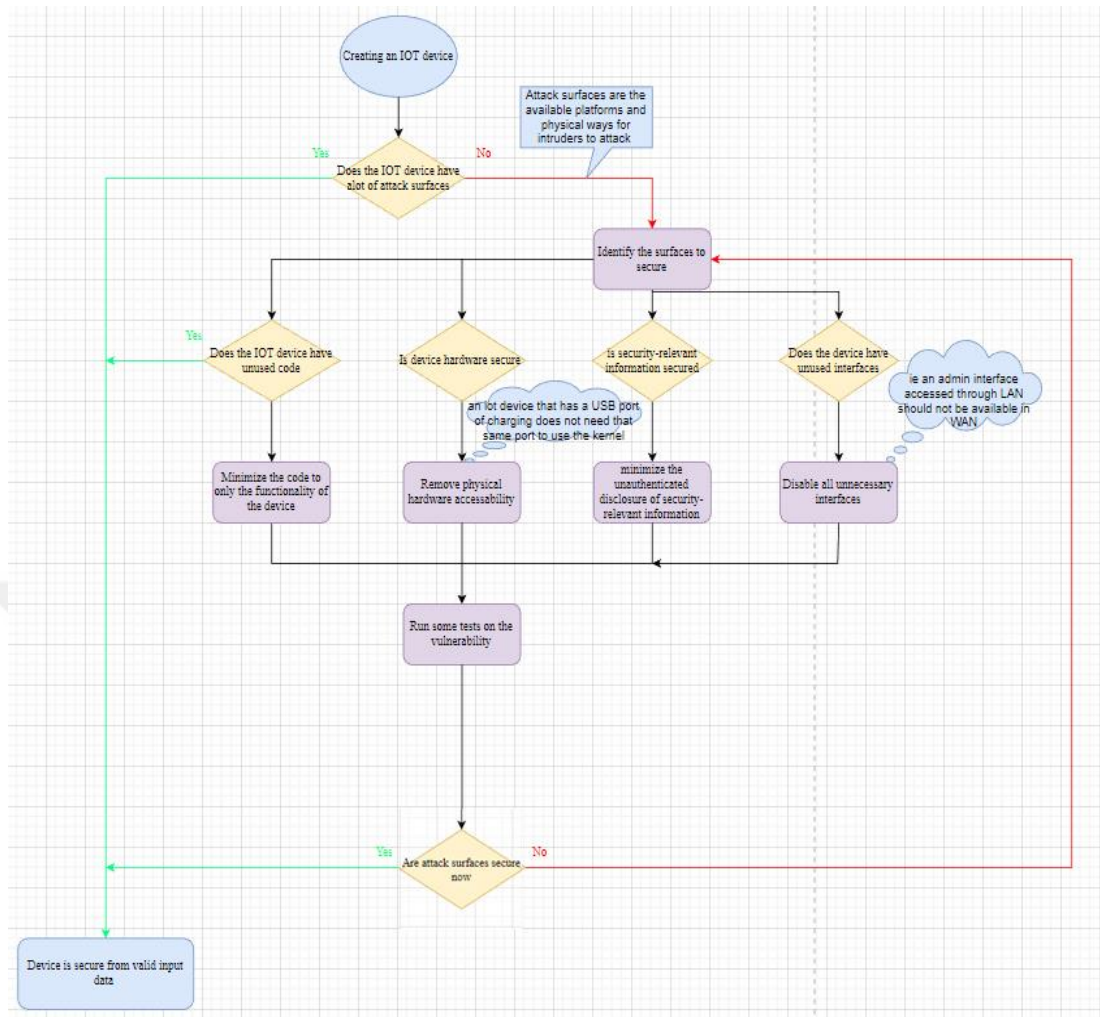


Figure 6 : Attack surfaces diagram

One of the most known attack types by hackers is abusing attack surfaces, The attack surface of an IOT software environment is all the different points where an unauthorized user can try to enter data to or extract data from an environment. Keeping the attack surface as small as possible is a basic security measure. In our diagram, the first thing the developer needs to do is identifying the surfaces that need to be secured. For example, If the IOT software has some unused interface like an admin interface that is accessed through LAN should not be accessible in Wan, the IOT developer should make sure to disable all the unnecessary interfaces. Next is making sure that security-relevant information is secured by minimizing the unauthenticated disclosure of security-relevant information. Next is cleaning the code used for IOT devices, since unused code can lead into many vulnerabilities, minimizing the code to do only the

functionality of the device is necessary. Last thing that should be looked upon is the hardware part of the device, Keeping the hardware secure by removing all physical hardware accessibility like USB ports is very important since having any access to the hardware means that when an attacker is present next to the IOT device he can get access and use the kernel however he wishes. After doing some tests on these major vulnerabilities and making sure of their security, a double check is recommended to see if we missed anything. If the device is secure from attack surfaces, the developer can move into securing the next aspect of IOT devices.

3.8.3 software integrity.

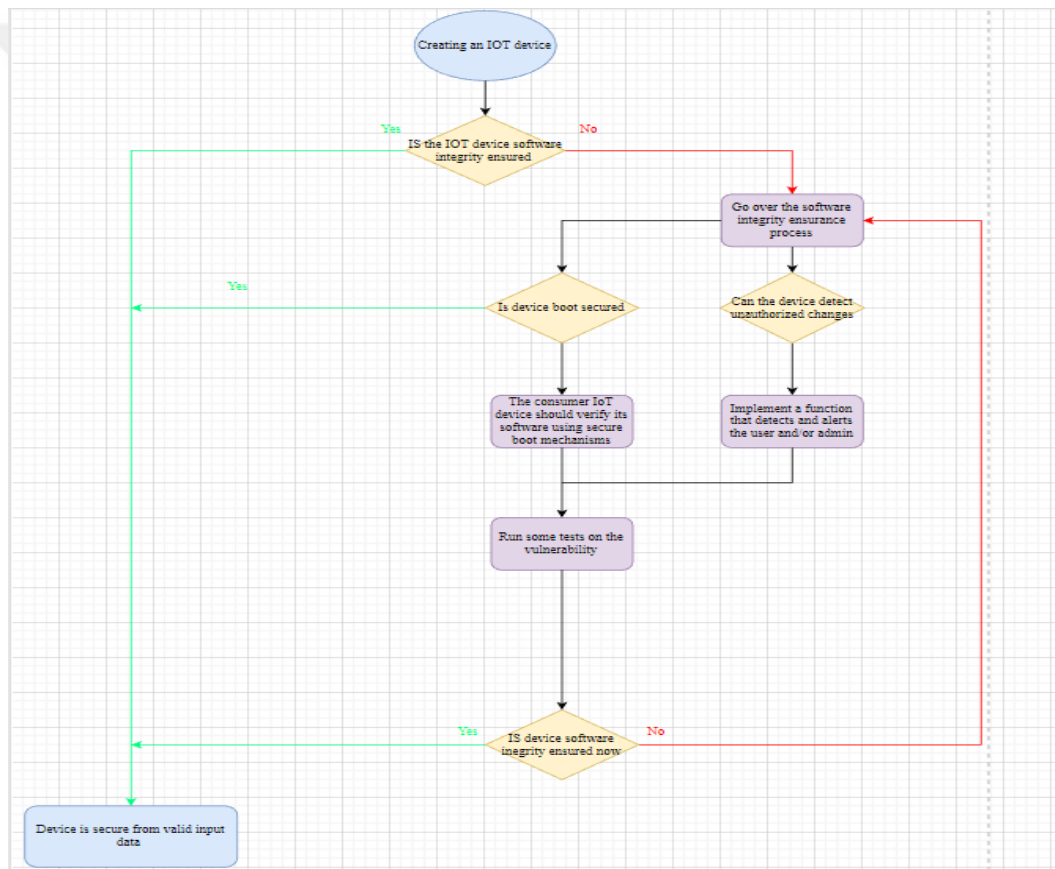


Figure 7 : Software integrity diagram

Software integrity is usually used when attackers have the knowledge that the software of the device is changeable and can be altered, so in this case, the IOT developer needs to do the following, First like every penetration testing sequence, run some test on the device to see if it is vulnerable or not, if it's vulnerable we go to more detailed test. We see if the device can detect unauthorized change, meaning if the

source code or some information that is usually not present in the device is found the device automatically informs the developer or the user, if not, the developer needs to implement a function that does detection and alerts the changes to the concerned parties. Next most important thing is device boot, the IOT developed need to be very sure and verify if the software is using secure boot mechanisms because if that is not the case, the attackers can use the boot sequence to run things in the background during the bootup sequence. These are the most important parts concerning the software integrity that need to be secure according to the standard, after making sure these two are protected, it is preferable to run some more test to retest if there are some more holes left. If the device is secure, we can move to the next vulnerability that needs to be protected against.

3.8.4 personal data security.

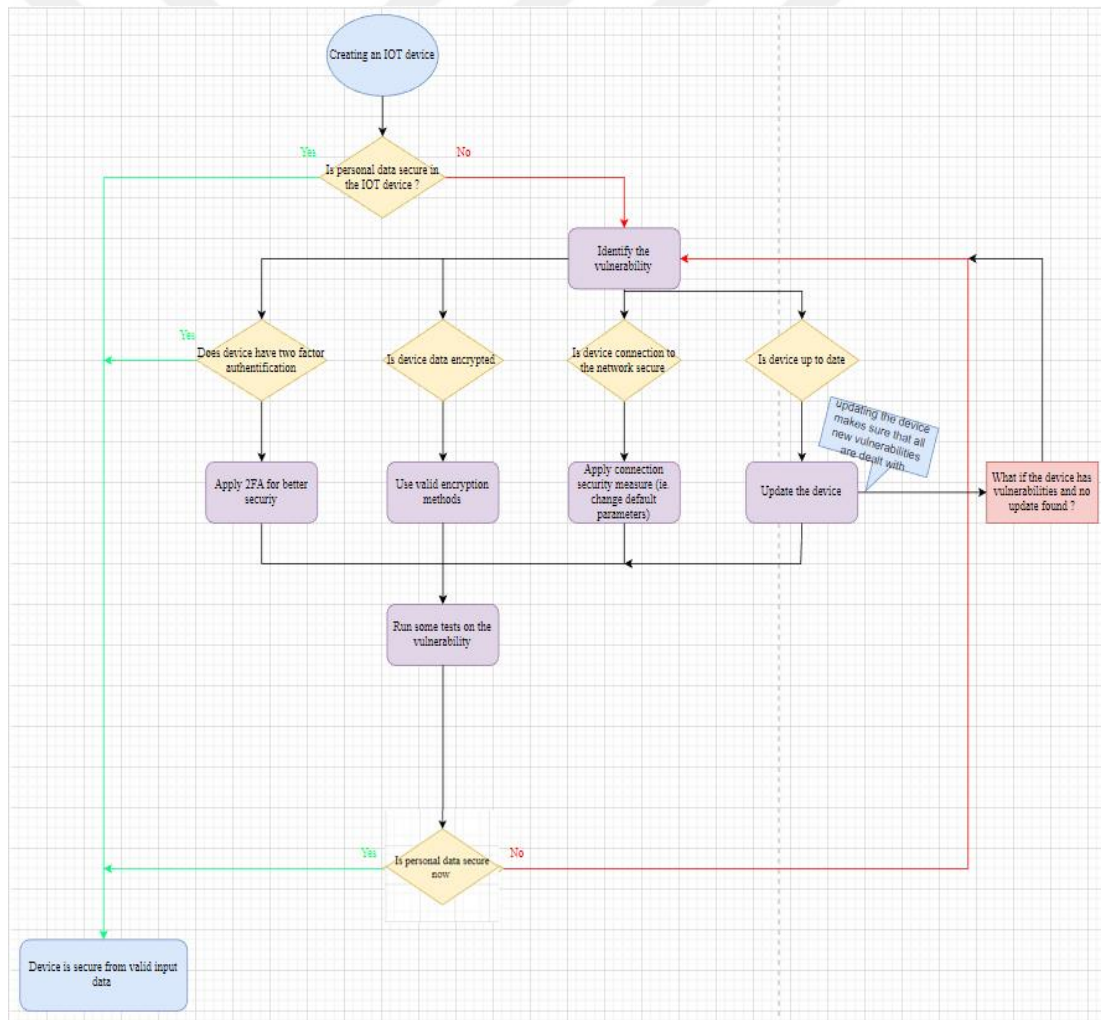


Figure 8 : Personal data security diagram

Software integrity is usually used when attackers have the knowledge that the software of the device is changeable and can be altered, so in this case, the IOT developer needs to do the following, First like every penetration testing sequence, run some test on the device to see if it is vulnerable or not, if it's vulnerable we go to more detailed test. We see if the device can detect unauthorized change, meaning if the source code or some information that is usually not present in the device is found the device automatically informs the developer or the user, if not, the developer needs to implement a function that does detection and alerts the changes to the concerned parties. Next most important thing is device boot, the IOT developed need to be very sure and verify if the software is using secure boot mechanisms because if that is not the case, the attackers can use the boot sequence to run things in the background during the bootup sequence. These are the most important parts concerning the software integrity that need to be secure according to the standard, after making sure these two are protected, it is preferable to run some more test to retest if there are some more holes left. If the device is secure, we can move to the next vulnerability that needs to be protected against.

3.8.5 valid input.

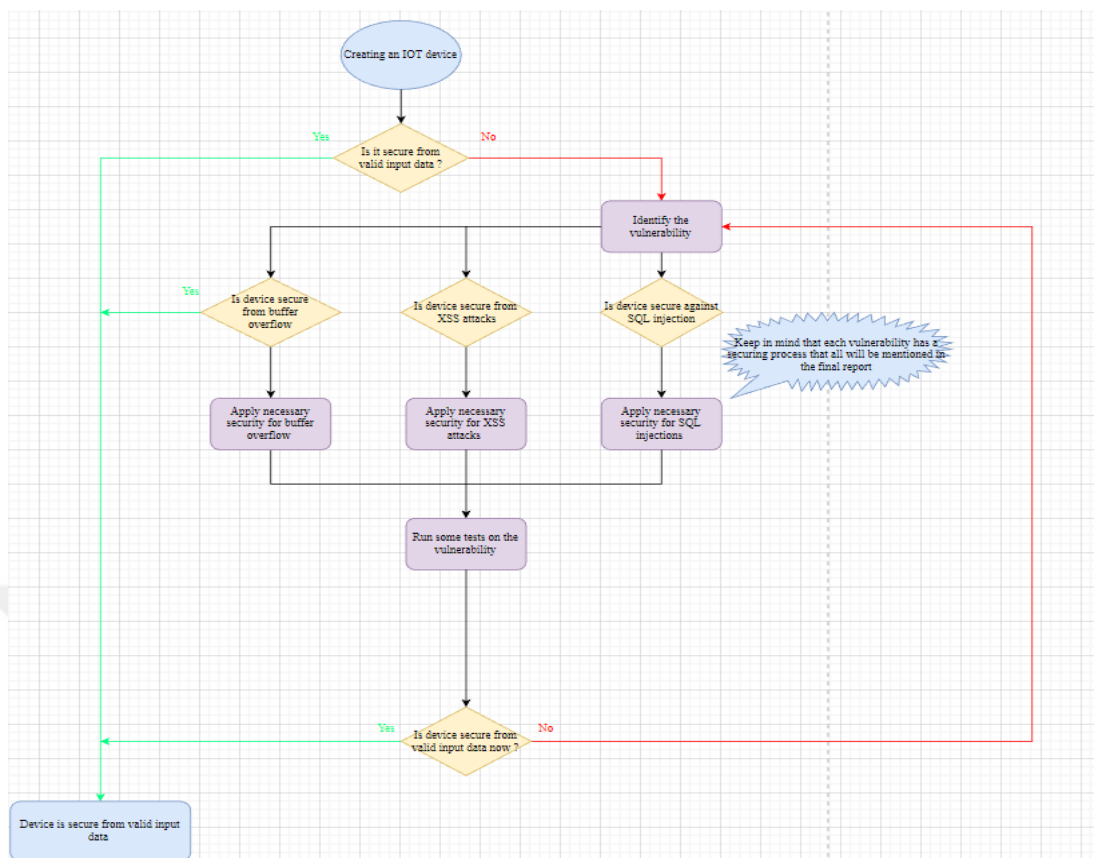


Figure 9 : valid input diagram

Valid input security is mandatory for any device that is connected to networks since having this vulnerability in your device can mean all your data is available for intruders. IOT developers need to run some tests on their devices and try to find weaknesses before selling their device in the market. There are 3 main types of vulnerabilities that can be categorized as valid input attacks. First is SQL injection which is without a doubt the most common way, by using parameterized database queries with constrained, typed parameters and cautiously using parameterized stored procedures in the database, developers may prevent SQL Injection vulnerabilities in web applications. Java, .NET, PHP, and other programming languages can all be used to do this. Next is XSS attacks where if the developer finds this vulnerability, he needs to make sure that all output data is encoded and all input data is validated. Finally, is buffer overflow where if it's found all necessary defence methods against it must be applied. After taking a look at these vulnerabilities, developers need to run some tests again to double-check things.

