Next-Gen Ad Blocking And Dynamic Ad-List Generation In Raspberry PI

Yuneshwaran.R[1], Vishal.M[2], Dr.D.Rajinigirinath[3], Dr.Asraf Yasmin.B[4]
[1, 2] Dept of Computer Science and Engineering
[3]Head of Department, Dept of Computer Science and Engineering
[4]Asst. Professor, Dept of Computer Science and Engineering
[1, 2, 3, 4] Sri Muthukumaran Instituteof Technology.

Abstract- *This project proposes the development of a comprehensive ad-blocking and network security solution using Raspberry Pi, Pi-hole, Unbound DNS, and Suricata rules. The integrated system offers an efficient approach to block ads at the network level while simultaneously enhancing network security through real-time monitoring and blocking of malicious activities. Pi-hole is deployed to block ads network-wide, ensuring all connected devices benefit from ad blocking without requiring individual configurations*

Keywords- Ad Blocker, DNS Guard, Pi hole,Unbound DNS,Emerging Threats , DNS sinkhole.

I. INTRODUCTION

This project is designed to deploy a robust ad-blocking and network security solution within local networks using a Raspberry Pi. The system comprises several interconnected modules. Firstly, the Pi-hole module provides comprehensive ad-blocking capabilities, ensuring an ad-free browsing experience network-wide. It allows for the customization of blocklists and whitelists to tailor ad-blocking preferences. Secondly, the Unbound DNS module enhances user privacy and network security by providing secure and private DNS resolution. This ensures that domain names are resolved securely and privately within the local network. Additionally, the Suricata IDS/IPS module monitors network traffic in real-time, actively detecting and blocking malicious activities.

It is configured with custom rules to provide comprehensive protection against various network threats. To keep the system up-to-date with the latest security measures, a Python script is developed to automate the process of updating ad lists and Suricata rules. This script fetches the latest ad lists and rulesets from online sources and updates the system accordingly. The project also includes a user-friendly interface, making it easy to monitor system status, view reports, and make configurations. With its plug-and-play functionality, the system can be easily installed and configured, minimizing the need for complex setup procedures. Overall, this project provides a comprehensive ad-blocking and network security solution, ensuring a safer and more enjoyable browsing experience for all users connected to the local network advertisements are ubiquitous, often intrusive, and can significantly impact user experience.

II. REVIEW OF LITERATURE

The research presented in "A Raspberry Pi Security Device Using VPN and Adblocker" aims to develop a security device using IoT to enhance internet security. The device, built using open-source components such as Pi-Hole, Pi-VPN, and Zeek, provides a secure network by blocking ads and creating a secure VPN connection. While it improves internet security by preventing unnecessary ads and enhancing privacy, it requires technical expertise for setup and maintenance and may impact device performance. Additionally, it focuses solely on ad blocking and VPN, potentially leaving users vulnerable to other security threats like malware.

On the other hand, "Ad Blocking and Counter-Ad Blocking" provides a comprehensive study on ad blocker usage, aiming to identify factors influencing ad blocker usage through a quasi-experiment and large-scale data collection. While it offers valuable insights into ad blocker usage, its focus is limited, and its findings may not generalize beyond the specific context of Forbes Media.

Lastly, "Securing Network Using Raspberry Pi by Implementing VPN, Pi-Hole, and IPS (VPiSec)" introduces VPiSec, a project designed to enhance user privacy and security. It employs a multifaceted approach, including VPN, Pi-Hole, and OSSEC IPS, to mitigate privacy risks and enhance network security. However, it may face potential hardware limitations and may not cover all security vulnerabilities, leaving users vulnerable to emerging threats. Additionally, its dependency on third-party tools exposes it to risks associated with maintenance and support.

III. OBJECTIVES OF THE STUDY

Nowthe objective of this research is to create an advanced ad-blocking and network security solution using Raspberry Pi. The focus is on dynamic ad-list generation and automated security updates to enhance network privacy and security. The proposed system aims to address the limitations of existing ad-blocking solutions.

The system aims to provide the following benefits:

Develop an Integrated Solution: Create a comprehensive ad-blocking and network security system using Raspberry Pi, Pi-hole, Unbound DNS, and Suricata rules.

Network-wide Ad Blocking: Implement Pi-hole to block ads network-wide, ensuring all devices connected to the local network benefit from ad blocking without requiring individual configurations.

