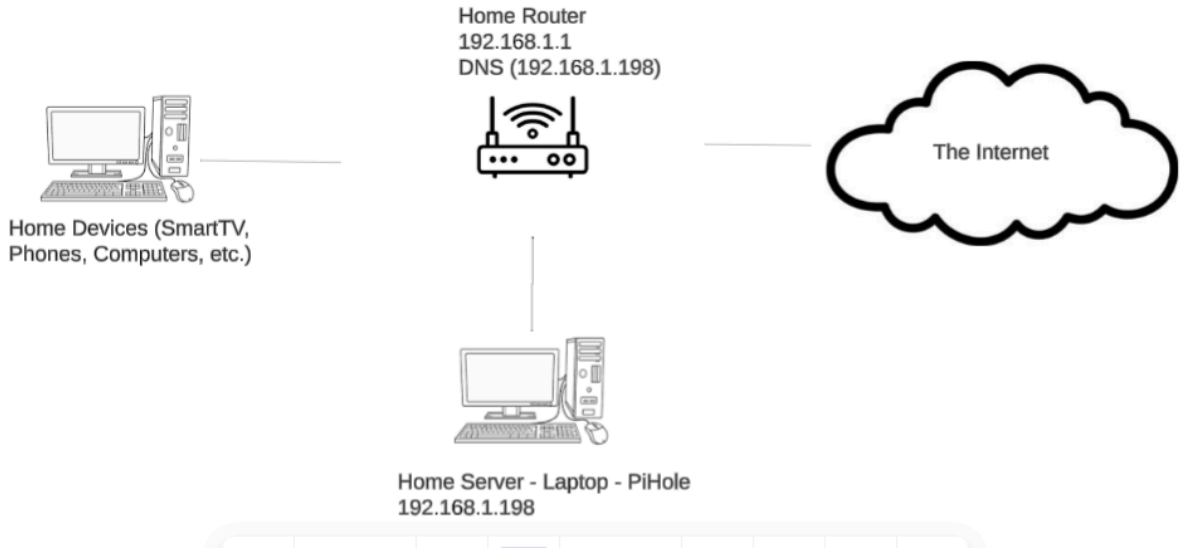
Eric Guzman 10/2/2025

PiHole Project

Description: In this project I will repurpose an old laptop that was laying around and put it to use. The first service I want on this home server is PiHole so that I can have a network wide ad and tracker blocker.

Topology:



Technologies and Skills Demonstrated:

- Ubuntu Server 24.04 LTS
- Pi-hole v5 + lighttpd + DNSmasq/FTL
- Network engineering (DHCP/DNS)
- Troubleshooting with nslookup/dig
- Netplan static IP configuration
- Linux administration (SSH, sudo, nano)
- Router configuration
- System hardening basics

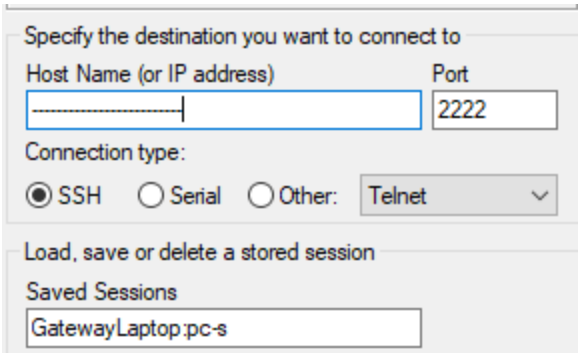
Key Syntax:

Term	Definition
pihole -g	Update PiHole blocklists
pihole restartdns	Restarts the PiHole DNS service
pihole -t	Tails the PiHole log watching it in real time

