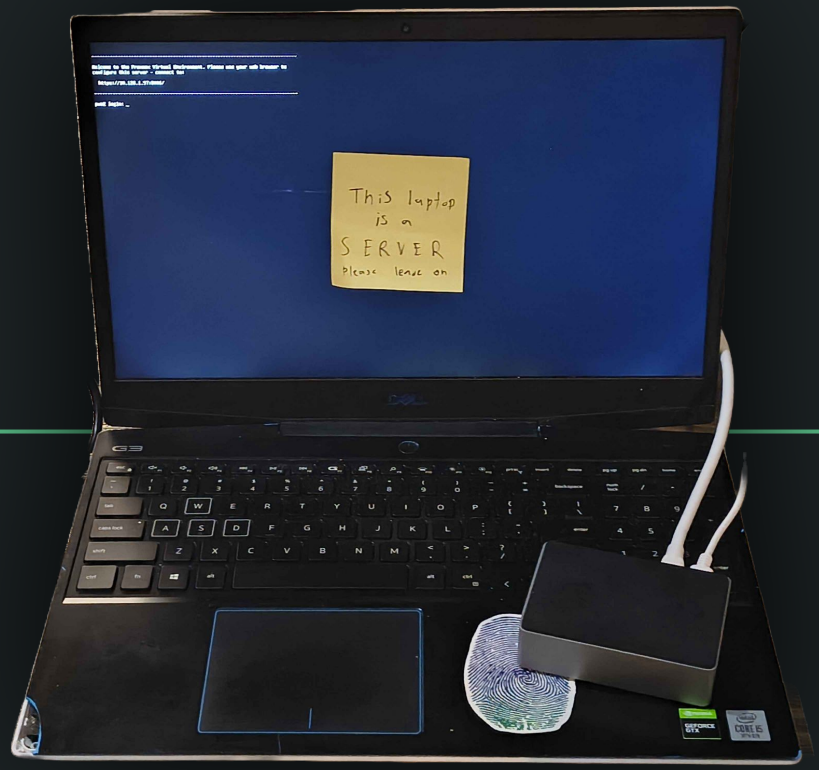
Who pays for one of these services?







An Introduction to Homelabbing



Starting at 5pm

Agenda

- About us
- What is a homelab
- Building your first homelab
- Our homelabs (and what they taught us)
- Skills to focus on
- Getting the most out of your homelab
- Your homelab roadmap
- Q&A

About us



- Senior at UTSA
- Member of cyber competitions teams
  - CCDC
  - CPTC
- Interned at Texas Instruments
  - Full time return offer for next summer



Nathan Bledsoe

- Senior at UTSA
- CTF Competitor
- Homelabber!
- Member of cyber competitions teams
  - CPTC

What is a homelab

What is a homelab

- A setup you use to experiment with cybersecurity
- That’s pretty much it
  - It can evolve to match what you are interested and what to learn

Okay, but what is it really?

- VMs / containers running in one or more networks
  - Services
  - Tools
  - Labs

Why should you build a homelab

- Expands on skills from classes and clubs with hands on experience
- Looks good to employers and shows interest
- Can help you save money on things you pay for



Building your first homelab

Getting started

When starting a homelab, there are many things to consider

- Hardware? What will your homelab actually run on?
- Operating system?
- Software?
- How can you access your lab remotely?

Hardware

Any computer can support a basic homelab! It does not have to be a super expensive server.

Some options include:

- An old laptop/computer
- Second hand computer (Thrift store, estate sale, ebay)
- Mini PC (Intel Nuc)



If hardware is a barrier of entry, you could also get started by simply using a virtual machine on your main computer/device

Operating system

There are a couple operating systems to choose from, but proxmox is what we would recommend.

- Free and open source
- Easy to use web interface
- Supports snapshots and rollbacks
- LOTS of tutorials and documentation available online
- Large thriving community



Software

Welcome to the wonderful world of self hosting. This is the fun part!

