National College of Ireland

Securing the IoT Landscape: A Home Office Cybersecurity Audit Tool

MSc Research Project
MSCCYBE

Eoin Kirwan
Student ID: x16472486

School of Computing
National College of Ireland

Supervisor: Michael Pantridge

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name:	Eoin Kirwan
Student ID:	X16472486
Programme:	MSCCYBE **Year:** 2023
Module:	MSc Cybersecurity
Supervisor:	Michael Pantridge
Submission Due Date:	14/12/23
Project Title:	Securing the IoT Landscape: A Home Office Cybersecurity Audit Tool

Word Count : 8230

Page Count: 22

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: Eoin Kirwan

Date: 11/12/23

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Securing the IoT Landscape: A Home Office Cybersecurity Audit Tool

Eoin Kirwan
x16472486

Abstract

This study presents the Home Office Security Audit Tool, a significant advancement in the ever-evolving area of cybersecurity, designed to detect vulnerabilities often found in home office networks that are typically overlooked. Residential networks often lack adequate safeguards, which is in stark contrast to business settings where robust security measures are commonplace. This creates a concerning blind spot. The tool specialises in performing comprehensive vulnerability assessments, which are especially crucial in the complex network of networked devices often seen in modern home offices. The increasing number of Internet of Things (IoT) devices, estimated to reach 75 billion worldwide by 2025, is leading to a rise in security vulnerabilities linked to these devices. The Home Office Security Audit Tool addresses this difficulty by integrating specialised functionalities that can identify vulnerabilities specific to IoT devices, providing a proactive approach to reducing possible risks. This research project presents the methodology, design, and implementation of the tool, with a focus on its user-friendly and automated approach to security. The program allows regular users to actively monitor the security of their home networks by automating the detection of vulnerabilities and unauthorised entry points. Automated reporting offers consumers actionable information to promptly mitigate any dangers, strengthening their home office networks against cyber-attacks. This study not only examines the intricacies of tool design but also assesses its effectiveness, providing a holistic solution to improve the security environment of modern home offices.

1 Introduction

Within the ever-changing field of cybersecurity, home office networks, which are often neglected, encounter a variety of possible dangers as a result of the swiftly developing environment. The need for a specialised Home Office Security Audit Tool becomes evident when considering the widespread deficiencies in conventional security measures used in both personal and professional environments. This innovative security approach is essential for several compelling reasons. While business settings often implement rigorous security measures and regular penetration testing, residential networks often lack such comprehensive protection. Although digital ecosystems are becoming more complicated, the majority of users seldom conduct thorough security checks on their home office installations. The absence of thorough examination gives rise to a worrisome blind spot, rendering these networks susceptible to diverse cyber-attacks that have the potential to compromise critical information and personal data.

The contemporary home office functions as a focal point where several gadgets, each with its own vulnerabilities, such as laptops, smart phones, smart home appliances, and Wi-Fi routers, come together. The interconnectivity of these gadgets creates an intricate network of possible vulnerabilities in terms of security.

The Home Office Security Audit Tool provides a specialised solution for conducting thorough vulnerability assessments in order to solve the security concerns present in this diversified environment. In the prevalent scenario of widespread adoption of the Internet of Things (IoT) in households, the security aspects of these interconnected devices are frequently overlooked. Research findings from IoT Analytics indicate that the global deployment of IoT devices surpassed approximately 27 billion in 2020.

Projections suggest a significant rise to 75 billion devices by 2025. In addition, statistics provided by (Wise, 2023) in a 2023 Earthweb article, indicates that sales of Amazon Alexa devices displayed consistent expansion from 2014 to 2021, resulting in a total of 228.4 million units sold over that timeframe. As the number of IoT devices increases, the corresponding dangers of security vulnerabilities rise. These gadgets, which are vulnerable to dangers such as unauthorised access to data, Denial of Service (DOS) attacks, and other harmful actions, provide an increased likelihood of major security breaches and events involving ransomware. The continuous increase in sales of IoT devices, as seen by the growing number of Amazon Alexa users, highlights the need to promptly address security issues in order to minimise possible negative outcomes in the developing realm of interconnected technology. Conventional security techniques tailored for large-scale networks may not effectively detect and address the unique risks found in IoT devices. The solution being presented aims to address this gap by including specialised features designed for identifying IoT devices, therefore enabling a comprehensive and efficient security assessment in domestic settings.

Ordinary people often do not possess the necessary resources and knowledge to carry out comprehensive security assessments manually. The Home Office Security Audit Tool enables users to proactively oversee their network's security by using automated reporting and requiring minimum human participation. The programme automates the identification of vulnerabilities, unauthorised access points, and possible risks, providing users with actionable information that can be swiftly addressed to strengthen the security of their home office networks against cyber-attacks.

This technology proposes a significant change by promoting a proactive approach to home security. Users may proactively use the tool to find and address vulnerabilities before a security problem occurs. By adopting a proactive approach, home users may successfully protect their digital assets in response to the changing threat scenario. The Home Office Security Audit Tool is a new and essential solution that fills the gap in security standards for home networks. The solution acknowledges the unique difficulties of home office settings and offers users a methodical way to strengthen their protection against cyber-attacks. The next parts of this paper will explore the complexities of the tool's design, deployment, and its crucial role in transforming the security environment of contemporary home offices.

The report will be structured into several parts, starting with an examination of relevant literature, and then outlining the research technique used. The next parts will provide a comprehensive explanation of the design specification and the subsequent implementation of the tool. A thorough assessment of the tool's performance will be conducted, followed by detailed sections devoted to a full analysis of the evaluation findings. The report will end with a concluding section that provides a summary and discusses potential areas for further research in the topic.

1.1 Aims

The objective of the research project is to create and use a reliable tool for auditing the security of home offices. This will be achieved by using Python on a Raspberry Pi server and integrating well-established technologies such nmap, nmapAutomator, nikto, and ffuf. The specific objectives include improving vulnerability scanning methodologies, using a nmap script to identify CVEs, implementing functionalities for recognising IoT devices, detecting rogue access points, and capturing packets for traffic analysis. The study aims to analyse the efficacy of the tool in systematically evaluating open ports, services, and vulnerabilities on home network devices. The framework and architecture encompass evaluating the tool's installation on a Raspberry Pi server, establishing a systemctl service for automated startup, and integrating email reporting for prompt distribution of comprehensive security reports, thereby improving user convenience and network safeguarding in home office settings.

2 Related Work

The introduction of Internet of Things (IoT) has changed the way devices can communicate with each other. IoT devices can make up a web of complex interconnected devices that can share data between them. The actual phrase "Internet of Things" was first introduced by Kevin Ashton back in 1999 but only gained popularity later in the early 2012. This was due to the broad accessibility of internet connections.

This technological approach has been used in several domains and areas. An example of some would be healthcare, agriculture, transportation, and manufacturing, broadening its capabilities to include a diverse range of devices, including wearable technology and industrial sensors. The number of networked IoT devices exceeded 27 billion in 2020, and projections indicate that it will increase to 75 billion by 2025. (Wise, 2023) statistics highlights a significant increase in the sales of Amazon Alexa devices, with a total of 228.4 million units sold from 2014 to 2021. The widespread impact of the Internet of Things is clearly seen in several areas, but it also brings up security issues, particularly related to the theft of data and cyber assaults. An inherent weakness in IoT ecosystems is the continued use of default passwords, worsened by the widespread emphasis on cost-efficiency rather than security in their development. In order to mitigate these vulnerabilities, it is essential to implement robust security measures to minimise risks and safeguard both networks and people.

