**INFRA – GATEWAY**

**Ubuntu Server 24.04 LTS – x64 Gen2**

**4CPU/16GB RAM**

* Local account : ubuntu (sudo) / Threathunt25

Installed software

* All software under **/OPT/DFIR** (git clone repo)
* Enable SSH service
* Enable XRDP
  + sudo apt install xrdp -y
  + sudo service xrdp start
  + sudo update-rc.d xrdp enable
  + sudo groupadd tsusers
  + sudo groupadd tsadmins
  + sudo usermod -aG tsusers rdp
  + sudo usermod -aG tsadmins rdp
  + sudo apt install kali-desktop-xfce -y
  + sudo service xrdp restart
  + sudo update-alternatives --config x-session-manager

A screenshot of a computer program

Description automatically generated

* Docker + docker-compose
  + sudo apt install docker.io
  + sudo apt install docker-compose
  + sudo usermod -aG docker $USER
  + newgrp docker
  + mkdir -p ~/.docker/cli-plugins/
  + curl -SL https://github.com/docker/compose/releases/download/v2.3.3/docker-compose-linux-x86\_64 -o ~/.docker/cli-plugins/docker-compose
  + chmod +x ~/.docker/cli-plugins/docker-compose
  + docker compose version
  + <https://www.digitalocean.com/community/tutorials/how-to-install-and-use-docker-compose-on-ubuntu-22-04>
* TRAEFIK (docker)
* Guacamole (docker)
  + RDP to student WIN
  + RDP to student Kali
  + RDP to central DC (trainers only)
  + RDP to GATE itself (trainers only)
* Portainer (docker)
  + User :
* Elastic + Kibana v8.17.1 (docker)

**CENTRAL DC**

**WINDOWS 2016 Active Directory – 2CPU/8GB RAM**

**A screenshot of a computer

AI-generated content may be incorrect.**

**Domain : acme.local**

**User : DA\_Admin / Threathunt25**

**DNS Server**

**Password complexity off**

**Kerberoastable service account**

* **Powershell commands**
* $secpasswd = ConvertTo-SecureString -String "Password123" -AsPlainText -Force
* New-ADuser -Name 'SVC\_SQL' -GivenName 'SVC' -Surname 'SQL' -DisplayName 'SVC\_SQL' -AccountPassword $secpasswd -enabled 1
* Enable-ADAccount -Identity SVC\_SQL
* Add-ADGroupMember -Identity "Domain Admins" -Members SVC\_SQL
* setspn -T acme -Q \*/\*
* setspn -A SVC\_SQL/sql.acme.local acme\SVC\_sql

**WIN10 Machines student**

**Windows10 PRO (22H2) – 4CPU/16GB RAM**

**A screenshot of a computer

AI-generated content may be incorrect.**

**Naming convention WIN10\_XX**

* Local account studentxx (no local admin) -> password : Threathunt25
* Local account studentxx\_adm (local admin) -> password : Threathunt25

Installed software

* Python3.x
* Visual studio 2022
* Visual studio 2019
* Visual studio code
* Sysinternals (c:\Sysinternals)
  + Sysmon64.exe (config files in github repo)
* C:\DFIR
  + Labs
  + Mdbook source files
  + Mdbook.exe

…

A screenshot of a computer

AI-generated content may be incorrect.

* Defender settings
  + Exception for
    - C:\DFIR
    - C:\TEMP
    - C:\USERS\STUDENTxx\Desktop
  + Sample submission turned off
* Domain joined acme.local

KALI MACHINES student

Kali-2024-3

4CPU/16GB MEM

A screenshot of a computer

AI-generated content may be incorrect.

Naming convention : KALI\_XX

* Local account : kali/kali - password : Threathunt25

Installed software

* All software under **/OPT/DFIR** (git clone repo)
* Enable SSH service
* Enable XRDP
  + sudo apt install xrdp -y
  + sudo service xrdp start
  + sudo update-rc.d xrdp enable
  + sudo groupadd tsusers
  + sudo groupadd tsadmins
  + sudo usermod -aG tsusers rdp
  + sudo usermod -aG tsadmins rdp
  + sudo apt install kali-desktop-xfce -y
  + sudo service xrdp restart
  + **sudo update-alternatives --config x-session-manager**

A screenshot of a computer program

Description automatically generated

* Docker + docker-compose
  + sudo apt install docker.io
  + sudo apt install docker-compose
  + sudo usermod -aG docker $USER
  + newgrp docker
  + mkdir -p ~/.docker/cli-plugins/
  + curl -SL https://github.com/docker/compose/releases/download/v2.3.3/docker-compose-linux-x86\_64 -o ~/.docker/cli-plugins/docker-compose
  + chmod +x ~/.docker/cli-plugins/docker-compose
  + docker compose version
  + <https://www.digitalocean.com/community/tutorials/how-to-install-and-use-docker-compose-on-ubuntu-22-04>
* Havoc (apt install havoc)
* MSF
  + sudo apt remove metasploit-framework
  + rm -rf ~/.msf4
  + sudo apt autoremove
  + sudo apt update
  + sudo apt install metasploit-framework