Some good first projects to set up:

- Jellyfin - Media streaming service (Your own netflix!)
- Navidrome - Music streaming service (Your own spotify!)
- Immich - Video and photo management (Your own Google Photos!)
- Docmost - Web based markdown editor
- Nginx proxy manager - Easy to use reverse proxy manager
- Forgejo - Self hosted alternative to github
- Nextcloud - Content collaboration (microsoft 365/google drive)









We love tailscale

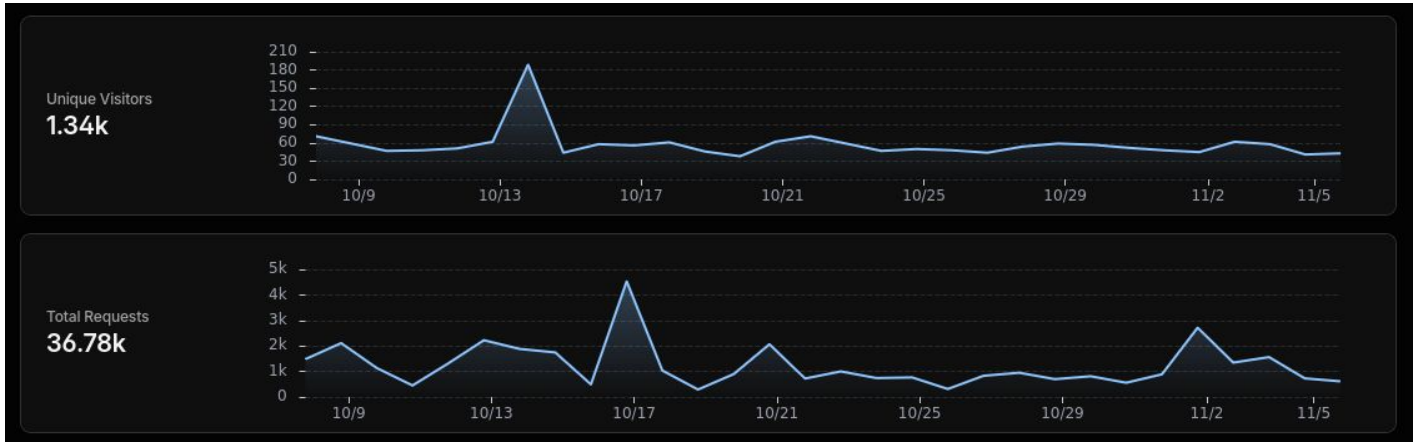
- Your new best friend
- Free and easy remote access for your lab
- It also grows with your homelab
- AVOIDS putting stuff on the public internet (scary)



tailscale

Why having your homelab exposed to the public internet is bad

- Could be security flaws in your homelab design
- Bots crawl the web constantly and will automatically scan and try to identify weak servers
- You (probably) can't patch fast enough to keep up with AI



Helper Scripts

- Helper scripts install an entire service in one command
- They are a great way to get started with a working service
- Eventually it can be better to move away from them