The study undertaken by Hernández-Ramos et al. (2015) presents a security architecture designed to enhance the security of Internet of Things (IoT) devices, specifically targeting their use in smart buildings, infrastructure, and Supervisory Control and Data Acquisition (SCADA) systems. The suggested solution presents a novel method for addressing security issues in the Internet of Things (IoT) domain. It is organised into four separate layers: IoT devices or end nodes, network, services, and application. At the core of this architecture lies the assignment of security tasks to specialised devices responsible for overseeing the management of Internet of Things (IoT) devices, instead of directly installing security measures on the devices themselves. This method is especially relevant for IoT devices that are characterised by limitations in resources. Nevertheless, it raises worries about the possible susceptibility of the whole Internet of Things (IoT) network in the case of a breach to the governing system. By entrusting the responsibility of security to IoT device management systems, the efficient use of resources is maximised, and the difficulties related to limited resources in IoT devices are reduced.

Nevertheless, this method also presents the potential for a solitary vulnerability that may be manipulated. The governance structure of the Internet of Things (IoT) network is vulnerable to a security weakness, with significant potential repercussions. It is important to emphasise that the suggested solution introduces a new approach to tackling security in the Internet of Things (IoT). However, it also highlights the unavoidable compromise between maximising resource efficiency and the potential vulnerability of a centralised system. Hence, doing more study is essential to establish robust security systems that might pre-emptively avert such calamities. The proposed security architecture poses a fundamental inquiry about the efficacy of this approach, necessitating more research endeavours to ascertain its appropriateness and robustness in practical application.

A research article written by (Agarwal, Oser and Lueders, 2019) introduces an extensive approach for detecting and identifying Internet of Things (IoT) devices in a large-scale network, significantly advancing the field of IoT security. The authors provide two tools, "NetScanIoT" and "Web-IoT Detection (WID)," that are successful in accurately detecting a wide range of IoT devices and their corresponding firmware versions. The research uncovers many security vulnerabilities present in IoT devices, such as the use of default passwords and obsolete firmware versions, via a human vulnerability evaluation. The authors suggest proactive measures to address the discovered vulnerabilities, providing practical advice for organisations aiming to improve the security of their IoT devices. The study's strength comes in its use of the extensive CERN network, which allows for the identification of a wide range of IoT devices and their vulnerabilities. The creation of the "NetScanIoT" and "Web-IoT Detection (WID)" tools represents a notable progress in the field of IoT security. In addition, the authors' non-invasive method, which avoids making any changes or installations on the device being tested (DUT), guarantees that the device's functioning stays unchanged throughout the evaluation. Nevertheless, a significant constraint of this study is its narrow concentration on detecting IoT devices that had a web user interface, possibly neglecting devices that lack such interfaces. Moreover, the potential impact of the recommended security measures has not been thoroughly investigated, which is a wasted chance to get more knowledge about their feasibility and effectiveness.

The study paper, titled "Cyber and Physical Security Vulnerability Assessment for IoT-Based Smart Homes," written by (Ali and Awad, 2018) provides a comprehensive analysis of the security vulnerabilities linked to smart homes based on the Internet of Things (IoT) technology. Using the OCTAVE Allegro methodology, the authors perform a thorough security risk assessment, identifying crucial cyber and physical assets and detecting about 15 security concerns originating from both internal and external sources inside smart homes. This complete strategy not only tackles cyber dangers, but also incorporates issues for physical security, so strengthening the study's resilience. An outstanding attribute of the article is its comprehensive approach to evaluating security risks, which includes analysing both cyber and physical vulnerabilities. The report employs a multi-perspective approach to provide a more nuanced comprehension of possible risks to smart homes based on the Internet of Things (IoT). Furthermore, the study results are shown to be practically applicable via the identification of 10 crucial information assets and the proposal of remedies for risk reduction. However, the study does have certain limitations. The authors expressly state that the study does not explore the intricacies of smart services, and no physical smart home system was built. Although the attention given to security risks, effects, and countermeasures is praiseworthy, the inclusion of a realistic implementation of the recommended countermeasures would have greatly enhanced the value of the work. Additionally, the authors acknowledge that because of time limitations and the large number of spreadsheets in the OCTAVE Allegro technique, many hazards were not included.

This constraint suggests that the evaluation may not include all possible dangers, highlighting the need for more investigation. Another acknowledged constraint is the paper's superficial examination of the trade-off between security and usability. While recognising the difficulty of balancing system security with usability, a thorough examination of this trade-off and the exploration of various ways to achieve equilibrium would have enhanced the conversation.

The Mirai botnet malware represents a substantial security threat to home office networks, with a special focus on exploiting susceptible Internet of Things (IoT) devices. This malicious software infiltrates these devices, assimilating them into a botnet controlled by the attacker, enabling them to manage the devices for diverse malevolent intentions. Typically, these infected devices are used in phishing campaigns or exploited in Distributed Denial of Service (DDoS) assaults. In an article written by (Elie Bursztein, 2017), they pointed out that in September 2016, Mirai caused significant and temporary harm to well-known services including OVH, Dyn, and Krebs on Security by launching large-scale DDoS assaults. OVH said that these assaults exceeded 1 Tbps, making them the largest on public record. At its peak, Mirai had effectively infiltrated more than 600,000 devices worldwide, highlighting the urgent need for preventative tool, such as the one suggested in this study, to protect home network devices against similar malware attacks.

The research paper, titled "Enhancing Smart Home Security: Anomaly Detection and Face Recognition in Smart Home IoT Devices Using Logit-Boosted CNN Models," by (Rahim *et al.*, 2023) undertakes a thorough examination of cutting-edge technology with the goal of strengthening security in smart homes. The research specifically focuses on the identification of anomalies and the recognition of faces, using Logit-Boosted CNN models. The work excels in its comprehensive examination of the suggested technique, including a comparative investigation of its effectiveness in face recognition and anomaly detection in relation to established methods. This comparison offers vital insights on the merits and limitations of the suggested methodology, enhancing the comprehensiveness of the study. The study thoroughly assesses the efficacy of the approach by employing multiple metrics, including accuracy, precision, recall, F1 score, and the area under the receiver operating characteristic curve (AUC-ROC). This analysis provides insights into the models' ability to accurately detect anomalies and recognise faces. Furthermore, the study highlights the practical significance of the suggested approach by emphasising its potential influence on the security of smart homes. The incorporation of varied datasets and the development of Logit-Boosted CNN models augment the practical usability of the study. The paper demonstrates a proactive approach by identifying potential areas for future research. These include investigating the applicability and reliability of the models in various smart home settings and datasets, as well as proposing the integration of advanced techniques such as transfer learning and privacy-preserving methods. Nevertheless, the paper does have certain drawbacks. The text briefly acknowledges the difficulties of installing deep learning models on IoT devices with limited resources. However, it does not thoroughly examine possible solutions or methods to overcome this difficulty, which might impede the actual use of the suggested technique. Moreover, while the research examines the unique behaviour of individual models in terms of accuracy, precision, recall, and F1 score, a more comprehensive evaluation of the performance of individual models and their combinations might provide more subtle insights. Finally, the study recognises the significance of privacy and security considerations but lacks in thoroughly examining methods for maintaining privacy while detecting anomalies and recognising faces. This creates an opportunity for additional research to improve the overall strength of the suggested approach.

