JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

A Unified DNS Sinkhole, Intrusion Prevention System (IPS), Firewall, and Secure File Sharing with Centralized Log Correlation and Administration

Manoj Prakash J
Department of Computer Science and Information Technology
Jain (Deemed-to-be University)
Bengaluru, India

Abstract: every gadget or devices on the world is now connected to the Internet, allowing humans to communicate more effectively. Regardless, this technique exposes the consumer to a security risk. Users are oblivious to the fact that there all information and data which travel through the wire or signals are can be intercept or even the internet service provider keeping them as a logs and other corporations may have access to the user information. Not only that they keep track of every site the user visit and every search term they enter are being captured by a firm that uses the user interests to provide ads and pop up according to that interest. Which becomes a problem when a firm acquires data and utilizes unethically. As a result, a device that can safeguard the user is required. This idea proposes a gadget that may mask the user identity by masking the Internet Protocol (IP) also shield from trackers and advertisements. Hide the user's IP address by disguising it using WireGuard VPN Protocol a server located in another country, so safeguarding the user from being monitored by an attacker. Furthermore, the Pi-Hole initiative of the online community is used to refuse any DNS request for a known malicious, tracking and advertising domain. Furthermore, the incorporation of Suricata (Intrusion Detection System) within the machine which effectively detect the attack by brute force from within the network or any other malicious attempt to take control of raspberry pi, offering further security. A raspberry pi file sharing setup using samba protocol allows for the centralized storage of files and data, making it simple for multiple users and devices to access and share the same files and with other users and devices on a network, without the need for complicated setup or configuration. It is also cost-effective, especially when compared to other storage solutions such as a dedicated server and lastly with a Centralized Log Correlation and Administration to easily monitor and control all this features and network logs.

Index Terms **- Raspberry Pi, WireGuard, Suricita, Samba, Pi-hole, Log Correlation and Administration**

I. INTRODUCTION

It is known that more than 63.3% of individuals actively engage in online activity. This figure indicates that many people are connected together and also interact with each other via internet, and make profit or income via the internet, exposing potential of information theft and exploitation. One method for dealing with these vulnerability concerns is to use a tunneling it can be done using a Virtual Private Network (VPN). Network refers “two or more devices that can interact regardless of whether they are connected through wired or wireless means, as long as they can communicate and share data”. Also “Things that people used to perform by hand are now readily done by computer and can be remotely controlled utilizing the network”. This has revolutionized the way people live. Every network-connected device has security threats which should be dealt with a security measure to prevent it. These might be insider threat or an illegal data or system permission which can be an attack like Denial of service or Man in the middle attacks or a malware. Few strategies may be utilized to avoid all of these cyberattacks, such as evaluating the sorts of attacks and implementing security technologies. There are several techniques to defend the network environment, including the usage of humans, hardware, and software. Learning a few technologies and its usage may help the user to eliminate the threat. After gaining a basis knowledge about network then is to utilize the software and hardware such as firewalls and intrusion detection systems and many more. Pi-Hole is used in this project to prevent adverts from being displayed on the end device also to prevent known malicious and tracking. Pi-Hole functions like a DNS black hole preventing requests containing advertising from the internet, as opposed to adware block extension or tools in browser, which can only conceal adverts. This project also includes a Suricita IDS which can also tuned into IPS for further security which is an open source application. Firewalls function as "intrusion prevention systems", but IPS are oriented on attack prevention on levels that most firewalls cannot yet decode. The purpose of this project is to construct a network utility that can defend the entire ecosystem from DDOS, MITM attacks, malware, and any possible suspects using Raspberry Pi technology. The updated with new system is then analyzed by examining its speed performance, numerous suspicious packets, and potentially harmful advertisements.

This initiative is made up of people who wish to protect their privacy and electronic devices. This paper offers a novel approach for building a VPN tunnel on Pi-Machine that can protect the end-to-end communication and connection between the devices to prevent hacker from intercepting the information and a detailed guide how to protect the network from adware and utilizing the Samba protocol enables centralized file storage, facilitating easy access and sharing across multiple users and devices on a network. This solution is straightforward to implement and doesn't require complex configuration. Additionally, it offers a cost-effective alternative to dedicated servers. Implementing a Centralized Log Correlation and Administration further enhances monitoring and control over network logs and features with a dedicated open source mobile application for any intrusion alert.

This has a lot of features and plugins that can be set and assist a lot with this project. The following is how the rest of this paper is organized: Section 2 discusses the literature review. Section 3 describes the methodology, which is followed by Section 4's testing and analysis. Finally, Section 5 contains final observations.

II. LITERATURE REVIEW

Some relevant studies and terminology are offered here to highlight the significance of including many aspects within the suggested tool.