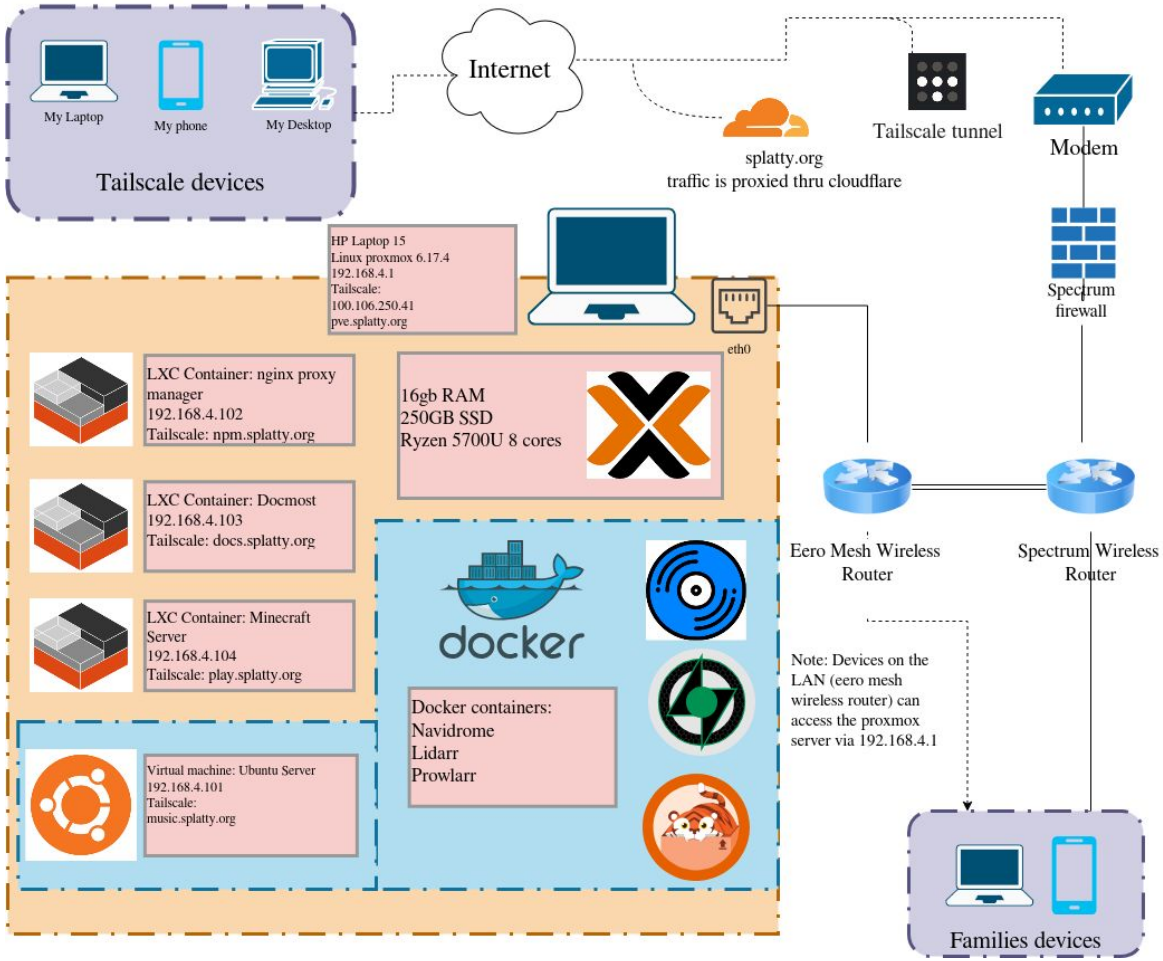


My first homelab!

This is what a beginner homelab can look like and where I got to after only a few weeks of learning.

What did I learn?

- Networking basics
- Docker
- Linux
- LXC containers
- Reverse proxy
- Firewalls