Academic study has shown an increasing worry about the security of Internet of Things (IoT) devices, namely in the context of smart homes. Notable advancements have been achieved in resolving these security weaknesses via recent studies, such as the study undertaken by (Hernández-Ramos *et al.*, 2015) and (Agarwal, Oser and Lueders, 2019). These works exhibit a layered security architecture designed to effectively manage the protection of IoT devices. Specifically, (Hernández-Ramos *et al.*, 2015) present a comprehensive framework organized into distinct layers for efficient management of IoT device security. Nevertheless, the centralised method raises concerns about the potential for a solitary point of failure. (Agarwal, Oser and Lueders, 2019) make a substantial contribution by creating tools like "NetScanIoT" and "Web-IoT Detection (WID)" to detect IoT devices. However, their study has limitations, including a narrow focus on devices with web interfaces and a lack of thorough investigation into the effectiveness of the suggested security measures. The study conducted by (Ali and Awad, 2018) about security vulnerabilities in IoT-based smart homes provides a thorough examination. However, it falls short in terms of practical application and fails to further explore the balance between security and usability. The research conducted by (Rahim *et al.*, 2023) presents innovative security measures utilising Logit-Boosted CNN models for detecting anomalies and recognising faces in smart homes. The study includes thorough evaluations; however, it does not adequately address the challenges associated with limited resources on IoT devices and the protection of privacy. The constraints of current solutions highlight the need for a specialised tool to examine and improve security especially in home office networks, taking into account the unique difficulties posed by the widespread use of IoT devices in this setting.

3 Research Methodology

This project aims to improve home office security by developing and evaluating a Python-based audit tool, in response to the changing environment of IoT devices. This section provides a comprehensive explanation of the study process, guaranteeing openness and adherence to rigorous scientific protocols.

3.1 Data Collection Technique and Procedure

The study uses a comprehensive methodology to assess the security of devices connected to a household network. Expanding upon the knowledge gained from Section 2, which emphasised the weaknesses present in IoT ecosystems, our approach is tailored to tackle particular security issues within the setting of a home office. The research approach used in this study involves the utilisation of the secondary case-study method, with a special emphasis on a home office security audit tool as the selected data-collection strategy. The reason for choosing the case-study technique is its capacity to provide a thorough assessment of instances related to the efficiency and difficulties of home office security audit instruments, with a focus on both automation and optimisation characteristics. The decision to use the case-study method is driven by its ability to reveal in-depth insights, factual data, examples, and justifications pertaining to the effectiveness of home office security audit tools in evaluating and improving security measures (Emma Bell, Bill Harley and Alan Bryman, 2022). The research seeks to use the case-study technique to perform a thorough analysis and establish how effective and sufficient home office security audit tools are in minimising effort during security assessments. The tools being evaluated include qualities such as automation and optimisation. Upon evaluating various secondary methodologies such as systematic review or literature study, it became apparent that these techniques would not provide the requisite specificity and comprehensive insights necessary for the unique context of home office security audits.

(Emma Bell, Bill Harley and Alan Bryman, 2022) endorse this viewpoint, emphasising the case-study technique as a more appropriate strategy for acquiring a detailed comprehension of the operation of home office security audit tools within particular instances.

3.2 Tool Development

The security audit tool developed, which is based on Python, is specifically intended to conduct a comprehensive evaluation of devices inside a home network. The programme utilises the ideas described in Section 2 of related research. It uses port scanning, service enumeration, and interaction with vulnerability databases such as CVE to find and evaluate possible security issues. It surpasses by verifying security configurations, resolving concerns like default passwords, and delivering users a thorough report for corrective action. The tool guarantees a strong method for improving the overall security of connected devices in the home network.

3.3 Evaluation Methodology

3.3.1 Equipment Setup

The tool is evaluated on a typical home network configuration, which encompasses routers, PCs, smart phones, and other pertinent IoT devices often seen in home office settings. The utility is installed on a specific server inside the network. I used a Raspberry Pi to execute the tool.

3.3.2 Techniques Used

A hybrid method is used in the area of security vulnerability detection, which incorporates both active and passive scanning approaches. The active scanning component is the methodical examination of devices to identify accessible ports and evaluate their vulnerability to possible vulnerabilities. Simultaneously, passive scanning is used to examine network traffic for abnormal patterns, following recognised best practices outlined in the available literature.

3.3.3 Generation of Results

The analysis of collected data yields definitive results regarding identified vulnerabilities, security configurations, and the overall efficacy of security measures in a home office environment. Subsequently, the user receives a report detailing the effectiveness of their home network's security.

3.3.4 Testing Scenarios

As part of the research project, a specialised tool to evaluate home office settings was created. The tool was then tested using a variety of realistic scenarios of various types of devices typically found on a home office network. These scenarios accurately simulate various use patterns, including common device interactions, data transfers, and communication techniques inside a home office environment.

Through subjecting the proposed tool to these realistic scenarios, our objective is to thoroughly evaluate its performance in practical circumstances. With this approach, we want to get a deeper understanding of the tool's flexibility, advantages, and possible constraints when it comes to meeting the actual requirements and user expectations in different home office situations. Using realistic scenarios is an effective way to evaluate how practical and useful a tool is in real-life situations. This contributes important results to the continuing discussion about developing and improving tools that are specifically designed for modern home work environments.

4 Design Specification

This section focuses on the precise methodology, architecture, and structure that form the foundation of the home office security audit tool implementation. The Python-based application utilises well-established tools like nmap, nmapAutomator, nikto, and ffuf to perform a thorough security audit. Furthermore, it has specific features such as identification of IoT devices, detection of unauthorised access points, and capturing packets for traffic analysis.

4.1 Scanning and Vulnerability Detection

4.1.1 Vulnerability Techniques

The program employs nmap, nikto and ffuf for the purpose of vulnerability scanning. This enhances the capability to find security vulnerabilities on the scanned devices. These technologies enhance the active scanning process by expanding the range of possible vulnerabilities that are taken into account. The program will execute a nmap script to identify potential vulnerabilities or CVEs linked to the open ports found on a device.

4.1.2 IoT device Recognition

The tool incorporates a capability for identifying IoT devices inside the network by using MAC address identification and device fingerprinting. This feature improves the tool's capacity to customise security evaluations according to device types, acknowledging the distinct security factors linked to IoT devices.

4.1.3 Rogue Access Point Detection

The solution uses a rogue access point detection method, backed by a tool named RogueAP Detector, to locate unauthorised access points inside the home network. This improves the overall security stance by identifying possible vulnerabilities that might be exploited by malevolent individuals.

4.1.4 Scanning Techniques

The utility uses nmap and nmapAutomator to do active scanning in order to detect open ports, services, and vulnerabilities on devices inside the home network. The use of these technologies guarantees a methodical and comprehensive assessment of possible security concerns.

4.1.5 Packet Capture and Traffic Analysis

In order to assess the regularity of device behaviour, the tool records the packets sent to and from each device during a designated time period. This facilitates the examination of traffic patterns, aiding in the detection of atypical or suspicious actions that might signify security risks.

4.2 Framework and Architecture

4.2.1 Raspberry Pi Server

The tool, developed in Python and compatible with many devices, was used in this instance on a Raspberry Pi to evaluate its efficacy. Exploiting the Raspberry Pi's small size and energy-saving features, the tool was deployed on this platform. The Raspberry Pi serves as a dedicated server for running the security audit tool, providing a simplified and cost-effective solution specifically designed for home office setups.

4.2.2 Systemctl Service

A service using the systemctl init system was created to automate the running of the audit tool on the Raspberry Pi server when it connects to the network and boots up. This configuration obviates the need for human involvement, since the audit tool starts immediately when the Raspberry Pi server is connected to the network and switched on—merely necessitating the insertion of an Ethernet connection and the act of switching the device on.