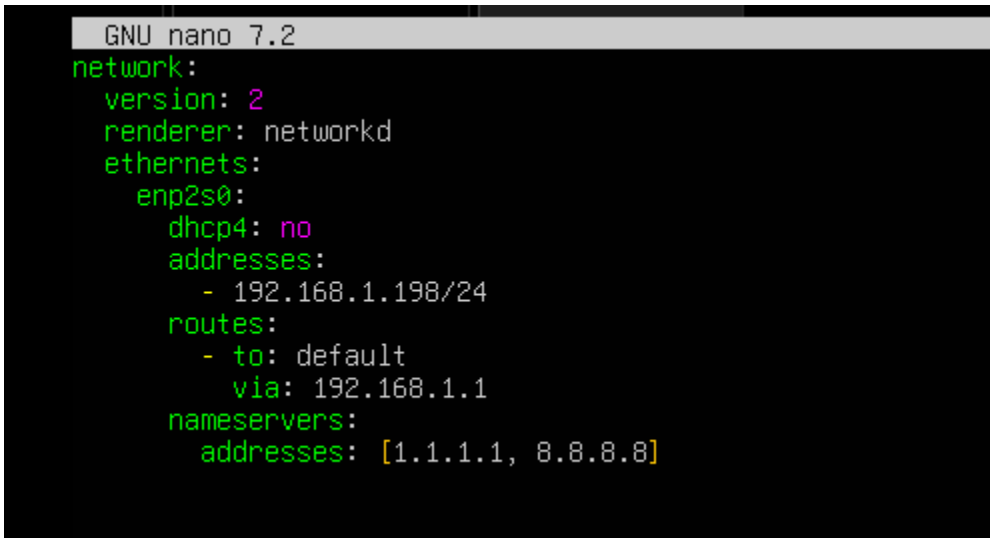
Nslookup flurry.com 192.168.1.198	Tests a known ad domain to see if it is blocked
nano /etc/netplan/*.yaml	Edits the netplan for Ubuntu

Verification:

1. I started off by installing ubuntu server 24.04.1 onto a flash drive, booting to the flash drive on the laptop and installing ubuntu server that way.
2. I then setup SSH via putty so that I could remotely setup the PiHole from my main PC.



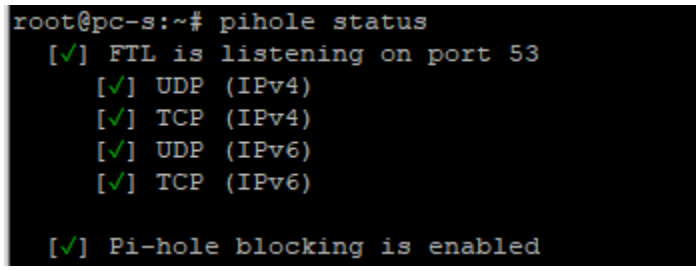
3. I went straight into setting a static IPv4 address for my ubuntu server by using the command sudo nano /etc/netplan/01-netcfg.yaml to edit the network configuration file.



