Enhancing Network Security with Raspberry PI 4: Leveraging Pi-Hole and Wireshark

Joshua Waithe & Nia Newell, Undergraduate Students
Vaughn College of Aeronautics and Technology, USA, Joshua.Waithe@vaughn.edu, Nia.Newell@vaughn.edu
Mentor: Aparicio Carranza, PhD
Vaughn College of Aeronautics and Technology, USA, Aparicio.Carranza@vaughn.edu

This Project is Funded by the Title V P031S200139 Grant

ABSTRACT

Nowadays, in the interconnected world, where online advertisements and potential security threats abound, ensuring the security and integrity of network traffic is paramount. AD blockers are essential tools for safeguarding users' online experiences. Pi-hole, a network wide AD blocker, operates at the Domain Name System (DNS) level, intercepting and filtering out malicious domains advertisements before they reach connected devices. Through packet inspection, Wireshark enables users to identify anomalies, detect potential threats, and troubleshoot network issues. Combining the capabilities of Pi-hole and Wireshark, users can bolster network security and enhance monitoring capabilities. We have implemented a system that automates packet capture and analysis that acts as Intrusion Detection Systems (IDS)

BACKGROUND

Pi-hole

- Runs on a Raspberry Pi or any other Linux-based system
- Utilizes DNS sink holing to block ads and tracking domains
- Administered through a web interface for configuration and monitoring
- Enhances network security by blocking known malicious domains