4.2.3 Email Reporting

After completing the security audit, the programme generates a thorough report that includes the identified vulnerabilities, security settings, and the overall effectiveness of the security measures. Afterwards, this report is sent by email, providing consumers with prompt and readily available information about the security condition of their home network. This efficient method improves user comfort by removing the need for manual examination of log files, since the scan findings are instantly sent to the user's email inbox.

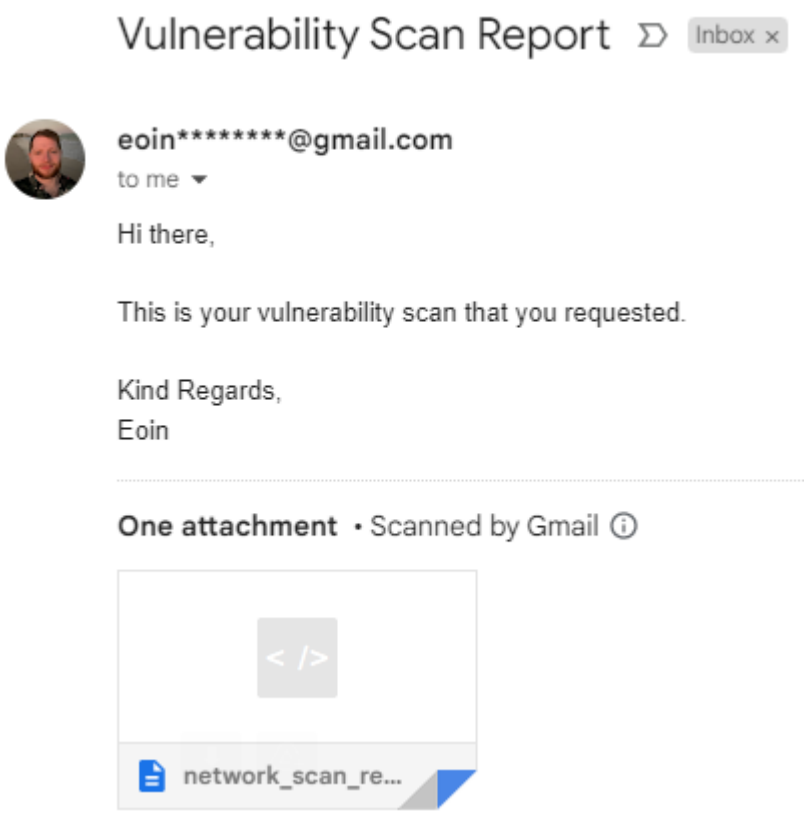

Figure 1: Email report sent by the tool

4.3 Associated Requirements

4.3.1 Tool Dependencies

Regularly updating the dependencies of the security audit tool is essential for maintaining its effective performance. The tool depends on the proper configuration and setup of external scanning tools, such as nmap, nmapAutomator, nikto, and ffuf. Regular upgrades to these tools are crucial for keeping up with developing vulnerabilities, assuring the continuous thoroughness and up-to-dateness of security assessments. The Raspberry Pi utilised in this case was set up to automatically update all the tools, guaranteeing the detection of the most recent vulnerabilities and CVEs during security assessments. Nevertheless, individuals using the tool on other devices must personally update these tools to guarantee the audit tool's effectiveness.

4.3.2 Network Access

To ensure that the security audit tool functions well, it is necessary to get the necessary network permissions in the home environment. Full access to all devices in the network is essential for the tool to do thorough scanning. Firewalls have the potential to hinder the tool, hence affecting its accuracy and capacity to provide exact findings.

4.3.3 Email Configuration

In order to guarantee effective email reporting, the programme necessitates accurate email setup settings, including SMTP server particulars and login credentials.

5 Implementation

The proposed approach involves creating a Python-based tool for conducting security audits in home offices. This application utilises a wide range of Python libraries and penetration testing tools to provide a strong and effective method for examining the security status of devices usually found in a home office network.

Python was crucial in developing the home office security audit tool, playing a key part in creating a flexible and efficient solution. The decision to choose Python was driven by its clear and understandable syntax, its ability to be easily expanded and customised, and the wide range of modules and frameworks that are crucial for doing security assessments. Python was used to easily integrate with robust scanning tools like as nmap, nmapAutomator, nikto, and ffuf. The use of these tools, in conjunction with Python's straightforwardness and adaptability, allowed the methodical analysis of devices inside the home network to identify weaknesses and possible threats. The codebase of the security audit tool mostly utilises Python and has an algorithm that meticulously coordinates port scanning, service enumeration, and interaction with vulnerability databases like CVE. The broad library support in Python facilitated the seamless use of these other tools, enabling a thorough assessment of security concerns. In addition, Python's modularity played a crucial role in the creation and execution of certain features, such as identifying IoT devices, detecting unauthorised access points, and capturing packets for traffic analysis. The language's versatility enabled the development of a codebase that is not just strong but also capable of adjusting to changing security demands. Python facilitated the seamless integration of the tool with a Raspberry Pi server, prioritising efficiency and energy saving. Python's lightweight design and cross-platform flexibility made it a perfect fit for deploying on the Raspberry Pi. This ensured that the tool could run well in contexts with limited resources. The tool also took advantage of multithreading by using the subprocess library in python. This allowed the tool to take the maximum efficiency of system resources on the device it’s running on and allows it to run more efficiently.

The nmap software is used for performing an initial network scan with the purpose of gathering vital information about the devices existing inside the network. This includes specific information such as the MAC address of the device, accessible ports, and, if discernible, the operating system it is using. The utility use a biphasic approach to ascertain the manufacturer of the device. At first, it attempts to directly extract this information from the nmap findings. If the first approach fails to get manufacturer data, the tool automatically switches to a secondary strategy. It uses a predetermined list of MAC address prefixes associated with manufacturer names to determine and show the device's manufacturer.