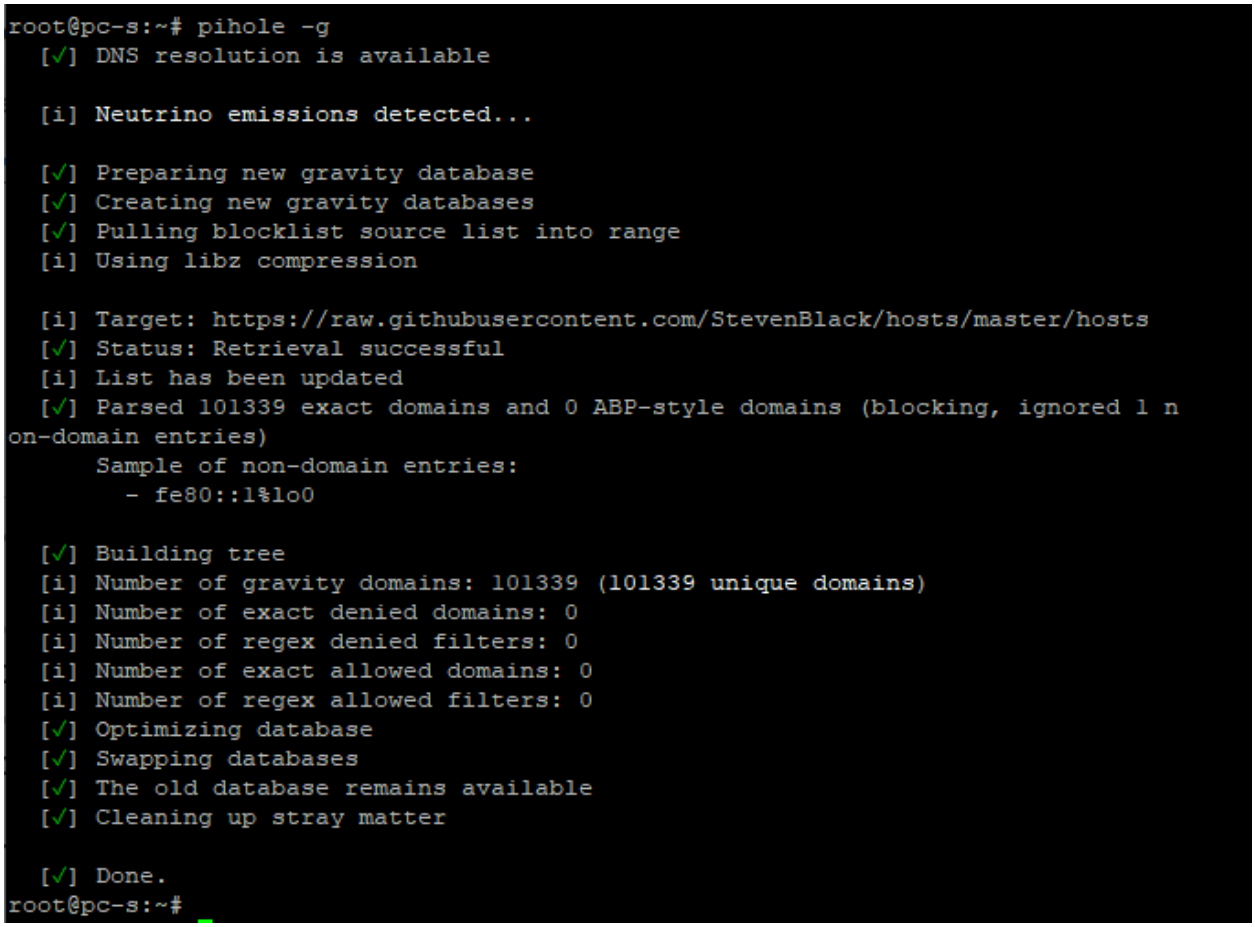
4. I then went to my router's configuration page and made a DNS entry to reserve an address so that my server always has the IP 192.168.1.198.

