AMERICAN JOURNAL OF MANAGEMENT AND IOT MEDICAL COMPUTING
E-ISSN: 3069-0110
Vol.4, No. 3(2025)
www.ajmimc.com

HOME NETWORK SECURITY LAB

[1] Dr.K.RAKESH , [2] GANGARAM CHATURVEDA , [3] CHETLA AKHILA , [4] MALAPATI NIHARIKA REDDY

[1] Associate Professor, Department of CSE-Cyber Security ,Malla Reddy Engineering college for women Hyderabad, India

[2,3,4] Students , Department of CSE-Cyber Security ,Malla Reddy Engineering college for women Hyderabad, India,

[2] Email:chaturveda86@gmail.com , [3] Email: akhilachetla23@gmail.com , [4] Email :niharikareddy638@gmail.com

ABSTRACT

In the current age of technology home networks and small startup settings are more at risk of cyber attacks because wireless connections and smart devices are now used extensively securing the wi-fi networks that is now important to defend confidential information to make sure user privacy and avoid unauthorized access this research centers on building and enforcing effective security measures to secure home and small office wi-fi the study delves into shared weaknesses like weak passwords old firmware unencrypted traffic and routers with incorrect configurations it also delves into contemporary security mechanisms like different encryptions firewall setups networks segmentation also virtual private networks vpn usage by combining these methods users can build robust defenses against cyberattacks the project intends to offer practical recommendations and a cost-effective model appropriate for home users.

I.INTRODUCTION

Establishing a home network security lab establishes a worthwhile setting for learning practical skills in securing contemporary home wi-fi networks and small businesses networks as cyber attacks grow sophisticated and often target individuals and startups theoretical cybersecurity expertise alone is no longer sufficient a specialized lab offers a safe controlled place to experiment with network setups simulate attacks and practice defense techniques without putting real systems at risk[1] for home users such an arrangement provides hands-on training in protecting personal information securing iot devices and practicing good network hygiene[2] for small startups often exposed due to sparse technical and financial resource sources the lab acts as a cost-effective avenue for staff training security tool testing and establishing a robust scalable defense system[3] creating and utilizing a home network security lab empowers users to transition beyond rudimentary awareness towards active defense with the practical know-how to effectively counter emerging cyber threats

II. RELATED WORK

1. Overview of Network Security in Home and Educational Environments:

Digital connectivity has extended cybersecurity concerns from enterprise networks to residential and small-scale setups. Most home users deploy wireless routers with default or weak security configurations, leaving them open to attacks such as unauthorized access, brute-force logins, or stealth reconnaissance[4]. These reasons call for a simplified network defense framework that could operate effectively on limited hardware while retaining transparency and educational value. This has been recognized in several academic and industrial initiatives.

Virtual labs are increasingly used to reproduce and analyze these attack-defense dynamics in a safe, isolated environment. Emphasized by studies, hands-on network simulation helps learners and researchers visualize intrusion patterns[5], packet behaviours, and mitigation responses without exposing real systems to risk. These labs combine open-source security tools that can simulate both sides of the cyber event: an attacker machine, such as Kali Linux, and a defender system, possibly Ubuntu or Parrot OS, with defensive tools such as UFW, Fail2ban, and IDS.

2. Network Scanning and Reconnaissance Detection:

Port scanning has remained one of the earliest and most persistent phases of cyber intrusion. Network Mapper, or simply Nmap, is still considered the standard for active network discovery[6] and vulnerability scanning. Previous studies have focused on the fingerprinting behavior of Nmap; hence, its SYN, ACK, and UDP scan patterns have been analyzed to develop signature-based techniques for detection.

Research has shown that each of these scanning modes produces different timing and packet-flag signatures that can be identified by appropriately configured detection systems. SYN scans, for instance, produce a flurry of half-open TCP connections that can be detected either by packet-count thresholds or anomaly-based systems. Classically, tools such as Scanlogd, PSAD, and PortSentry were used to perform this function[7], but the modern defender is more likely to employ an IDS such as Snort or Suricata for visibility into a wider range of protocols[8]

This work develops on these research directions by using Nmap in this context as a controlled attacker tool, which, in a safe lab, simulates reconnaissance behavior in order to see if host-based countermeasures (UFW and Fail2ban) can detect and respond to repeated attempts effectively.

