Securing Your Home Network: A Guide to Parrot OS Tools

Luis Raúl Ortiz-Serrano
Master in Computer Science
Advisor: Alfredo Cruz-Triana, Ph.D.
Electrical & Computer Engineering and Computer Science Department
Polytechnic University of Puerto Rico

Abstract *— This master project presents a comprehensive exploration of the realm of ethical hacking, emphasizing its crucial role in protecting home systems from cyber threats. This master's work delves into the importance of proactive measures to identify vulnerabilities and counteract possible attacks in domestic environments. Through the lens of ethical hacking methodologies, the project focuses on five prominent tools that are integral to contemporary cybersecurity practices. By immersing yourself in a real-world home scenario, your goal is to deepen your understanding of these cybersecurity tools, systems, and principles, fostering a culture of prevention and response. A central element of the research is the examination of the impact of ethical hacking on educational paradigms, with the aim of improving students' understanding of the nuances of cybersecurity in a domestic context. By integrating ethical hacking exercises into education, the project strives to equip students with basic skills and knowledge to mitigate modern threats to home network security, thereby strengthening personal data protection and system integrity. Eventually, this effort seeks to contribute both theoretically and practically to the field of cybersecurity, fostering a more professional and vigilant student community, equipped to confidently navigate the changing cybersecurity landscape.*

Key Terms *— Computer Security, Cybersecurity Exercise, Education, Ethical Hacker, Parrot OS Tools.*

INTRODUCTION

To start the project, it begins with the following definition: Pentesting cybersecurity technique consisting of attacking computer environments with the intention of discovering vulnerabilities in them. Pentesting is sometimes called a white hat attack or ethical hacking, because those responsible for an organization's systems attempt to bypass their own security measures to expose security vulnerabilities. Today, ethical hacking has been established as a fundamental practice to guarantee information security in an increasingly vulnerable digital environment. In this context, the creation of a real domestic pentest laboratory is presented as a unique opportunity to test and improve ethical hacking skills in a controlled and safe way. The Parrot OS operating system has stood out as a robust and versatile platform for carrying out penetration testing, thanks to its wide range of specialized tools. Combine these tools in a real home pentest lab gives cybersecurity enthusiasts and professionals the opportunity to hone their skills and knowledge in a controlled and secure environment. With the implementation of a laboratory of this type, the aim is to promote the ethical practice of hacking, training participating students to identify and correct vulnerabilities in computer systems, thus contributing to strengthening cybersecurity. In this project, the importance of following an ethical and legal approach in all pentesting activities is promoted, guaranteeing respect for the privacy and integrity of the information.

PROBLEM STATEMENT

Despite the exponential growth of internet connected devices in modern households, the security of home networks and Internet of Things (IoT) devices remains a significant concern. Lack of awareness about security best practices, complexity in network configuration, and the proliferation of vulnerabilities in insecure devices create an environment ripe for cyber-attacks and privacy breaches. The absence of accessible tools and resources for homeowners to understand and

protect their home networks against emerging cyber threats poses a significant challenge. Furthermore, the lack of training and expertise in cybersecurity among home users contributes to the spread of botnets, ransomware attacks, and exposes sensitive personal data to security risks. Therefore, there is a need to address this security gap by creating effective cybersecurity awareness, education, and training strategies for homeowners. This entails developing accessible tools, programs, and resources that enable users to understand and mitigate security risks in their home networks and IoT devices. The challenge lies in designing and implementing comprehensive and practical solutions that empower homeowners to proactively protect their home networks, thereby reducing exposure to cyber threats and strengthening information security in the home environment. Additionally, it is crucial to ensure that these solutions are user friendly, cost effective, and adaptable to the diverse needs and technical proficiencies of homeowners, fostering a culture of cybersecurity awareness and resilience in the domestic setting.

