Rough outline of the project:

Project outline

1. Create management space
   1. Kill switch
      1. Using nftables – drop and disable all network access within all virtual machines
      2. Create script **on host computer** to ensure constant kill-switch access if VM is exposed
   2. Management network
      1. Logical and physical addressing
      2. Utilising VirtualBox snapshot rollbacks
      3. Used to access all virtual machines
2. Create Virtual Environment
   1. Lab VM
      1. Runs vanilla honeypot. Basic, unconfigured cowrie honeypot emulating an IP IoT device
      2. Runs sandboxed high-interaction honeypot
         1. Cowrie honeypot within a FireJail and Docker combination container
         2. Uses linux kernel seccomp for network egress blocking
   2. Analysis VM
      1. Runs, processes and analyses pcaps from the Lab VM.
      2. Off-the-network (act as a centralised server)
      3. Retrieves and stores logs using ElasticSearch and associated tools
3. Network topology
   1. Define segments
      1. Assign IP addressing to IoT devices
      2. Assign addressing to VMs
      3. Link to management network
         1. Host machine + VMs (Isoloated)
      4. Create DMZ zone
         1. Holds both honeypots and VMs
   2. Internal Routing
      1. Virtual router / firewall connecting all virtual machines to DMZ
4. IoT device simulation
   1. Simulate various IP devices within LAN

Attacker -> DMZ -> Honeypots -> IoT Lan

Logs -> Management Network -> Analysis VM (need IPC for this)

* Vanilla honeypot: Low-interaction honeypot deployed on the virtual network (inside VM) segment with no container
  + Used to mimic an IoT device to capture attackers [What is a honeypot? How honeypots help security](https://www.kaspersky.com/resource-center/threats/what-is-a-honeypot)
* Sandboxed honeypot: Identical to a vanilla honeypot, but rather deployed inside a container for high-interaction
  + Used to thoroughly and safely analyse malicious risks

Problem:

Low interaction vanilla honeypots may be considered weak in nature due to only simulating basic IoT devices, with zero in-depth analysis measures – in essence, weak simulation.

On the contrast, high-interaction honeypots (within a sandboxed environment) provide much greater security by creating an isolated environment for malicious attacks [honeypot vs sandbox](https://tssc.mx/EN/honey.php) where such are able to be evaluated and thoroughly processed. It permits for OS resources to be monitored.

The purpose of comparing is to evaluate how vanilla honeypots do not have any overhead and aren’t as undetectable by attackers.