A. Virtual Private Network

When it comes to network security, the most important factor is privacy. A VPN's objective is to give security and anonymity when communicating over the internet VPN builds a channel from a device that is connected to the web via a VPN service and encodes all information that passes through it to prevent data leakage and sniffing by unauthorized parties. Open-source VPN is an excellent VPN solution since it can be adjusted to the user's preferences andis maintained by the community. Pi-VPN is a software that makes it easier to configure a VPN (Virtual Private Network)on a Raspberry Pi. It may be used to establish a secure internet connection to a network, letting users to accessnetwork resources remotely and securely. The software runs on a Raspberry Pi running Raspbian OS and supports a variety of protocols, including OpenVPN and WireGuard. Wireguard is a cross- platform software that allows users to setup and use it on a variety of operating systems (OS) [1]. This is in contrast to any other VPN service, which always creates a VPN that is only available for limited operating system. But Wireguard supports Most of the operating system namely windows and Linux, making it versatile also completely adaptable. This project employs Pi-VPN along with Wireguard protocol since it is extensively used by the VPN community and gives many features and plugins to setup, which greatly aids in the completion of this project.

B. Intrusion Prevention System

Network intrusion prevention systems (IPS) were developedin response to the evolving threat environment to provide extra protection. That beyond capacities of intrusion detection. An intrusion prevention system, as opposed to anintrusion detection system, monitors network behavior throughout the network to avoid unwanted activities such as Malware attack , Brute force attack , Denial of services , Man In the Middle attack or any kind of dangerous attack that can cause harm will be prevented and captured as a log by the IPS [2].

C. Samba

Network Attached Storage aka NAS device enables for network-based file storage and sharing. A Raspberry Pi was used in this project to build a low-cost and low-power NAS device but with use samba protocol and web interface and connecting it to a Hard Disk or Solid State Disk or even Pen drive. Once configured, the Raspberry Pi may be used by other network devices to exchange and view files using a dedicated user credentials.

D. DNS sinkhole using Pi-Hole

Pi-hole which they describe "a sinkhole for ads" Most ad blockers need installation on individual devices, whereas thePi-hole prevents adverts over an entire LAN. Pi-hole used on network-capable devices such as the Raspberry Pi. Ad block and Pi-hole use distinct approaches to ad blocking. Ad blockers restrict webpages from showing adverts inside the browser. The advertisements continue to be retrieved and presented, but they are concealed by Ad block. While on theother hand Pi-hole does not permit the DNS query for the advertisements to enter the network, implying that the advertisements are not even downloaded to the user's network.

E. Raspberry Pi

The Raspberry Pi is a single-board computer that was created in the United Kingdom by the Raspberry Pi Foundation. Its primary function is educational, but it has also gained popularity as a low-cost, low-power device for hobbyists, manufacturers, and embedded systems. The Raspberry Pi comes in a variety of variants with varying processing power, memory, and peripheral choices. It may be used for a variety of projects, like establishing a media center, a home automation system, setting up a VPN, and making a vintage gaming arcade, among others. It operates on a number of operating systems, the most common of which being Raspbian, a Linux variant [3].

Securing networks with Raspberry Pi is a popular topic that many academics are discussing and developing. One idea advocated employing a Pi device in home network to provide VPN the link between the local network as well as the public network. Their primary VPN connection is Wireguard integrated with Pi-VPN that is then configured onthe Raspberry Pi.

III. METHODOLOGY

A. Design Phase

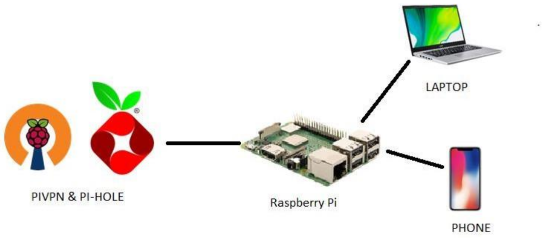


Figure 1: prototype model

The designing step includes the use of a pictorial model for the initial problem state and the remedy to the scenario. Following that, an example diagram was created to depict the system architectural design. Figure 1 depicts a graphical scenario for protecting a network connection using a Raspberry Pi. The Raspberry Pi was required to connect to the PI-VPN in this configuration. Along with the PI-VPN, a Pi-hole was inserted. The user devices needed to be setup so that the devices default gateway could be transmitted to the Raspberry Pi. The system secured all data that passed via the VPN since the Raspberry Pi used IPS to prevent any suspicious packets. All traffic entering the user's computer will be screened to look for known threats or bothersome web adverts. All traffic entering the user's computer will be screened to look for known threats or bothersome web adverts. The user will feel safe and will be able to surf the internet without fear of data leakage or assault.