PROJECT GOAL

The main objective of the project is to provide comprehensive training in the effective basic use of essential cybersecurity tools in the context of a master's laboratory focused on a controlled home network. Specifically, participants will be taught to use tools such as NMAP, Wireshark, Bettercap, Burp suite and Metasploit on the PARROT OS operating system, which will serve as a controlled learning platform. In this controlled environment, participants will receive detailed instruction on how to employ these tools to identify and mitigate potential threats on the real home network. Starting with NMAP, you will learn to perform basic analysis of network infrastructure, identify connected devices, and discover potential vulnerabilities that could be exploited by attackers. They will then be guided in using Wireshark to analyze network traffic, allowing them to examine packets in detail and detect possible malicious activity or anomalies in the simulated network. Bettercap will also be explored as a tool for real time traffic interception and manipulation, allowing them to understand and mitigate potential security risks in the controlled home network. Additionally, training will be provided in using Burp suite to perform security testing on web applications, identifying and exploiting common vulnerabilities to evaluate the security of simulated applications. Finally, students will be introduced to Metasploit for penetration testing and vulnerability exploitation, allowing them to identify and explore vulnerabilities in target systems in the controlled environment. At the end of the project, it is expected that participants will have acquired practical skills and essential knowledge in the use of these cybersecurity tools in a home network environment.

RESEARCH QUESTIONS

Discussion topics will be tailored to the context and particular objectives of the discourse. Presented below are a selection of stimulating questions pertaining to ethical hacking, Parrot OS tools, and their practical implications within the realm of computer security:

- How can you identify vulnerabilities in your home network using ethical hacking tools like Nmap and Metasploit?
- What cybersecurity measures can be implemented in a home environment to protect against hacker attacks?
- How can you perform an internal penetration test on a home network using tools like Burp Suite and Bettercap?
- What is the importance of computer security education to prevent cyberattacks at home?
- How can you simulate a cybersecurity exercise in a home environment using different ethical hacking tools?

RELEVANCE AND SIGNIFICANCE

Ethical hacking in a home network using tools like Nmap, Wireshark, Bettercap, Burp Suite, and Metasploit within the Parrot OS operating system

holds significant relevance due to several key aspects. Firstly, it offers proactive protection by enabling students to identify and address security vulnerabilities in their home networks before they are exploited by malicious actors. This provides them with the opportunity to take proactive measures to safeguard their personal information and the integrity of their computer systems. Furthermore, it supports students in raising awareness about home security. By conducting penetration testing and security assessments on their own home network, students gain a deeper understanding of the potential threats and vulnerabilities they face. This empowers them to make informed decisions on how to strengthen their cybersecurity and implement appropriate preventive measures. Additionally, it guides and trains students against emerging threats. In a constantly evolving digital environment, staying abreast of the latest threats and attack techniques is crucial. Ethical hacking on a home network allows students to become familiar with these emerging threats and develop effective defense strategies to mitigate them. Instead of relying solely on external experts, students can actively participate in protecting their data and the privacy of their homes. Encouraging the practice of ethical hacking in domestic environments promotes a culture of cybersecurity where information protection and cyberattack prevention become fundamental priorities. This contributes to creating safer and more resilient communities in the digital realm.

METHODOLOGY

To conduct a security assessment project on a home network, a structured methodology will be followed, covering various stages. Initially, the objective is established to evaluate the network's security to identify and mitigate potential vulnerabilities. This involves defining the project's scope, including assessing all connected devices, from computers to IoT devices and routers. Once the scope is set, the reconnaissance phase begins using tools like Nmap and Bettercap to scan the network and gather information about devices, services, and open ports, serving as the basis for further analysis. Subsequently, network traffic is analyzed using Wireshark to capture and examine communication patterns, potential attacks, or unusual behaviors indicating vulnerabilities or threats. The traffic interception and manipulation phase follows, employing Bettercap to simulate potential attack scenarios and evaluate the network's response via ARP spoofing attacks. A web application assessment using Burp Suite identifies potential vulnerabilities such as command injections or authentication failures. Finally, Metasploit explores and exploits potential vulnerabilities in network services and devices, with controlled penetration testing assessing the network's resilience to real-world attacks. A laboratory environment simulating a local network is set up, using a private local network and controlled configurations to conduct testing without affecting a real network. Documentation is integral, recording each step, including configurations, scan results, traffic captures, and security findings, culminating in a detailed report with vulnerability descriptions, proof of concept tests, and mitigation recommendations. Throughout, security and ethics are paramount, with proper consent obtained for real home networks and tests conducted responsibly to avoid harm. Upon completion, a detailed report outlines test results, recommendations, and corrective actions to enhance home network security.