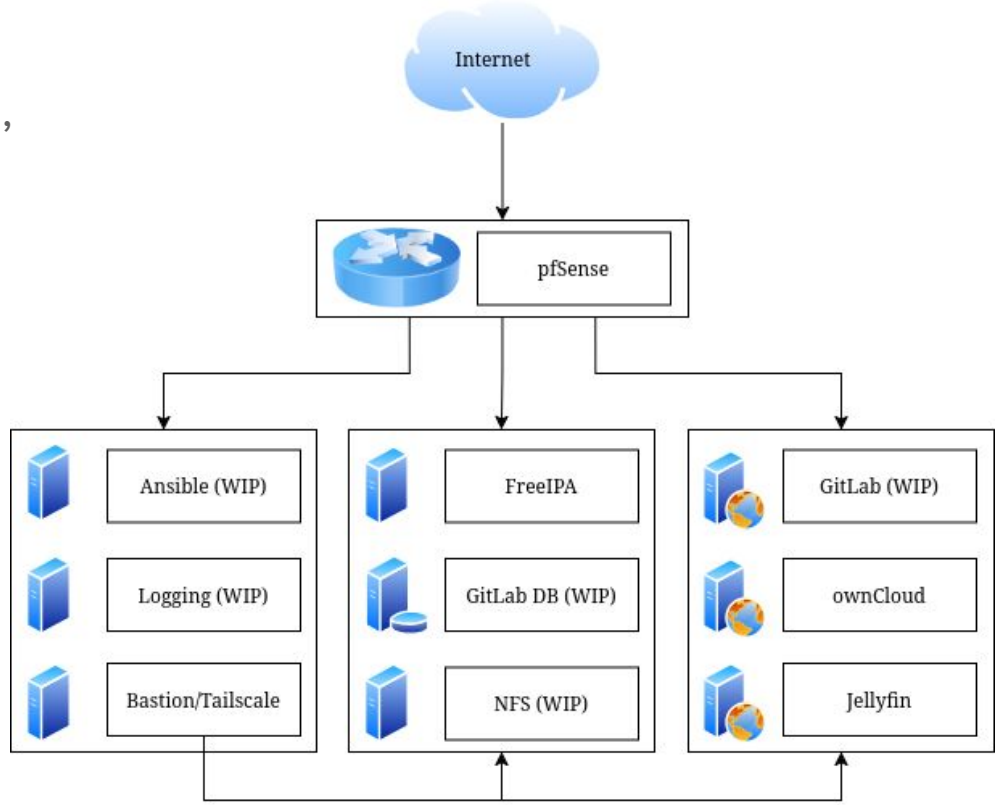


How a homelab grows

My homelab

My homelab started out like Nathan's, but grew as I started to learn more.

- One router with 3 networks
- Centralized auth with FreeIPA
- ownCloud for file storage
- GitLab for coding projects



Growing into multiple networks

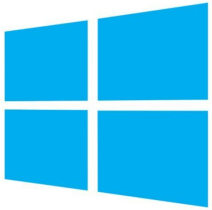
- One flat network will work for most things you do
- Understanding of networking is important in cybersecurity
- Study network layouts online before you start
- I recommend pfSense or OPNsense



Centralized authentication

Eventually I got tired of keeping track of passwords for every VM

- FreeIPA / Windows Active Directory
- Overkill for a one-person lab
- OAuth (Authentik) is easier for apps



Active Directory

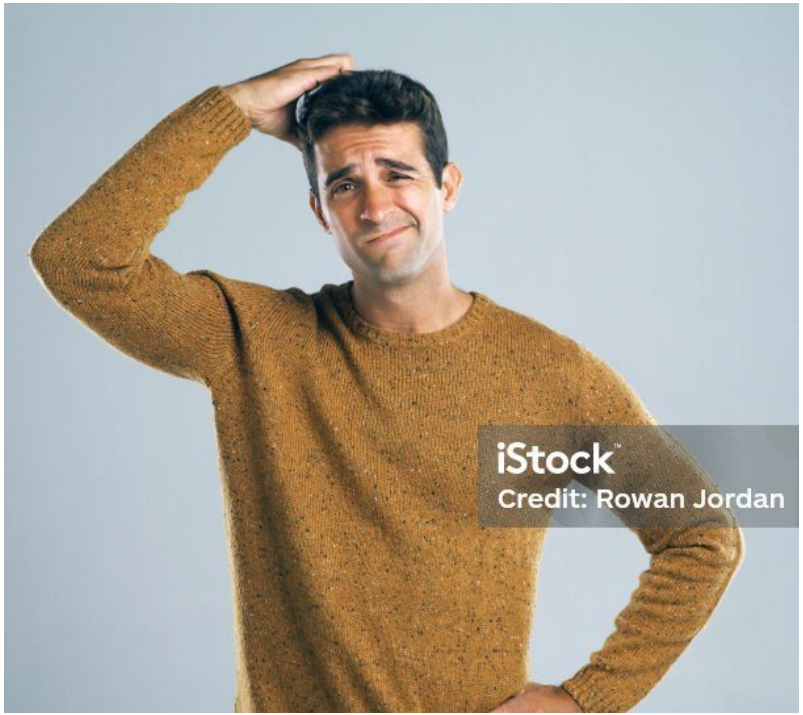


FreeIPA

Open Source Identity Management Solution

I had no idea what I was doing

- Dove into network segmentation with no plan
- Ran a domain controller for one user: me
- Best learning experience of my homelab