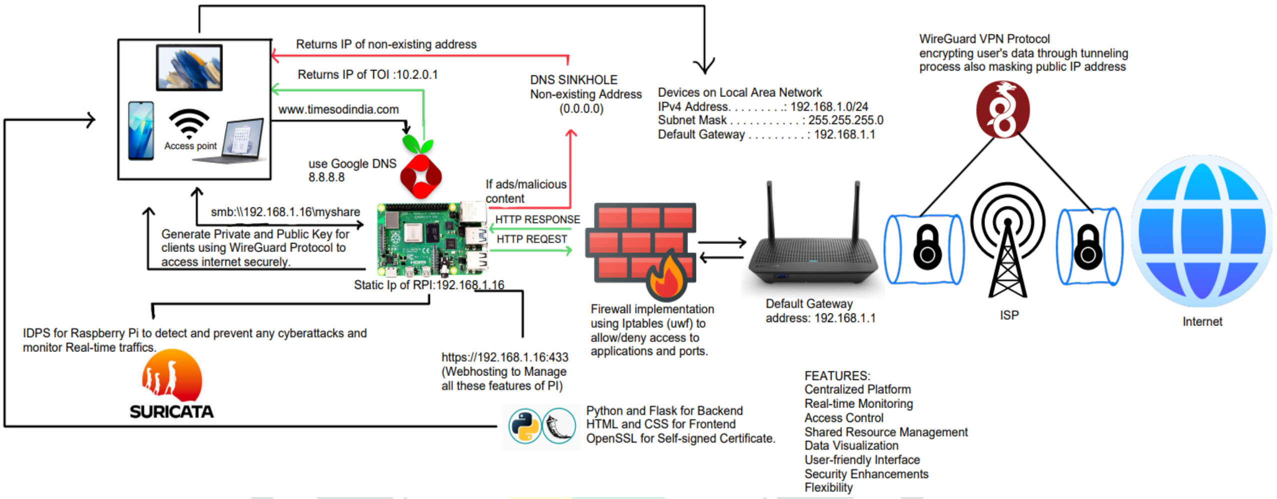

Returns IP of non-existing address
Returns IP of TOI :10.2.0.1
www.timesodindia.com
Access point
DNS SINKHOLE
Non-existing Address
(0.0.0.0)
Devices on Local Area Network
IPv4 Address. . . . .: 192.168.1.0/24
Subnet Mask . . . . : 255.255.255.0
Default Gateway . . . . : 192.168.1.1
WireGuard VPN Protocol
encrypting user's data through tunneling
process also masking public IP address
use Google DNS
8.8.8.8
If ads/malicious
content
smb:\\192.168.1.16\myshare
HTTP RESPONSE
HTTP REQEST
Generate Private and Public Key for
clients using WireGuard Protocol to
access internet securely.
Static Ip of RPI:192.168.1.16
Firewall implementation
using Iptables (uwf) to
allow/deny access to
applications and ports.
Default Gateway
address: 192.168.1.1
ISP
Internet
IDPS for Raspberry Pi to detect and prevent any cyberattacks and
monitor Real-time traffics.
SURICATA
https://192.168.1.16:433
(Webhosting to Manage
all these features of PI)
Python and Flask for Backend
HTML and CSS for Frontend
OpenSSL for Self-signed Certificate.
FEATURES:
Centralized Platform
Real-time Monitoring
Access Control
Shared Resource Management
Data Visualization
User-friendly Interface
Security Enhancements
Flexibility

Figure 2: full system design

An architectural system is an intellectual model that encapsulates the construction, operation, and other aspects of a technology. It is a basic term and visualization of a system that is designed in such a manner that understanding about the state's architecture and functions is possible. A system architecture may comprise entire system, enlarged subsystems, system connections, and other modules that could collaborate to complete the full system. The overall concept of the projected system architecture is depicted in Figure 2. Raspbian was installed as the operating system on the Raspberry Pi. After the OS installation was completed, remote connection options were enabled to let users manage the Raspbian Machine and build a “bridge connection” from the public Network and the local device connected through wire or Wi-Fi. The Pi Machine was configured with suricita and linked with VPN and Pi-hole also created a secure localhost with self-signed SSL certificate to manage all this in web interface made with flask. It was used to log and monitor all traffic before blocking it. To guarantee that the user's data was secure and encrypted, our project employed PI-VPN as a wireguard VPN connection. The next step is to utilize Pi-Hole in conjunction with PI- VPN to restrict any search quires that made relating to adware containing web or any unsecure website by blocking the DNS request, ensuring no reader or user media consumption are get interrupted by any unwanted pop ups or adware and establishing clean and peaceful surfing environment. The Pi machine then boot up Debain based Linux system for embedded board that is Raspberry Pi. After all of the necessary setting for remote connection has been completed, the Raspberry Pi may be linked remotely using Putty. After installation Intrusion Prevention system and configured on the Raspberry Pi to activate protection service and aggressive reaction for preventing form unusual activities, letting it to remotely disable potentially malicious transmissions. Finally, a Web interface which is made with flask in python is installed, which provides a web-based interface for controlling all the features along with mobile notification using ntfy for any customized alert to user, including file sharing configuration, user and permission setup, and storage management. It also has built-in support for additional features like remote access, backups, and monitoring.