VirtualBox is a free and open-source virtualization product developed by Oracle Corporation [1]. It’s a software application that allows users to create and run virtual machines on their computers, which simulate the hardware and software configuration of a real computer. With VirtualBox, users can experiment with different operating systems without altering their main system. It supports various host operating systems, including Windows, macOS, Linux, and Solaris, and can run a wide range of guest operating systems. VirtualBox offers features like snapshotting, cloning, and virtual disk encryption, along with flexible networking options for communication between virtual machines and the

host system. It also provides integration features such as seamless mode and shared folders to enhance user experience. Popular among developers and testers, VirtualBox is widely used for software development, testing, and debugging purposes. First of all, make sure you have VirtualBox installed on your computer. Figure 1 represents the screen to create a new virtual machine, pressing *new* button in application.

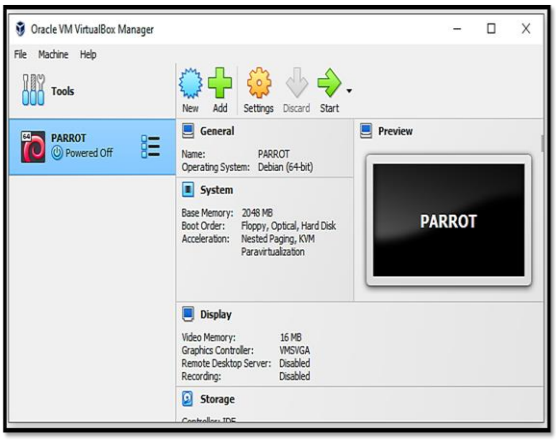

Figure 1
Install Parrot OS with VirtualBox

The operating system for this laboratory will be Parrot OS is a security-oriented operating system based on Debian Linux. It comes with a wide range of security tools for various purposes, such as penetration testing, forensics, and general security assessments. Parrot OS allows the user to completely hide their identities when surfing the Internet and, therefore, remain relatively undetectable when engaging in cybersecurity counterattacks against hack attempts [2]. Figure 2 below represents the Parrot Operating System Desktop screen.

Figure 2
Desktop Parrot OS

Network Mapper (Nmap) is a free and open-source tool for network exploration and security auditing. It is used to discover hosts and services on a computer network, thus creating a map of the network. To start scan an IP and detect potential vulnerabilities, you can use the Nmap tool. Nmap is commonly used for security audits, many systems and network administrators find it useful for routine tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime [3]. Figure 3 represents the command *nmap* 192.168.0.1. This command will initiate a scan of the target host.

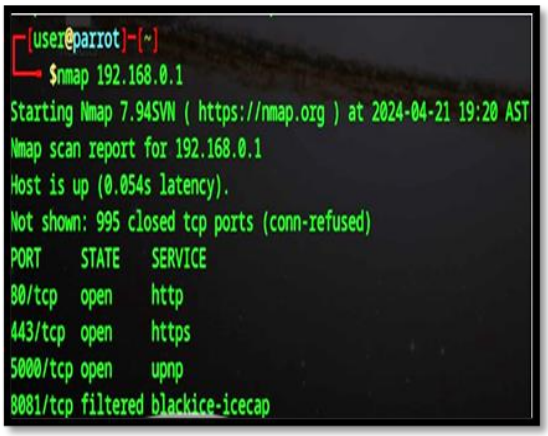

Figure 3
First Command NMAP Tool

Wireshark is a network packet analyzer. It captures network packets and displays detailed information about them. It is used for network troubleshooting, analysis, and security auditing. Wireshark is one such tool that can offer an in-depth view of network activities, diagnose network performance issues, or identify potential security threats [4]. Wireshark's powerful filtering capabilities allow users to quickly identify and isolate specific packets or conversations within a large capture. By analyzing the packet contents, security professionals can detect and respond to potential threats, such as unauthorized access or data breaches. Additionally, Wireshark's graphical interface makes it easy to visualize network traffic and identify patterns and anomalies, making it a valuable tool for network administrators and security teams. Figure 4 represents the process that involves using filters and examining the contents of

packets to search for sensitive information, potential vulnerabilities, or any abnormal behavior that may hint at security threats.