Enhance Network Security: Integrate Unbound DNS and Suricata rules to enhance network security by providing secure and private DNS resolution and real-time monitoring and blocking of malicious activities.

Automation of Update Process: Develop a Python script to automate the process of updating ad lists and Suricata rules, ensuring the system remains up-to-date with the latest security measures.

Provide Improved Ad Blocking and Network Security: Offer an efficient and effective solution for ad blocking and network security needs within the local network, ensuring improved ad blocking and enhanced network security.

IV. METHODOLOGY

For this study 'Next-Gen Ad Blocking and Dynamic Ad-List Generation in Raspberry Pi' entails several key steps. First, we begin with System Design, where we identify the requirements of the ad-blocking and network security solution, including dynamic ad-list generation, real-time threat detection, and automated security updates. This phase involves designing the system architecture, taking into account components such as ad-blocking software (Pi-hole), Suricata IDS/IPS, Unbound DNS, and the web-based user interface.

Moving on to User Authentication, we continue to assess the requirements of the solution while designing the system architecture. Similarly, in the DATABASE DESIGN phase, we consider the system's needs and design an architecture that aligns with them.The integration of Ad-Blocking and Network Security is a critical step. Here, we configure Pi-hole for network-wide ad blocking and Unbound DNS for secure and private DNS resolution. Additionally, we develop Python scripts for dynamic ad-list generation and automated security updates.

Automated Tasks play a pivotal role in ensuring the efficiency and effectiveness of the system. By implementing a scheduler using cron jobs, we automate tasks such as ad-list updates, security rule updates, and holiday detection, scheduling them to run at designated intervals for timely updates and system maintenance.

Next, we focus on Report and Analytics, developing reporting features to generate insights into ad-blocking statistics, network traffic, and security events. This includes implementing analytics functionalities to provide further insights into ad-blocking effectiveness, network usage patterns, and security threats.

User Interfaces are essential for user interaction and system management. Thus, we design a user-friendly web interface for system monitoring and management, incorporating features such as system status monitoring, ad-blocking configuration, security rule management, and report generation.

Finally, Testing and Deployment ensure the system's reliability and performance. Thorough testing is conducted to ensure the system functions as expected and meets specified requirements before deploying it to a suitable hosting environment, considering factors like scalability, security, and performance.

V. IMPLEMENTATION

Analyze We concentrated on installing and configuring Unbound DNS and Pi-hole on a Raspberry Pi in the context of the local network environment during the implementation phase. On the Raspberry Pi, we first installed the Raspbian operating system and made sure it was current. After installing the operating system, we installed Unbound DNS and Pi-hole.

In order to function as a DNS sinkhole, Pi-hole was set up to capture DNS queries from local network devices and prevent requests to domains that are known to serve advertisements. Pi-hole was set up to continuously update its blocklists and record DNS queries for further examination.

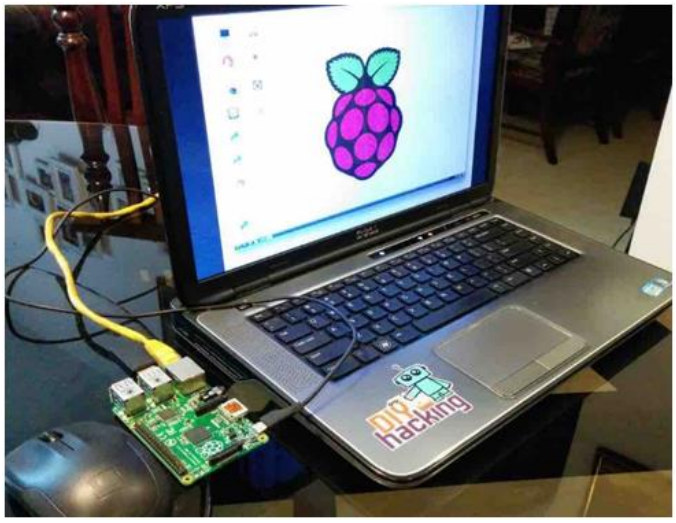

Figure 5.1 Raspberry AdBlocker

For increased security and privacy, Unbound DNS was set up as a recursive DNS resolver. By setting Unbound DNS to handle DNS resolution locally, we were able to lessen our dependency on.