B. Setup phase

a) Wireguard installed through Pi-VPN then it is configure to use specially made DNS using the Pi- Hole DNS. The Pi-hole IP has been added to the wireguard server config file as the Name server, while the other standard DNS server has been disabled by putting a comment to the config file. The Pi-hole installed before using simple bash script file with that a simple guide default is done.

b) Setting up samba protocol for file sharing on a Raspberry Pi is a relatively straightforward process just have to run a script and modify the config file according to the network. A web interface using Flask is created where user should enter the IP of Pi Machine in any web browser. The default login is "admin" for the username and "admin" for the password. Next, go to the "Services" page and activate any other services you want to utilize.

c) Installation of suricita there are many script available to install Suricita automatically but in this project we will installing few base files first that are “php php-cli php-common libapache2- mod-php apache2-utils sendmail inotify-tools apache2 build-essential gcc make wget tar zlib1g-dev libpcre2-dev libpcre3-dev unzip libz-dev libssl-dev libpcre2-dev libevent- dev build-essential“ for Suricita then we have to install agent for the machine we need either IDS/IPS and install raspberry Pi as a server to prevent attacks and monitor logs The Raspberry Pi was then configured with Ipsec so that it could link to the VPN connection that had already been established. A start query is entered for each module after they have all been properly configured in order to start them collectively. Also, check that you have a proper power supply and a good HDD/SSD, as those factors will affect the performance and stability of your file sharing setup.

d) The Pi-VPN create a data that was produced when a new user was formed in new device. The WireGuard client, Wireguard application, was installed on the user's devices. The user can use QR code or enter the details manually given by the server the client application or even import from the file was subsequently sent to it for connection. The user then connects to the VPN tunnel with the file provided by the details given at the time new user created, to set login credentials. The Pi Machine also linked ensuring all communications passing through it are encrypted and safe. [4]. Following the configuration of the Raspberry Pi's IP address as the machines or even any device's gateway, every traffic transferred out from device to the web are tunneled thru the VPN and protected by the IPS, as well as suricita and firewall may inspect and prohibit any unusual transmissions that travel through all the networks. Any network transmission is encoded, letting users to connect to the web without risk of their information leaking or malware attack. Lastly implementing the samba setup in the machine by Configuring the system by setting up the basic settings for your system,such as hostname and time zone, configuring storage devices, and enabling additional services. Then Setting up user access like creating users and groups, and setting up permissions and access rights to the shares also creating and configuring shares setting up permissions and access rights, and configuring for better performance. Finally monitoring andmaintaining the system logs, updating the system, and troubleshooting any issues that may arise.

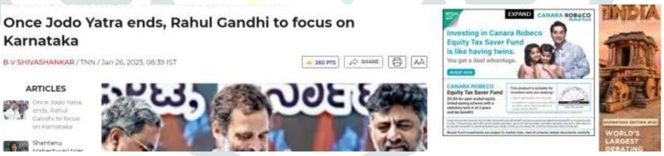
IV. TESTING AND ANALYSIS

This part tests three (4) major features. The first test is putting the Pi-hole function to the test, which blocks any searches that match pi-hole adware Database with the tracker Database input that the user's device has been programmed to use while browsing the internet. The second is the user's anonymity in internet, and whether or not the information which travel through the internet can be captured in between by doing man in the middle attack. The third test is DNS leak test for any DNS leak occur while using VPN. The final test in assessing the IPS installed within the machine. The brute force assaults carried out on target machine to determine the Intrusion Prevention System is operational or not.

A. *Pi-hole Testing for Ads Blocking*

The experiment was carried out on the website timesofindia.indiatimes.com, which publishes the latest newson sports, business, entertainment, blogs, and opinions from top columnists. The website was picked because it has several unpleasant advertising which interrupt the readerfrom reading the content they want to read.

Figure 3 depicts a webpage article that has multiple adverts. If you see the right side of the figure 3 there is advisement on mutual funds and federal bank.



Once Jodo Yatra ends, Rahul Gandhi to focus on Karnataka

B V SHIVASHANKAR / TNN / Jan 26, 2023, 08:39 IST

ARTICLES

Once Jodo Yatra ends, Rahul Gandhi to focus on Karnataka

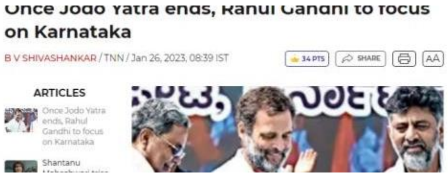
Investing in Canara Robeco Equity Tax Saver Fund is like having twins.

You get a dual advantage.

CANARA ROBECO Equity Tax Saver Fund

Figure 3: An article on that contain ads in TOI

As seen in Figure 3, the site shows so many advertising that the viewer becomes irritated while reading the text. Figure 4 demonstrates the outcome of implementing Pi-hole, which indicates that the identical item in the webpage is disappeared no ads or any pop ups.