5. This screenshot shows that I then installed PiHole on my ubuntu server.

6. This screenshot is showing that PiHole is properly running and blocking trackers/ads on my network.

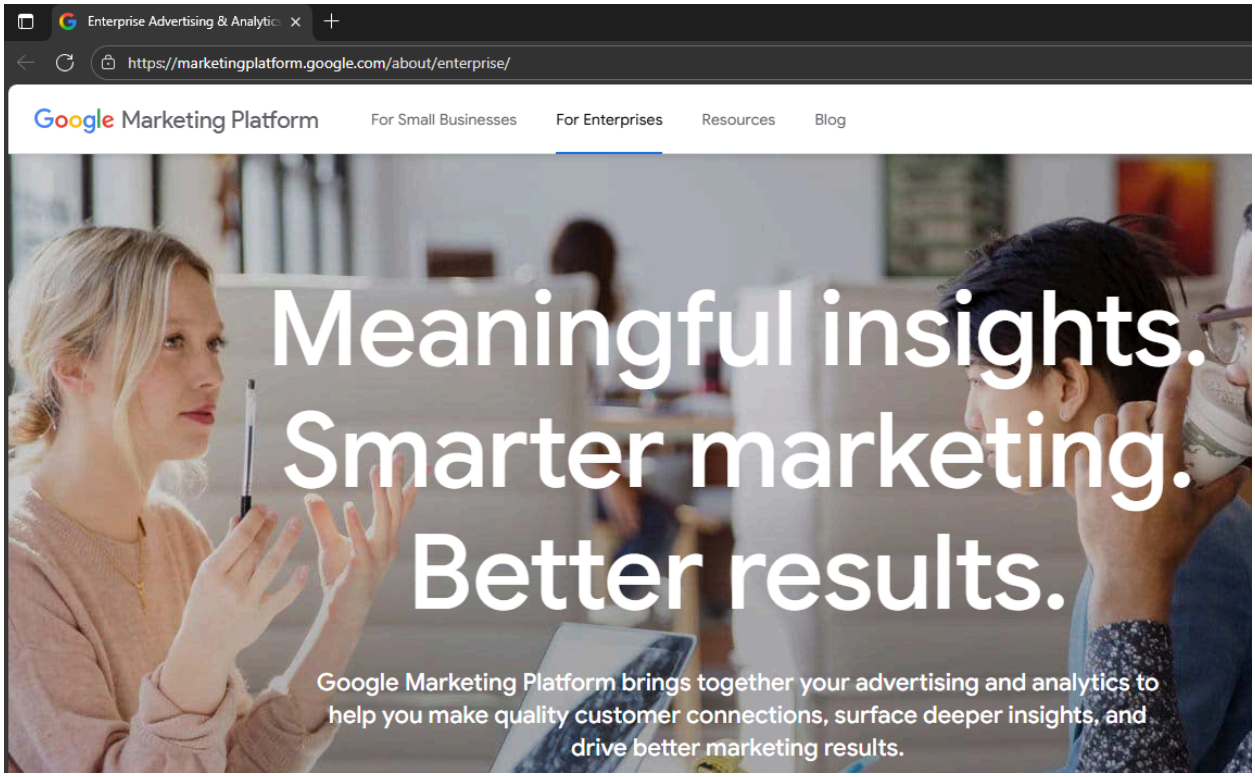


7. This screenshot shows that the blocklist was downloaded and correctly applied.

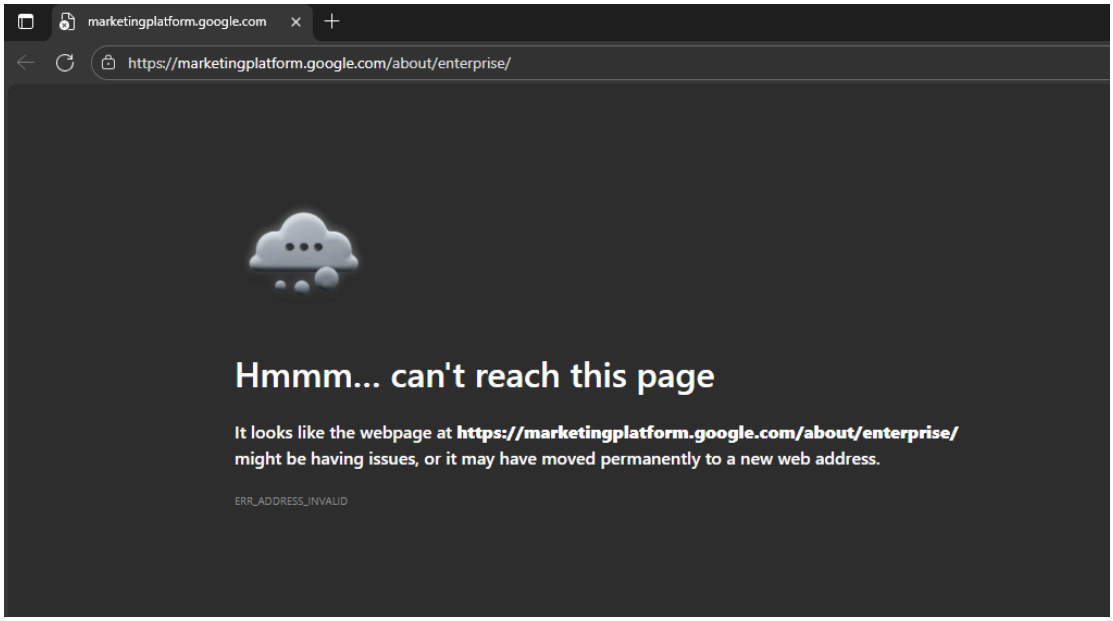


8. This is a screenshot of the web ui, allowing monitoring of all blocked traffic, also showing all clients using the PiHole.