3.8.6 conclusion.

In conclusion, activity diagrams are an indispensable tool in the realms of business analysis and software development. By graphically modeling the flow of activities, decisions, and actions within a system, they provide a comprehensive understanding of how the system operates and facilitate the identification of areas for improvement. The visual representation provided by activity diagrams makes it easier for stakeholders to grasp complex processes. Moreover, the use of activity diagrams promotes work organization by providing a systematic view of interactions between elements within a system and the flow of control from one activity to another. In today's dynamic business world, having streamlined and efficient processes is increasingly important. Activity diagrams are a valuable asset that can aid organizations in streamlining their operations, reducing inefficiencies, and boosting productivity. As a thesis student, I firmly believe that activity diagrams are necessary and highly useful for making work easier and more organized.

4 : Penetration Testing Methodology

4.1 Types Of Penetration Testing

The most widely used method of penetration testing is network penetration testing, which involves evaluating an organization's network infrastructure for vulnerabilities. This type of testing aims to identify weaknesses in network devices such as routers, switches, and firewalls, as well as any services running on them. The tests typically include scanning the network for open ports, services, and vulnerabilities, attempting to exploit those vulnerabilities to gain access to the network, and testing the network's defenses to determine if they can prevent unauthorized access to sensitive information. This type of testing accounts for **54%** of all penetration testing.

Web application penetration testing is the second most commonly used type of penetration testing, accounting for **32%** of all testing. It involves evaluating the security of web applications, such as e-commerce websites, online banking portals, and social media platforms. The goal of this testing is to identify vulnerabilities in the application's code, design, and configuration that could be exploited by attackers to gain unauthorized access or steal sensitive information. The tests typically involve identifying the application's entry points, attempting to inject malicious code, and testing the application's defenses to see if they can prevent the attacker from accessing sensitive information.

Mobile application penetration testing accounts for **7%** of all penetration testing and involves evaluating the security of mobile applications, such as those used for online banking, social media, and e-commerce. The objective of this testing is to identify vulnerabilities in the application's code, design, and configuration that could be exploited by attackers to gain unauthorized access or steal sensitive information. The tests typically involve analyzing the application's code, attempting to inject malicious code, and testing the application's defenses to see if they can prevent the attacker from accessing sensitive information.

Physical penetration testing accounts for **4%** of all penetration testing and involves evaluating the physical security of an organization's facilities, such as data centers, offices, and warehouses. The aim is to identify vulnerabilities in physical

security measures such as locks, access control systems, and surveillance cameras. The tests typically involve attempting to gain unauthorized access to the facility, either through social engineering or physical force, and testing the physical security measures to see if they can prevent the attacker from accessing sensitive information.

Social engineering testing accounts for **3%** of all penetration testing and involves evaluating an organization's employees' susceptibility to phishing attacks, spear-phishing attacks, and other social engineering tactics. The objective is to identify vulnerabilities in employee behavior, such as clicking on suspicious links or divulging sensitive information to unauthorized individuals. The tests typically involve creating phishing emails, phone calls, or other forms of communication that attempt to trick employees into divulging sensitive information.

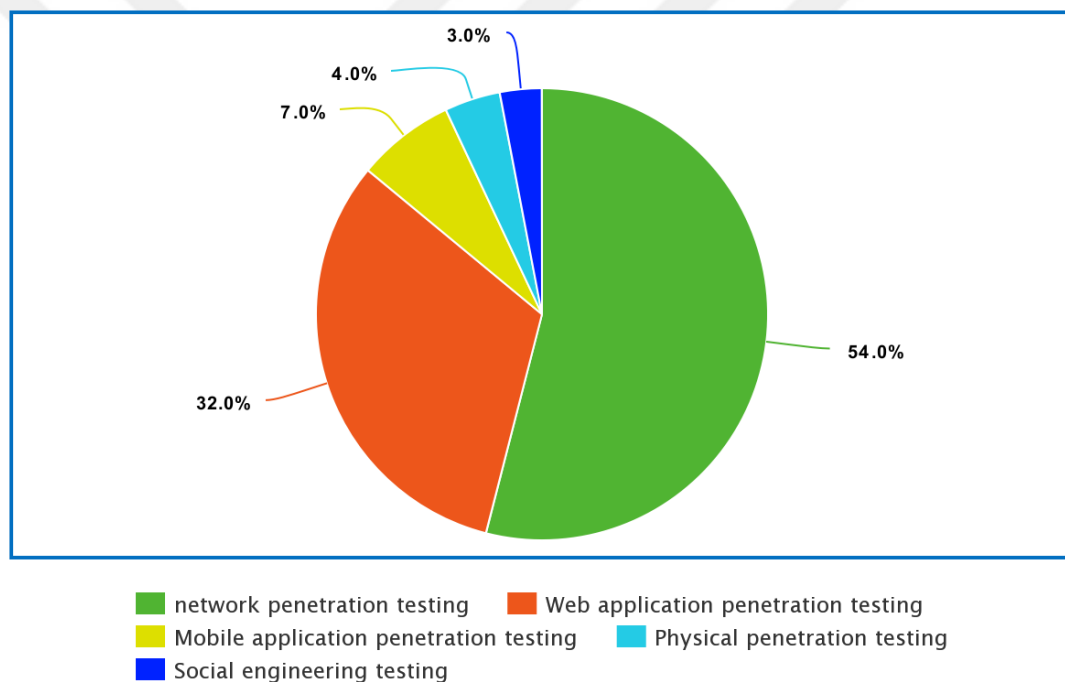


Figure 10 : Percentage of use of penetration testing methods pie chart made using meta-chart

To be more specific, now we will be talking about the penetration testing methods for IOT devices:

The analysis of firmware is a method for identifying vulnerabilities in IoT devices by examining their firmware. This involves scrutinizing the security mechanisms of the firmware, searching for hardcoded passwords and encryption keys,

and identifying any backdoor accounts. The goal is to identify any weaknesses that could be exploited by an attacker.

Wireless network testing focuses on assessing the security of wireless communication protocols such as Wi-Fi, Bluetooth, and ZigBee that are commonly used by IoT devices. This involves testing the network for vulnerabilities such as weak encryption, default passwords, and insecure data transmission.

RF analysis involves examining the RF signals emitted by IoT devices to identify vulnerabilities. This includes analyzing the strength of the signal, searching for signal leaks, and scrutinizing the data transmitted over the RF signal.

Physical access testing evaluates the physical security of IoT devices. This includes testing the strength of the device's casing, analyzing the security of the device's ports and connectors, and testing the security of any tamper-resistant seals.

Cloud infrastructure testing examines the security of the cloud infrastructure that is used by many IoT devices to store and process data. This involves identifying vulnerabilities in the cloud infrastructure and testing the security of the communication between the IoT device and the cloud.

4.2 Penetration Testing Phases

Penetration testing is a process of testing an organization's computer systems, networks, and applications to identify vulnerabilities and security weaknesses. It is an important part of a comprehensive security program and helps organizations identify and remediate security weaknesses before they can be exploited by attackers. Penetration testing is typically divided into several phases, each of which is designed to identify and exploit different types of vulnerabilities.

In a typical penetration testing engagement, the phases can include:

- **Planning and reconnaissance:** In this phase, the penetration tester works with the organization to understand the scope of the engagement, identify the target systems and applications, and gather information about the organization's security posture.
- **Scanning:** In this phase, the penetration tester uses automated tools to scan the target systems and applications for known vulnerabilities, open ports, and other security weaknesses.

- **Enumeration:** In this phase, the penetration tester uses manual techniques to identify the services running on the target systems, including their version numbers, configuration settings, and other important information.
- **Exploitation:** In this phase, the penetration tester attempts to exploit the vulnerabilities identified in the previous phases to gain access to the target systems or applications.
- **Post-exploitation:** In this phase, the penetration tester attempts to maintain access to the target systems or applications, escalate their privileges, and extract sensitive information.
- **Reporting:** In this phase, the penetration tester documents their findings and presents them to the organization, along with recommendations for remediation.

When it comes to penetration testing for IoT devices, the process is similar, but there are some unique challenges and considerations. IoT devices often have limited processing power, memory, and battery life, which can make traditional penetration testing techniques difficult to use. Additionally, IoT devices often use wireless communication protocols, which can be more difficult to secure than wired networks.

The phases of penetration testing for IoT devices are:

Planning and reconnaissance: In this phase, the penetration tester works with the organization to identify the IoT devices to be tested, the communication protocols they use, and the types of data they transmit.

Scanning: In this phase, the penetration tester uses specialized tools to scan the IoT devices and the surrounding wireless networks for vulnerabilities and weaknesses.

Enumeration: In this phase, the penetration tester uses manual techniques to identify the services running on the IoT devices, including their version numbers, configuration settings, and other important information.

Firmware analysis: In this phase, the penetration tester analyzes the firmware of the IoT devices for vulnerabilities, such as hardcoded passwords and encryption keys.

Wireless network testing: In this phase, the penetration tester analyzes the security of the wireless networks used by the IoT devices, including Wi-Fi, Bluetooth, and ZigBee.

Radio frequency (RF) analysis: In this phase, the penetration tester analyzes the RF signals emitted by the IoT devices to identify vulnerabilities.

Physical access testing: In this phase, the penetration tester tests the physical security of the IoT devices, including the strength of their casing and the security of their ports and connectors.

Cloud infrastructure testing: In this phase, the penetration tester analyzes the security of the cloud infrastructure used by the IoT devices, including the security of the communication between the devices and the cloud.

Reporting: In this phase, the penetration tester documents their findings and presents them to the organization, along with recommendations for remediation.

It's important to note that the specific phases of penetration testing for IoT devices may vary depending on the organization's specific needs and the types of devices being tested. Additionally, the testing process may need to be adapted as new vulnerabilities and threats emerge.

5: APS penetration testing and ETSI EN 303 645 implementation

An advanced people sensing system that counts passengers is beneficial for the urban transportation industry. The system transfers the counting data to a cloud platform, which generates actionable reports for real-time access to valuable information. Data-based decision-making can be made quickly as a result. However, securing this valuable information is critical for APS users. As the number of IoT cyber threats increases, this task is becoming increasingly challenging for all APS providers.

5.1 What Advanced People Sensor Device We Are Testing On :



Figure 11 . APS counting device HELLA Aglaia

HELLA Aglaia's APS is a cutting-edge passenger counting sensor that employs 3D image processing algorithms to examine the movement of people, achieving counting accuracy of 99 percent or higher. It improves usability, optimizes emerging remote connectivity choices, and automates several procedures that usually demand manual intervention. This leads to savings in expensive labor costs needed to set up, activate, and manage traditional APC units.

5.2 APS Penetration Testing :

5.2.1 information gathering.

The first part of any penetration testing is gathering as much information as possible also known as enumeration. The moment attackers establish a connection or find a hole in the system during this enumeration, they can send directed queries or payloads to extract information or to make it do things that it is not supposed to do.

VPN.

A VPN, or Virtual Private Network, is a type of network connection that allows users to securely access and transmit data over the internet. When a user connects to a VPN, their device establishes a secure and encrypted connection to a remote server operated by the VPN service provider. This connection creates a "tunnel" through which all data transmitted between the user's device and the internet is routed. One of the primary benefits of a VPN is enhanced security and privacy. Because all data transmitted through the VPN is encrypted, it is more difficult for hackers or other unauthorized users to intercept or access the data. Additionally, VPNs can be used to hide a user's IP address and location, providing a higher level of anonymity and privacy when browsing the internet. A VPN is needed to mask our identity and as a penetration tester this is a much needed tool.

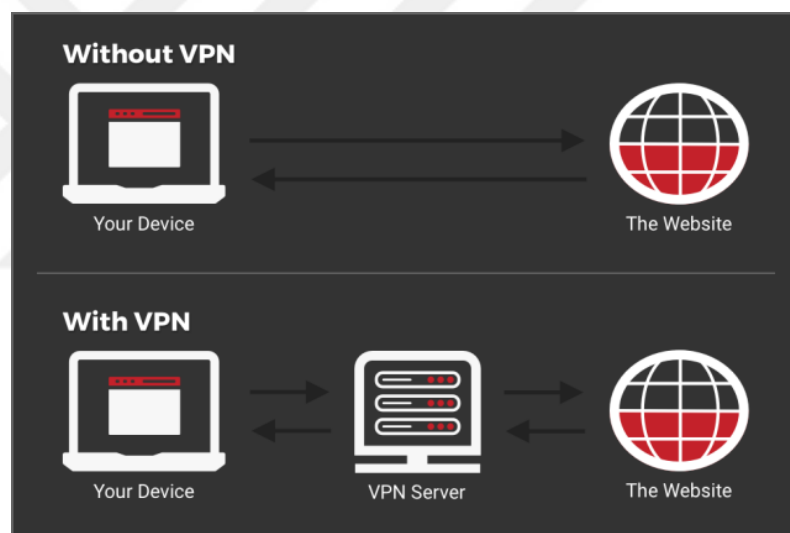


Figure 12 : How a VPN works

5.2.1.1 website technologies, version and flaws.

To get an idea on the technology used to create the website interface used by the APS device we used the “Wappalier” tool which provides instant access to website technology stacks, company and contact details, social media profiles, email verification and more.