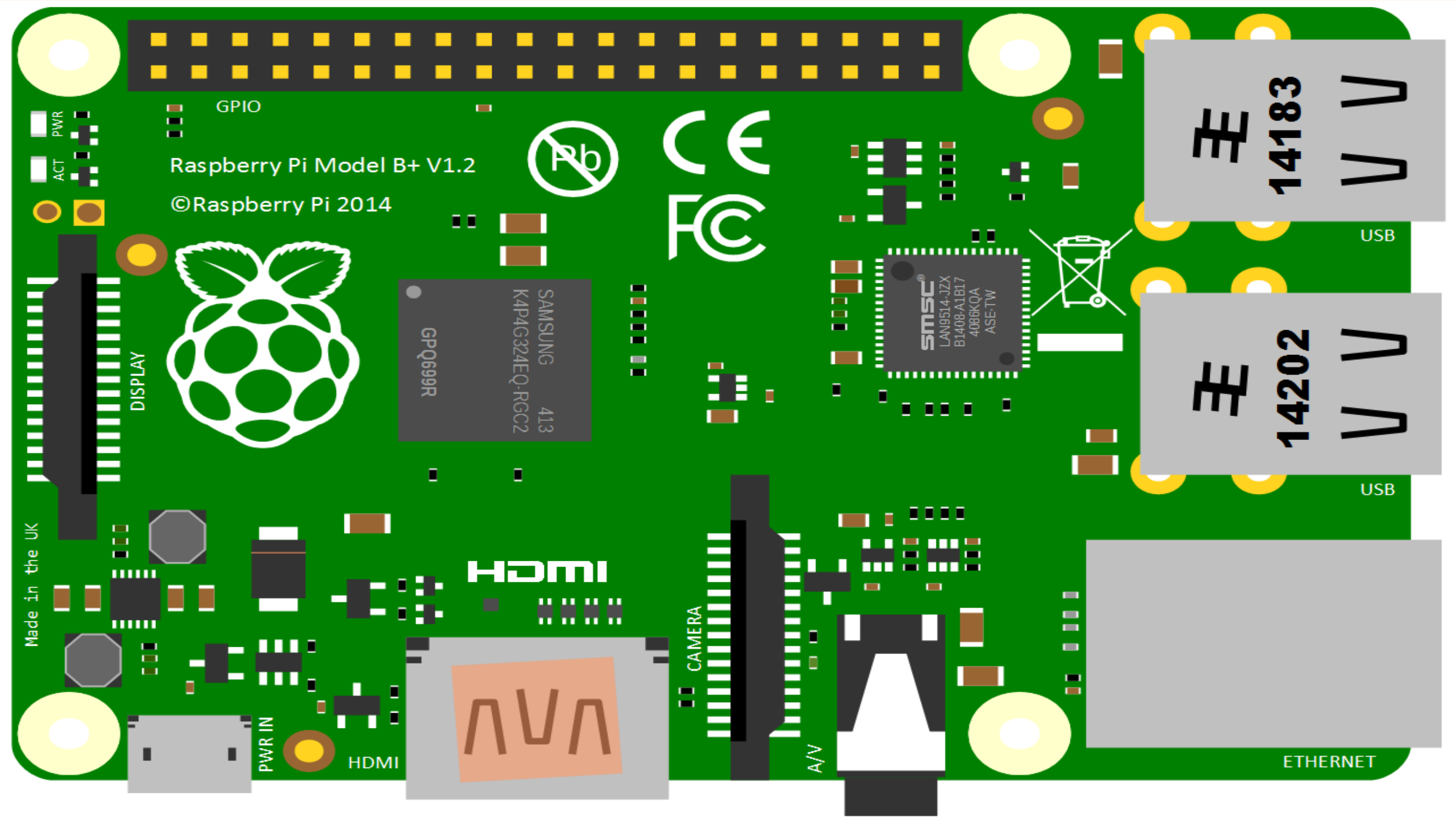
Wireshark

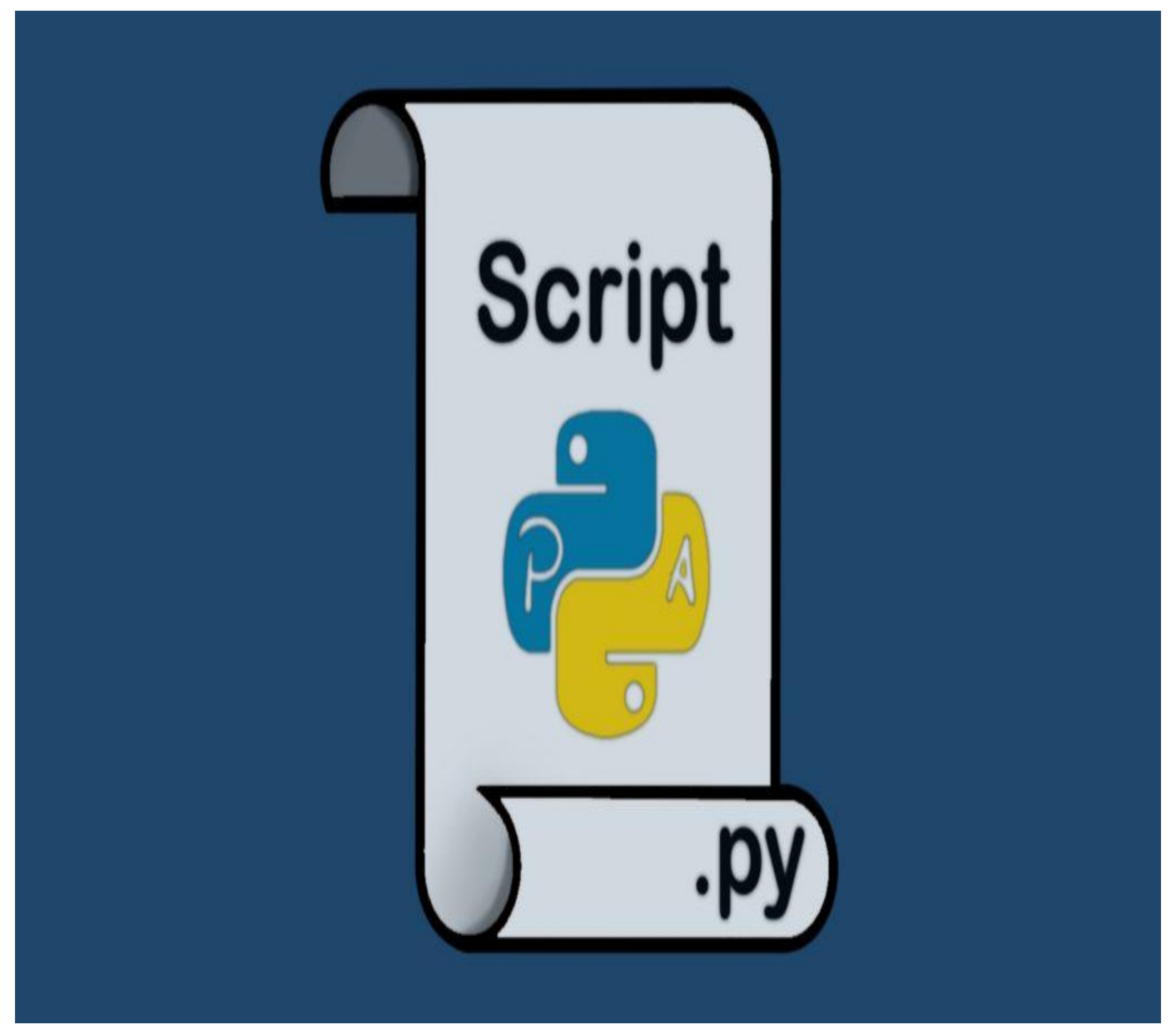
- Open-source packet analyzer used for network troubleshooting, analysis, and protocol development
- Supports capturing and displaying the data traveling back and forth on a network in real-time
- Offers extensive protocol support, allowing users to inspect traffic at various OSI model layers
- Features powerful filtering and search capabilities to focus on specific network traffic