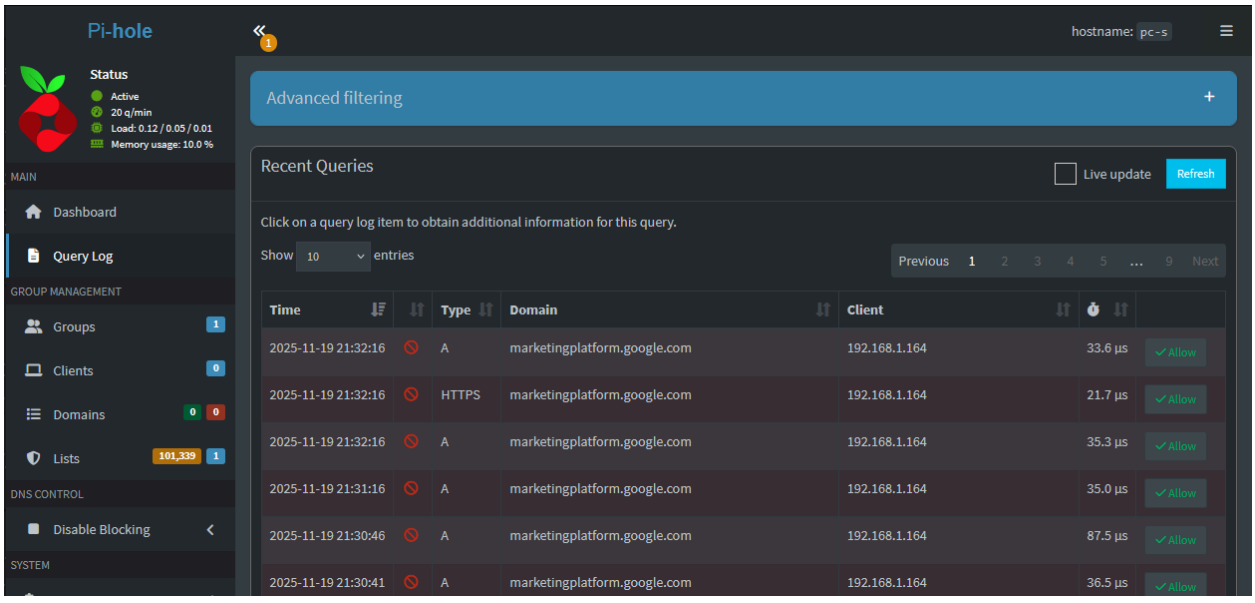
9. To verify that the PiHole properly functions, I can try to go to Google's marketing platform site (which is included in the blocklist) while we do not have the PiHole as our DNS server. As you can see the site loads properly.



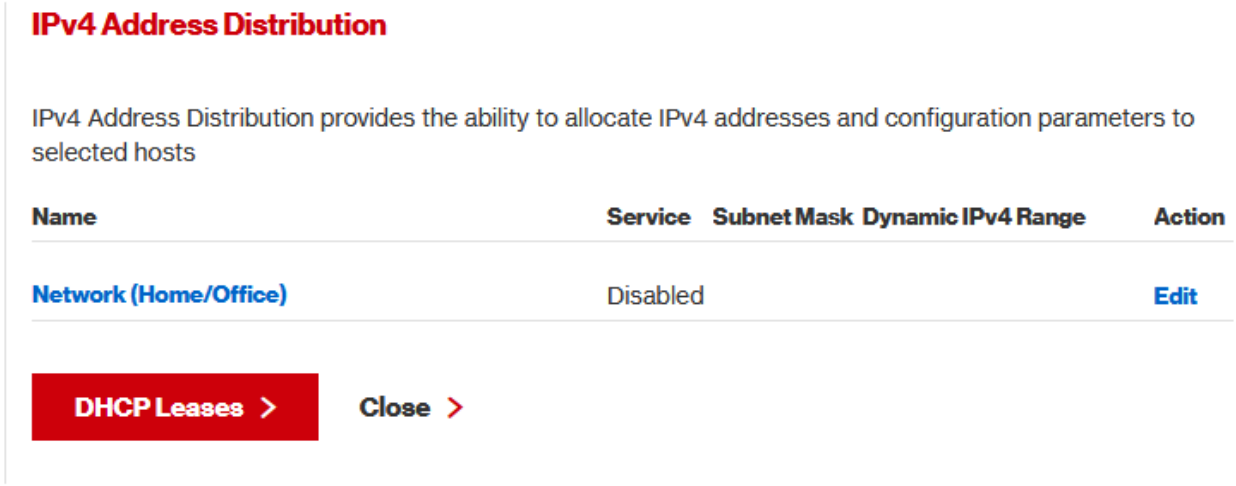
Once we change our DNS server to the PiHole, the site no longer loads which means that the PiHole blocklist is working properly.