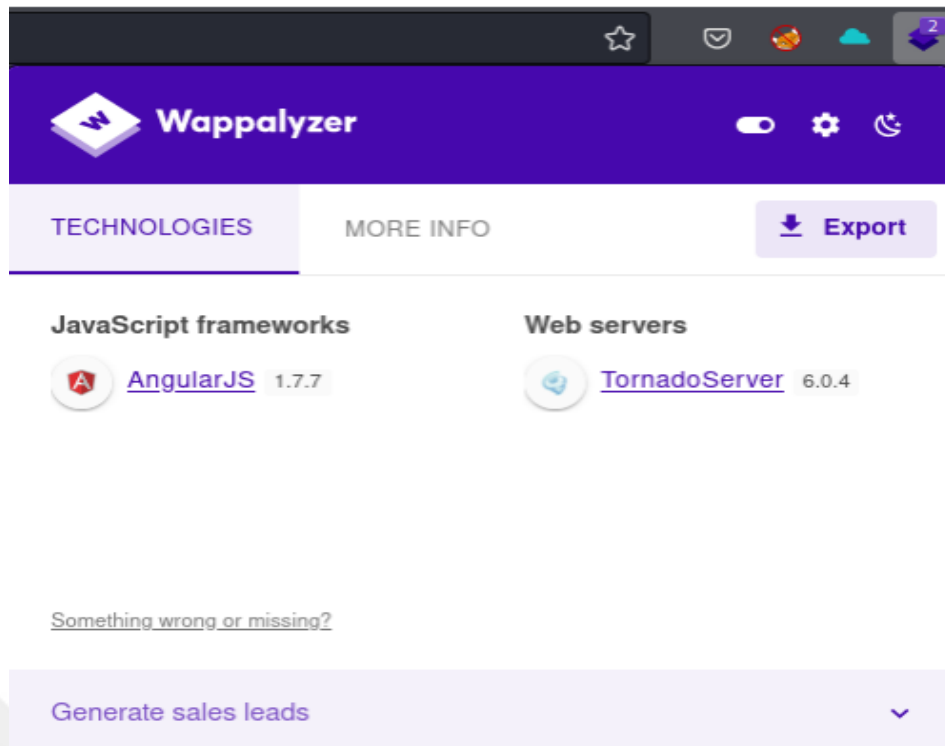


Figure 13 : Technology used to create the APS interface Website

Using this tool we can see that the website was made using AngularJS and JavaScript as a framework.

AngularJS 1.7.7 is known to allow cross site scripting (XSS) which leads us to the possibility of an unsanitized or unclean code in the client-side website.

This vulnerability can be more recognised In the NVD analysts website CVE-2020-7676 which has a vulnerability score of 5.4 which is Medium level vulnerability.

5.2.1.2 APS device client side web interface.

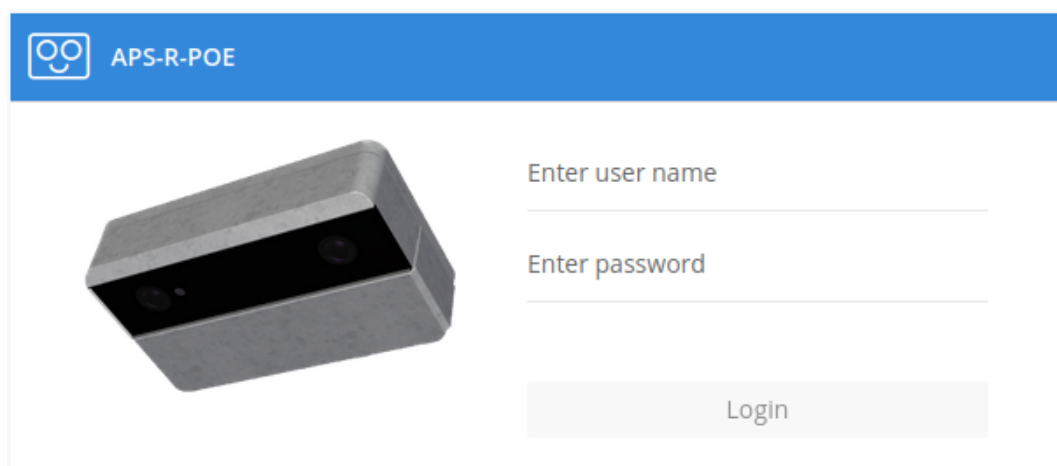


Figure 14 : Login Page

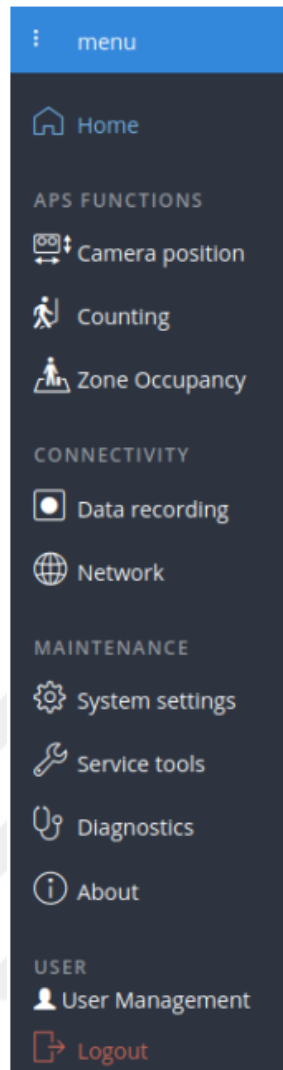


Figure 15 : Web interface menu

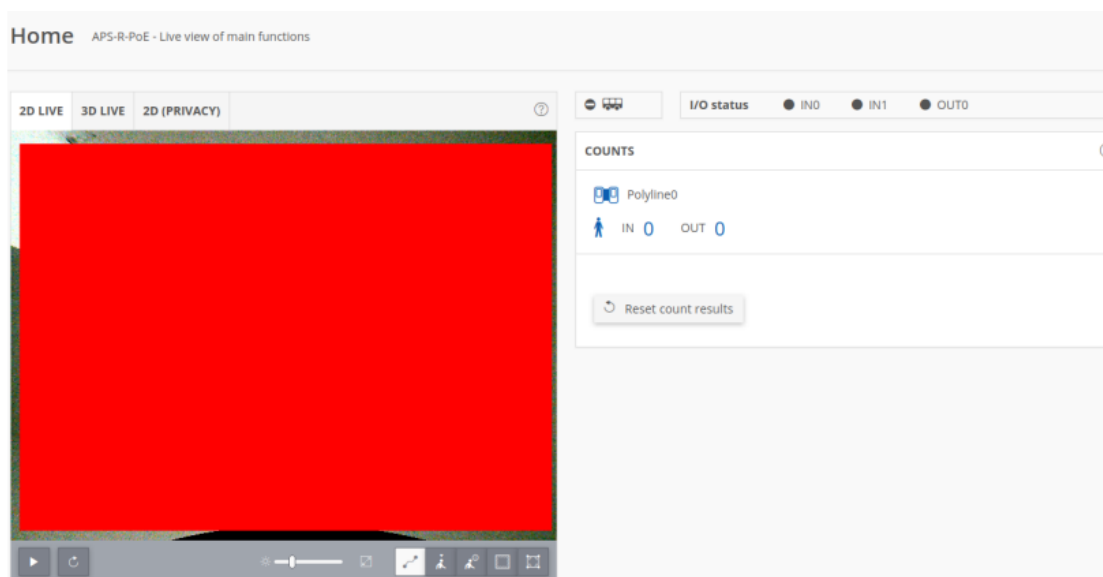


Figure 16 : Home page / 1st page

Functions:

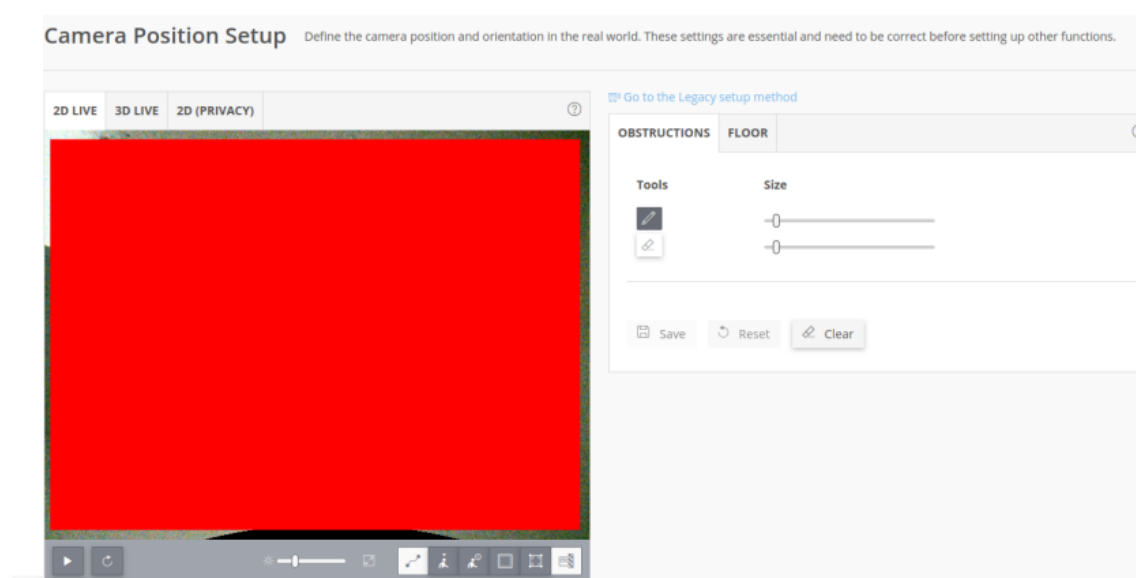


Figure 17 : Camera positioning menu

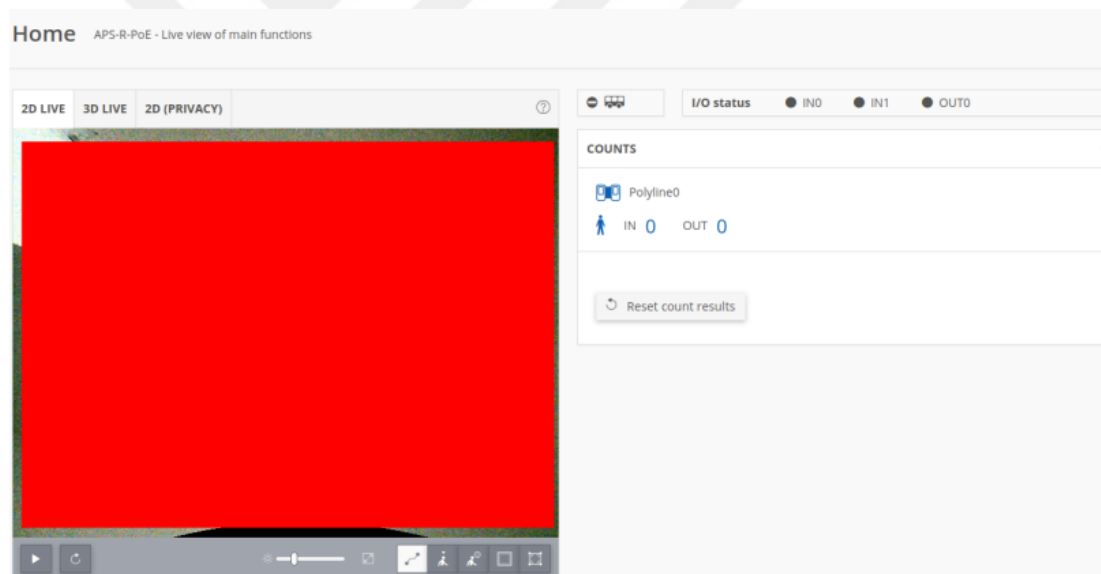


Figure 18 : Counting menu

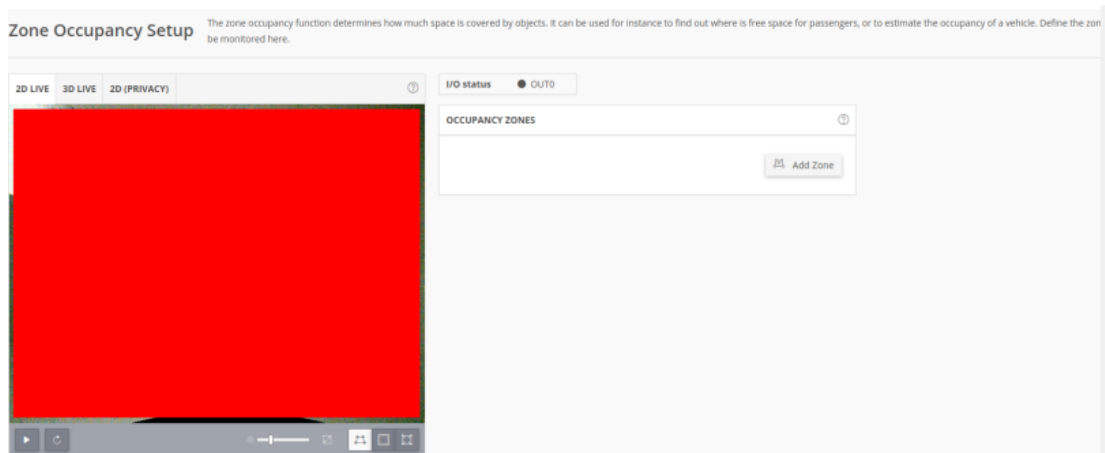


Figure 19 : Zone Ocuupancy Setup menu

Device connectivity :

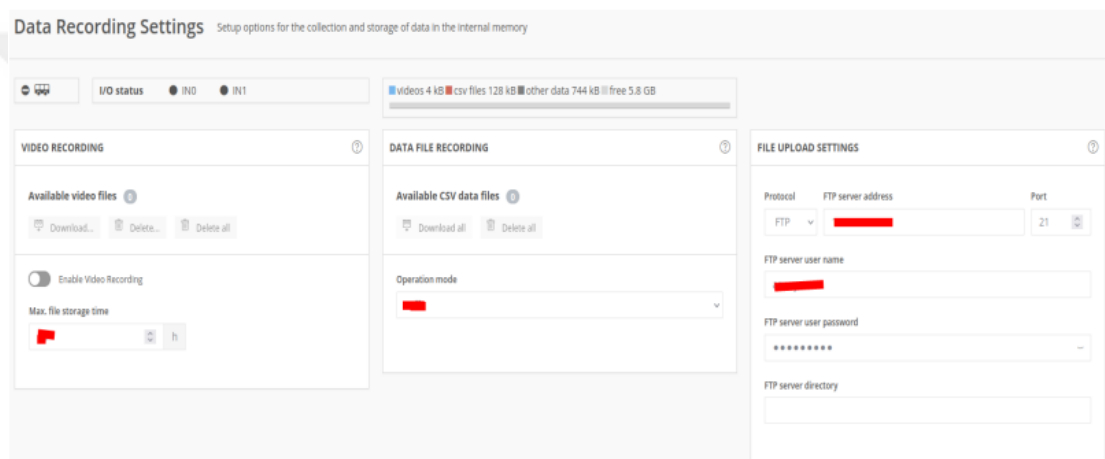


Figure 20 : Data recording menu

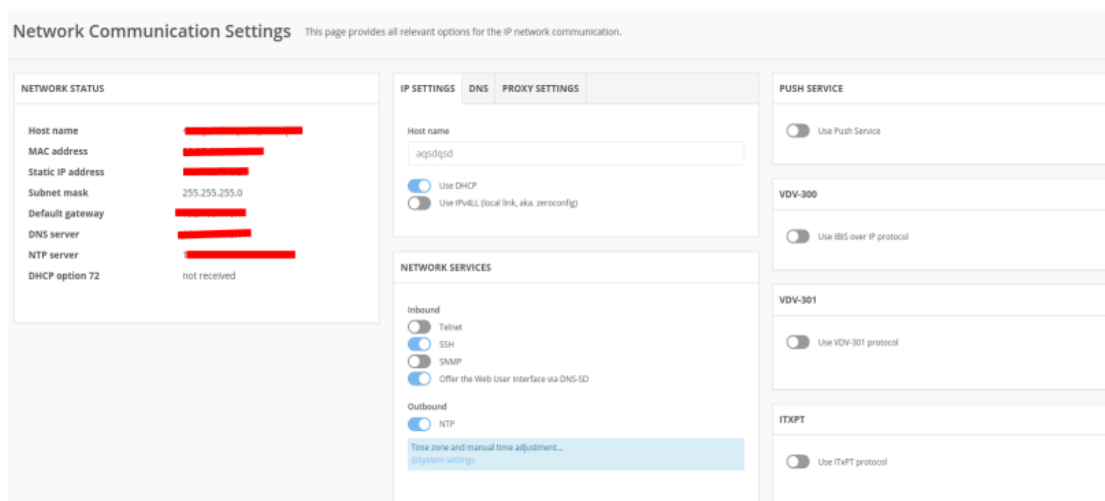


Figure 21 : Network communication settings menu

Maintenance:

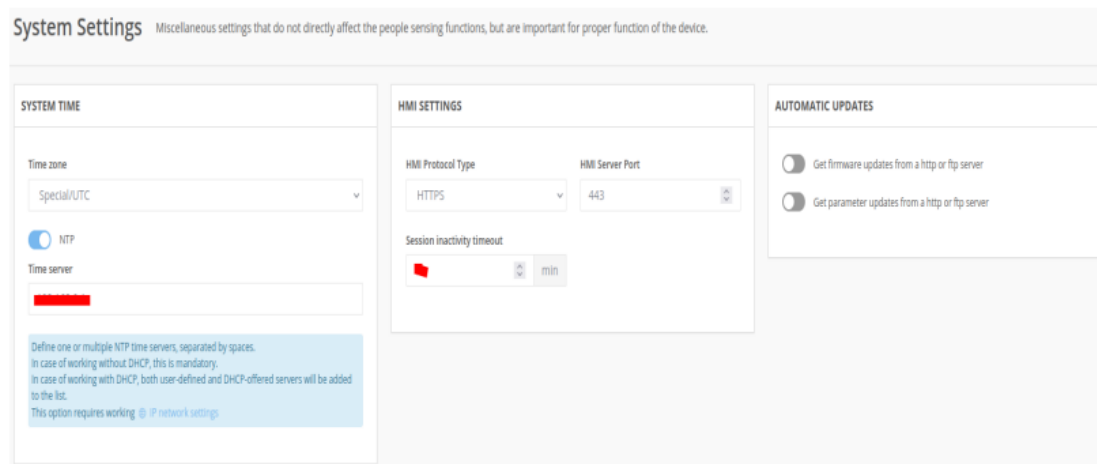


Figure 22 : System settings menu

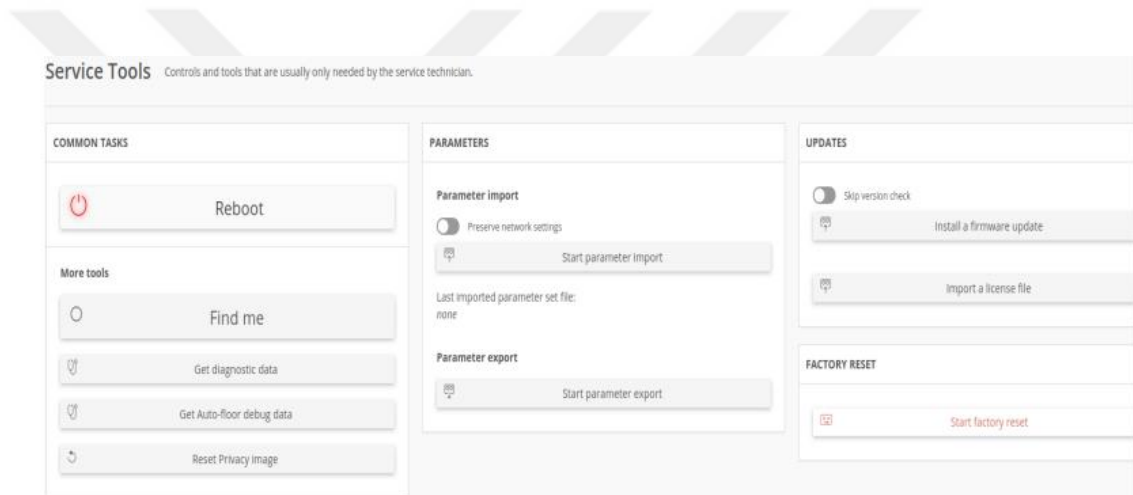


Figure 23 : Service Tools menu

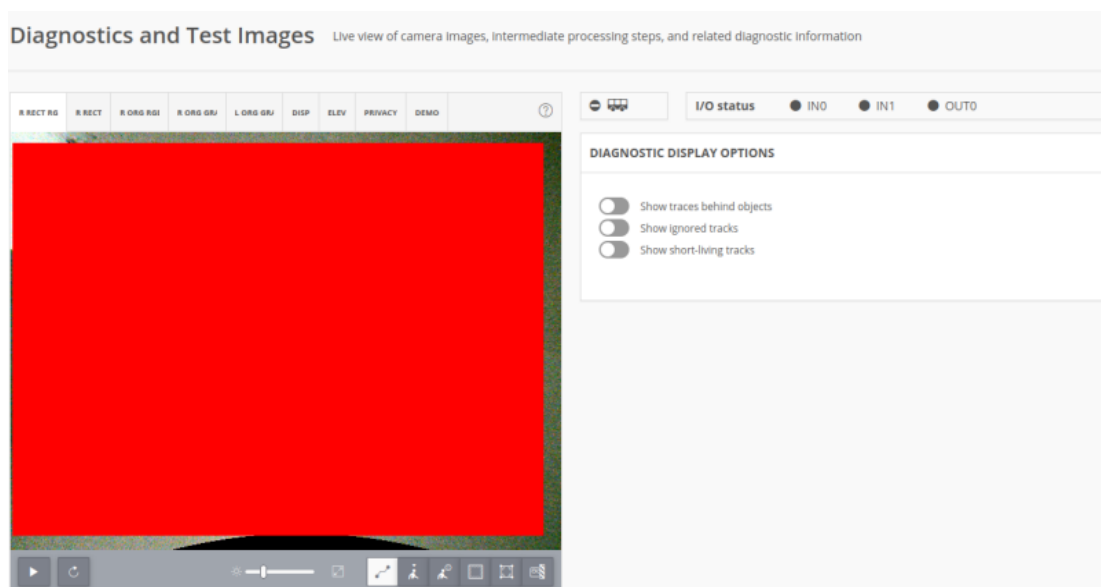


Figure 24 : Diagnostics and Test images menu

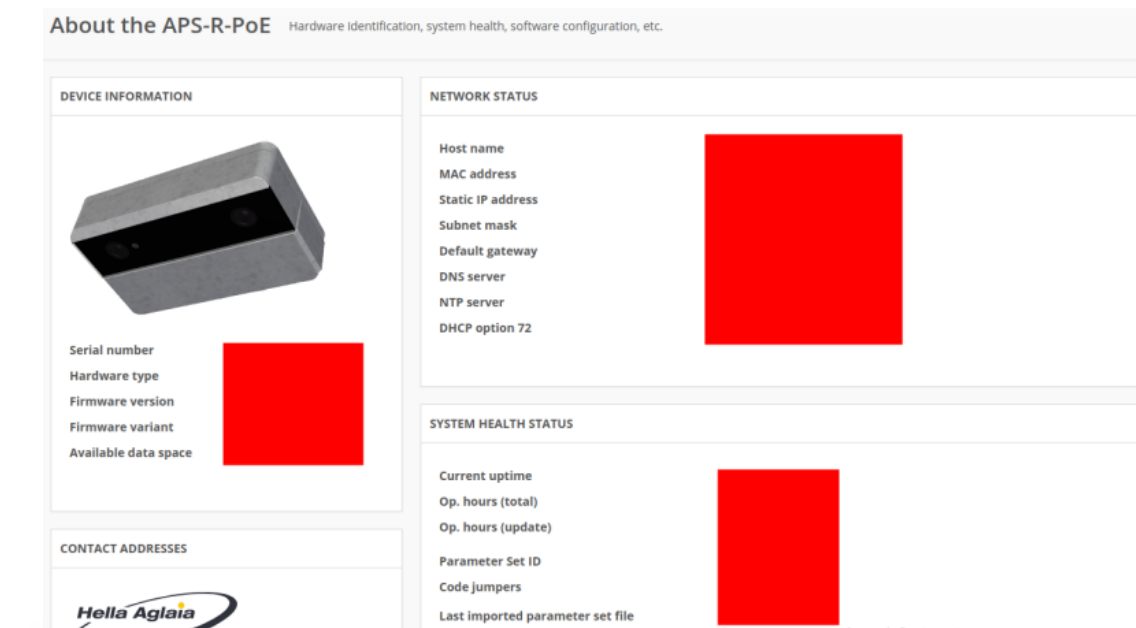


Figure 25 : About menu

Device User:

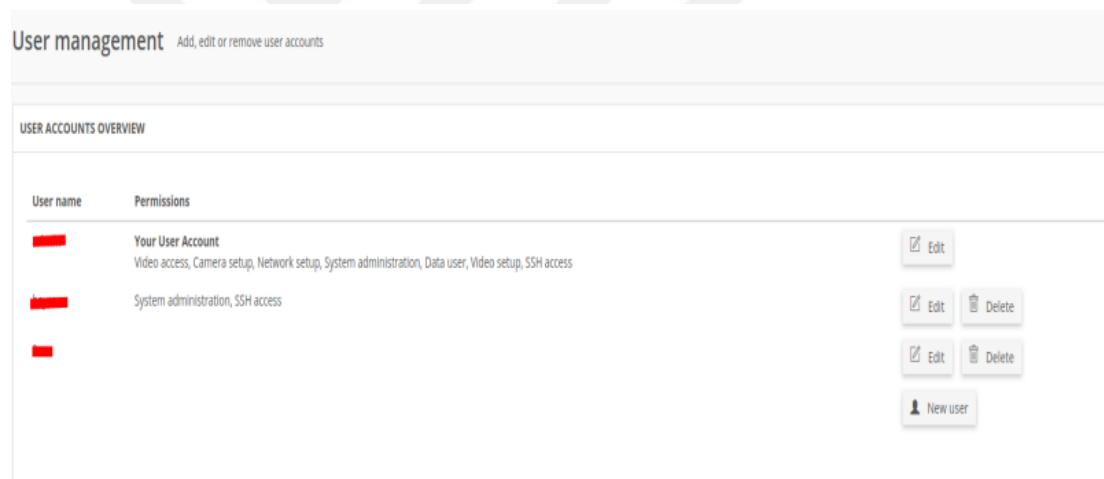


Figure 26 : User management menu

5.2.2 Burpsuite target discovering

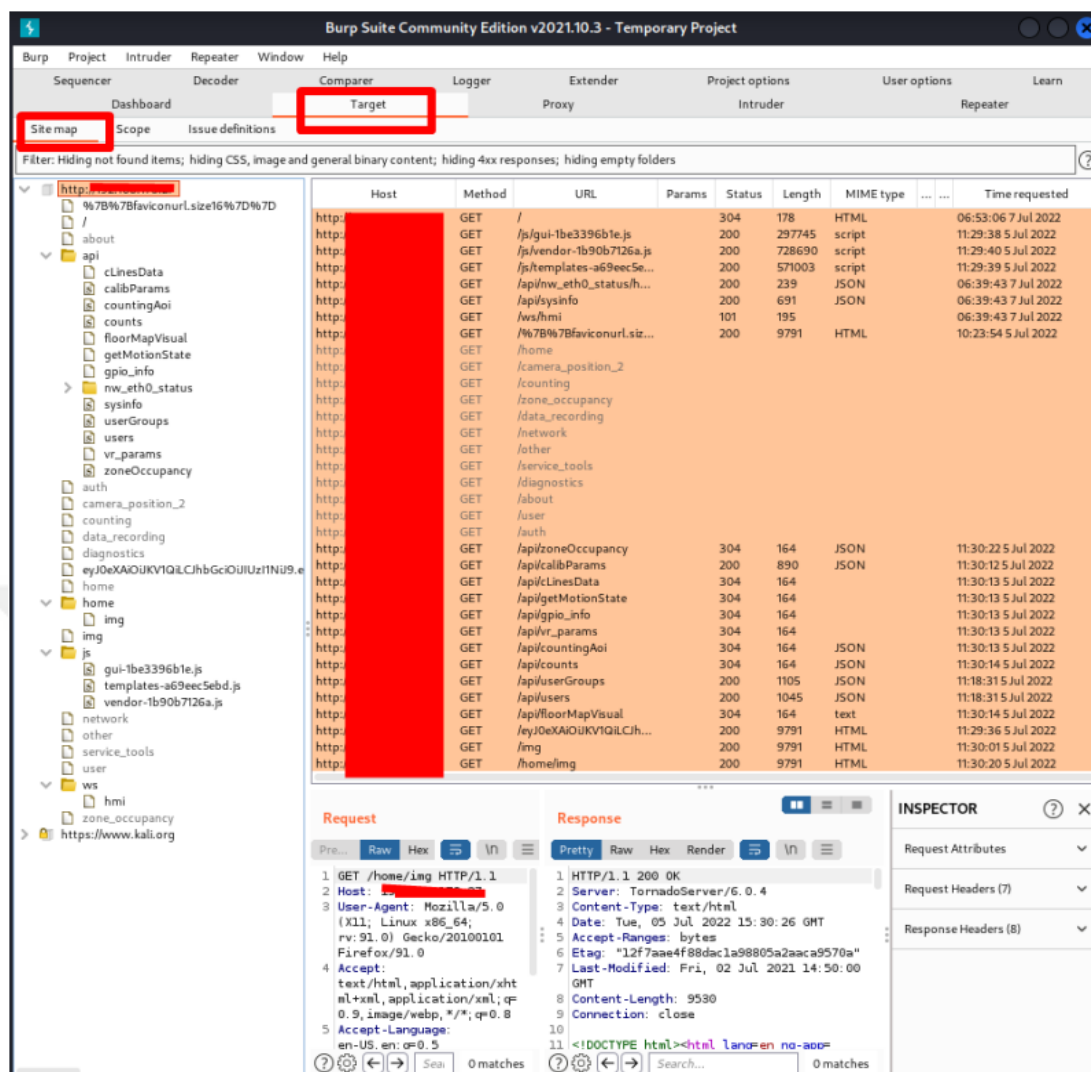


Figure 27 : Burpsuite

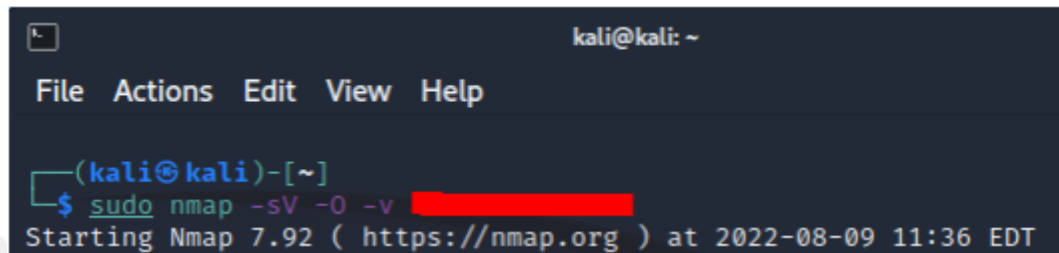
Burp Suite is a well-known software tool utilized for testing the security of web applications. It is a potent platform equipped with a diverse set of tools that are specifically designed to identify and potentially exploit any security weaknesses present in web applications. The figure shown above shows us all the information the Burp gathers about the website.

5.2.3 nmap scan.