Once Jodo Yatra ends, Rahul Gandhi to focus on Karnataka

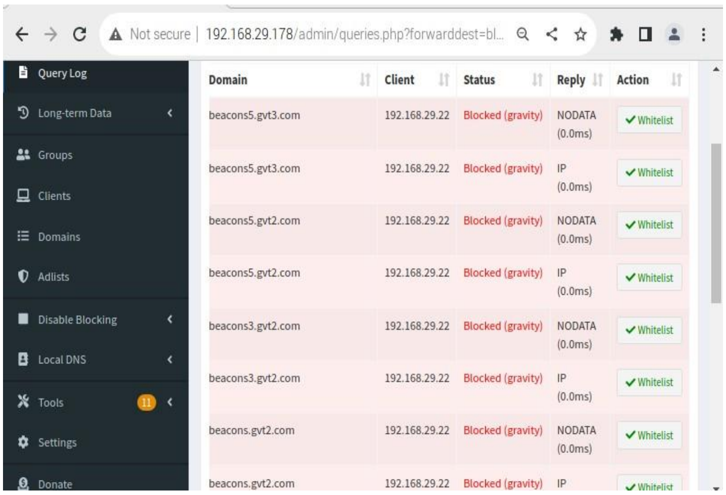
B V SHIVASHANKAR / TNN / Jan 26, 2023, 08:39 IST

ARTICLES

Once Jodo Yatra ends, Rahul Gandhi to focus on Karnataka

Figure 3: An article on that does not contain ads after pi-hole implementation IN TOI

Furthermore, site now loading speed is increased than when Pi-hole is not installed. Figure 4 shows the output of the Pi- hole GUI, which demonstrates advertisement blocking. Thatsuggests Pi-hole was successful in blocking the TOI advertising enquiry. Thus, Pi-hole demonstrated its capacity to block advertisements on a website.

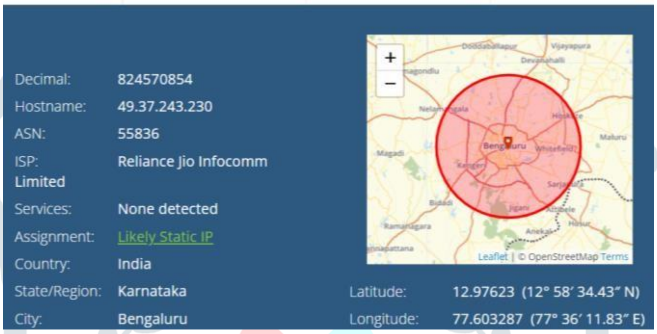


Domain	Client	Status	Reply	Action
beacons5.gvt3.com	192.168.29.22	Blocked (gravity)	NODATA (0.0ms)	✓ Whitelist
beacons5.gvt3.com	192.168.29.22	Blocked (gravity)	IP (0.0ms)	✓ Whitelist
beacons5.gvt2.com	192.168.29.22	Blocked (gravity)	NODATA (0.0ms)	✓ Whitelist
beacons5.gvt2.com	192.168.29.22	Blocked (gravity)	IP (0.0ms)	✓ Whitelist
beacons3.gvt2.com	192.168.29.22	Blocked (gravity)	NODATA (0.0ms)	✓ Whitelist
beacons3.gvt2.com	192.168.29.22	Blocked (gravity)	IP (0.0ms)	✓ Whitelist
beacons.gvt2.com	192.168.29.22	Blocked (gravity)	NODATA (0.0ms)	✓ Whitelist
beacons.gvt2.com	192.168.29.22	Blocked (gravity)	IP	✓ Whitelist

Figure 4: The Pi-hole GUI output

B. *VPN Anonymity and DNS Leak Test*

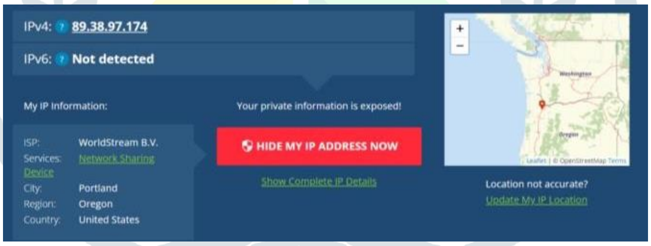
The programme is used using an existing internet connection without the use of a VPN for the first portion of this testing. Figure 5 depicts the testing results, which revealthat the user's IP address location is disclosed. The attacker can leverage this vulnerability to track the user's current position.



Decimal: 824570854
Hostname: 49.37.243.230
ASN: 55836
ISP: Reliance Jio Infocomm Limited
Services: None detected
Assignment: Likely Static IP
Country: India
State/Region: Karnataka
City: Bengaluru
Latitude: 12.97623 (12° 58′ 34.43″ N)
Longitude: 77.603287 (77° 36′ 11.83″ E)

Figure 5: Internet Protocol, ISP, ASN and live Location LT in the absence of Pi-VPN

The next step to use the tool after connecting to the VPN. Asseen in Figure 6, the network's ISP has been switched from Reliance Jio infocomm to Digital unknown. Furthermore, theIP address has been substituted with the VPN server's IP address. The IP address is revealed, according to the tool display, however it is the IP address provided by VPN server.