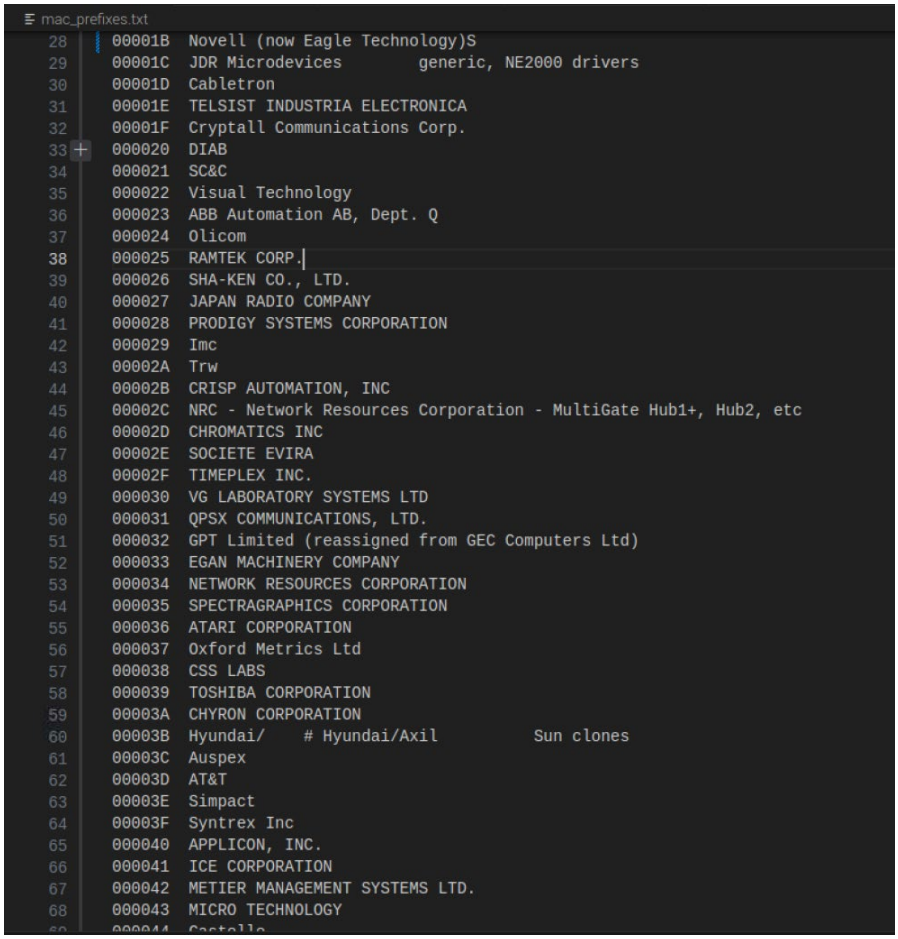

Figure 2. Mac address prefix list

The utility enhances its functionality to include the detection of Internet of Things (IoT) devices inside the network. This is accomplished by analysing the MAC address of devices discovered on the network and comparing it with a pre-established list of accepted IoT MAC address prefixes to accurately identify IoT devices on the network. Afterwards, the programme performs a reverse DNS lookup operation using the python library socket in order to get the hostname of each device on the network. After completing the initial data collection process, the programme continues to do a nmapAutomator scan on each device that has been discovered inside the network. The programme uses the port information gathered during the first scan to identify the current services operating on those ports. The program performs a variety of nmap scripts that are customised to the individual services and ports found on the device, based on the open ports and their related services. Moreover, the utility gets the information on the version of the operating system (OS) that was obtained during the original nmap scan. Using this information, the programme chooses and carries out the suitable nmap script to evaluate possible vulnerabilities linked to the specified operating system version on the device. This comprehensive methodology improves the tool's ability to detect and assess security weaknesses on various devices and their corresponding operating systems inside the network.

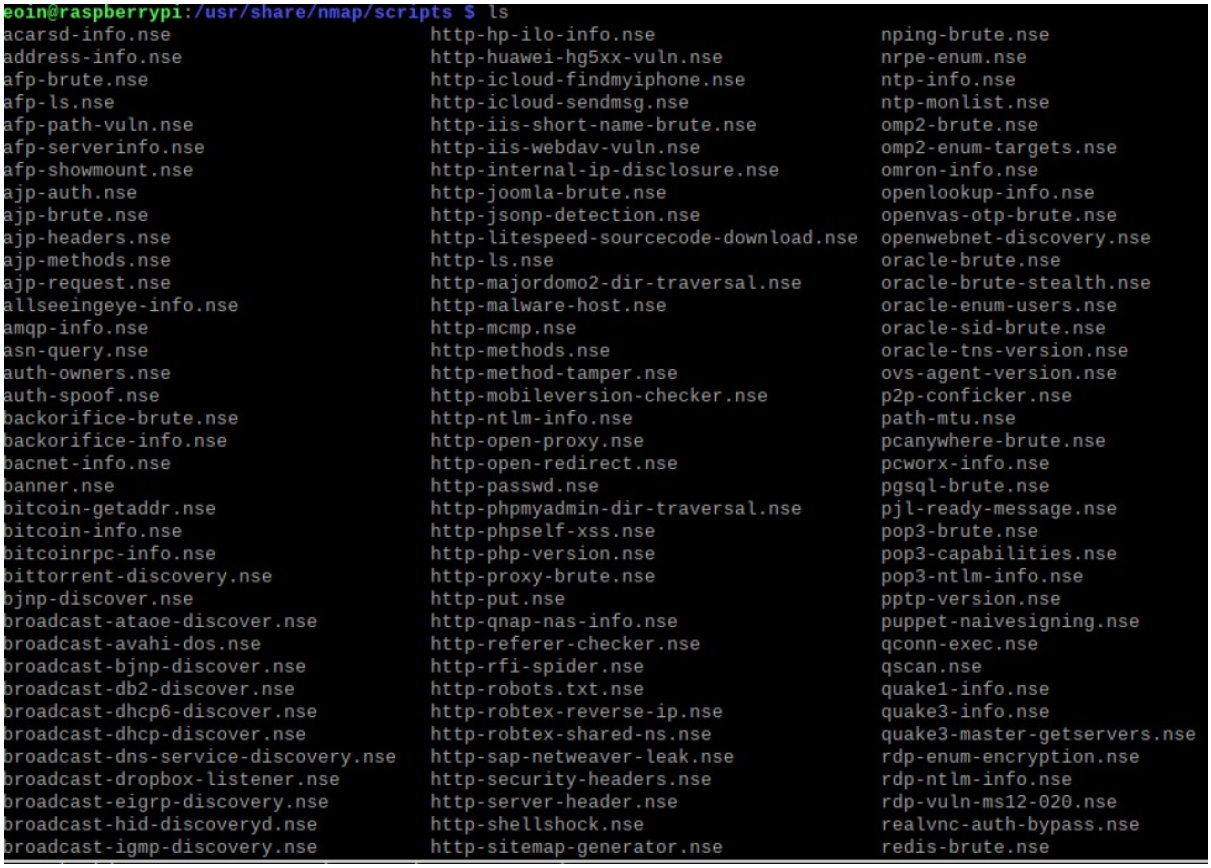

Figure 3. List of some nmap scripts available to the home office security audit tool

This is an example of a collection of nmap scripts that the tool may run on a device, depending on the initial reconnaissance performed by the programme. This highlights the tool's ability to identify a wide range of vulnerabilities and Common Vulnerabilities and Exposures (CVEs) that are common across various device kinds and operating systems (OS) used on these devices. This programme demonstrates its scanning powers by offering a wide range of 599 probable scripts, showcasing its tremendous depth and completeness.

```
PORT      STATE SERVICE         VERSION
1080/tcp  open  socks5          (No authentication; connection failed)
6543/tcp  open  http            Cisco Meraki firewall httpd
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
| 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 and hold
|       them open as long as possible.  It accomplishes this by opening connections to
|       the target web server and sending a partial request. By doing so, it starves
|       the http server's resources causing Denial Of Service.
|
|     Disclosure date: 2009-09-17
|     References:
|       http://ha.ckers.org/slowloris/
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
8888/tcp  open  tcpwrapped
10001/tcp open  ssl/scp-config?
|_ssl-ccs-injection: No reply from server (TIMEOUT)
|_sslv2-drown:
MAC Address: 40:F6:BC:C1:7E:61 (Unknown)
Service Info: Device: firewall
```

Figure 4. Example of an output of nmap script scan, showing a found vulnerability and CVEs associated

In order to maintain the accuracy of the evaluation, a systematic elimination of past log files and scan results is carried out, eliminating any dependence on obsolete reports. Afterwards, the application automatically creates a new folder when it is executed. This folder is specifically designed to store separate reports for each device that is analysed. Subsequently, a comprehensive ffuf scan and nikto scan are methodically conducted on every device, and the results are scrupulously arranged in output files located in a predefined folder that corresponds to the IP address of each device.

The programme uses a rogue access point detection capability by utilising the RogueAP-Detector, an established open-source utility specifically developed to identify unauthorised Wi-Fi access points and prevent possible data theft by criminal individuals. In addition, the tool has the ability to collect and analyse packets using the sniff function from the Scapy Python library. This function allows the device to monitor and analyse packets sent and received over the network for a specified interval (in this case, 5 minutes). It is useful for detecting possible malware infestations. It is worth mentioning that devices, particularly those related to the Internet of Things (IoT), usually send a little amount of data only when it is required. Therefore, a sudden increase in packet activity might be a sign that the device has been hijacked.