Nmap is an open-source tool that is used for network exploration, management, and security auditing. It is commonly utilized by network administrators, security professionals, and ethical hackers to uncover hosts and services on a computer network and pinpoint possible security weaknesses and risks. Nmap employs a variety of methods to scan network hosts and retrieve network-related details such as open ports,

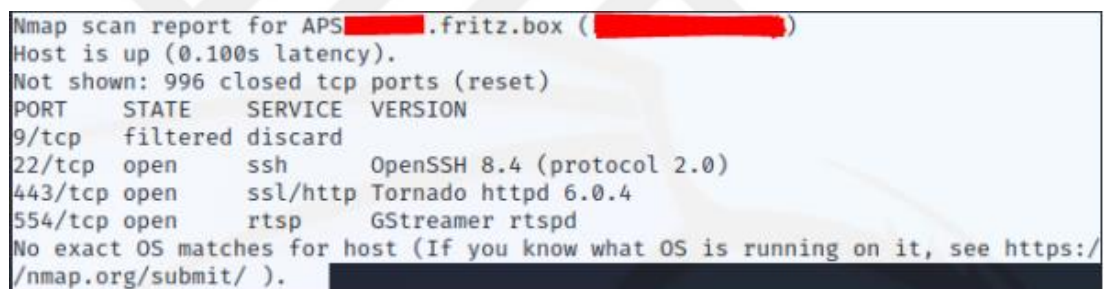
operating systems, and services. It is also capable of executing advanced network discovery and mapping procedures like TCP/IP fingerprinting, IP address spoofing, and OS detection. Furthermore, Nmap can perform more intricate tasks such as firewall evasion, packet crafting, and vulnerability scanning.

We will be running Nmap on the client-side website to check for any open ports. We will be using -SV to probe open ports, -O to detect the operating system used, and -v to Increase verbosity level



```
kali@kali: ~  
File Actions Edit View Help  
  
(kali@kali)-[~]  
$ sudo nmap -sV -O -v [redacted]  
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-09 11:36 EDT
```

Figure 28 : Using Nmap on Kali terminal

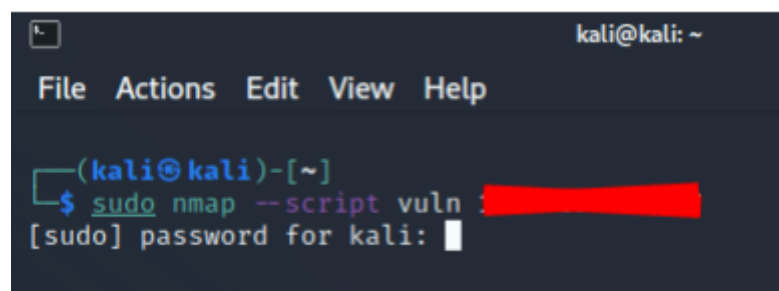


```
Nmap scan report for APS[redacted].fritz.box ([redacted])  
Host is up (0.100s latency).  
Not shown: 996 closed tcp ports (reset)  
PORT      STATE      SERVICE      VERSION  
9/tcp     filtered  discard  
22/tcp    open      ssh          OpenSSH 8.4 (protocol 2.0)  
443/tcp   open      ssl/http     Tornado httpd 6.0.4  
554/tcp   open      rtsp         GStreamer rtspd  
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
```

Figure 29 : Result / Open ports found

Nmap scans the top 1000 ports for each scan protocol requested, usually is catches 93% of the TCP ports and 49% of UDP ports.

After our scan we found 4 open ports, 22,443,554. Next we will run a vulnerability scan using the same tool.



```
kali@kali: ~  
File Actions Edit View Help  
  
(kali@kali)-[~]  
$ sudo nmap --script vuln [redacted]  
[sudo] password for kali: [redacted]
```

Figure 30 : Looking for possible vulnerabilities.

```

|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-slowloris-check:
|   VULNERABLE:
|   Slowloris DOS attack
|   State: LIKELY VULNERABLE
|   IDs: CVE:CVE-2007-6750
|   Slowloris tries to keep many connections to the target web server open

```

Figure 31 : Result of the vulnerability scan.

According to the figure above, the device is likely vulnerable to DOS attacks.

5.2.4 XSS vulnerability testing.

Stored XSS, also known as Persistent XSS, is a web application vulnerability that enables attackers to insert malicious code into a web page, which is then stored on the server-side. This code is subsequently displayed to all users who access the affected web page, potentially compromising their browsers and stealing sensitive data. The danger of Stored XSS attacks lies in their ability to impact multiple users and go unnoticed for extended periods. Additionally, removing or locating the injected code from the server-side can be challenging, making it harder to address the vulnerability.

While running some payloads on unput fields, we found a vulnerable input field in the “Network communication settings menu” (Figure 21).

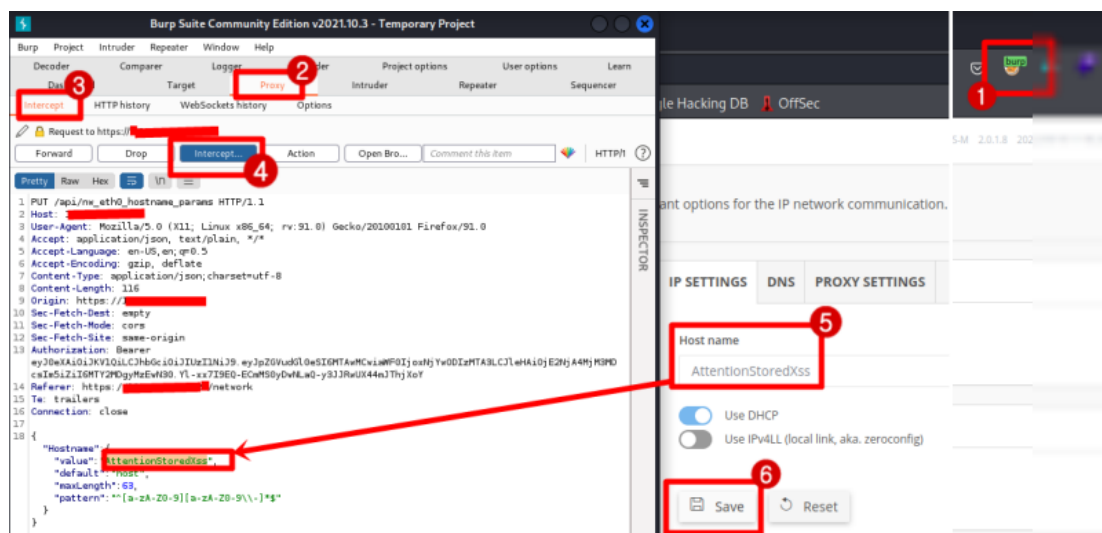


Figure 32 : Request interception

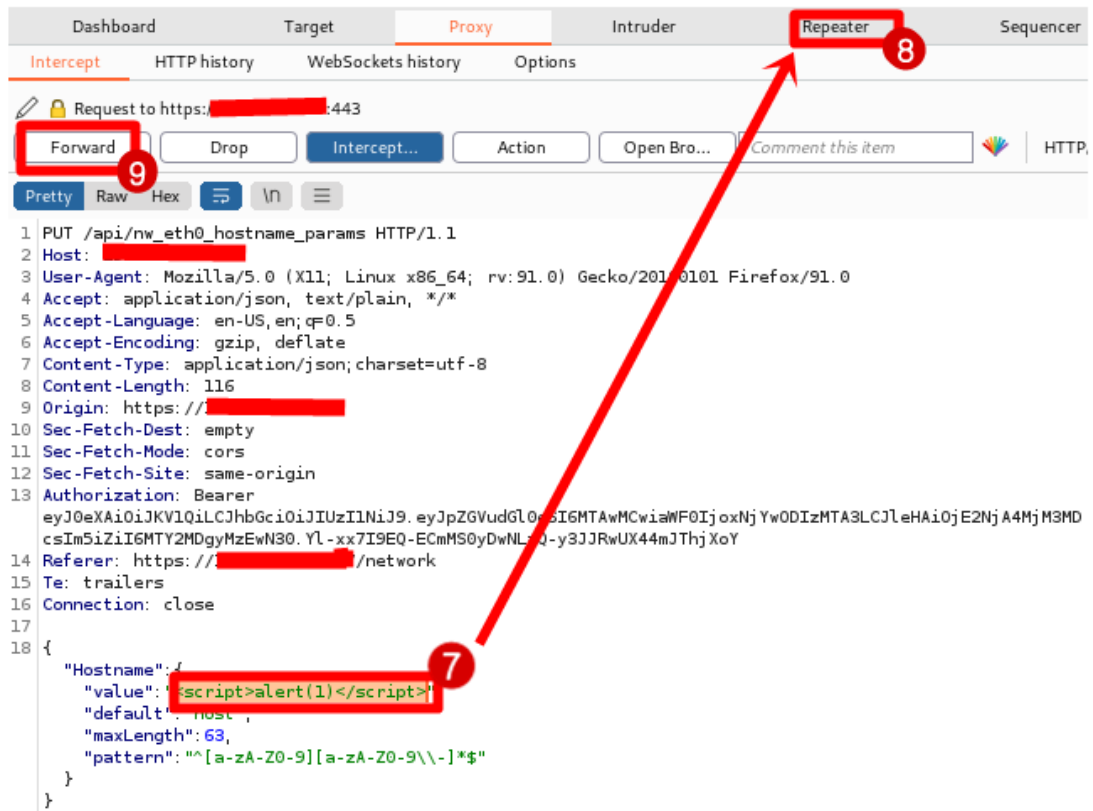


Figure 33 : XSS payload injection

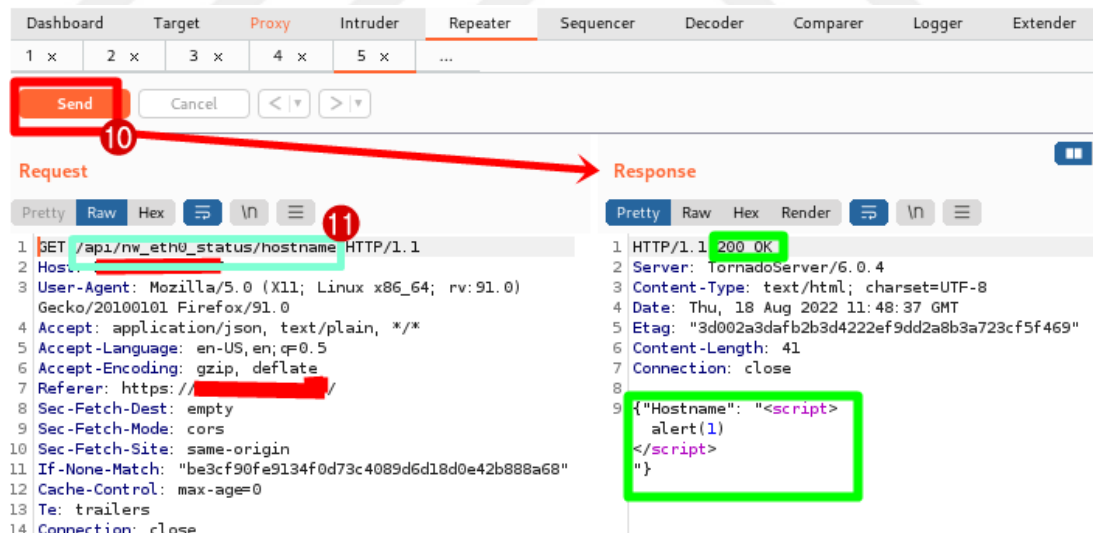


Figure 34 : Verification for the request acceptance

5.2.5 enumeration results.

There were three vulnerabilities found in the client-side website:

- Stored XSS.
- Open ports.

- Vulnerable to DDOS attack.

5.3 Exploitation

We have identified the vulnerabilities and now it's time to exploit them. In this section we will attempt to exploit the vulnerabilities found in the information gathering phase.

5.3.1 Bruteforcing.

Using Burpsuite, after intercepting the request before it reaches the server, we can retransfer it the the “intruder” section. After that we can chose what to input in our payloads.

We want to figure out what is the correct “username” and “password” so we selected them and the we chose the attack type which is “cluster bomb” which is using multiple wordlists.