IPv4: 89.38.97.174
IPv6: Not detected

My IP Information:

ISP: WorldStream B.V.
Services: Network Sharing Device
City: Portland
Region: Oregon
Country: United States

Your private information is exposed!

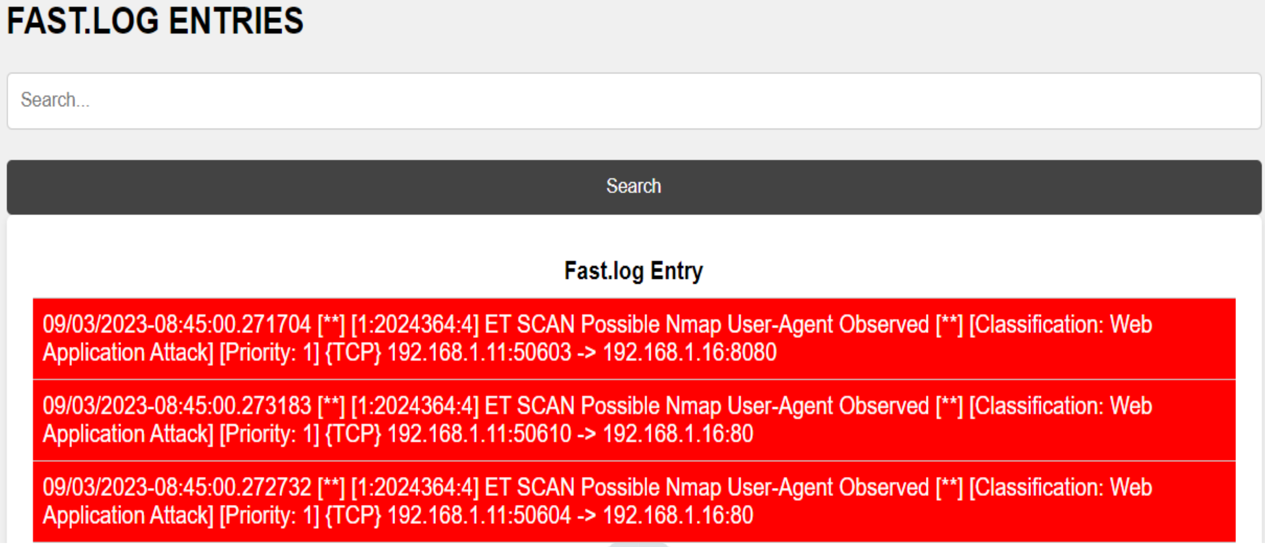
Figure 6: IP and Location LT with Pi-VPN

C. *DNS test*

This DNS-LT was also performed on a device that is not connected to a PI-VPN at the start of the testing later connected and tested again. The outcome of the DNS leak test, which displays the DNS queries that wererevealed. That means that the ISP may have access to all DNS queries performed by the user when accessing theinternet. ISPs may monitor consumers' surfing habits as wellas all sensitive data supplied and received. Furthermore, if a MITM attack is launched against the Internet Service provider & Domain Name System server, the hacker can obtain sensitive data from the users. The test was then repeated when the network was connectedto the VPN. The Domain Name system provider moved from the original Internet service provider to WorldStream B.V, and the Internet protocol addresses of four DNS providers have been disclosed. According to the tool, the DNS is exposed because it is unaware that network is already been established and linked to PI-VPN to inhibit DNS response being monitored alsoseized by ISPs. The DNS-LT performed on a device that was not connected to a Pi-VPN at the start of the test. The outcome of the DNS-LT, this test shows the DNS queries that were revealed. That means that the ISP may have accessto all DNS queries performed by the user when accessing the internet. ISPs may monitor consumers' surfing habits as well as all sensitive data supplied and received. Furthermore, if an MITM attack is launched against - ISP's DNS server, the attacker may obtain sensitive data from the users.

D. IPS test

This IPS testing is carried out using Parrot Sec, a basis Nmap scan to obtain target machine information. Without the using IPS/IDS, the attack was effective, and the hacker able to find the all the information such as hostname, services running.