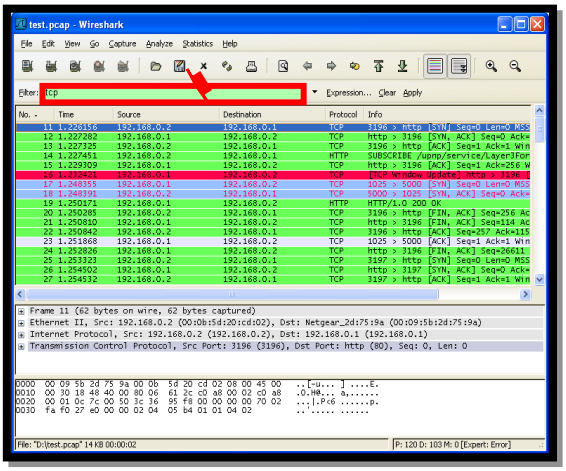

Figure 4
Capturing Packages

When done, the student sees the captured network traffic for signs of malicious activity, intrusion attempts, suspicious communications, or any other indicators that could suggest a security breach on the home network.

Bettercap is a comprehensive network security and hacking framework that performs various attacks and combines different tools into a single cohesive platform. It is used for penetration testing, network monitoring, and other security-related tasks. Developed in the Go programming language, it enables security professionals to analyze and assess the security posture of their networks comprehensively [5]. Bettercap offers a command-line interface that allows users to interact with its various modules and features effectively. Bettercap's modular design allows users to customize their workflows and automate tasks, making it an efficient tool for repetitive testing and monitoring tasks. By leveraging its extensive library of plugins and modules, security professionals can conduct a wide range of network attacks, including ARP spoofing, DNS spoofing, and man-in-the-middle attacks, among others. Figure 5 represents the sending out probe packets to identify active hosts on the network and explores the services running on each device by probing for open ports associated with specific devices or services, providing valuable insights into potential attack vectors.

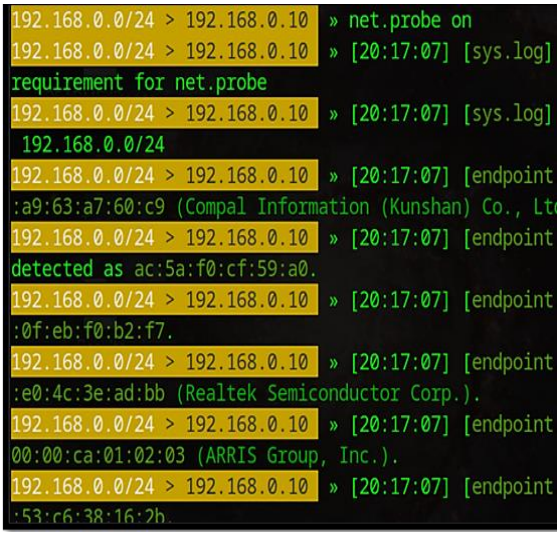

Figure 5
net.probe on Command

Burp Suite is a set of tools used for penetration testing of web applications [6]. It is developed by the company named Portswigger, which is also the alias of its founder Dafydd Stuttard. Burp Suite aims to be an all-in-one set of tools and its capabilities can be enhanced by installing add-ons that are called BApps. Is a set of web application security tools. It includes a variety of functions, such as web vulnerability scanning, exploitation, and other security testing tasks. It is commonly used for web penetration testing purposes. Figure 6: represents how proxy adjusting settings such as the proxy listener port, intercept options, and other proxy related configurations are necessary to customize your web traffic analysis and manipulation process. With Burp Suite, the student can identify potential security weaknesses, test different input values, The tool its capability to intercept, modify, and analyze traffic for evaluating and enhancing the security of web applications. Once Burp Suite is configured, navigate to the Proxy tab, and ensure that the Intercept is on button is toggled on. This enables Burp Suite to intercept and analyze HTTP and HTTPS traffic between your browser and the target web application. With the proxy running, browse the target web application as you normally would. Burp Suite will intercept all

requests and responses between your browser and the web application.