After doing scans and vulnerability assessments, the application systematically compiles all findings into an easily navigable HTML file. To address the inherent complexity and readability difficulties presented by Nmap and nmapAutomator scan outputs, a Python class has been developed to filter and retrieve relevant information with regular expressions or regex. The refined data is smoothly included into the HTML report, which is then sent to the user using the tool's inherent email reporting functionality. This strategic approach relieves the user from the laborious effort of sifting through log files and scan reports, simplifying the retrieval of relevant information about their network security status.

In order to maximise user convenience, the utility is programmed to execute automatically on a Raspberry Pi server upon startup. This is accomplished by creating a systemctl service that triggers the audit tool when the Raspberry Pi server is powered on and connected to the network. This intentional process of automating reduces the need for human involvement, resulting in a smooth and user-friendly solution for evaluating the security of home offices.

6 Evaluation

It is essential to evaluate the effectiveness of the home office security audit tool in order to confirm its practical usefulness in improving the security of home networks. This section provides a methodical assessment of the tool's performance, including its capacity to detect vulnerabilities, identify unauthorised access points, recognise IoT devices, and demonstrate overall operational efficiency.

In order to assess the efficacy of the tool, a sequence of meticulously controlled tests was carried out. A multitude of networks were established, integrating a wide range of devices including routers, smart phones, PCs, and IoT devices such as smart speakers and light bulbs. The tool was then implemented in various situations to evaluate its efficacy. This review used an iterative methodology, whereby testing was performed, and in the event that the tool generated a false negative, the scan results were scrutinised to comprehend the underlying causes for the tool’s failure to identify certain vulnerabilities. Afterwards, the programme underwent enhancements, gradually enhancing its capability to detect flaws. Furthermore, deliberate vulnerabilities and Common Vulnerabilities and Exposures (CVEs) were deliberately included into certain devices inside the network to evaluate the tool's ability to effectively identify them. A concrete instance is the tool's identification of an OpenSSL Common Vulnerabilities and Exposures (CVE) on a Linux device inside the defined network.

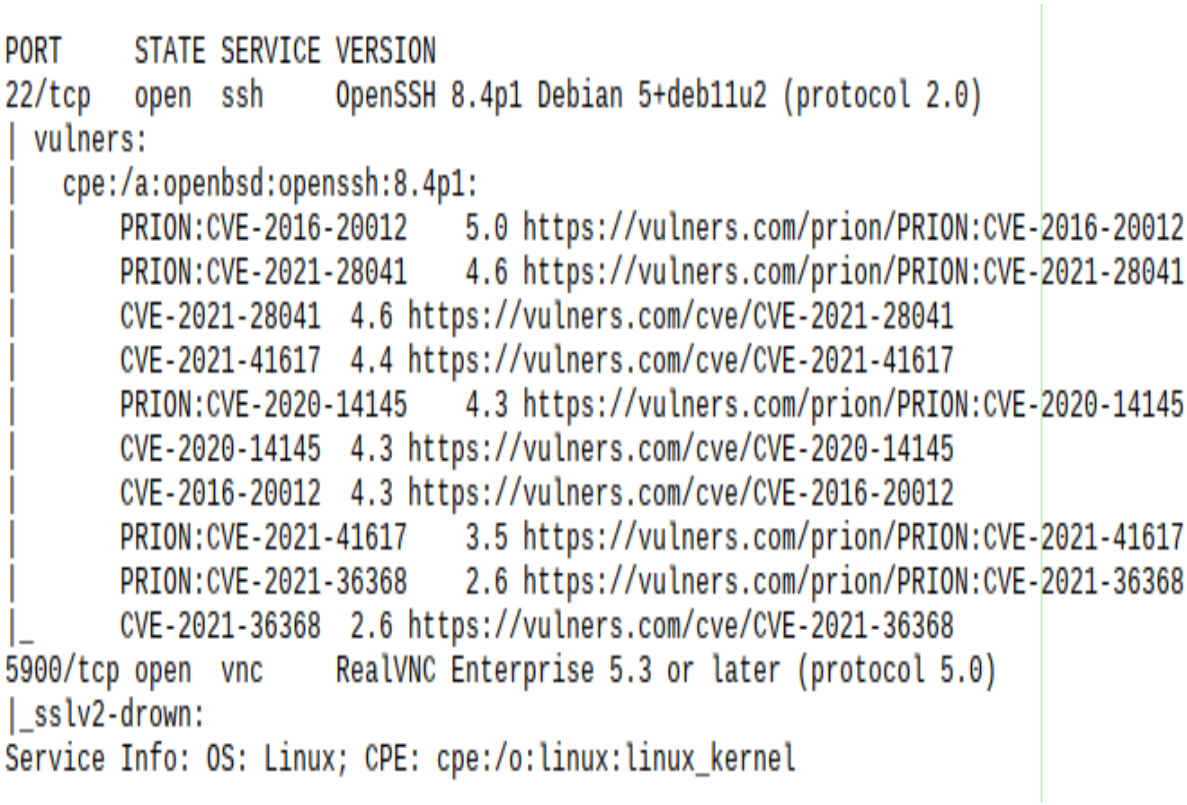

Figure 5. Report from the tool which indicates a CVE present with OpenSSL on a device on the network

To test the tool's capacity to identify rogue access points and ensure its operational correctness, a deliberate access point was set up, mirroring the review process used for vulnerability assessment. In order to carry out this test, a Kali Linux distribution was installed on a virtual computer that was set up inside the network. The establishment of the rogue access point was made possible by using a tool called Wi-Fi Pumpkin 3.