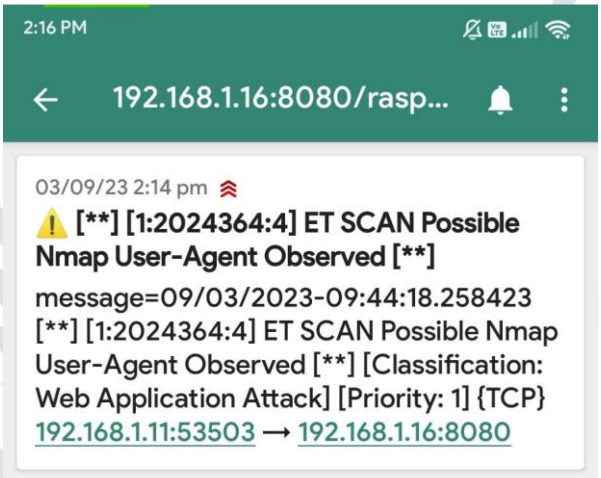
FAST.LOG ENTRIES

Fast.log Entry

```
09/03/2023-08:45:00.271704 [**] [1:2024364:4] ET SCAN Possible Nmap User-Agent Observed [**] [Classification: Web Application Attack] [Priority: 1] {TCP} 192.168.1.11:50603 -> 192.168.1.16:8080
09/03/2023-08:45:00.273183 [**] [1:2024364:4] ET SCAN Possible Nmap User-Agent Observed [**] [Classification: Web Application Attack] [Priority: 1] {TCP} 192.168.1.11:50610 -> 192.168.1.16:80
09/03/2023-08:45:00.272732 [**] [1:2024364:4] ET SCAN Possible Nmap User-Agent Observed [**] [Classification: Web Application Attack] [Priority: 1] {TCP} 192.168.1.11:50604 -> 192.168.1.16:80
```

Figure 8: Log entry in Web-interface for user to analyze and take action

The attack, on the other hand, was unsuccessful because the IPS was on alert. IPS is continually blocking any suspicious traffic and also actively logging every activities on the Raspberry Pi. An attacker running a basic port scanning on the target IP to acquire information. Figure 8 depicts the activities recorded by the IPS in Web Interface and Figure 9 is mobile notification of the alert through ntfy.



03/09/23 2:14 pm

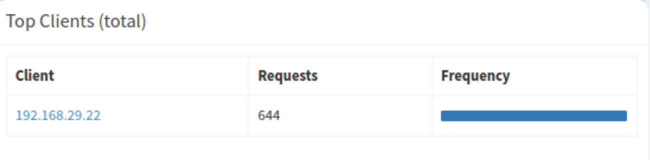
⚠ [**] [1:2024364:4] ET SCAN Possible Nmap User-Agent Observed [**]

message=09/03/2023-09:44:18.258423 [**] [1:2024364:4] ET SCAN Possible Nmap User-Agent Observed [**] [Classification: Web Application Attack] [Priority: 1] {TCP} 192.168.1.11:53503 → 192.168.1.16:8080

Figure 9: Mobile Notification of the event using ntfy.sh to alert the user

IV. RESULTS AND DISCUSSION

Based on the tests and results, it can be concluded that the project's output allows to access the Internet without any advertisements since they are stopped by implementing Pi-hole with predefined list of 517,614 as you could see figure 11.

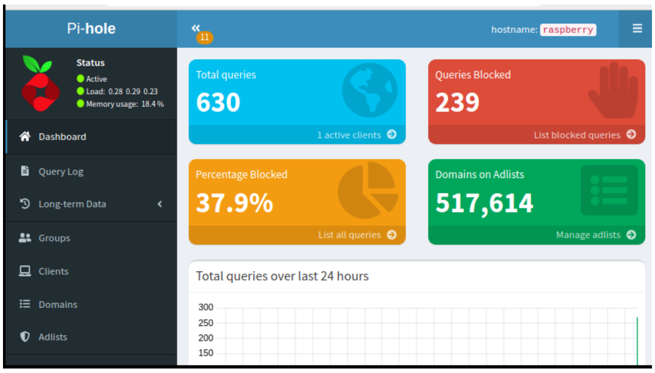


Top Clients (total)

Client	Requests	Frequency
192.168.29.22	644	▬

Figure 10: Number of client used pi-hole during the test

Figure 10 depicts the number of requests made by user andwith user IP address and the request frequency. Figure 11 depicts the number of queries made by webpage during theinternet surfing by the user and the number of adware and pop-ups banned by DNS sinkhole in an hour.



Total queries 630 — 1 active clients

Queries Blocked 239 — List blocked queries

Percentage Blocked 37.9% — List all queries

Domains on Adlists 517,614 — Manage adlists

Total queries over last 24 hours

Figure 11: Pi-hole GUI

Figure 11 is a clip from the Pi-hole GUI that displays the number of searches for the advertising intercepted and banned by Pi-hole during an hour of Internet surfing by a single user. During the surfing hour, a total of 630 inquiries were performed by unique users, and 239 searches were banned. This indicates that around 37.9% of all searches contain advertising and have been answered. The Pi-hole successfully blocked the path. Figure 12 depicts a graph of blocked requests during the previous 24 hours. The time graph depicted is the outcome of one day of Internet browsing by the user. This demonstrates that the Pi-hole feature is completely capable of blocking ads on the network. The green line indicate the total queries searchedby a user and blue line in the graph indicate the total queries blocked by the Pi-Hole.