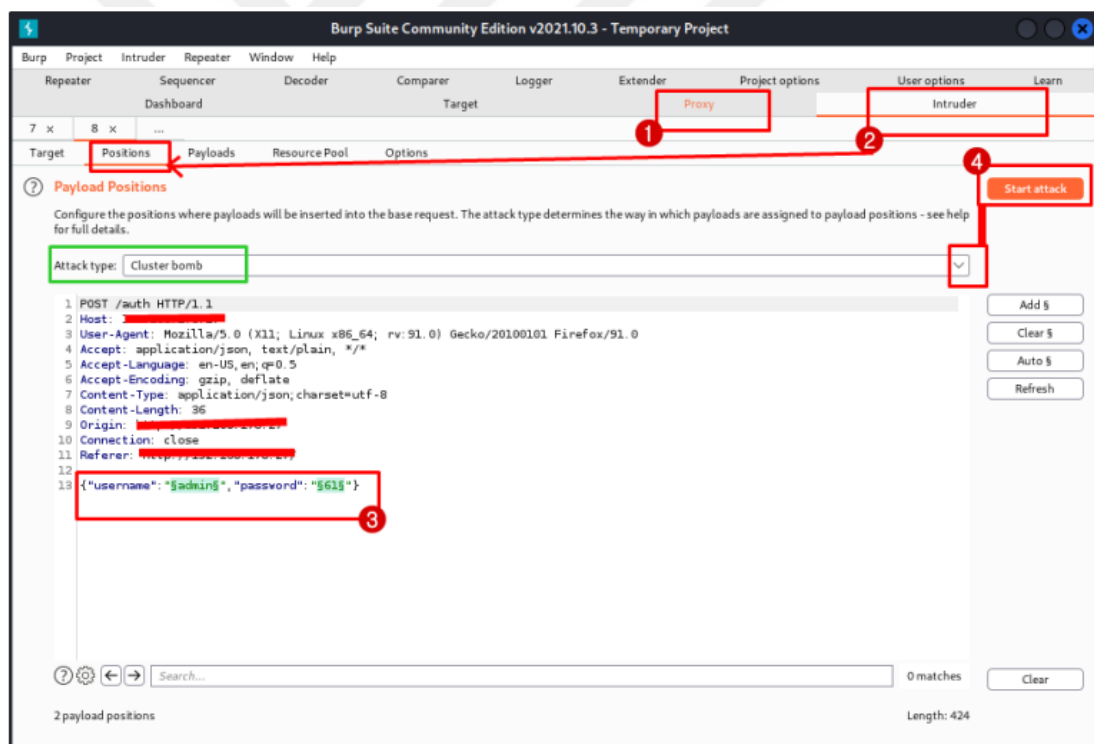


Figure 35 : Selecting payload and attack type

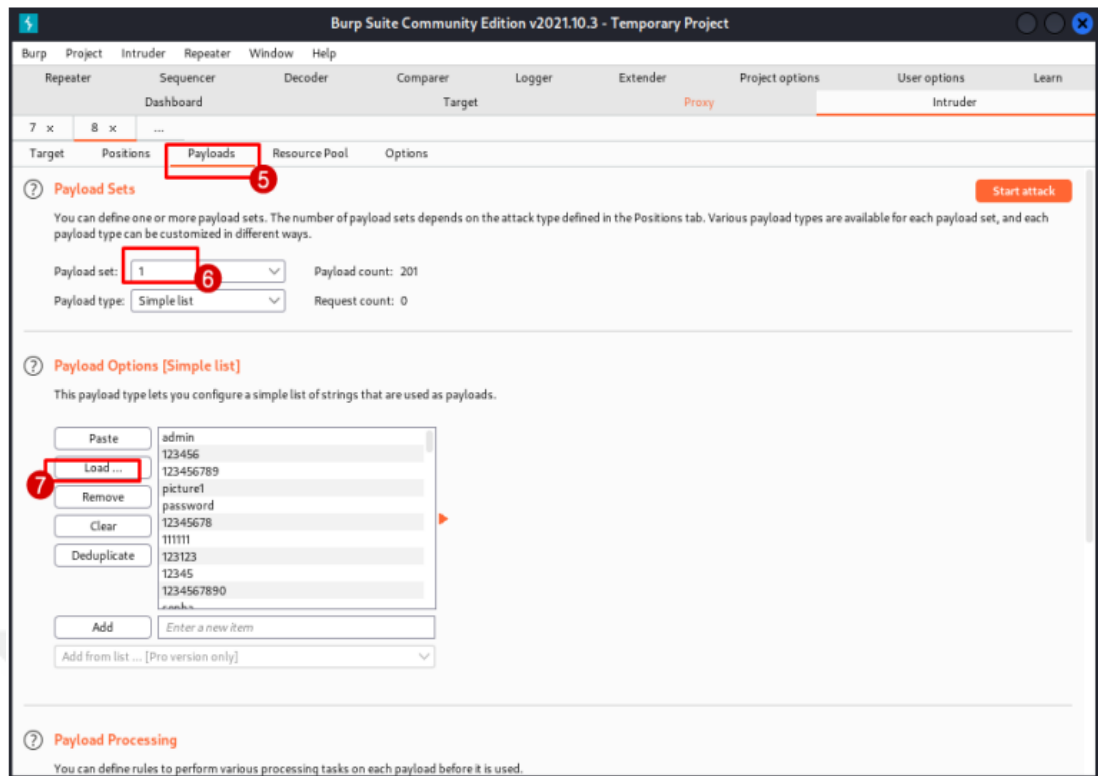


Figure 36 : Choosing the username word list

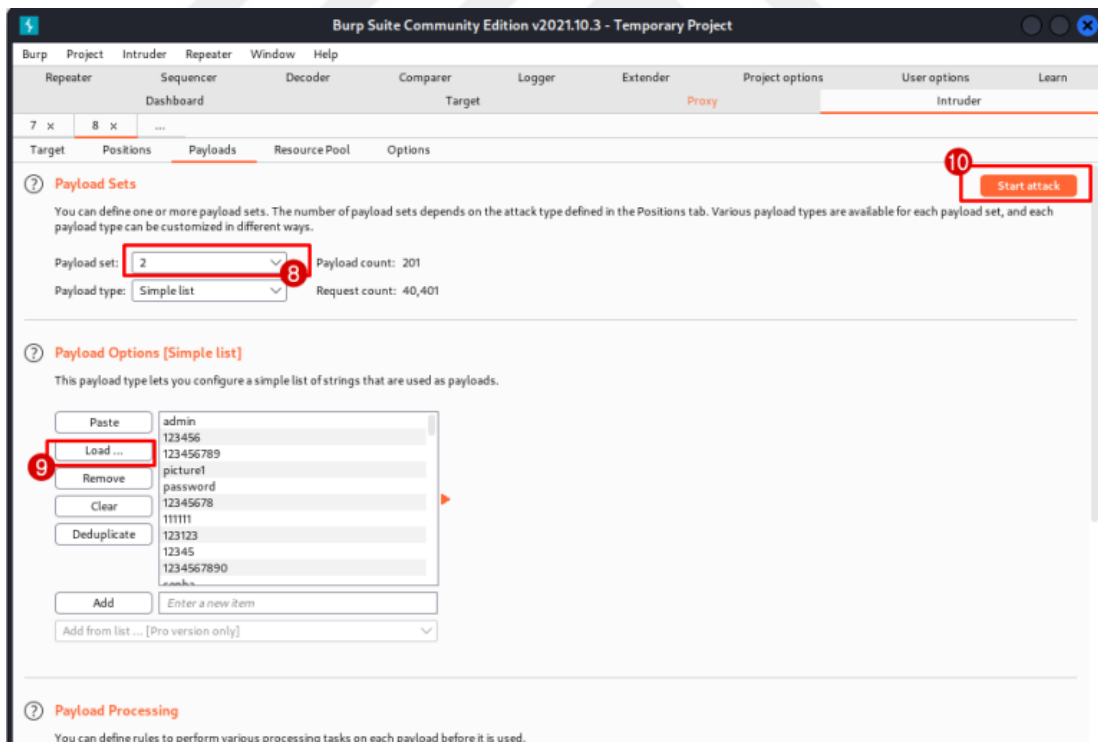


Figure 37 : Choosing the password word list

After choosing these 2 payloads we can simply start the attack.

The screenshot displays the Burp Suite interface during an intruder attack. The title bar reads "8. Intruder attack of 192.168.178.27 - Temporary attack - Not saved to project file". The "Results" tab is active, showing a table of attack results. The table has columns: Request, Payload 1, Payload 2, Status, Error, Timeout, Length, and Comment. The first row is highlighted in orange and has a red box around it. The "Status" and "Length" columns for this row are highlighted with green boxes. Below the table, the "Request" tab is selected, showing a POST request to /auth HTTP/1.1. The request body is in "Pretty" format and shows a successful login response with status 200.

Request	Payload 1	Payload 2	Status	Error	Timeout	Length	Comment
1	admin	admin	200			1025	
3	aaren	admin	401			198	
4	aarika	admin	401			228	
5	aaron	admin	429			225	
6	aartjan	admin	429			225	
7	aarushi	admin	429			225	
8	abagael	admin	429			225	
9	abigail	admin	429			225	
10	abahri	admin	429			225	
11	abbas	admin	429			225	
12	abbie	admin	429			225	
13	abbey	admin	429			225	
14	abbi	admin	429			225	
15	abbie	admin	429			225	
16	abby	admin	429			225	
17	abbye	admin	429			225	
18	abdalla	admin	429			225	
19	abdallah	admin	429			225	
20	abdul	admin	429			225	

```
1 POST /auth HTTP/1.1
2 Host: 192.168.178.27
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
4 Accept: application/json, text/plain, */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/json; charset=utf-8
8 Content-Length: 39
9 Origin: http://192.168.178.27
10 Connection: close
11 Referer: http://192.168.178.27
```

Figure 38 : Attack results

We can see that we successfully got the credentials for the client side website with the 200 status as shown in the figure above (status 200 the request was successful) and the user name and password were “admin, admin”

5.3.2 cross site scripting vulnerability (XSS).

XSS attacks are injection type attacks where malicious JS code is injected into a web application with the intention of being executed by other users when logging in or while surfing the website.

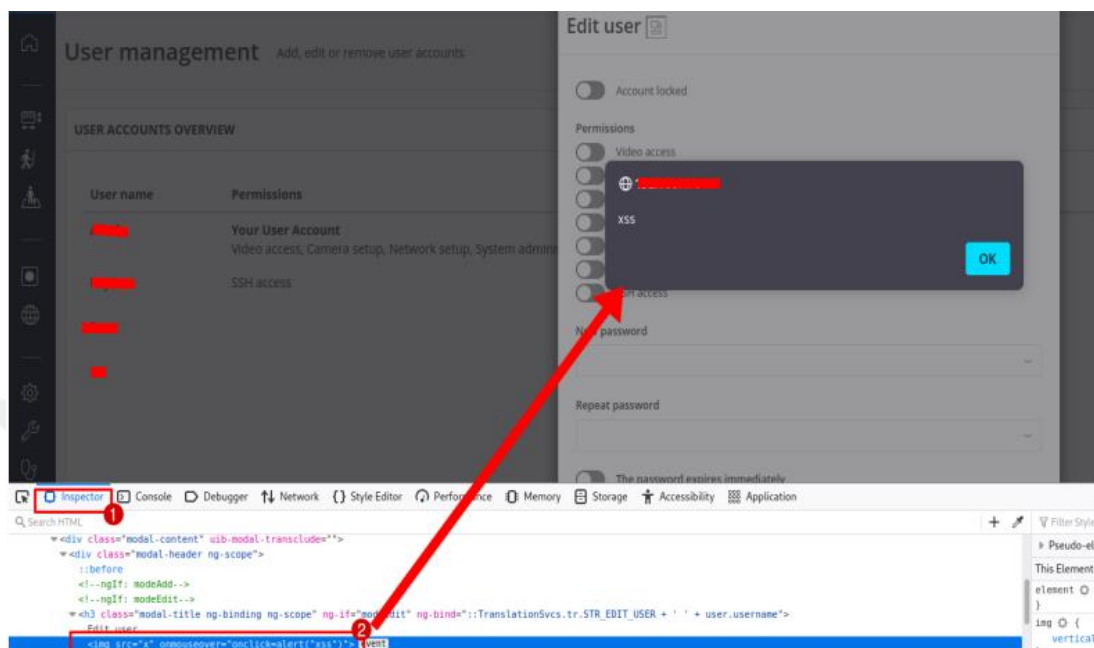


Figure 39 : XSS alert

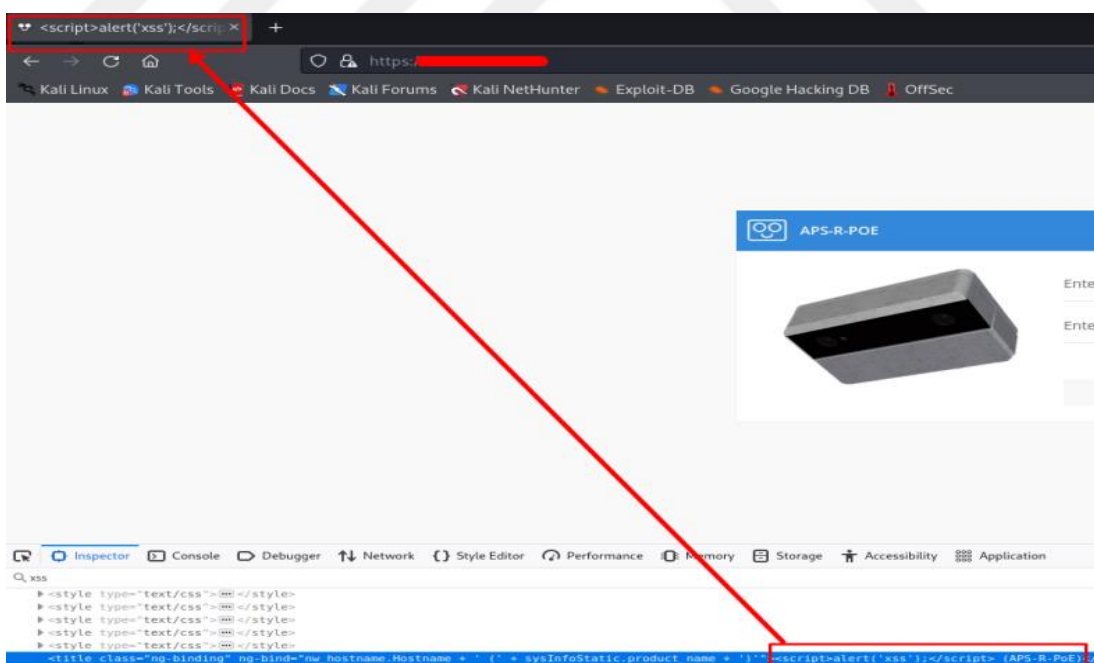


Figure 40 : Finding the XSS script

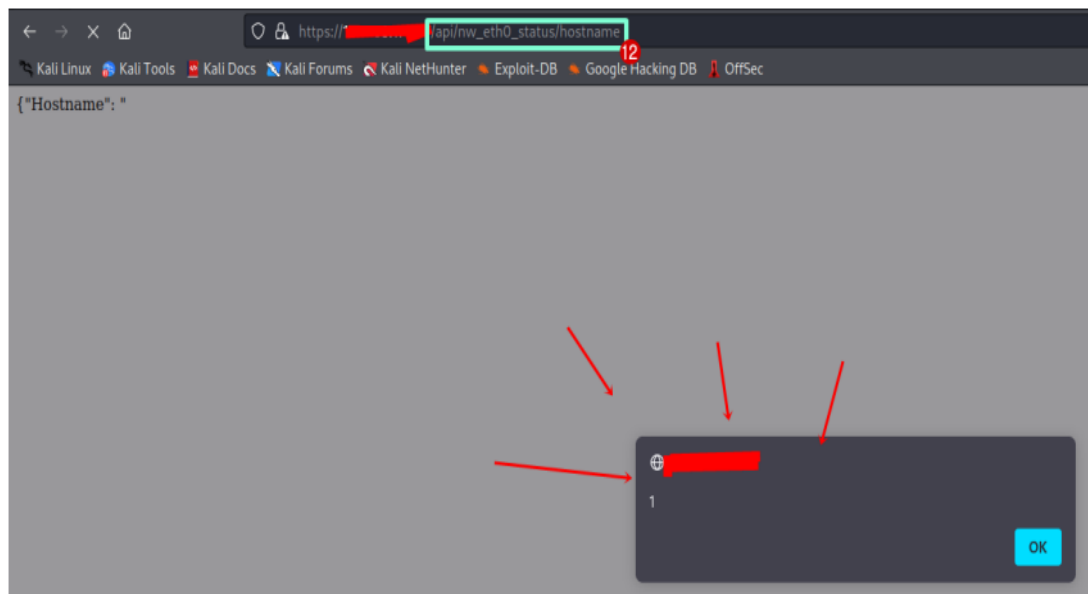


Figure 41 : Alert pops-up

Now that we know that the vulnerability exists and works we can use any payload at our disposal to get any information out of the XSS, for example we can use `<script> alert(document.cookie)</script>` to steal the user's cookies and then use them to access their profiles or steal other data.

5.3.3 DDOS attacks.

Previously we found that the website is vulnerable to DDOS attack (denial-of-service attack) which is attempting to disrupt normal traffic of a target server, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic. For this attack we will be using a DDOS tool available on Kali.