OBJECTIVES

- Setup Raspberry Pi 4, Install and configure Pi-hole, and install Wireshark
- Utilize Pi-hole to block malicious domains and advertisement at the DNS level
- Employ Wireshark for real-time packet capture and analysis
- Automate scheduled packet capture sessions
- Port 53 is the default port used by the Domain Name

METHODS



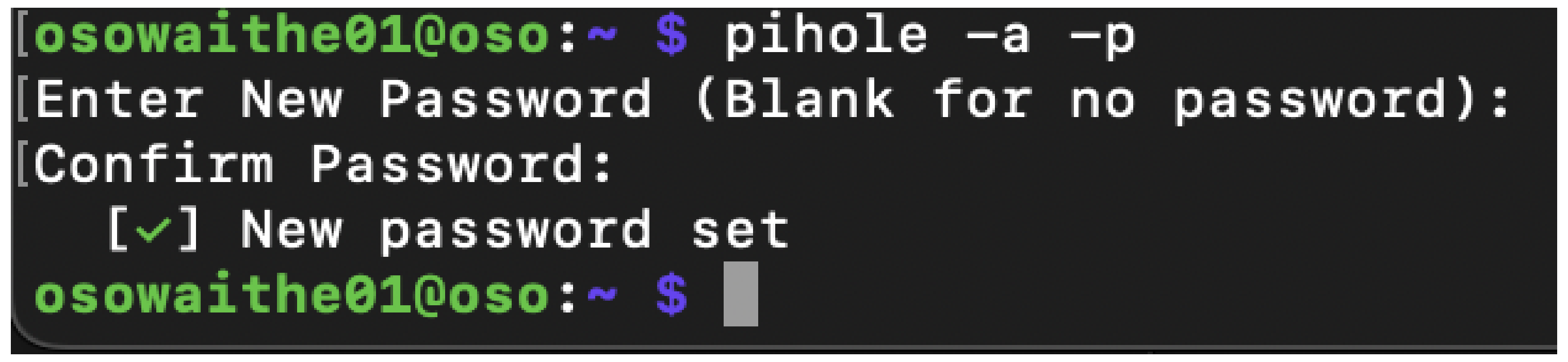


Pi-hole®
wide ad blocking via your own Linu

wireshark

- Alerting and notification mechanisms for proactive threat detection
- Creating shell script(Python)
- Virtual Environment

