# Synthèse

## Membres du groupe :

Tim, Aksel, Léo

## Lien GitHub :

https://github.com/AkselCaubel/SAE5.Cyber-Devcloud

## Bilan des rendus :

Au cours de ces semaines où nous avons travaillé sur le déploiement de solutions de défense dans un environnement vulnérable (GOAD), nous avons pu réaliser plusieurs tâches qui sont toutes réparties ci-dessous. Cela va de l'automatisation au déploiement de SIEMs connus comme Wazuh,Splunk et la suite Elastic jusqu'à l'attaque et donc la confirmation de fonctionnement de notre infrastructure. On peut résumer notre travail en quelques points importants :

## L'organisation :

- Utilisation de l'onglet 'Projects' de Github pour avoir un suivi des tâches. Ici *** /!\Pour voir cette partie vous devez accepter l'invitation reçus /!\ ***
- Utilisation de la plateforme Slack pour la communication.

## Le déploiement :

- Installation de l'environnement GOAD avec VirtualBox. Ici
- Installation de l'environnement GOAD avec Proxmox. Ici
- Installation de SIEMs : Splunk, Wazuh, ELK. Ici
- Mise en place d'un serveur de logs : OpenWEC. Ici
- Mise en place d'un accès distant VPN avec OpenVPN.

## L'automatisation :

- Scripts (Bash et Ansible) permettant l'installation de Wazuh sur une machine Debian 12 vierge ainsi que le déploiement des agents nécessaires (avec l'ajout de Sysmon) et qui configure également le serveur directement. Ici
- Scripts (Bash et Ansible) permettant l'installation de Splunk sur une machine Debian 12 vierge ainsi que le déploiement des agents nécessaires. Ici
- Mise en place avec Terraform et Ansible de la stack ELK avec le déploiement automatisé des agents. Ici

## La sécurisation :

- Réalisation d'un tutoriel complet pour créer des règles Wazuh ainsi que l'utilisation de l'active response (IPS). Ici
- Mise en place de l'IDS Suricata sur la stack ELK.
- Lecture de logs avec Chainsaw et Hayabusa. Ici

### Un PoC de fonctionnement :

- Détection d'une attaque de type Kerberoasting Ici

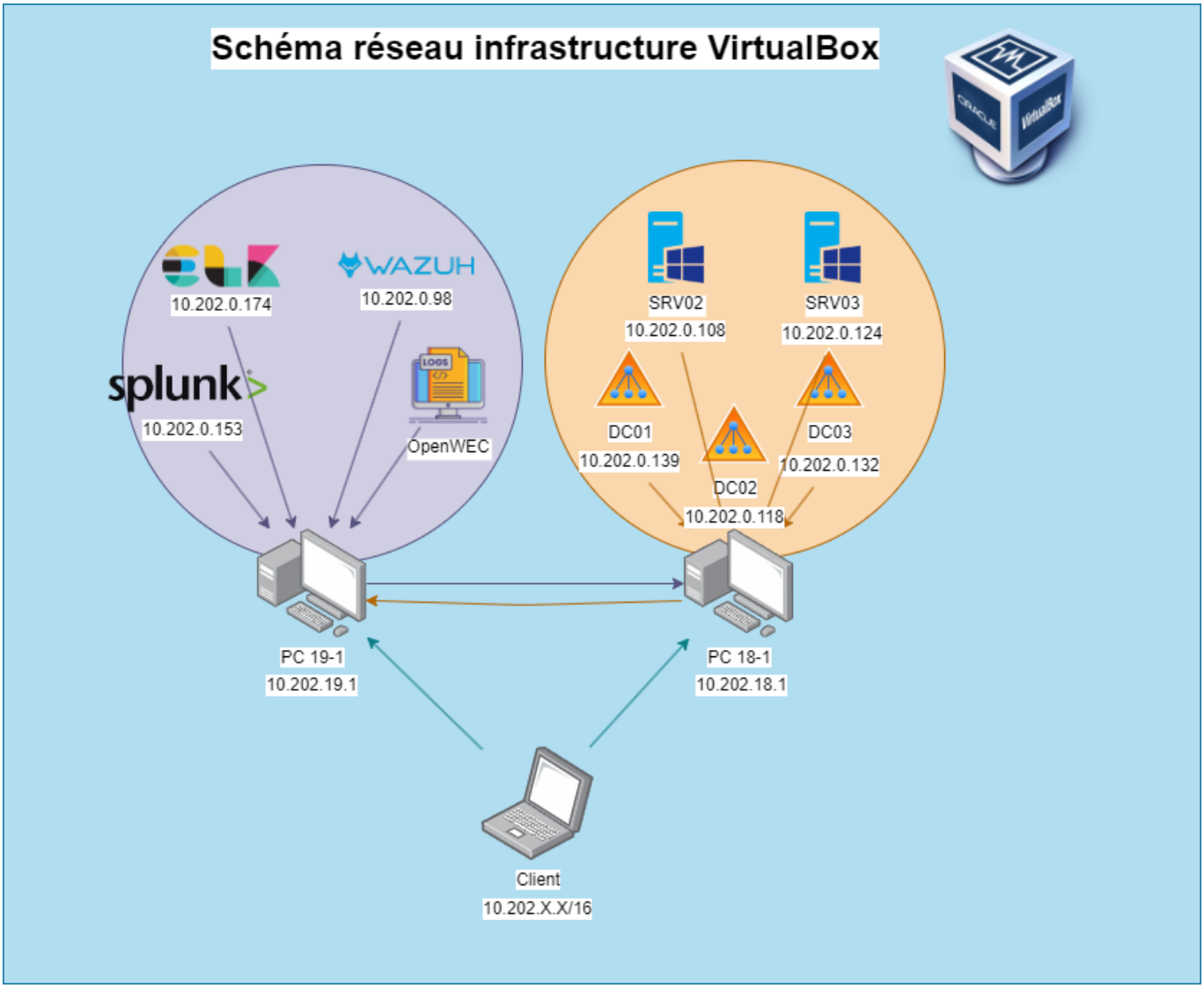
### Un audit de l'infrastructure GOAD :