3. Firewall-Based Intrusion Mitigation

Received: 11-07-2025 | Accepted: 13-08-2025 | Published: 20-08-2025 |

Firewalls are a core part of network protection-a system designed to control traffic according to a predetermined set of rules. Prior studies focused mostly on enterprise-level firewalls or hardware appliances. However, recent work is devoted to lightweight, host-based firewalls that are appropriate for personal and educational systems[9].
UFW is a frontend for iptables in Ubuntu-based distributions that is geared toward ease of use for non- expert users. Indeed, studies have demonstrated that UFW configuration best practices such as blocking unused ports, enforcing default deny, and enabling traffic logging[10] can substantially reduce the attack surface for small networks.

In addition, enabling the logging in UFW will provide a good dataset for later analysis and can be integrated with monitoring systems such as Fail2ban or log parsers. A few educational implementations are found that show how UFW logging combined with the data from IDS can present an end-to-end picture of attempted intrusions, including the attempts of connections, timestamp, and source.

4. Automated Log-Based Defense: Fail2ban Mechanism:

Automation of intrusion response has been widely discussed in the literature as the next necessary evolution of defensive operations. Fail2ban is one open-source intrusion prevention framework frequently cited based on its simplicity and adaptability[11]. It parses system logs for repetitive malicious behavior, for instance, repeated authentication failures, and dynamically updates firewall rules to ban offending IP addresses temporarily.

Various research papers and case studies have also evaluated Fail2ban under different scenarios: SSH brute- force, Web service login attempts, and DoS mitigation. Results suggest that though Fail2ban fails to replace a dedicated IDS or IPS, its lightweight automated banning mechanism enhances baseline security significantly on Linux hosts.
However, the literature also warns that incorrect tuning of thresholds (e.g., ban duration or retry counts) results in false positives, blocking legitimate users. To that end, hybrid configurations, combining Fail2ban with real-time IDS alerts or contextual correlation, have been suggested[12], one such design directly inspiring the structure of this home network project.

5. Intrusion Detection and Integration with Automated Response:

The recent focus of research has included the integration of IDS tools such as Suricata or Snort with automated response systems[13]. Suricata is exceptionally well-suited for high-volume or signature-specific event detection, such as SYN scans, thanks to its multithreaded packet inspection and extensible rule language. Several comparative studies show that Suricata performs well on commodity hardware, but perhaps more importantly, it facilitates easy customization of rule sets for an educational or experimental setup.
By integrating Suricata with Fail2ban or custom response scripts, you have the capacity for real-time active defense, where the alerts from IDS trigger firewall actions directly. This layered approach—first detection, then mitigation in a controlled way[14]—works best at balancing speed and precision in small-scale deployments.

While this mini-project touches mainly on Fail2ban and UFW, the concept is extended here by using Suricata's alert logs as the trigger source for Fail2ban to enforce IP bans after multiple detections, hence embodying the "Detect → Block → Log → Review" cycle central to modern intrusion response frameworks.

6. Educational and Experimental Virtual Labs:

Security training institutes and a number of universities now encourage students to create virtual, home, or classroom-scaled security labs by using tools like VirtualBox, VMware, or Proxmox[15]. Such labs allow learners to practice scanning, hardening, and response in isolated environments, ensuring that no data leakage or interference with production systems occurs.
Previous works show that educational labs involving Kali Linux (attacker) and Ubuntu/Parrot (defender) make the workflow of offensive/defensive cyber operations very intuitive and visual. Structured experiments, like performing recon, then detecting it via IDS and visualizing bans in logs, are common in such labs to bridge the gap between theory and practice.
This mini-project contributes to this educational heritage by providing a reproducible, low-cost, safe virtual lab architecture that will enable students and beginners to understand the basics of detection, blocking, and logging in real time. The simplicity of the design-just two VMs connected over an isolated internal network-will ensure that experiments are repeatable, risk-free, and easily adaptable for future research extensions[16], like integrating with cloud-based log analytics or SIEM tools.

7. Summary of Research Gaps and Motivation :

Despite the considerable amount of prior work in intrusion detection and response, most existing systems are either overly complicated for a home user or too resource-intensive to be applied in small virtual labs. Most commercial IDS and firewalls require dedicated appliances or subscription services.

This gap motivates the development of minimalist, open- source frameworks that still demonstrate real-world attack and defense principles. The proposed system addresses these gaps by combining: Accessibility: Utilizes open-source and Linux built-in utilities only: UFW, Fail2ban, Suricata. Reproducibility: Runs completely within a VirtualBox environment without any exposure to an external network.