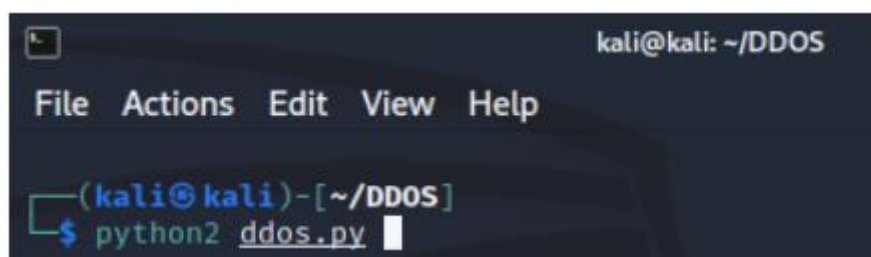


Figure 42 : DDOS attack command

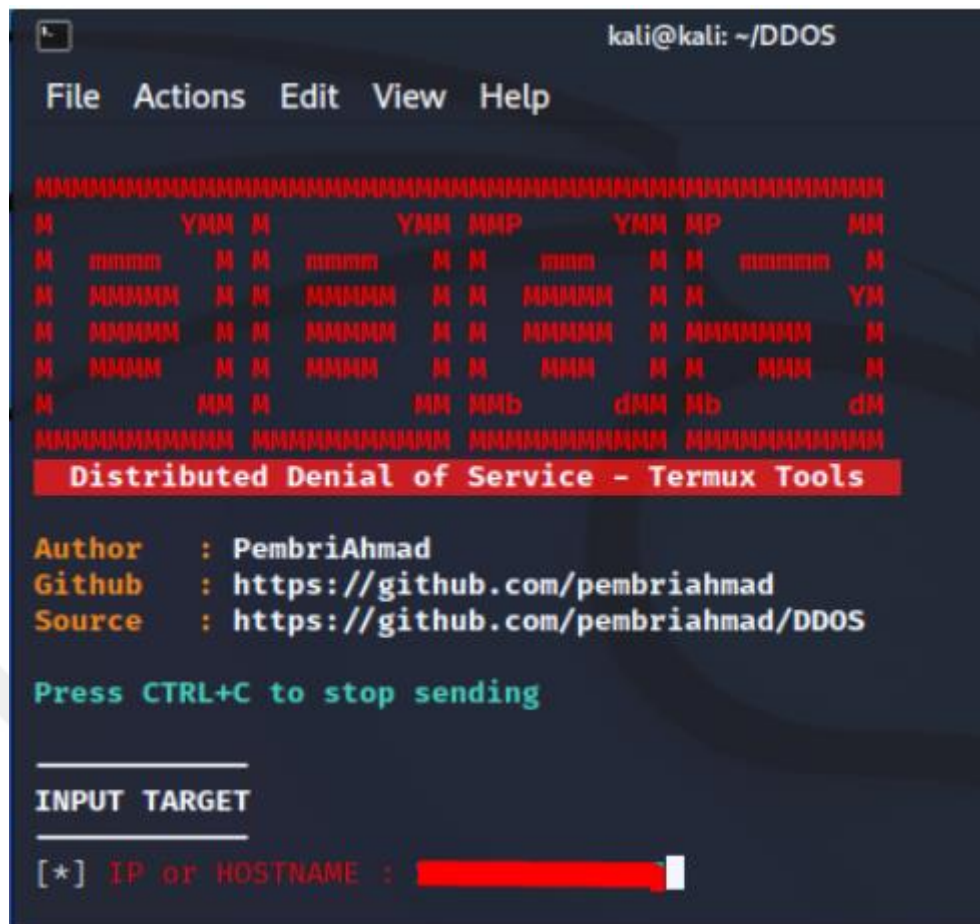


Figure 43 : Starting the DDOS attack

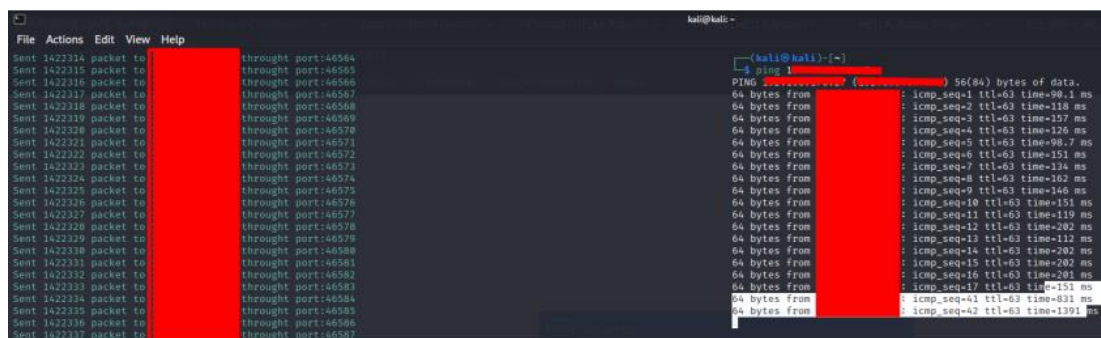


Figure 44 : DDOS attack result

Looking at the previous figure, we can see that pinging the device shows that it is very slow and the latency is very high compared to normal (1391ms) and that is because of the huge amounts of traffic coming from a range of IP addresses of bots called a 'botnet'. A 'botnet' is a network of private computers infected with malicious software that can be controlled as a collective group with the knowledge of the owners.

5.4 Implementation of ETSI EN 303 645 standard

After performing the penetration testing on the device to fully understand how it works and the weaknesses it has, we now need to evaluate its security according to the ETSI EN 303 645 standard to finalize what needs to be reviewed for the device and to set a baseline for future devices to look on before marketing their product to ensure the safety of their client from the minimum type of attacks.

5.4.1 evaluation of the APS according to the standard.

To evaluate the device according to the standard we will be using a table provided by the official documentation of the standard to give information about the implementation of the provisions.

The table will have the following format:

- **The reference column:** Will contain the reference to the provisions
- **The status column:** Will contain the status of the provision

Notation:

M : The provision is a mandatory requirement

R : The provision is a recommendation

M C: The provision is a mandatory requirement and conditional

R C: The provision is a recommendation and conditional

EX: Example

- **The support column:** will use the following notation:

Y : Supported by the implementation

N : not support by the implementation

N/A : the provision is not applicable (the provision is not applicable for the product in question)

- **The detail column:** Will be filled by the writer of this report as a further explanation

If a provision is supported by the implementation, the entry in the detail column is to contain information on the measures that have been implemented to achieve support.

If a provision is not supported by the implementation, the entry in the detail column contains information on the reason why implementation is not possible.

If a provision is not applicable, the entry in the detail column will say so.

Table for implementation of the standard			
Reference	Status	Support	Detail
5.1 No universal default password			
Provision 5.1-1	M C (1)	EX-1: N	There is a possibility of using universal usernames and password i.e “admin, admin” and users are not obliged to make a change while using the device
		EX-2: N	There is no multifactor authentication (2FA) to access the device
		EX-3: Y	Device unique immutable identities MAC address and static IP address
Provision 5.1-2	M C (2)	EX-1: N/A	No generated pre-installed password
		EX-2: N/A	No generated pre-installed password Can use easy guessable passwords
Provision 5.1-3	M	N: http Y:https	When used in http there is a possibility to capture credentials When switching to https, authentication credentials become encrypted
Provision 5.1-4	M C	EX-1: Y	Users can change password anytime
		EX-2: Y	Admins can restrict other users from changing passwords
Provision 5.1-5	M C (5)	N	There is no specific attempts limit only a 20s period between 3 wrong attempts No brute force detection on the ssh open ports
5.2 Implement a means to manage reports of vulnerabilities			
Provision 5.2-1	M	N	No public VDP (Vulnerability Disclosure Policy)
Provision 5.2-2	R	N	No VDP
Provision 5.2-3	R	EX-1: Y	We can find active interfaces for continuous monitoring like automatic updates in the “system settings” and updates under “service tools” which allows the user to continuously monitor the system

		EX -2: Y	No VDP just contact page. You can send a feedback for the product so the developpers can improve the product.
5.3 Keep software updated			
Provision 5.3-1	R	Y	You can updates the product
Provision 5.3-2	M C	Y	You can get the updates directly from the server of the manufacturer You can allow/disallow firmware downgrades from the menu service tools > updates > skip version check
Provision 5.3-3	M C	Y	You can download updates from system setting and install it from the parameters menu
Provision 5.3-4	R C	EX -1: N	No automatic upadate mechanisms
		EX -2: Y	The device can detect Software and Hardware update problems and ensure the recovery of the device
Provision 5.3-5	R C	N	No automatic device updates check
Provision 5.3-6	R C	N/A	Device does not support automatic updates so not applicable
Provision 5.3-7	M C	Y	There is cryptographic features for the update
Provision 5.3-8	M C	Y	Updates can be available on the device website
Provision 5.3-9	R C	Y	The user can access the download portal where you can download the latest updates and documentation with full detail and factcheck and you can send an email to people.counter.support@hella.com if you encounter any issue with the update and report it to the developers
Provision 5.3-10	M	Y	You receive update from the official servers
Provision 5.3-11	R C	Y	Notification from email
Provision 5.3-12	R C	Y	Notification with the update information on the device via email
Provision 5.3-13	M	Y	All update infos are available on the webite people-sensing.com

Provision 5.3-14	R C	N/A	Not applicable
Provision 5.3-15	R C	N/A	Not applicable
Provision 5.3-16	M	Y	Model designation is available in the about section in the web interface
5.4 Securely store sensitive security parameters			
Provision 5.4-1	M	Y	Sensitive security parameters like cookies and data are secured by web analytics services like “PIWIK PRO cloud” and stored in well known secure servers that use encryption.
Provision 5.4-2	M C	EX -1: Y	Resist identity tampering by software
		EX -2: N	Not mentioned
		EX -3: N	No notification available
Provision 5.4-3	M	Y	No security parameters are exposed in source code
Provision 5.4-4	M	Y	Unique CSP per device
5.5 Communicate securely			
Provision 5.5-1	M	Y	Protocol version TLSv1.3
Provision 5.5-2	R	Y	Cipher suite TLS_AES_256_GCM_SHA384
Provision 5.5-3	R	EX -1: Y	Signature scheme: RSA-pSS-SHA256
		EX -2: N	Not mentioned on their website
Provision 5.5-4	R	Y	Every user can access his own account to the device and his functionalities assigned to him by the developers
Provision 5.5-5	M	Y	The admin can give access to device security setting
Provision 5.5-6	R	Y	In the case of HTTPS the data is encrypted in transfer
Provision 5.5-7	M	EX -1: Y	Remote communication is secure
		EX -3: Y	After a period of time of no activity (IDLE) the session is expired automatically and the user has to authenticate again
Provision 5.5-8	M	N	Not mentioned
5.6 Minimize exposed attack surfaces			
Provision 5.6-1	M	Y	All unused network and interfaces are disabled and all usable ones are available in the website with a description to the functionality

Provision 5.6-2	M	Y	No security relevant information is exposed on the website
Provision 5.6-3	R	Y	All usable interfaces are lighten up in the client side website
Provision 5.6-4	M C	N/A	No debug interface that is accessible
Provision 5.6-5	R	EX -2: Y EX -3: Y	Important services are neabled and explained with a description for each service
Provision 5.6-6	R	Y	Code is secure (according to the factsheet on the website)
Provision 5.6-7	R	Y	the only privilege the user has is controlling the device and communicating with the main servers for updates
Provision 5.6-8	R	N	Provision not mentioned anywhere for the device
Provision 5.6-9	R	Y	The debelopment process for the device is secure (according to the description in the website)
5.7 Ensure software integrity			
Provision 5.7-1	R	N	No hardware root device is used or mentioned by the manufacturer
Provision 5.7-2	R	EX -1: Y	You can run a diagnostic data which helps the device understand if there is any problem by going to the service tools section and get diagnostic data
		EX -2: N	Chnages are not alerted to the user
		EX -3: Y	Can restore original default settings with factory reset
5.8 Ensure that personal data is secure			
Provision 5.8-1	R	EX -1: Y	The device can use HTTPS encryption so no data can be captured by using for example wireshark
		EX -2: Y	The device can use HTTPS encryption so no data can be captured by using for example wireshark
Provision 5.8-2	M	Y	The device can use HTTPS encryption so no data can be captured by using for example wireshark
Provision 5.8-3	M	Y	All functionalites of the device are available on the website and pdf file provided by the manufacturer https://people-sensing.com/public-transport/

			https://people-sensing.com/wp-content/uploads/2022/03/HELLA_Aglaia_People_Sensing_APS-R-PoE.pdf
5.9 Make systems resilient to outages			
Provision 5.9-1	R	Y	The use of Operating volatage power over ethernet PoE (mentioned on the website) is capable of making the device work during a power outage
Provision 5.9-2	R	Y	The device has a storage capacity of 5.8 GB that allows it to store recorded videos and saving them in case of power outage
Provision 5.9-3	R	N	The device cannot reconnect atomatically and not secure against a DDOS attack as proved earlier
5.10 Examine system telemetry data			
Provision 5.10-1	R C	Y	You can run a diagnostic check which helps the device support and understand the problems, Service_tools > get diagnostic data You can also check debug data in the same manner Service_tools > get auto-floor debug data.
5.11 Make it easy for users to delete user data			
Provision 5.11-1	M	Y	In the website it is mentioned that the personal data of the user is safe with the manufacturer people-sensing.com/data-protection-declaration/
Provision 5.11-2	R	Y	You can send an email to the company people.counter.support@hella.com and after verifying your identity you can delete your account and after the deletion all you personal data provided will be subsequently deleted.
Provision 5.11-3	R	Y	In their website people-sensing.com/data-protection-declaration/ you can find the reason of processing of the user data in all cases when visting the website, when using the contact form, when setting up a user account, when web hosting and

			finally when submitting a feedback
Provision 5.11-4	R	Y	You can demand at any time to delete your personal data stored by the company and you can request information to confirm that all your data has been deleted
5.12 Make installation and maintenance of devices easy			
Provision 5.12-1	R	Y	Updates are always ready ou can just download them and install.
Provision 5.12-1	R	N	No help or guidance
Provision 5.12-1	R	EX -1: N	No help or guidance
		EX -2: Y	You can use a VPN
5.13 Validate input data			
Provision 5.13-1	M	Y	All inputs are validated for syntax and content but there is always the odd case when you can bypass by randomly putting in default universal credentials
6 Data protection provisions for consumer IoT			
Provision 6.1	M	Y	All included in the website people-sensing.com/data-protection-declaration/
Provision 6.2	M C	Y	You have the right to object to the processing of your data at any time according to Art.21 GDPR
Provision 6.3	M	Y	You have the right to object to the processing of your data at any time according to Art.21 GDPR
Provision 6.4	R C	Y	You have the right to demand restriction of processing of your personal data at any time according to Art.18 GDPR
Provision 6.5	M C	Y	All included in the website people-sensing.com/data-protection-declaration/

Table 1 : Table of implementation of the standard

5.4.2 result.

After performing the conformity assessment of the advanced people sensor IoT device and looking over each provision in detail we can safely say that the device failed to secure the basic functionalities which can lead to multiple threats.

5.4.3 Recommendation for enhancement of the APS device according to the ETSI EN 303 645.

In order to improve the device and enhancement plan must be made and upgrade points must be followed, in the next table we will mention these points to fix the device vulnerabilities

Table of enhancement using the standard				
Reference	Status	Support	Priority	Detail
5.1 No universal default passwords				
Provision 5.1-1	M C	EX -1:N	Urgent	Authetification should be unique (unique password and unsername)
		EX -2:N	Urgent	Implementation of multifactor authentication (password+OTP for example)
Provision 5.1-5	M C	N	Urgent	Passwords should be unique and able to mitigate Bruteforcing attacks
5.3 Keep software updated				
Provision 5.3-4	R C	N	Medium	Updates should install automatically to make sure everyone is up to date
5.4 Securely store sensitive security parameteres				
Provision 5.4-2	M C	N	Urgent	Adding the capability to automatically notify the user upon discovery of an unauthorized physical acess attempt
5.5 Communicate securely				
Provision 5.5-3	R	N	Low	Using an updated cryptographic algorithms

Provision 5.5-8	M	N	Urgent	Key management implementation
5.6 Minimize exposed attack surfaces				
Provision 5.6-8	R	N	Standard	Include a hardware-level root access control mechanism
5.7 Ensure software integrity				
Provision 5.-1	R	N	Standard	Secure the firmware
Provision 5.7-2	R	N	Standard	Provide alerting system for the user and the admin by notifying him if an unauthorized change happened
5.9 Make systems resilient to outages				
Provision 5.9-3	R	N	Standard	Capability of reconnecting to the network in case of an outage and the capability to mitigate DoS attack
5.12 Make installation and maintenance of devices easy				
Provision 5.12-2	R	N	Standard	Should help new users set up the device in a secure manner
Provision 5.12-3	R	N	Standard	Should provide guidance to check whether the device is set securely or not
5.13 Validate input data				
Provision 5.13-1	M	N	Urgent	Implement strong login credentials to secure the login process and sanitize input fields to prevent XSS attacks

Table 2 : Device enhancement using the standard.

5.4.4 conclusion.

After performing the penetration testing on the device, finding the vulnerabilities, evaluating the device and recommending what is needed to be fixed the device manufacturers now can perform fixes to be able to conform the minimum of security for IoT devices, but we can actually make the standard better by suggesting these changes. In the next section we will talk about how to possibly make the Standard better and more up to date.