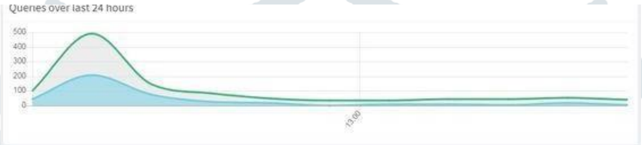


Figure 12: graph of blocked requests during the previous 24hours

Furthermore, IPS may both block and log all anomalous network activity. It also offers an alert rate. Level three alerts, for example, correspond to any successfulor allowed occurrences such as successful login attempts, but level six alerts refer to danger. Figure 13 depicts a graphof warnings during the previous 60 minutes of network activity. It shows that the IPS is monitoring and logging the brute-force attack that was tested during the IPS test and analysis to identify the performance of IPS in Raspberry PI and also the Nmap scan performed by the attacker during this period.

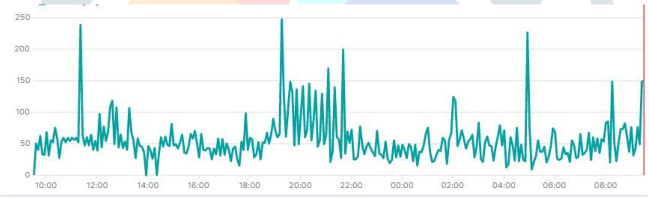


Figure 13: graph of IPS logs during port scanningand brute-force attack

Trial	Before IPS, VPN & Pi-hole			After IPS, VPN & Pi-hole		
	Ping(ms)	*Download(Mbps)*	*Upload(Mbps)*	*Ping(ms)*	*Download(Mbps)*	*Upload(Mbps)*
1	20	48.77	27.53	28	29.42	26.82
2	21	49.23	25.20	26	30.40	29.40
3	23	40.61	28.11	29	22.30	23.71
4	20	49.52	20.15	31	21.06	38.95
5	24	38.12	25.14	27	28.98	26.74
6	27	31.95	26.55	26	31.05	35.53

TABLE 1

A network performance test was also performed to assess theimpact of implementing the project, which includes VPN, DNS Sinkhole, and IPS into the Raspberry Pi Device. The test was conducted to see the performance which consist of ping test and downloading the uploading speed of user after using the data and internet through the Raspberry Pi. This testing measures ping, download, and upload speeds before and after utilizing all of the features because these are the usual statistics that users worry about in order to be satisfiedwith this project. The results of the tests are shown in Table I. The outcome of the bandwidth utilization after using the project was a minor drop in terms of download speed. However, the upload speed increased somewhat afterutilizing the project compared to before using it in the previous 6 trials. These results demonstrated that the project may have a minor impact on customers' experience when downloading web content, but it provides them with a faster upload speed. Meanwhile, the ping findings revealed thatthe project lengthens the time it takes to request and respondto messages.

P-value		
Ping	Download	Upload
0.0250	0.0097	0.2172

TABLE 2

Nonetheless, a paired T-test was performed to see if there is a substantial difference before and after the project wasimplemented. The computed p-value in Table 2 was more than, indicating that there is no significant change in downloading and uploading speeds before and after executing this project. However, it provides a comparable p-value for ping activity. It confirms that this initiative had a minor effect on ping. This may have an impact on users' experiences, particularly in gaming. A ping rate of 20 to 100 ms, on the other hand, may allow you to enjoy the gaming but may not provide optimal performance in online gaming where timing is essential.

V. Conclusion

The project's setup is easy since it is intended for even inexperienced users to secure their network easily by doing few steps installation to safeguard their network. After setting up and installation process the user need to changehis default gateway in his/her device for an internet connection that passes through the Raspberry PI, which functions as a middleman for Internet access. This was used to tests the functions of the VPN, Pi-hole, and Suricita IPS and samba. The VPN test revealed that the user's IP address and location were masked, indicating that it is operational. Furthermore, the Pi-hole test revealed that ads had successfully banned programs as well as websites. If an advertisement service creates a new site tracker query, the user must update the blacklist to ensure that Pi-hole can continue to block adverts. The IPS deployed within the computer then displayed logs on abnormal actions within the machine. It effectively prevented intrusion attempts while only protecting users on the same network asthe computer. It will not monitor or prohibit any actions occurring outside of the network. Only by using the Raspberry Pi as the default gateway will the network environment be safe. This Raspberry Pi project proposes a method that would automatically update DNS sink-hole database. Modifies the settings for the Internet Protocol table to redirect all traffic that enters the Raspberry Pi.

References

[1] S. Taylor, “VPN Ad Blocker – The Best and the Worst,” RestorePrivacy, 20-Sep-2019.

[2] S. Wilkins, Basic Intrusion Prevention System (IPS) Concept andConfiguration, Cisco Press, 29-Jun-2011.

[3] W. Gary (2014). Raspberry PI Hardware Reference. Technology in Action.

[4] Dr.Sathish Kumar P.J., Surya K.R., “Raspberry Pi Turns into VPN &NAS server”, 2021 Volume25.