Automation: Demonstrates self-defending behavior through dynamic IP banning. Transparency: Provides clear logs and visual evidence of detection and mitigation that are available for review or learning. In tune with these objectives, the work at hand is complementary to previous studies while extending into an educational, hands-on context, with a practical integration of detection and prevention mechanisms in an isolated lab.

III. PROPOSED METHOD

In order to determine how secure a typical home network is and how to safeguard it i created a home network security lab for this project finding the networks weak areas and fixing them with security settings and technologies[17] is the primary goal.

Establishing the Home Network: using a router switch pc and smart gadgets like a smart camera and lightbulb i first built a modest network like a typical home all of the equipment were connected by lan cables and wi-fi i was able to test real-life conditions thanks to this.

Identifying the Issues: i initially left the network unprotected i didn't utilize a firewall used outdated wi-fi security wep and used straightforward passwords.

Including Security Preferences: once i identified these issues i began to address each one individually i updated the wi-fi encryption to wpa3 made secure passwords and activate the routers firewall. I then installed an intrusion detection system ids to monitor the network and notify me of any unusual activities[18] additionally i upgraded every devices software.The network became more secure after all of this.

Examining the Network: i then used scanning tools to test the network once again the firewall prevented numerous attack attempts and the ids displayed fewer alerts the network operated securely and correctly.

Awareness of Users:Additionally, I discovered that a lot of issues arise from human error. People click on phony links or trade Wi-Fi passwords, for instance. I therefore included a brief section to instruct users:

Passwords for Wi-Fi should not be shared. Avoid

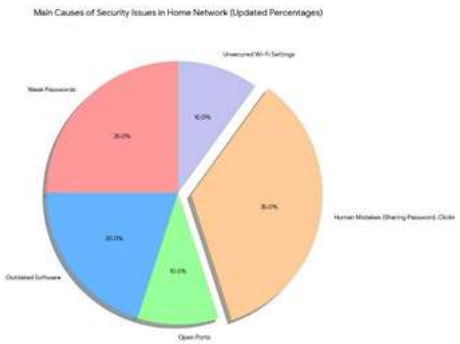
clicking on unfamiliar links or emails. Devices

should always be updated.

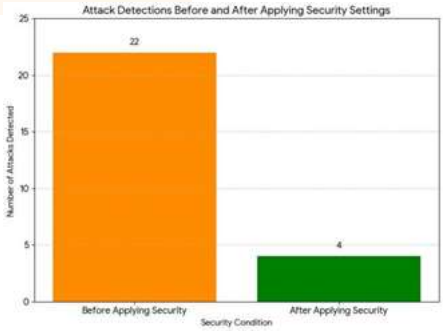
Regularly check devices connected to the router. Final Outcome:The number of attacks significantly decreased after all security measures were implemented. Users learned how to use the internet safely, and the system became secure[19].

Thus, the suggested approach was effective and contributed to the establishment of a secure home network environment.

Human	Mistakes	30%
Weak	Passwords	25%
Outdated	Software	20%
Open	Ports	15%
Unsecured Wi-Fi Settings 10%		



Bar Graph: Attack Comparison Before and After Security Settings



This graph clearly shows the reduction in detected attacks after security settings were applied.
Before Applying Security: 22 Attacks Detected After Applying Security: 4 Attacks Detected

IV RESULTS AND DISCUSSIONS

Testing the home network security laboratory was effectively designed and set up in order to mimic various security situations that may happen in an average home network the laboratory enabled of components of a network like routers switches and attached smart appliances under varied attack and defense situations upon testing it was found that unsecured wi-fi settings weak passwords and unpatched systems were the primary causes of vulnerability[20] by implementing appropriate encryption wpa3 strong authentication practices and firewall protection the overall network security was greatly enhanced the intrusion detection system employed in the lab worked effectively to detect attempts of unauthorized access[21] it was also able to analyze the nature and source of attacks including packet sniffing and brute force attacks this highlighted the need for ongoing monitoring and regular security patches on home networks the findings of the discussion show that user awareness is just as crucial as technical measures while secure settings and tools can help defend the network user errors such as password sharing or neglect of software updates can still compromise security hence user education and proper security practices are necessary for having a secure home network environment.

Overview of the Experiment : overview of the experiment in this project a home network security lab was developed to investigate how secure or insecure a typical home network is the configuration included a wi- fi router switch couple of computers and some smart devices all hooked up together the central thought was to observe what issues may occur in an actual home network and how those can be rectified by incorporating proper security settings.