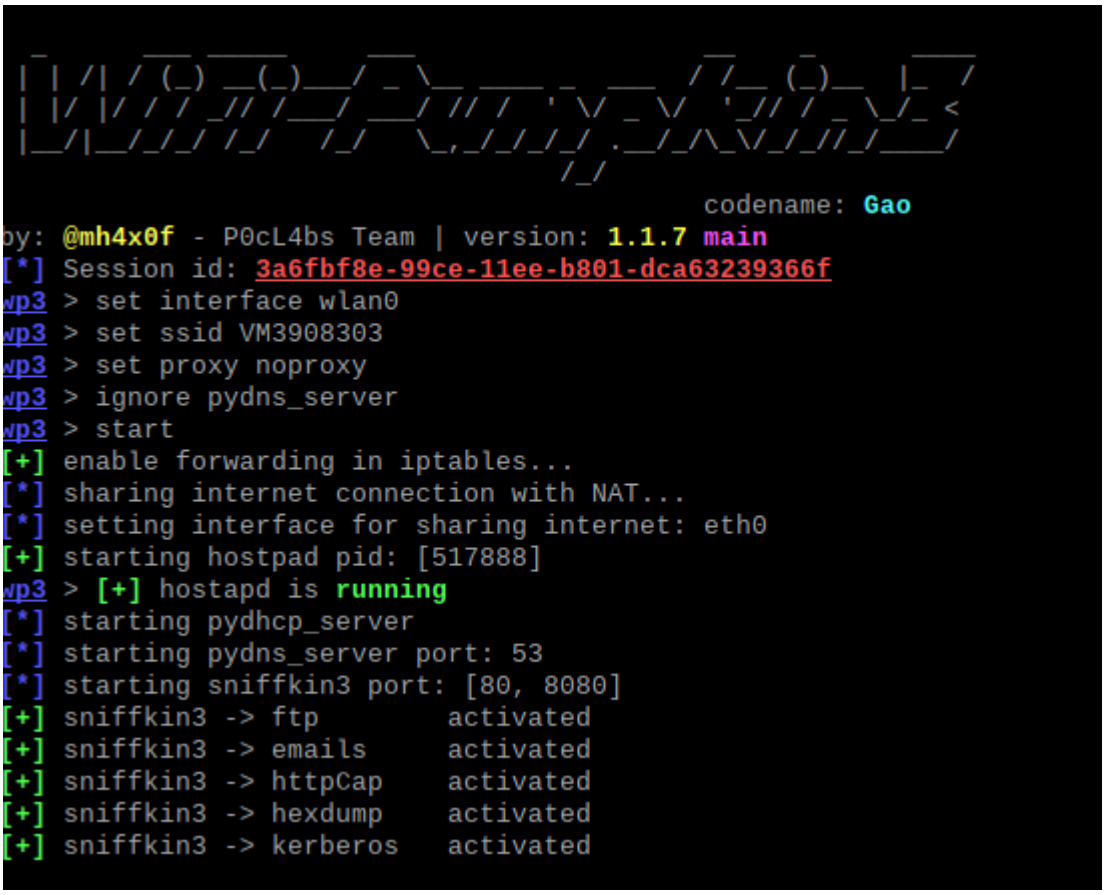

Figure 6. Wifi-Pumpkin3 setup to emulate a rogue access point

The tool did in fact manage to find the rogue access point and include it into the report.

Figure 7. Report from tool showing the presence of a rogue access point

A wide range of Internet of Things (IoT) devices were included into the network being studied to evaluate the effectiveness of the tool in detecting these devices. The tool shown an impressive performance by accurately detecting 80% of the interconnected IoT devices. A diverse range of IoT gadgets, such as Amazon Echos, Ring doorbells, and smart light bulbs, were used to guarantee a comprehensive and inclusive sample. Although the tool is proficient, there is still potential for improvement via future research efforts. An important constraint that has been noticed relates to the dependence on a predetermined inventory of IoT MAC address prefixes. The tool's identification skills might be greatly enhanced by

including an extended database that includes a larger number of IoT MAC address prefixes. This improvement would provide a more precise and thorough recognition of various IoT devices inside the network.

The packet capture function was also tested on a variety of different devices by initiating the scan and having the device send and or receive packets on the network.

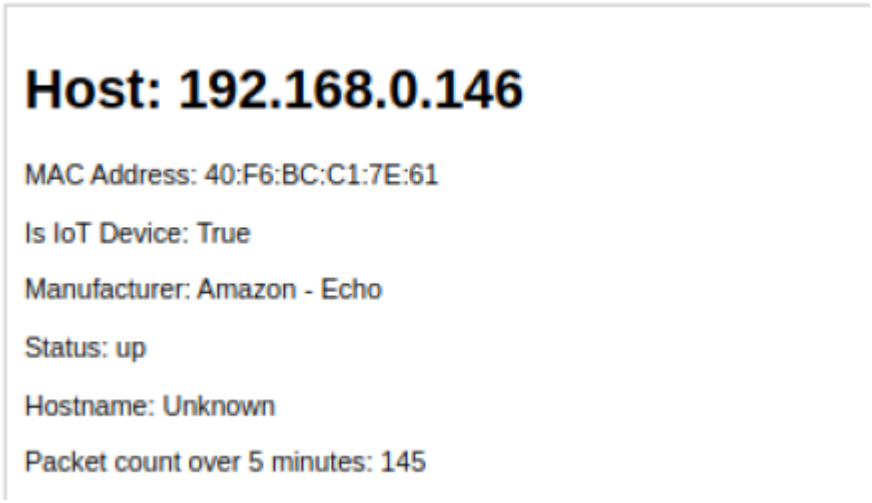

Figure 8. Packet capture count displayed in the report

6.1 Discussion

The assessment of the home office security audit tool signifies a crucial advancement in tackling the urgent issues related to the security of Internet of Things (IoT) devices in residential settings. Nevertheless, a thorough analysis of the completed experiments uncovers both positive aspects and areas that need improvement, necessitating a candid evaluation of the effectiveness of the experimental design in accomplishing the study's goals.

The experimental design included a systematic series of controlled testing, with the goal of thoroughly evaluating the tool's performance. The design is praiseworthy because to its incorporation of many networks and devices, intentional introduction of vulnerabilities, and the iterative approach for refining tools. Nevertheless, it is important to recognise certain constraints. The sample size, while offering insights, may not comprehensively reflect the wide array of home network settings. Moreover, the dependence on pre-established IoT MAC address prefixes implies a possible limitation in the tool's capacity to recognise a wider range of IoT devices.

The literature evaluation provided a strong basis for comprehending the wider scope of research on IoT security. Prior research conducted by (Hernández-Ramos *et al.*, 2015), (Agarwal, Oser and Lueders, 2019), (Ali and Awad, 2018), and (Rahim *et al.*, 2023) has emphasised the progress, approaches, and difficulties associated with ensuring the security of Internet of Things (IoT) devices in residential settings. Our study expands on these discoveries, notably focusing on the unique security considerations of home offices, where the use of IoT devices is growing.

6.1.1 Findings and Improvements

The accuracy of IoT device detection was seen to be 80%, but, the tool's dependency on a predefined inventory of IoT MAC address prefixes was identified as a restricting issue. In order to enhance precision, future versions of the tool could contemplate integrating a broader and constantly refreshed library of IoT MAC address prefixes. This improvement is in line with the recommendations from prior research, highlighting the need of adopting a complete strategy to acknowledge the changing environment of IoT devices.

The discussion on the packet capture function was not precise enough in terms of the results and difficulties faced throughout the test. Enhancing the depth of our results would be achieved by conducting a more comprehensive investigation of the tool's performance in collecting packets on different devices. Subsequent research should include a more thorough investigation of this particular feature, offering valuable perspectives on the tool's efficacy in monitoring network activity.

The research recognised the possible constraints on generalisability arising from the small sample size and controlled experimental circumstances. In order to tackle this issue, future research should contemplate broadening the scope to include a wider array of home office settings. This may include engaging with users in real-life environments to evaluate the tool's suitability in various network topologies and use situations.

Considering the dynamic nature of IoT security, future versions of the tool should investigate the possibility of incorporating preexisting security mechanisms or frameworks suggested in prior research. An illustrative instance is the security framework proposed by Hernández-Ramos et al. (2015), which may be used as a point of reference for integrating stratified security measures customised to address the unique difficulties encountered in home offices.

To summarise, while the experimental design showed many advantages, such as its iterative methodology and intentional incorporation of weaknesses, there are areas that need improvement. To strengthen the efficiency of the tool in safeguarding home office networks, it is necessary to overcome these constraints by implementing adjustments such as expanding the IoT MAC address database, doing more extensive analysis of packet capture functions, and increasing the tool's generalizability. By combining our discoveries with the knowledge obtained from prior investigations, we enhance the continuing discussion on IoT security, aiming to provide effective remedies for the changing difficulties encountered by users in home office settings.

7 Conclusion and Future Work

7.1 Conclusion

This study aimed to investigate the core issue of improving the security of home office networks by creating and assessing a security audit tool based on Python. Our main goals were to create a platform that can do comprehensive security audits, with a specific emphasis on detecting vulnerabilities, recognising IoT devices, and identifying rogue access points. The programme used well recognised tools such as nmap, nikto, and ffuf, in conjunction with a Raspberry Pi server for execution.