Lesson 1: Try things and make mistakes

You learn by trying new things and seeing what goes wrong. But try to make your mistakes less painful than mine

- Backup your data often (3-2-1 if possible)
  - 3 copies, 2 media types, 1 off-site
- Don’t make things rely on something you might not need

Tore down every old service

I wanted to get a fresh start with my homelab, so I took everything down

I went through every old service and made backups of data

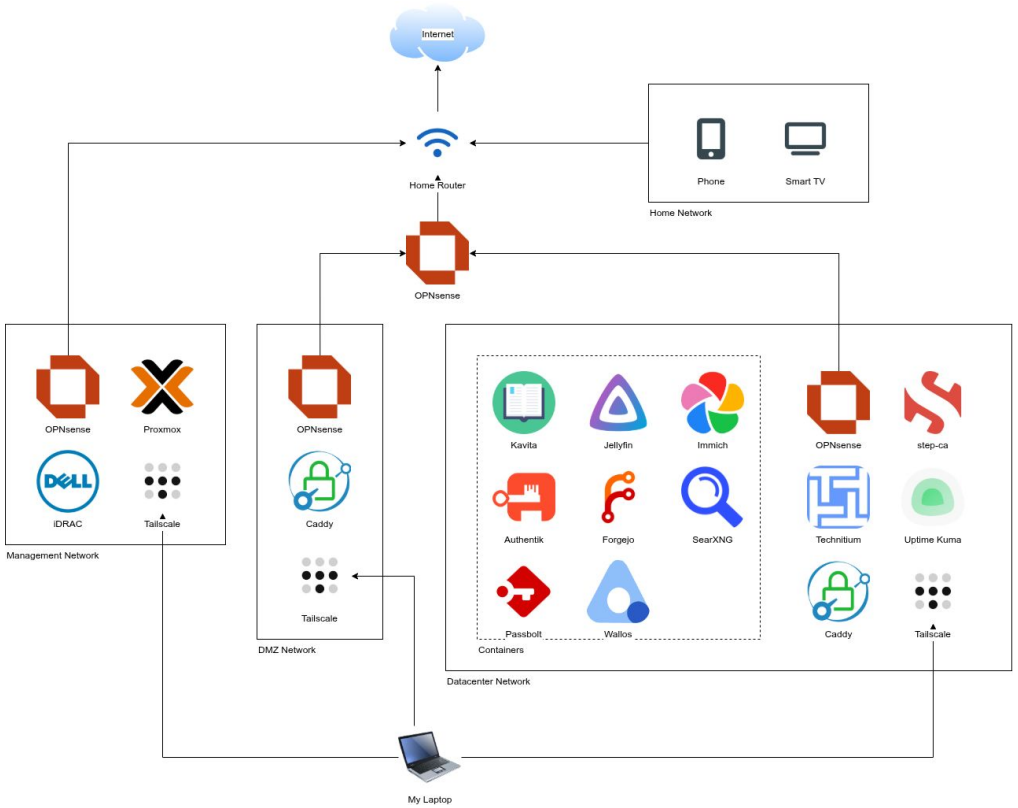
I did this too late into the teardown and ended up fighting against services that were half working