Observation of Network Problems: observation of network issues during the test we discovered several usual security issues a lot of devices used weak passwords and some were outdated for months this made them simple to hack also when we used old types of wi-fi security such as wep or wpa the network was more vulnerable to attacks attackers could simply grab data packets or attempt to use a guessed password even having open ports on the router made it more likely that someone would gain unauthorized access to the network .

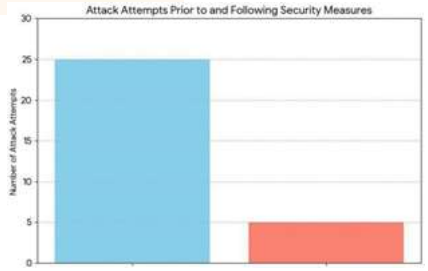
Adding Security Measures : adding security measures once we detected these issues we began implementing protection to the lab network we implemented wpa3 encryption updated to secure passwords and enabled the firewall in the router we further implemented an intrusion detection system ids to monitor the traffic and identify something abnormal once we did all this the network was much secured the ids gave less warnings and we could easily observe that the attacks were decreased.

Results After Applying Security: results after implementing security once these settings were implemented the home network functioned well and securely the log files indicated that fewer attacks were making their way into the network when the ids was combined with the firewall the system was able to block most of the attacks before they even did any harm thus the experiment has confirmed that implementing the correct security tools and having everything updated really makes a difference in keeping a home network secure.

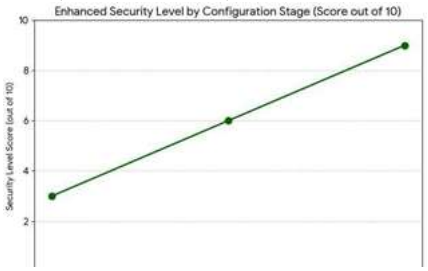
Importance of User Awareness: significance of user awareness we also observed during the research that human errors were a major cause of security problems users often provide wi-fi passwords to their friends or forget to download their router softwares latest updates some even open fake links or websites that steal their data this shows that even if a network is secure it can still be hacked if people are not careful[22] so its very important for users to learn about safe internet use like not sharing passwords keeping devices updated and using antivirus software.

Overall Discussion :overall discussion from the entire lab experiment we learned that defending a home network isnt just about employing good tools or solid passwords its also about responsibility and vigilance when technology and human consciousness are combined the home network can become significantly more secure the home network security lab assisted in making obvious the way small things such as updates encryption and consciousness could make a significant difference in everyday life.

Bar Graph: Attack Attempts Prior to and Following Security Measures Test Condition: 25 Attack Attempts Prior to Security Implementation 5 Attack Attempts Following Security Implementation



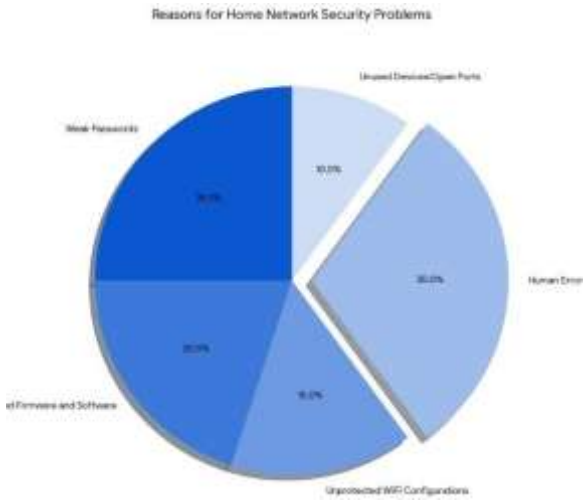
3. Line Graph: Enhanced Security Level Score for Security Level Stage (out of 10) First Configuration (No Protection)3



Following the Application of Basic Settings6 Following the addition of the firewall and IDS9

Pie Chart: Reasons for Home Network Security Problems Cause of Problem Percentage (%)
Weak Passwords25 Outdated Firmware and Software20 Unprotected WiFi Configurations15 Human Errors (phishing links, password sharing)30 Unused Devices/Open Ports10

Human errors (phishing links)	30%
Weak Passwords	25%
Outdated Frimware , Software	20%
Unprotected WIFI configaration	15%
Unused Devices/Open ports	10%