The research has effectively accomplished its aims, as shown by the tool's performance in controlled experiments. The main discoveries include the tool's capacity to identify vulnerabilities, accurately identify IoT devices with an 80% success rate, and successfully detect rogue access points.

The incorporation of automatic scanning algorithms, email reporting tools, and a dedicated Raspberry Pi server enhanced the tool's operating efficiency and user-friendliness. The significance of this study is substantial, especially considering the increasing ubiquity of IoT devices in home office environments. The solution offers consumers a proactive method to protect their home networks by tackling the security problems linked to these devices. The automated nature of the tool, along with its ability to generate email reports, simplifies the security assessment process, improving user convenience and minimising the need for human scrutiny of log files. Although the study has shown effectiveness, it is crucial to recognise certain constraints. The tool's reliance on a pre-existing inventory of IoT MAC address prefixes was seen as a limitation, emphasising the need for ongoing upgrades to meet the changing environment of IoT devices. Furthermore, the limited number of participants and the carefully regulated experimental circumstances may limit the applicability of the results to a wider variety of home office settings.

7.2 Future Work

Future research should prioritise efforts to overcome the stated constraints and enhance the capabilities of the home office security audit tool.

In order to enhance the precision of IoT device identification, further iterations of the tool should have a broader and consistently refreshed repository of IoT MAC address prefixes. This method is in line with the ever-changing nature of IoT security and guarantees the tool's efficacy in detecting a broader spectrum of IoT devices. Performing a comprehensive research of the tool's efficacy in gathering and analysing packets on various devices will provide significant data. This may include evaluating the effectiveness of the tool's packet capture feature in monitoring a wide range of network events by conducting tests on various devices and network environments. In order to address any limitations regarding the number of participants and controlled experimental circumstances, future studies should broaden their focus to include a wider range of home office environments. Interacting with users in actual settings will provide a more comprehensive assessment of the tool's appropriateness across different network structures and use cases. Given the ever-changing nature of IoT security, further iterations of the tool might investigate the integration of current security methods or frameworks proposed in previous research. Implementing extensive security measures, as suggested by established standards, would improve the tool's capacity to tackle the distinct issues faced in home offices.

References

Agarwal, S., Oser, P. and Lueders, S. (2019) 'Detecting IoT devices and how they put large heterogeneous networks at security risk', *Sensors (Switzerland)*. MDPI AG. Available at: https://doi.org/10.3390/s19194107.

Ali, B. and Awad, A.I. (2018) 'Cyber and physical security vulnerability assessment for IoT-based smart homes', *Sensors (Switzerland)*, 18(3). Available at: https://doi.org/10.3390/s18030817.

Ali, F. and Mathew, S. (2022) 'An efficient multilevel security architecture for blockchain-based IoT networks using principles of cellular automata', *PeerJ. Computer science*, 8. Available at: https://doi.org/10.7717/PEERJ-CS.989.

Ashton, K. (2009) 'That "internet of things" thing', *RFID journal*, 22(7), pp. 97–114.

Bremler-Barr, A., Levy, H. and Yakhini, Z. (2020) 'IoT or NoT: Identifying IoT Devices in a Short Time Scale', in *NOMS 2020 - 2020 IEEE/IFIP Network Operations and Management Symposium*, pp. 1–9. Available at: https://doi.org/10.1109/NOMS47738.2020.9110451.

Cheng, Y. *et al.* (2023a) 'VERI: A Large-scale Open-Source Components Vulnerability Detection in IoT Firmware', *Computers & Security*, 126, p. 103068. Available at: https://doi.org/10.1016/J.COSE.2022.103068.

Cheng, Y. *et al.* (2023b) 'VERI: A Large-scale Open-Source Components Vulnerability Detection in IoT Firmware', *Computers & Security*, 126, p. 103068. Available at: https://doi.org/10.1016/J.COSE.2022.103068.

Elie Bursztein (2017) *Inside the infamous Mirai IoT Botnet: A Retrospective Analysis*, *cloudflare.com*.

Emma Bell, Bill Harley and Alan Bryman (2022) 'Business research methods', *Oxford University Press*, p. 647.

Hameed, A. and Alomary, A. (2019) 'Security issues in IoT: a survey', in *2019 International conference on innovation and intelligence for informatics, computing, and technologies (3ICT)*. IEEE, pp. 1–5.

Hernández-Ramos, J.L. *et al.* (2015) 'SAFIR: Secure access framework for IoT-enabled services on smart buildings', *Journal of Computer and System Sciences*, 81(8), pp. 1452–1463. Available at: https://doi.org/10.1016/J.JCSS.2014.12.021.

Johnson, A.P., Al-Aqrabi, H. and Hill, R. (2020) 'Bio-Inspired Approaches to Safety and Security in IoT-Enabled Cyber-Physical Systems', *Sensors (Basel, Switzerland)*, 20(3). Available at: https://doi.org/10.3390/S20030844.

Kotenko, I., Izrailov, K. and Buinevich, M. (2022) 'Static Analysis of Information Systems for IoT Cyber Security: A Survey of Machine Learning Approaches', *Sensors (Basel, Switzerland)*, 22(4). Available at: https://doi.org/10.3390/S22041335.

Mrabet, H. *et al.* (2020) 'A Survey of IoT Security Based on a Layered Architecture of Sensing and Data Analysis', *Sensors (Basel, Switzerland)*, 20(13), pp. 1–20. Available at: https://doi.org/10.3390/S20133625.

Rahim, A. *et al.* (2023) 'Enhancing Smart Home Security: Anomaly Detection and Face Recognition in Smart Home IoT Devices Using Logit-Boosted CNN Models', *Sensors*, 23(15). Available at: https://doi.org/10.3390/s23156979.

Rana, M., Mamun, Q. and Islam, R. (2023) 'Enhancing IoT Security: An Innovative Key Management System for Lightweight Block Ciphers', *Sensors (Basel, Switzerland)*, 23(18). Available at: https://doi.org/10.3390/S23187678.

Roy, S. *et al.* (2022a) 'IoT Security and Computation Management on a Multi-Robot System for Rescue Operations Based on a Cloud Framework', *Sensors (Basel, Switzerland)*, 22(15). Available at: https://doi.org/10.3390/S22155569.

Roy, S. *et al.* (2022b) 'IoT Security and Computation Management on a Multi-Robot System for Rescue Operations Based on a Cloud Framework', *Sensors (Basel, Switzerland)*, 22(15). Available at: https://doi.org/10.3390/S22155569.

Williams, P. *et al.* (2022) 'A survey on security in internet of things with a focus on the impact of emerging technologies', *Internet of Things*, 19. Available at: https://doi.org/10.1016/j.iot.2022.100564.

Wise, J. (2023b) *Amazon Echo Sales Figures for 2024 - EarthWeb*. Available at: https://earthweb.com/amazon-echo-sales-figures/ (Accessed: 13 December 2023).

Wu, J.-S., Hsu, F.-H. and Lee, C.-H. (2021) 'Identifying IoT Devices with SMTP', in *2021 IEEE International Conference on Consumer Electronics-Taiwan (ICCE-TW)*, pp. 1–2. Available at: https://doi.org/10.1109/ICCE-TW52618.2021.9603238.

Yin, F. *et al.* (2021) 'IoT ETEI: End-to-End IoT Device Identification Method', in *2021 IEEE Conference on Dependable and Secure Computing (DSC)*, pp. 1–8. Available at: https://doi.org/10.1109/DSC49826.2021.9346251.