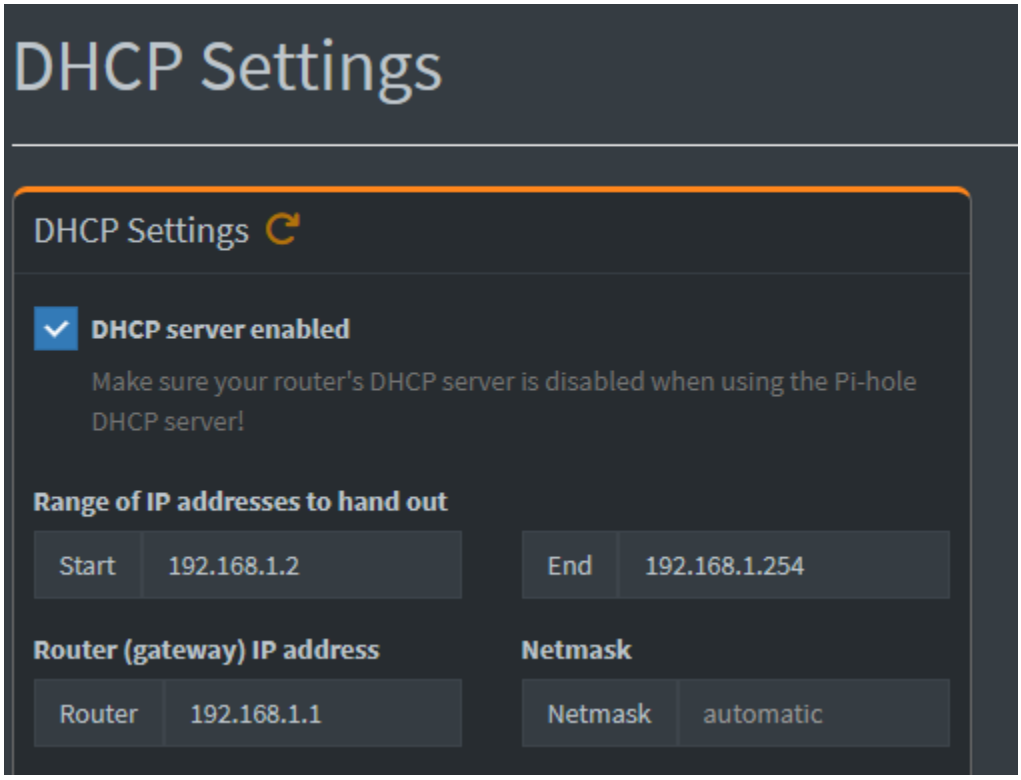


10. We can check the web ui to make sure our query was blocked. It does show up here meaning that everything is working properly.



11. The final step is to make sure all of my network devices use the PiHole as their DNS server. I can do this by logging into my router and changing the main DNS server to the PiHole. Once this is complete, every device that is on my network will block ads and trackers making this project a complete success.





Security:
Even though this is a home project and not a production environment, I applied best security practices to protect the server and network.

Measure	Implementation	Reason
Disabled root SSH login	I edited the /etc/ssh/sshd_config files PermitRootLogin rule to no	Prevents root brute force attacks
Restricted SSH to key only authentication	I disabled password authentication rule and only used keys to SSH in	Stops the possibility for password guessing attacks
Enabled uncomplicated firewall	I only allowed used ports and allowed SSH only from inside the LAN	Only in LAN IPs can SSH into the server
Changed web app password	Changed the web app password to be strong	Only allows authorized access to the dashboard

Results:
I let the PiHole run for about a week to get statistics on how useful it is and here were the results:

Metric	Value
Total DNS queries processed	312,851
Queries blocked	58,198
Unique domains on blocklist	101,339
Common blocked domains	googlesyndication.com, doubleclick.net, pubmatic.com

Conclusion:

This project was a fairly simple and fun way to repurpose a very old laptop that was not getting any practical use anywhere else. It is nice to know that all devices on my home network using my server for DNS are blocking ads and trackers. I am excited to add other services onto it and expand my home server even more.

References:

1. https://docs.pi-hole.net/
2. https://raw.githubusercontent.com/pi-hole/pi-hole/master/automated%20install/basic-install.sh
3. https://netplan.readthedocs.io/en/stable/
4. https://github.com/StevenBlack/hosts