Starting from scratch with a security focus

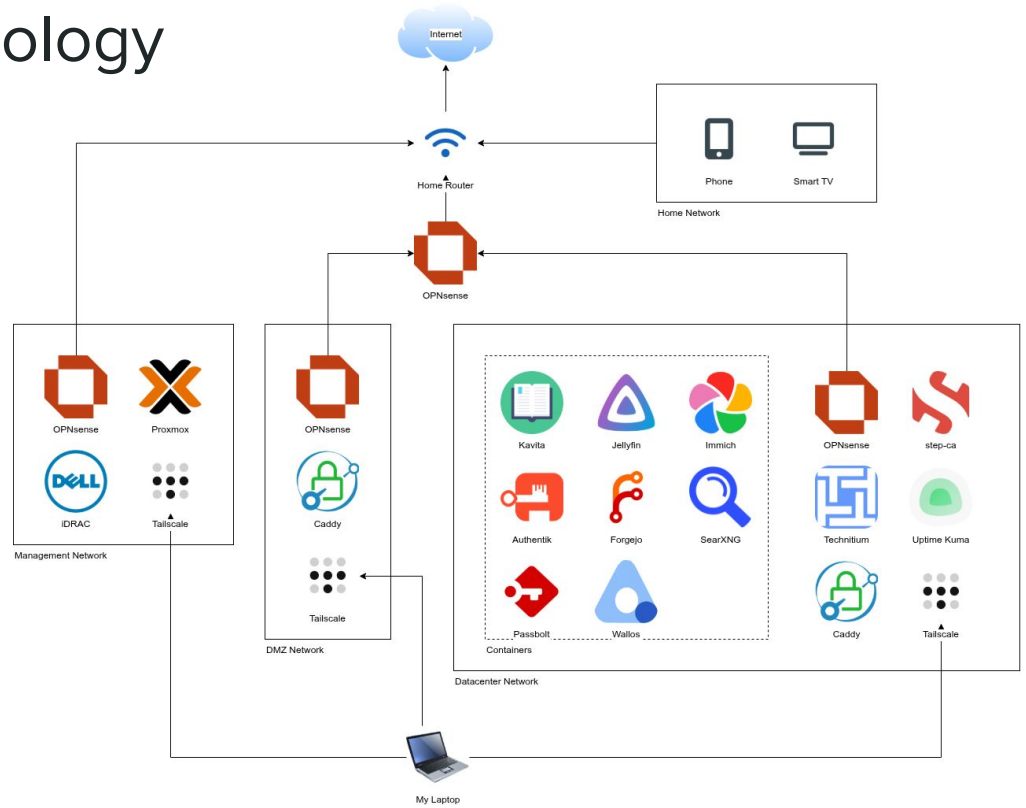
My Current Homelab

- Multiple networks with OPNsense
- Centralized authentication for apps with Authentik
- Certificate Authority for HTTPS
- It took a long time to get here



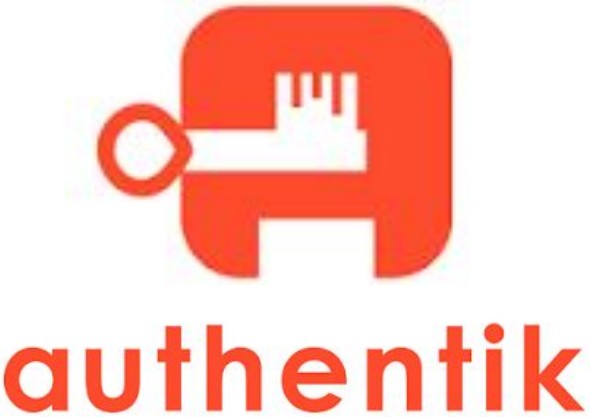
A whole new network topology

- Planned first: diagram and firewall rules
- Multiple routers for stronger isolation
- Switched from pfSense to OPNsense



Migrated to SSO instead of a full DC

- Provides a single account shared across services
- Hosts still use local authentication
  - A break in SSO doesn’t lock me out of my VMs



Used fewer LXCs

Because I was going for a security focus I wanted stronger isolation for my services

- Prioritized using VMs since LXCs share the host kernel
- Ran rootless containers on top of VMs