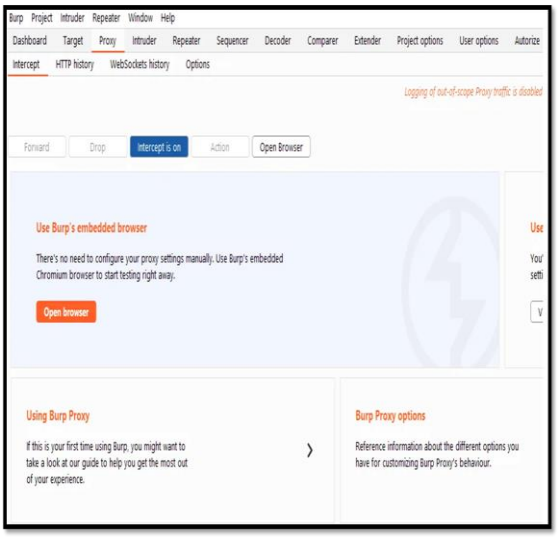

Figure 6
Burp Suite Additional Tools Opens in a New Window - rahulk2903.medium.com

Metasploit is used for network enumeration, identifying vulnerabilities, developing payloads, and executing exploit code against remote target machines [7]**.** Basically, it is a penetration testing framework that includes tools for developing, testing, and executing exploit code. It is widely used for testing the security of computer systems and for penetration testing exercises. Familiarize yourself with the different functions and commands available in Metasploit. Also have an extensive database of exploits and modules allows users to quickly and easily identify and exploit vulnerabilities, making it a powerful tool for simulating real-world attacks and assessing the security of networks and systems. To get a general list of commands, **type *help*** and **press Enter**. This command in Metasploit is used to display a list of available commands and provide detailed information on how to use them. Simply type help in the Metasploit console and you will be shown a list of commands, along with a brief description of each. The student can also use help followed by the name of a specific command to get more information on how to use it correctly. Figure 7 represents an example of the help command with the word search in the CLI command line interface.

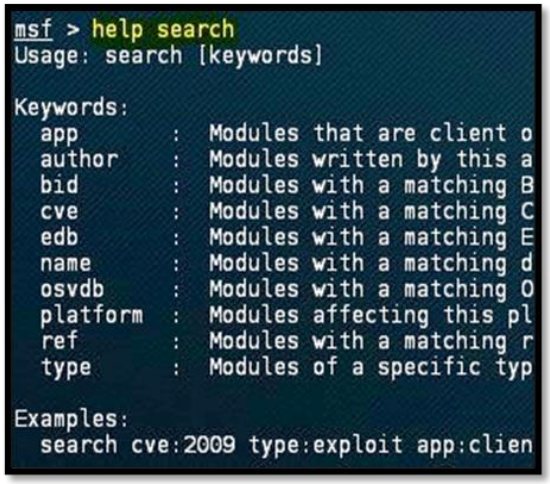

Figure 7
Help command Metasploit

RESULTS & DISCUSSION

To identify vulnerabilities in their home network, the individual used ethical hacking tools such as Nmap and Metasploit. They began by scanning the network with Nmap and running a network scan to identify connected devices and open ports on those devices. For example, they used the command *nmap -sS 192.168.1.0/24* to scan all devices on the 192.168.1.0/24 subnet. After identifying open services and ports, they utilized other tools and complemented their analysis with Metasploit to explore the vulnerabilities found during the Nmap scan, focusing on the identified services and software versions to determine if the network is susceptible to attacks.