- Réalisation d'une 'cheatsheet' pour permettre le pentest d'un environnement GOAD. Ici
- Audit de l'infrastructure GOAD en mode RedTeam. Ici

### Ce qu'on aurait voulu approfondir :

Nous n'avons malheureusement pas eu le temps d'approfondir plus la partie RedTeam sur le test de pénétration ainsi que sur le côté sécurité avec l'implémentation des règles Sigma.

### Schéma réseau de l'infrastructure virtualisée avec VirtualBox :




### Schéma réseau de l'infrastructure virtualisée avec Proxmox :

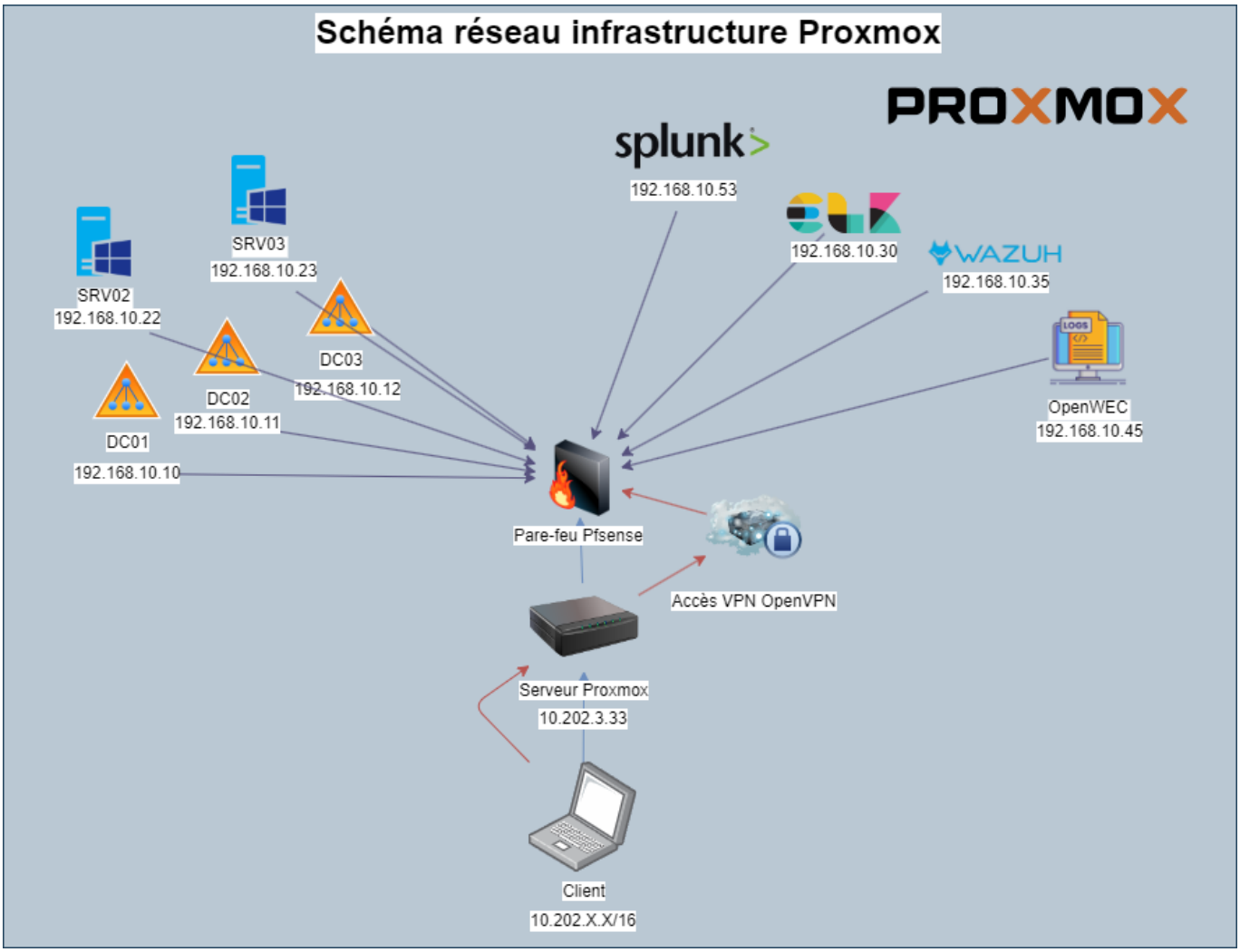


Schéma réseau infrastructure Proxmox
PROXMOX
splunk>
192.168.10.53
SRV03
192.168.10.23
192.168.10.30
WAZUH
192.168.10.35
SRV02
192.168.10.22
DC03
192.168.10.12
OpenWEC
192.168.10.45
DC02
192.168.10.11
DC01
192.168.10.10
Pare-feu Pfsense
Accès VPN OpenVPN
Serveur Proxmox
10.202.3.33
Client
10.202.X.X/16