Learned a lot about Docker/Podman

Lesson 2: Plan ahead and design proactively

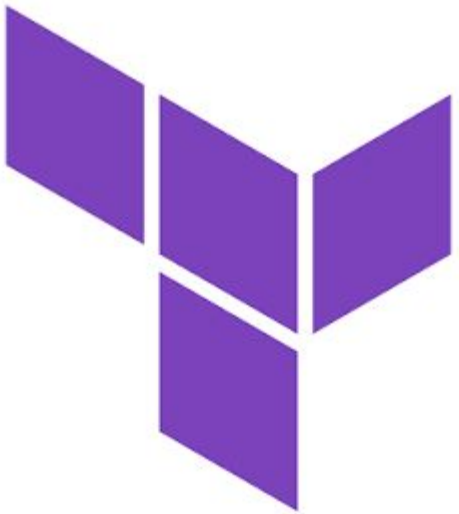
For any services you want to use every day, it's better to research and plan ahead before implementing something.

- A plan can catch mistakes before you make them
- It gives you a set goal to work towards
- Your first design is not going to be perfect

Where it’s headed next

Terraform based Cyber Range

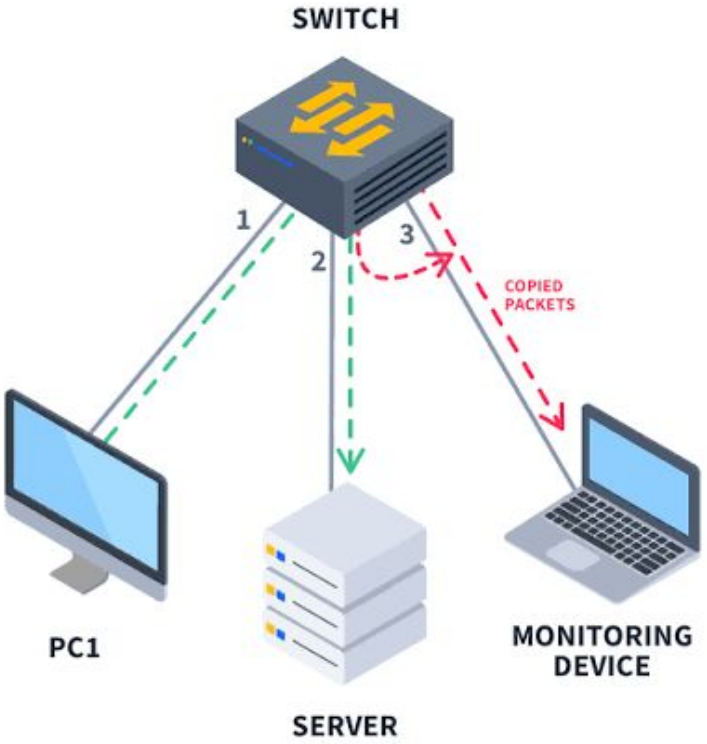
- Terraform to design and deploy a whole network via code
- Cyber range for testing more destructive things like malware
- Want to have separate hardware to run this on



HashiCorp
Terraform

Logging and a SIEM

- Building out a SIEM stack, likely Wazuh or ELK
- Makes use of port mirroring to capture every packet



Skills to focus on

Networking and Logging

- Networking
  - Fundamental to cybersecurity
  - Experiment with different network topologies
  - Test firewall configurations
- Logging / SIEM
  - Builds visibility into your lab network
  - Learn how to build alerts, detections, and dashboards
  - Enhances what you can learn from every other part of your lab



Hands on experience with common tech

- Containers
  - Practice dev & deploy workflows with an app you develop
  - Learn the security implications by practicing container escapes
  - Expand to kubernetes for orchestration and scaling
- Windows AD
  - Classes don’t teach it because of licensing requirements
    - Windows Server has an evaluation period
  - Learn about applying GPOs and on-boarding machines