In fortifying their home environment against potential hacker attacks, the individual prioritizes several key cybersecurity measures. Firstly, they ensure the use of strong, unique passwords for all devices and accounts. By employing complex passwords and avoiding common phrases or easily guessable information, they mitigate the risk of unauthorized access. Additionally, they diligently keep all software and firmware up to date, enabling automatic updates whenever possible to promptly apply security patches and address known vulnerabilities. Network encryption, particularly utilizing protocols like WPA2 for Wi-Fi, serves as another crucial layer of defense. By encrypting network traffic, the individual prevents

unauthorized interception and access to sensitive information. Moreover, they have implemented a security system to monitor and control incoming and outgoing network traffic, thereby reducing the attack surface and blocking potential threats. Complementing these measures, they have installed reputable antivirus and antimalware software on all devices, ensuring regular updates to stay protected against evolving threats. Finally, they exercise caution when browsing the internet, avoiding clicking on suspicious links or downloading unknown files to mitigate the risk of malware infections or falling victim to phishing attempts.

When performing an internal penetration test on their home network using tools like Burp Suite and Bettercap, the individual adopted a systematic approach to assess its security. Firstly, the student configured Burp Suite to function as a proxy, enabling the interception and analysis of network traffic. This setup allowed them to meticulously inspect HTTP requests and responses for vulnerabilities and potential security weaknesses. This proactive measure helped the individual identify and address potential threats within their home network, enhancing its overall security posture and resilience against potential cyber-attacks. Simultaneously, the individual utilized Bettercap to execute ARP spoofing attacks and other network-based exploits within their home environment. By leveraging ARP spoofing, they were able to redirect network traffic through their machine, providing an opportunity to analyze and potentially exploit vulnerabilities across various devices connected to the network. This proactive approach allowed the individual to identify and address potential security risks, enhancing the overall resilience of their home network against malicious activities. Throughout the penetration testing process, the individual simulated diverse attack scenarios to comprehensively evaluate the resilience of their home network's security defenses. This involved attempting to intercept sensitive data, exploiting known vulnerabilities in network services or devices, and assessing the efficacy of implemented security controls such as firewalls and intrusion detection systems. The individual took the initiative to address any weaknesses identified during the testing, ensuring the continued protection of their network assets. By conducting internal penetration testing with tools like Burp Suite and Bettercap, the individual can systematically identify and address vulnerabilities within their home network.

Computer security education holds immense importance in thwarting cyber-attacks within the home environment. It serves as a fundamental pillar in empowering individuals to safeguard their digital assets and personal information effectively. By acquiring knowledge about prevalent attack techniques, individuals can discern potential threats and respond proactively. Understanding cybersecurity best practices is paramount, as it enables individuals to fortify their defenses and minimize vulnerabilities within their home networks. Ultimately, computer security education empowers individuals to take proactive steps in protecting their home networks, thereby mitigating the risks posed by cyber adversaries.

Simulating a cybersecurity exercise in a home environment using a variety of ethical hacking tools involves creating a controlled environment. Various security tools and techniques can be meticulously tested to improve understanding and proficiency in cybersecurity practices. To start the exercise, simulated attacks are configured using tools such as Wireshark, Nmap, Metasploit or Burp Suite. These tools enable replication of common cyber threats and vulnerabilities within the home network, allowing for extensive testing of security measures and incident response capabilities. This hands-on approach deepens understanding of cybersecurity principles and provides the skills necessary to harden a home network against real-world threats. Overall, conducting cybersecurity exercises in a home environment using ethical hacking tools serves as a proactive measure to improve cybersecurity proficiency and bolster the resilience of digital defenses.

The security assessment of the home network revealed a positive security posture with several strengths. The network utilizes WPA2 encryption, the current industry standard, along with strong

passwords for devices and access points. This significantly reduces the risk of unauthorized access. Additionally, user keeps router firmware and device software up to date, addressing known vulnerabilities and strengthening overall security. Employing Wireshark for network traffic monitoring demonstrates a proactive approach to security, allowing for the detection of potential anomalies. Furthermore, a collaborative security policy established with family members promotes cybersecurity awareness within the household. However, there is room for improvement. The default router administrator password should be replaced with a strong and unique one. Additionally, enabling two-factor authentication on the router, if possible, would add another layer of security. Further recommendations include customizing firewall rules for granular control over network traffic, implementing a separate guest network, and conducting periodic security reviews. It is crucial to emphasize regular security checks, highlighting the ongoing nature of network security maintenance. It is not a one-time set and forget process but requires continuous monitoring and reassessment.