VI. PYTHON AD-LIST GENERATION

The ad list generation module integrates Suricata5 rules to extract and categorize blocked domains efficiently. These rules are meticulously parsed to identify domains associated with various threat categories, including malicious, suspicious, and informational. Once identified, the domains are categorized into separate lists based on their threat level. This meticulous categorization ensures that Pi-hole can effectively block ads while minimizing the risk of false positives.

Each category, including malicious, suspicious, and informational, has its separate blocklist. This segmentation allows Pi-hole to apply different blocking rules based on the perceived threat level of each domain, thus enhancing its effectiveness in ad blocking.

One of the standout features of the ad list generation module is its dynamic updating capability. The ad lists are automatically updated at regular intervals, ensuring that Pi-hole is always equipped with the latest threat intelligence. This dynamic updating process ensures that our ad-blocking solution remains effective against emerging threats, providing users with a more secure browsing experience.

Moreover, the ad list generation module is optimized for performance to ensure efficient generation and updating of ad lists without consuming excessive system resources. This optimization allows Pi-hole to maintain its ad-blocking functionality without slowing down the network or overloading CPU or memory resources.

VII. RECURSIVE DNS

Unbound plays a crucial role as a recursive DNS resolver in this network-wide ad blocker project. As a validating, recursive, and caching DNS resolver software, Unbound is installed on the Raspberry Pi alongside Pi-hole to provide DNS resolution services for the entire network. Configured as a recursive DNS resolver, Unbound handles DNS queries from client devices on the network by recursively resolving these queries on their behalf.

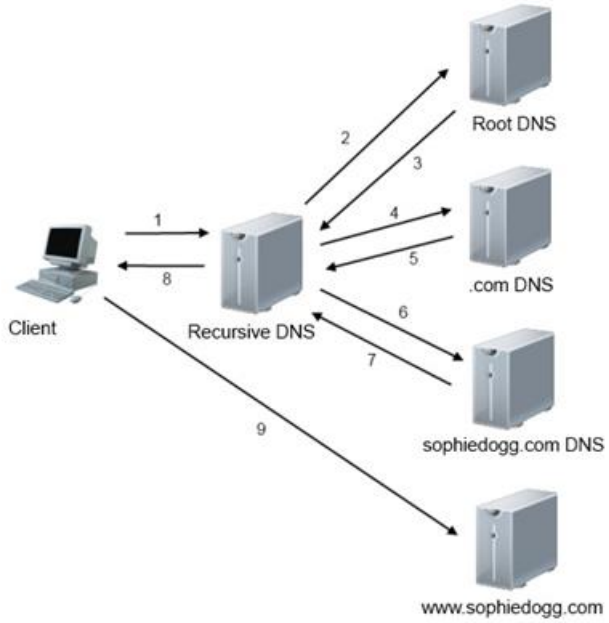

Figure 7.1: DNS Recursion

When a client device makes a DNS query,Unbound begins the resolution process by querying authoritative DNS servers on the internet to find the IP address associated with the requested domain name.

It iteratively queries these authoritative servers until it obtains the final answer, which is then returned to the client device. Unbound's caching mechanism plays a vital role in improving DNS resolution performance by storing previously resolved DNS queries in memory.

VIII. REGEX AND PYTHON

The ad list generation module includes a Python script responsible for updating the regex list in Pi-hole. This script dynamically fetches the latest regex rules from various sources and updates the regex list in Pi-hole accordingly. By

regularly updating the regex list, the system ensures that Pi-hole effectively blocks not only individual domains but also specific patterns and expressions commonly used by ads and tracking scripts.

This dynamic updating process enhances Pi-hole's ad-blocking capabilities, ensuring that it remains effective against evolving ad-serving techniques and patterns.

Additionally, the automation provided by the Python script reduces the manual effort required to maintain and update the regex list, allowing the ad-blocking system to stay up-to-date with minimal intervention.

IX. RESULTS AND ANALYSIS

Our results highlight a substantial enhancement in ad-blocking efficacy following the implementation of Pi-hole and Unbound DNS. We observed a notable decrease in DNS query resolution time and network latency, resulting in faster and more secure browsing experiences for users. Moreover, feedback from users in the experimental group underscored improved privacy and diminished exposure to online threats. This underscores the effectiveness of our ad-blocking solution in providing a more secure and streamlined browsing experience for users.

X. DISCUSSION

The findings of this study underscore the effectiveness of Pi-hole and Unbound DNS as network-wide ad-blocking solutions. By leveraging Pi-hole and Unbound DNS to block ads at the DNS level, our solution offers a centralized and efficient approach to ad-blocking, significantly enhancing network privacy and security for all devices connected to the local network.