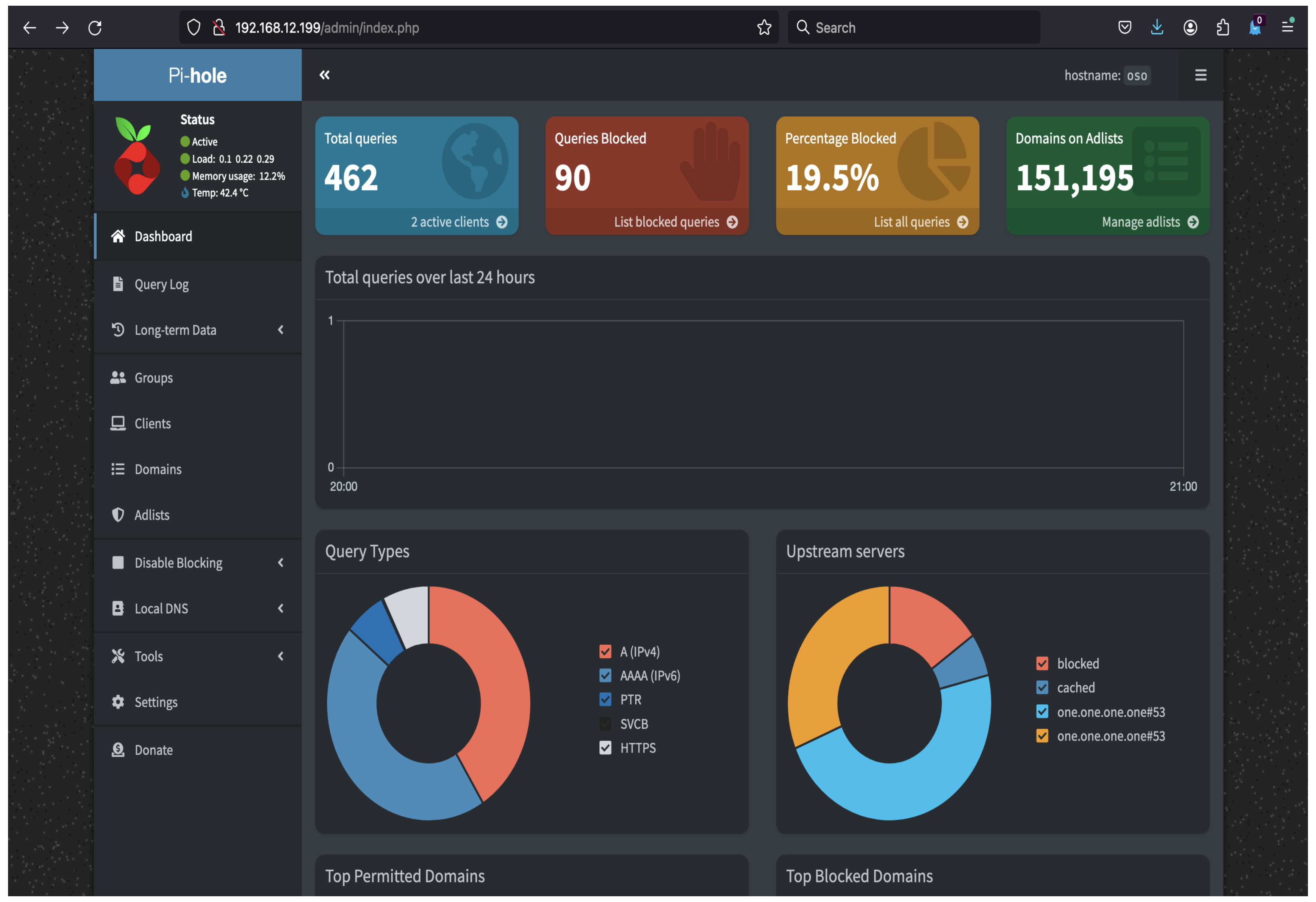
RESULTS



```
[osowaithe01@oso:~ $ pihole -a -p
[Enter New Password (Blank for no password):
[Confirm Password:
  [✓] New password set
osowaithe01@oso:~ $ 
```

- Using the Raspberry pi as the DNS my score report was 96%
- Using my home router as the DNS my score was 89%
- Therefore, based on the configuration of my Pi-hole it is effective in blocking ads over a network

RESULTS (continued...)