This document outlines the ethical hacking activities conducted on a specific target network to identify security vulnerabilities and provide mitigation recommendations. The scope of the exercise was focused on the specified network and systems. Various methodologies, including network scanning, vulnerability analysis, traffic interception, and web application analysis, were utilized to uncover weaknesses in the target network. Findings revealed issues such as misconfigured security settings, lack of security updates, unnecessary open ports, and known vulnerabilities in outdated software. To mitigate these risks, it is essential to regularly update security configurations, apply patches, close unnecessary open ports, and replace outdated software. Implementing a comprehensive security policy, conducting security assessments, and providing cybersecurity training can strengthen defenses against cyber threats. The document highlights the security impacts in a home network, such as data breaches, identity theft, privacy loss, compromised devices, risks for children, and service disruptions. Recommendations include implementing basic security measures like changing default passwords, updating devices, and using VPNs. In essence, safeguarding home networks against cyber threats is crucial in today's digital age. Strong password practices, regular software updates, data encryption, antivirus software, securing IoT devices, and cybersecurity education are essential steps to enhance home network security. Education on cyber threats and safe online practices is crucial in fostering a culture of vigilance within the home environment.

FUTURE WORK

Some comments from and shortcomings of this project, which are worth noting, are:

- *Expanding the scope of cybersecurity topics:* The project should cover a wider range of topics beyond the basics, including network security, cryptography, secure coding, incident response, and regulatory compliance. This helps students gain a more well-rounded understanding of the field.
- *Integrating more cybersecurity tools*: Exposing students to a variety of tools used in vulnerability assessment, intrusion detection, log analysis, threat intelligence, etc., equips them with a broader skillset and the ability to choose the right tool for the job.
- *Utilizing real life scenarios:* Integrating practical scenarios like simulated cyberattacks, incident response, and red/blue team exercises allows students to apply their theoretical knowledge and develop practical skills in a safe environment.

CONCLUSION

The conclusion emphasizes the significance of integrating cybersecurity tools into educational curricula, highlighting the numerous benefits they offer. Through practical learning, students enhance their skills and comprehension of real-world cyber threats. By engaging in cybersecurity exercises, students not only reinforce their theoretical

knowledge but also gain hands-on experience in identifying vulnerabilities, managing risks, and responding to security incidents. This experiential learning cultivates confidence among students as they navigate the complexities of cybersecurity. The conclusion asserts that these exercises serve as a valuable platform for students to explore diverse topics, tools, and techniques within the cybersecurity domain, including penetration testing, vulnerability assessment, incident response, and digital forensics. By expanding their understanding of cybersecurity and fostering a culture of hands-on learning, students are equipped to adapt to the evolving digital landscape and pursue lifelong learning and innovation in the field. Ultimately, cybersecurity exercises play a crucial role in educating students, providing them with the practical skills, knowledge, and experience necessary to succeed in addressing the challenges of an increasingly digitized world.

REFERENCES

[1] F. Filipsson. (January 23, 2024). *What is VirtualBox? A Complete Guide to Virtualization* [Online]. Available: https://redresscompliance.com/what-is-virtualbox-a-complete-guide-to-virtualization/.

[2] Kingsland University. (2024). *What Are the Best Linux Distros for Cybersecurity Students?* [Online]. Available: https://kingslanduniversity.com/best-linux-distros-cybersecurity.

[3] G. Lyon. (January 1, 2009). *NMAP Network Scanning* [Online]. Available: https://nmap.org/book/man.html.

[4] K. Terrell. (2024). *What is Wireshark?* [Online]. Available: https://www.techtarget.com/whatis/definition/Wireshark.

[5] A. Santhosh. (July 19, 2023). *Bettercap: Unleashing the Power of Network Security* [Online]. Available: https://santhosh-adiga-u.medium.com/bettercap-unleashing-the-power-of-network-security-35de1d1d8552.

[6] Geeks for Geeks. (September 30, 2022). *What is Burp Suite?* [Online]. Available: https://www.geeksforgeeks.org/what-is-burp-suite/.

[7] Try hack me. (2024). *Metasploit* [Online]. Available: https://tryhackme.com/module/metasploit.