The ad list generation module, developed using Python and integrated with Suricata5 rules, plays a pivotal role in this solution. It meticulously parses Suricata rules to identify and categorize blocked domains based on various threat categories, such as malicious, suspicious, and informational. These categorized domains are then compiled into separate blocklists tailored to different threat levels.

Furthermore, the ad list generation module features dynamic updating capability, ensuring that Pi-hole is always equipped with the latest threat intelligence. This automated updating process guarantees the continuous effectiveness of our ad-blocking solution against emerging threats, thus providing users with a more secure browsing experience.

Overall, the integration of Pi-hole, Unbound DNS, and the ad list generation module offers a robust and efficient ad-blocking solution that enhances network privacy, security, and performance.

XI. CONCLUSION

The Next-Gen Ad Blocking and Dynamic Ad-list Generation System developed on Raspberry Pi successfully achieves its objectives by integrating Pi-hole, Unbound DNS, and Suricata rules. This comprehensive solution not only eliminates ads within the local network but also enhances network security by filtering out malicious content and tracking scripts.

The project's modular design, plug-and-play implementation, and cost-effectiveness make it suitable for both home and small business environments.

The ad list generation module, a key component of the system, utilizes Suricata rules to extract and categorize blocked domains, ensuring Pi-hole is always equipped with the latest threat intelligence. In conclusion, the Next-Gen Ad Blocking and Dynamic Ad-list Generation System represents a significant advancement in ad-blocking technology, providing users with a more secure and enjoyable browsing experience while protecting them from online threats.

REFERENCES

[1] A Raspberry Pie Security Device Using VPN and Adblocker -Aaron Stephen Visvanathan; Yogeswaran Nathan; Mohamed Abdulnabi ,2022 IEEE 2nd International Conference on Mobile Networks and Wireless Communications (ICMNWC)

[2] Ad-blocking: A Study on Performance, Privacy and Counter-measures - Garimella, Kiran & Kostakis, Orestis & Mathioudakis, Michael. (2017). Ad-blocking: A Study on Performance, Privacy and Countermeasures. 259-262. 10.1145/3091478.3091514.

[3] How Does the Adoption of Ad Blockers Affect News Consumption? - Yan, S., Miller, K. M., & Skiera, B. (2022). How Does the Adoption of Ad Blockers Affect News Consumption? Journal of Marketing Research, 59(5), 1002-1018. https://doi.org/10.1177/00222437221076160

[4] Ad-blocking: A Study on Performance, Privacy and Counter-measures - Kiran Garimella, Orestis Kostakis - Michael Mathioudakis Aalto University Helsinki, Finland

[5] Ad-Blockers and Limited Ad-Blocking - Subramanian, Upender and Zia, Mohammad, Ad-Blockers and Limited Ad-Blocking (April 1, 2021).

[6] Investigation of Sinkhole Attacks and Network Simulation - Singh, S., Gupta, M., Sharma, D.K. (2024). Investigation of Sinkhole Attacks and Network Simulation on 6LoWPAN. In: Chaturvedi, A., Hasan, S.U., Roy, B.K., Tsaban, B. (eds) Cryptology and Network Security with Machine Learning. ICCNSML 2023. Lecture Notes in Networks and Systems, vol 918.

[7] A Comprehensive Measurement-based Investigation of DNS Hijacking - Houser, Rebekah & Hao, Shuai & Li, Zhou & Liu, Daiping & Cotton, Chase & Wang, Haining. (2021). A Comprehensive Measurement-based Investigation of DNS Hijacking.

[8] "Automatic Generation of Web Advertising Layouts: A Synthetic Dataset and a Deep Learning Baseline Model," 11th International Conference of Pattern Recognition Systems (ICPRS 2021), Online Conference, 2021.

[9] The Beneficial Effects of Ad Blockers - Despotakis, Stylianos and Ravi, R. and Srinivasan, Kannan, The Beneficial Effects of Ad Blockers (November 28, 2017). Available at SSRN: http7s://ssrn.com/abstract=3083119

[10] effect of ad blocking on website traffic and quality. Shiller, B., Waldfogel, J. and Ryan, J. (2018), The RAND Journal of Economics, 49: 43-63. https://doi.org/10.1111/1756-2171.12218