**GITHUB REPO: https://github.com/crimsoncore/dfir**

**A diagram of a computer

AI-generated content may be incorrect.**

**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)
* git
* 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

Fixing the locale:

locale -a  
sudo nano /etc/locale.gen

“Uncomment the lines for en\_US.UTF-8 and any other locales you need. Save and exit the editor”.

sudo locale-gen

sudo update-locale LC\_ALL=en\_US.UTF-8 LANG=en\_US.UTF-8

locale

* 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 : Admin/Threathunt25
* Elastic + Kibana v8.17.1 (docker) -> compose and .env (hidden!) file in git repo
  + vmax size for elastic!!!
  + User : elastic/elastic
  + Als we van het hele SSL verhaal afkunnen van elastic zou beter zijn

**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

**Installed software**

* sysmon64
* winlogbeat 8.17.1 (c:\program files\winlogbeat)
  + config in github repo

**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

* Git for windows
* Python3.x
  + On windows first install python3
  + Then install python2.7 under c:\python27
    - in c:\sysinternalssuite
    - mklink python2.7 c:\python27\python.exe
    - add PATH C:\SysinternalsSuite
* Visual studio 2022 (C and C# SDK)
* Visual studio 2019 (C and C# SDK and v141 tools)
* A screenshot of a computer

  Description automatically generated
* Visual studio code
* HxD : <https://mh-nexus.de/en/downloads.php?product=HxD20>
* SystemInformer (new processhacker) : <https://www.systeminformer.com/downloads>
* PEStudio : https://www.winitor.com/download
* 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
    - Powershell commands (run as administrator):
      * Set-MpPreference -ExclusionPath C:\DFIR
      * Set-MpPreference -ExclusionPath C:\TEMP
      * Set-MpPreference -ExclusionPath C:\USERS\...\Desktop
      * PowerShell Set-MpPreference -SubmitSamplesConsent NeverSend
      * Set-MpPreference -MAPSReporting Disabled
* Domain joined acme.local
* winlogbeat 8.17.1 (c:\program files\winlogbeat)
  + config in github repo
* filebat 8.17.1 (c:\program files\filebeat)
  + For ETW logs
  + config in github repo

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)
* Git (preinstalled denk ik)
* Enable SSH service
* Enable XRDP (RDP user toevoegen in tsusers/tsadmins)
  + 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