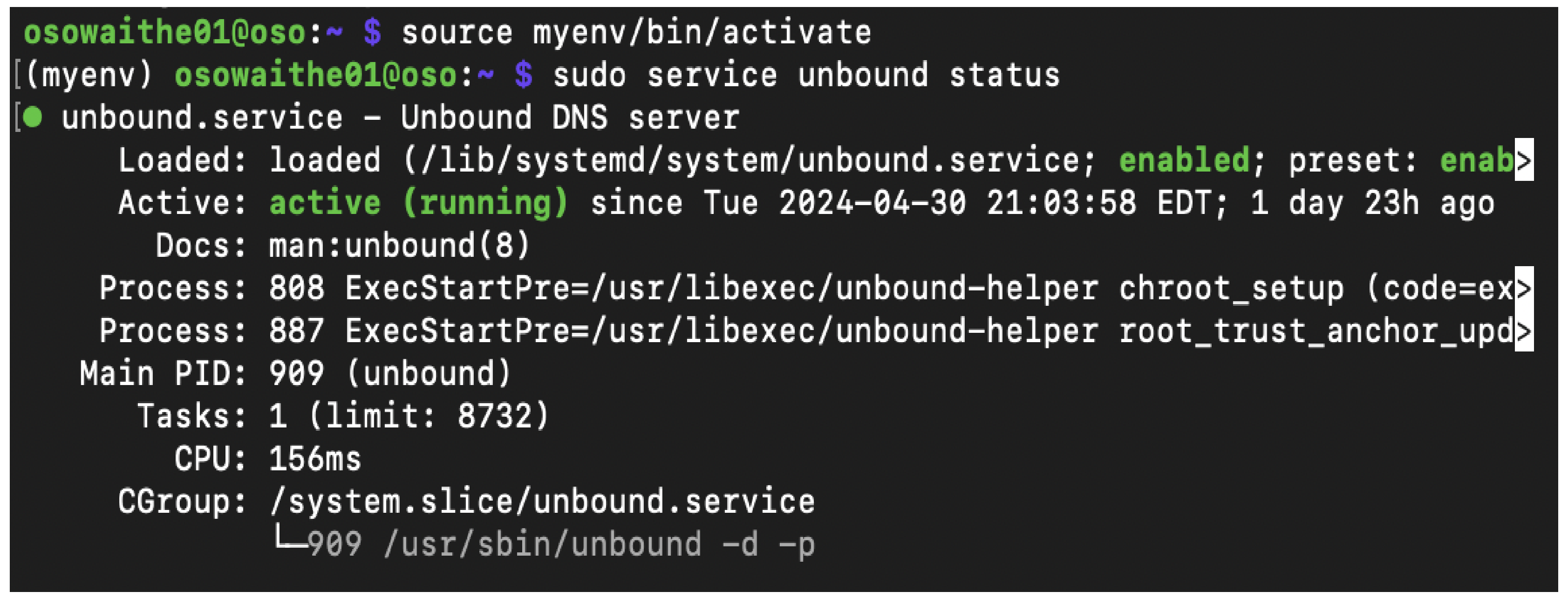


192.168.12.199/admin/index.php

Pi-hole — hostname: oso

Status: Active; Load: 0.1 0.22 0.29; Memory usage: 12.2%; Temp: 42.4 °C

Total queries: 462 (2 active clients)
Queries Blocked: 90 (List blocked queries)
Percentage Blocked: 19.5% (List all queries)
Domains on Adlists: 151,195 (Manage adlists)



```
osowaithe01@oso:~ $ source myenv/bin/activate
[(myenv) osowaithe01@oso:~ $ sudo service unbound status
[● unbound.service - Unbound DNS server
     Loaded: loaded (/lib/systemd/system/unbound.service; enabled; preset: enab>
     Active: active (running) since Tue 2024-04-30 21:03:58 EDT; 1 day 23h ago
       Docs: man:unbound(8)
    Process: 808 ExecStartPre=/usr/libexec/unbound-helper chroot_setup (code=ex>
    Process: 887 ExecStartPre=/usr/libexec/unbound-helper root_trust_anchor_upd>
   Main PID: 909 (unbound)
      Tasks: 1 (limit: 8732)
        CPU: 156ms
     CGroup: /system.slice/unbound.service
             └─909 /usr/sbin/unbound -d -p
```

FUTURE WORK

- Packet Analysis & Capture: Successful packets are captured and analyzed in Wireshark

CONCLUSIONS

- *By harnessing the combined capabilities of Raspberry Pi 4, Pi-hole, and Wireshark, users can significantly enhance network security*
- *Empower yourself with the tools and knowledge to safeguard your network against cyber threats and maintain the integrity of your digital infrastructure*

The OAS Summit of Engineering for the Americas: 22nd LACCEI International Multi-Conference for Engineering, Education, and Technology. July 17-19, 2024
"Sustainable Engineering for a Diverse, Equitable, and Inclusive Future at the Service of Education, Research, and Industry for a Society 5.0". San Jose, Costa Rica