5.5 Enhancement of ETSI EN 303 645 standard

To recap, the ETSI EN 303 365 standard is a set of guidelines aimed at ensuring security and privacy in the rapidly evolving IoT landscape. It is a crucial step in the right direction as IoT continues to grow and expand, bringing new challenges and threats to the security of devices and systems. However, there are several areas where the standard could be improved or upgraded to make it more effective. One of the most important upgrades that could be made is to require for the developers of the devices a stronger level of encryption for communication between IoT devices and servers. Encryption is a technique used to protect data from unauthorized access by encoding information in such a way that only authorized users can decipher it. It is a critical component of cybersecurity, and any standard aimed at protecting IoT devices and systems must include guidelines on encryption and in the standard it is only mentioned to secure the data and communication but never mentioned any methods. Currently, many IoT devices and systems use weak encryption algorithms or no encryption at all. This makes them vulnerable to attacks and unauthorized access. To improve the ETSI EN 303 365 standard, it is essential to require a minimum level of encryption for all communication between IoT devices and servers. The level of encryption required should be strong enough to prevent unauthorized access to sensitive data like personal and financial information. The next enhancement I propose is to add the necessity of multi-factor authentication. Multi-factor authentication is a security measure that requires users to provide multiple forms of identification before being granted access to a device or system. This could include a password, a fingerprint scan, or a voice recognition system. By requiring multi-factor authentication, the standard can help prevent unauthorized access to IoT devices and systems, even if an attacker has obtained the user's password. The standard should also include guidelines for secure data storage and transfer. Data is at the heart of IoT, and it is essential to ensure that

sensitive information is always protected. Guidelines for secure data storage and transfer should include recommendations for encryption, access control, and data backup. By following these guidelines, IoT devices and systems can ensure that data is protected against unauthorized access, accidental deletion, or corruption. In addition to these priority upgrades, the ETSI EN 303 365 standard could be completely overhauled to include requirements for secure software development practices. Secure software development practices are a set of guidelines and best practices aimed at ensuring that software is developed with security in mind from the beginning. By mandating secure software development practices for IoT devices and systems, the ETSI EN 303 365 standard can help prevent security vulnerabilities from being introduced into software during the development process. Secure software development practices should include guidelines for code reviews, secure coding practices, and security testing. Code reviews involve examining the code line by line to identify potential vulnerabilities or weaknesses. Secure coding practices involve writing code that is resistant to attacks, such as buffer overflows or SQL injection attacks. Security testing involves testing software to identify vulnerabilities that could be exploited by attackers. By including guidelines for these practices, the standard can help ensure that IoT devices and systems are developed with security in mind from the getgo. The final upgrade that I propose is the requirement of running security testing and penetration testing and auditing for new IoT devices by the manufacturers themselves, or hiring a third-party experts to test the security of the product before launching it to the market.

All these upgrades are just some of the upgrades and enhancements that should happen to the standard to make the life of IoT device consumers more secure and should serve as the baseline of defence from unwanted attackers.

Results

As a result of this work, we can confirm that IOT devices especially the ones that are fully connected to the network are in a dire need of a better security to insure the safety of it's users. The standard mentioned before (ETSI EN 303 365) works as a good bare minimum of security since it covers good grounds and is generally an all round good security for IOT devices, but this standard can be furthered improved as mentioned before. IOT devies are becoming more and more present in our daily lives

and with this much exposure to our data it can be very dangerous to use any device without thinking about the consequences.



6: Conclusion and recommendations

The world of IOT does not have nearly enough recognition in the security department and is often overlooked when it comes to securing the personal data for the consumer meaning when the buyer gets the device, he is putting himself in much risk therefore it is necessary to set a basic standard for the developers to abide by to ensure the safety of the customer. Basically, an unprotected IoT device that is connected to the network of the customer serves as an open door for attackers to steal information and that is why it is necessary to further develop the cyber security aspect of the world of IoT technology.

The aim of this project was to find vulnerabilities in a device “APS” using a methodology of first performing penetration testing then evaluating what we got as a result according to “ETSI EN 303 645” standard to further prove that these devices as expensive and complex they seem they overlook the security aspect.

The significance of conducting penetration testing on IoT devices cannot be overstated. The proliferation of IoT devices, combined with their inherent vulnerabilities, makes them attractive targets for cyber threats. To ensure the security of these devices and protect sensitive data, it is essential to conduct thorough and regular penetration tests. By doing so, organizations can identify vulnerabilities, assess risks, and implement appropriate security measures to safeguard their IoT infrastructure.

Here are some recommendations for conducting effective penetration testing on IoT devices:

Adopt a Comprehensive Testing Approach: Employ a holistic testing approach that encompasses all aspects of the IoT ecosystem, including device hardware, firmware, communication protocols, mobile apps, cloud services, and backend infrastructure.

Simulate Real-World Scenarios: Replicate realistic attack scenarios to evaluate the security posture of IoT devices. This includes analyzing device behavior in different network conditions, simulating physical tampering, and assessing resistance to various types of attacks.

Promote Secure Development Lifecycle: Encourage IoT device manufacturers to follow secure development practices, such as adhering to security standards, conducting code reviews, performing threat modeling, and ensuring secure firmware updates.

Implement Regular Updates and Patch Management: Establish a robust process for promptly applying security updates and patches. This involves defining clear responsibilities for IoT device vendors, service providers, and end-users to ensure timely deployment of security fixes.

Enhance User Education and Awareness: Educate end-users about best practices for securing IoT devices, such as using strong passwords, enabling two-factor authentication, and regularly maintaining their devices. It is crucial to raise awareness about potential risks associated with IoT devices and encourage users to promptly report vulnerabilities to manufacturers.

Examples of Businesses in the Field of Penetration Testing and IoT Devices:

Synack: Synack is a cybersecurity company that specializes in offering penetration testing services for IoT devices. Their platform connects organizations with a global network of ethical hackers who excel in identifying vulnerabilities in IoT infrastructure.

Rapid7: Rapid7 is a leading provider of security analytics and automation solutions. They offer tailored penetration testing services for IoT devices, assisting organizations in identifying weaknesses within their IoT ecosystem and implementing effective security measures.

NCC Group: NCC Group is a global cybersecurity and risk mitigation company that provides specialized IoT penetration testing services. They help businesses identify and address vulnerabilities in their IoT deployments, ranging from individual devices to complete ecosystems.

Examples of IoT Device Developers:

Nest (Google): Nest, owned by Google, is a prominent developer of IoT devices, particularly smart home products such as thermostats, cameras, and doorbells. Their focus lies in integrating intelligent features into everyday household devices, enhancing convenience and energy efficiency.

Ring (Amazon): Ring, an Amazon subsidiary, develops a range of IoT devices for home security, including video doorbells, security cameras, and alarm systems. Their products aim to provide homeowners with enhanced security and monitoring capabilities.

Philips Hue: Philips Hue is a well-known developer of smart lighting solutions. Their IoT devices allow users to control and customize their home lighting through smartphone apps or voice commands, offering convenience, energy efficiency, and ambiance customization.



7: REFERENCES

A. M. S. A. S. F. M. (2014). H.265 Codec over 4G Networks for Telemedicine System Application (pp. pp292-297). AMSS 16th International Conference on Computer Modelling and Simulation (UK) Alam, S., Chowdhury, M. M., & Noll, J. J. W. P. C. (2011). Interoperability of security-enabled internet of things. 61(3), 567-586.

A. I. C. C. & H. G. (2015). Internet of Things: Security vulnerabilities and challenges. Paper Presented at the 2015 IEEE Symposium on Computers and Communication (ISCC) Aras, E., Ramachandran, G. S., Lawrence, P., & Hughes, D. (2017). Exploring the security vulnerabilities of LoRa. Paper presented at the 2017 3rd IEEE International Conference on Cybernetics (CYBCONF)

A. E. R. G. S. L. P. & H. D. (2017). Exploring the security vulnerabilities of LoRa. Paper Presented at the 2017 3rd IEEE International Conference on Cybernetics (CYBCONF).

A. S. (2017). SDN-Based Load Balancing Scheme for Fat-Tree Data Center Networks. (pp. pp.1047-1056). Al-Nahrain Journal for Engineering Sciences (NJES), Vol.20, No.5. Askar, S., Zervas, G., Hunter, D. K., & Simeonidou, D.

A. S. Z. G. H. D. K. & S. D. (2011). Service differentiation for video applications over OBS networks (pp. pp.200-203). 16th European Conference on Networks and Optical Communications, Newcastle-Upon-Tyne. D. Evans, "The internet of things - how the next evolution of the internet is changing everything," White Paper. Cisco Internet Business Solutions Group (IBSG), 2011.

P. M. P. K. A. J. T. (2013). Forecast: The internet of things, worldwide,

R. R. P. N. A. J. L. (2010). Securing the internet of things," Computer, vol. 44, no. 9 (pp51-58).

A. W. (2011). How the internet of things helps us understand radiation levels (pp. pp51-58). <http://readwrite.com/2011/04/01/ow-the-internetof-things-help>

D. V. A. F. Z. (2008). International Journal of Advanced Pervasive and Ubiquitous Computing (IJAPUC), vol. 2, no. 2 (pp. 33-40).
<http://readwrite.com/2011/04/01/ow-the-internetof-things-help>

H. S. N. K. M. P. B. T. M. N. A. A. O. (2011). Smart cities and the future internet: Towards cooperation frameworks for open innovation (pp. 431-446). In The Future Internet, ser. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 2011, vol. 6656. <http://readwrite.com/2011/04/01/ow-the-internetof-things-helpJ>.
Zhou, Z. Cao, X. Dong, and A. V. Vasilakos, "Security and privacy for

(2017). Cloud-based IoT: Challenges (pp. 26-33). IEEE Commun. Mag., vol. 55, no. 1.. Xiao, Y. Li, G. Han, G. Liu, and W. Zhuang, "PHY-layer spoofing detection with

(2016). Reinforcement learning in wireless networks (pp. 10037-10047). IEEE Trans. Veh. Technol., vol. 65, no. 12.M. Abu Alsheikh, S. Lin, D. Niyato, and H. P. Tan, "Machine learning in wireless

(2014). Sensor networks: Algorithms, strategies, and applications (pp. 1996-2018). IEEE Commun. Surveys Tutorials, vol. 16, no. 4.L. Xiao, C. Xie, T. Chen, and H. Dai, "A mobile offloading game against smart

L. X. Y. L. X. H. A. X. J. D. (2017). Cloud-based malware detection game for mobile devices with offloading (pp. 2742-2750). IEEE Trans. Mobile Comput., vol. 16, no. 10.

M. O. I. E. F. T. Y. V. S. R. K. A. H. V. P. (2015). Machine learning methods for attack detection in the smart grid (pp. 1773-1786). IEEE Trans. Neural Networks and Learning Syst., vol. 27, no. 8.

L. D. X. W. H. A. S. L. (2014). Internet of things in industries: A survey (pp. 2233-2243). IEEE Trans. Industrial Informatics, vol. 10.

G. G. Z. L. A. J. J. (2011). "Internet of things security analysis," in Internet Technology and Applications (iTAP) (pp. 1-4). 2011 International Conference on. IEEE, 2011.

Q. P. Y. G. M. O. A. F. D. A. L. X. (2016). Advanced internet of things for personalised healthcare systems (pp. 132-149). A Survey,” Pervasive and Mobile Computing.

P. Y. M. H. J. Q. Z. D. F. D. A. D. F. (2015). Improving the validity of lifelogging physical activity measures in an internet of things environment (pp. 2309-2314). In CIT/IUCC/DASC/PICom. IEEE.

G. (2014). Gartner Says By 2020, More Than Half of Major New Business Processes and Systems Will Incorporate Some Element of the Internet of Things. “<http://www.gartner.com/newsroom/id/3185623>”

E. K. (2016). Brian Krebs’s Blog Hit by 665 Gbps DDoS Attack. <http://www.securityweek.com/brian-krebs-blog-hit-665-gbps-ddosattack>

O. (n.d.). Top 10 2014-I5 Privacy Concerns. https://www.owasp.org/index.php/Top_10_2014-I5_Privacy_Concerns

K. L. Kali Linux. “Kali Linux Official Documentation”. <http://docs.kali.org/>

D. A. B. A. V. M. M. (2014). Comparative study and analysis of network intrusion detection tools (pp. 312-315). International Conference on Applied and Theoretical Computing and Communication Technology (ICATccT), 2015.

N. W. (2012). A Practical Network-Based Intrusion Detection and Prevention System. IEEE Xplore.

8: Webography

Penetration testing: identifying vulnerabilities

https://books.google.com.tr/books?hl=en&lr=&id=rEFPDwAAQBAJ&oi=fnd&pg=PP1&dq=penetration+testing+on+iot+devices&ots=DqGgs-HAro&sig=cRpQc0YYqqo-r2GVZoI8iRKIRCY&redir_esc=y#v=onepage&q=penetration%20testing%20on%20iot%20devices&f=false

Penetration testing of secure networks:

https://books.google.com.tr/books?hl=en&lr=&id=xukgDgAAQBAJ&oi=fnd&pg=RR23&dq=advanced+people+sensor+penetration+testing&ots=LpLsly7yb&sig=b4guYQxRuwAe-_wj7BcPyWS0-60&redir_esc=y#v=onepage&q=advanced%20people%20sensor%20penetration%20testing&f=false

Security Issues and Vulnerability of IoT Devices:--

<https://ijsab.com/wp-content/uploads/690.pdf>

Management platform of threats information in IoT environment:

<https://link.springer.com/content/pdf/10.1007/s12652-017-0581-6.pdf>

Security and Privacy Issues with IoT in Healthcare:

<https://publications.eai.eu/index.php/phat/article/view/1290/1111>

Penetration Testing for Internet of Things and Its Automation:--

<https://ieeexplore.ieee.org/abstract/document/8622982>

Penetration testing tool for Internet of Thing devices PENTOS:--

<https://ieeexplore.ieee.org/abstract/document/8228241>

Penetration Testing of Intrusion Detection and Prevention

System in Low-Performance Embedded IoT Device:--

<https://ieeexplore.ieee.org/abstract/document/8624734>

https://en.wikipedia.org/wiki/Internet_of_things

<https://www.techtarget.com/iotagenda/definition/Internet-of-Things-IoT>

Hacking Iot device (baby monitor):

<https://media.kasperskycontenthub.com/wp-content/uploads/sites/63/2015/11/21031739/Hacking-IoT-A-Case-Study-on-Baby-Monitor-Exposures-and-Vulnerabilities.pdf>

IoT Penetration Testing: Security analysis of a car dongle--

<https://www.diva-portal.org/smash/get/diva2:1334244/FULLTEXT01.pdf>

"Types of Penetration Testing: White Box, Black Box, and Grey Box Testing." HackerOne:

<https://www.hackerone.com/resources/types-of-penetration-testing>. Accessed 18 Mar. 2023

"What is Penetration Testing?" Cybersecurity and Infrastructure Security Agency:

<https://www.cisa.gov/what-is-penetration-testing>

"Penetration Testing." SANS Institute:

<https://www.sans.org/penetration-testing/>

Penetration Testing of IoT Devices:

<https://www.sans.org/white-papers/39480/>

penetration testing phases resources:

"The Penetration Testing Execution Standard (PTES)." PTES, www.pentest-standard.org/index.php/Main_Page.

IoT Penetration Testing: Challenges and Best Practices." Synopsys, 16 Mar. 2021 :

www.synopsys.com/blogs/software-security/iot-penetration-testing-challenges-best-practice