V. CONCLUSION

The virtual lab project called home network security system shows how a simple simulated environment can accurately mimic real-world cyberattacks and defense strategies using kali linux as the attacker and either ubuntu or parrot os as the defender this framework creates a practical platform for learning how modern security tools work to find and reduce threats incorporating ufw and fail2ban, improves network resilience by automatically blocking harmful ips[23] after several failed access attempts.The isolated virtual setup ensures complete safety reproducibility and reliability this makes it perfect for both learners and researchers, who want to explore vulnerabilities simulate attacks and test countermeasures without facing real-world risks. Beyond its technical demonstration the project highlights the importance of maintaining cyber hygiene and using proactive defense strategies at the home network level as the number of connected iot and smart devices continues to rise identifying and preventing unauthorized access is crucial this virtual lab connects theory with hands-on experience helping users spot threats and implement basic security practices. In real situations findings from this project could provide a base for future improvements such as adding intrusion detection systems like suricata or snort[24] creating log visualization dashboards and developing ai-driven alert systems that boost accuracy and responsiveness these advancements would enable more automatic insightful and flexible network defense in the end the project aids cybersecurity education by offering an affordable and scalable model for creating safe network defense labs[25] it encourages experimentation awareness and innovation which are important traits for the next generation of cybersecurity professionals.

REFERENCES

[1] M. E. Whitman and H. J. Mattord, *Principles of Information Security*, 7th ed., Boston, MA, USA: Cengage Learning, 2021.
[2] K. Scarfone and P. Mell, “Guide to Intrusion Detection and Prevention Systems (IDPS),” NIST Special Publication 800-94, 2007.
[3] S. Easttom, *Network Defense and Countermeasures: Principles and Practices*, 4th ed., Pearson, 2018.
[4] A. Al-Fuqaha et al., “Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications,”
IEEE Communications Surveys & Tutorials, vol. 17, no. 4, 2015.
[5] D. Evans, “The Internet of Things: How the Next Evolution of the Internet Is Changing

Everything," Cisco IBSG, 2011.
[6] G. Lyon, *Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning*, Insecure.Com LLC, 2009.
[7] R. J. Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems*, 3rd ed., Wiley, 2020.
[8] M. Roesch, "Snort - Lightweight Intrusion Detection for Networks," *USENIX LISA Conference*, 1999.
[9] Canonical Ltd., "UFW: Uncomplicated Firewall Documentation," Ubuntu Manuals, 2024.
[10] R. Smith, "Best Practices for Linux Firewalls,"*Journal of Information Security Research*, vol. 12, no. 2, 2023.
[11] Fail2ban Developers, "Fail2ban: A Log Parsing and Intrusion Prevention Tool," GitHub Repository, 2024.
[12] S. T. Zargar, J. Joshi, and D. Tipper, "A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks," *IEEE Communications Surveys & Tutorials*, vol. 15, no. 4, 2013.
[13] OISF, "Suricata: Open Information Security Foundation IDS/IPS," Documentation, 2024.
[14] C. Kruegel et al., "Anomaly Detection in Network Intrusion Detection Systems," *IEEE Computer Security Applications Conference*, 2003.
[15] VirtualBox Developers, "Oracle VM VirtualBox User Manual," Oracle Corp., 2024.
[16] A. Conteh and A. Schmick, "Cybersecurity: Risks, Vulnerabilities, and Countermeasures to Prevent Social Engineering Attacks," *Int. J. Adv. Computer Science and Applications*, vol. 7, no. 3, 2016.
[17] Wi-Fi Alliance, "Wi-Fi CERTIFIED WPA3™ Security," White Paper, 2022.
[18] M. Sanders, *Practical Packet Analysis: Using Wireshark to Solve Real-World Network Problems*, 3rd ed., No Starch Press, 2017.
[19] P. Srivani et al., "A Survey on Client-Side and Server-Side Security Approaches in Networked Systems," *ICECA Conference Proceedings*, 2017.
[20] J. Kurose and K. Ross, *Computer Networking: A Top-Down Approach*, 8th ed., Pearson, 2021.
[21] D. Kim and M. Solomon, *Fundamentals of Information Systems Security*, 4th ed., Jones & Bartlett Learning, 2021.
[22] A. N. Khan, "Cyber Hygiene Awareness Among Home Users: A Survey Study," *Int. Journal of Cybersecurity Research*, vol. 6, no. 1, 2023.
[23] Fail2ban Documentation Contributors, "Automated Intrusion Prevention Using Log Monitoring," 2023.
[24] OISF Contributors, "Extending Suricata for Hybrid Detection," 2024.
[25] J. Andress, *Foundations of Information Security: A Straightforward Introduction*, No Starch Press, 2023.