Build and attack

- Learn pentesting on purpose-made boxes like Juice Shop
- Pentest your own lab and publish the report
- Turn your attacks into SIEM detections



How to get the most out of your homelab

Share what you are doing

- Make write-ups
  - Don’t just say what you did, explain the process
  - Focus on decisions, mistakes, and reasoning
  - Proves to employers you can think things through
- Publish configs
  - Use comments to explain your reasoning
  - Don’t accidentally share secrets
    - Bots scan for them automatically
  - Someone might use your configs some day

Make your lab enjoyable to work on

- Run services you'll actually use
  - Great motivation to keep your lab working and secure
  - Can replace things you pay for or make them more private
    - Immich, Vaultwarden, and Wallos
- Document your lab
  - Makes it easier to come back after a break
  - Keep track of your own setup
    - Tech stack, config directories, network topology
  - It's an important skill to have
    - Helps projects survive longer
    - Differentiating factor in internships

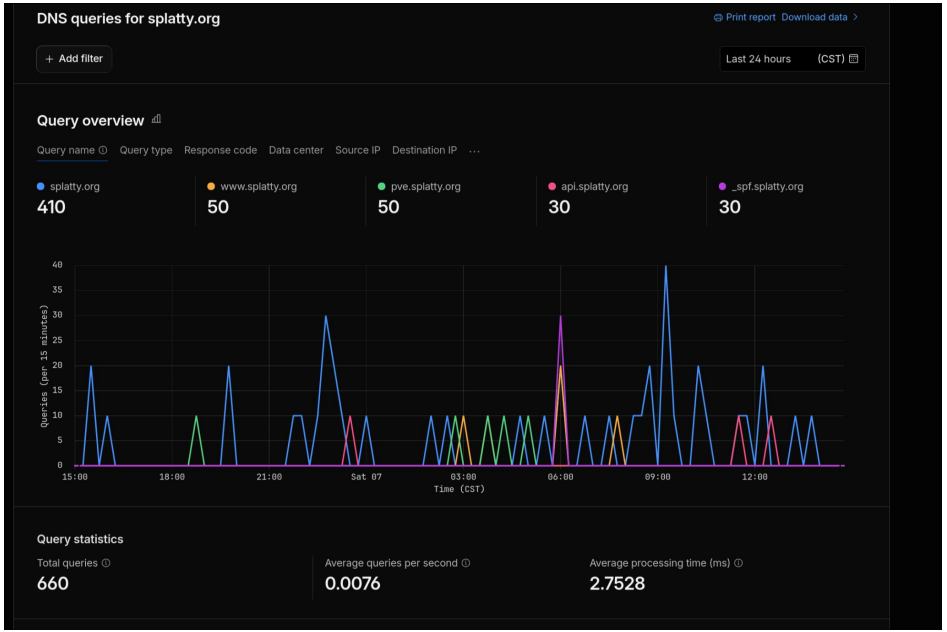
Your homelab roadmap

Start simple and small

- One network, a couple services
  - Set up an app and track it with Uptime Kuma
  - Deploy an app that runs across multiple containers
  - Try setting up mail (notoriously tricky)
- Pentest practice
  - Spin up a Kali box and Juice Shop
- Get familiar with the deployment process

Use a domain name for better organization

- Static IPs are hard to keep track of
- .internal or .home.arpa are free
- For a more fancy one (.org, .com, etc) they are usually cheap (under $15/year)
- Can get cool analytics if it is bought from or transferred to cloudflare



Expand to two networks

- Networking is the backbone of cybersecurity
- Set up a network with NAT and port forward a service
- Host your application behind a reverse proxy
- Experiment with firewall rules

Follow your interests

- Lots of online resources for homelabs
  - r/homelab
  - Proxmox helper scripts
  - FUTO’s self hosted life wiki
- Look at what other people have done
- Find something specific to you to do for your homelab

Our info



LinkedIn
William Anderson



Website
williamanderson.dev



LinkedIn
Nathan Bledsoe



Website
nathancyber.com

Questions?