Rapport

Mise en place d’une infra Blue Team.

Sommaire

1. Organisation du projet

1.1 - Contexte du projet

Pour notre projet fil rouge du **Ydays** “Lab SSI”, nous sommes partis sur la mise en place d’une infrastructure “Blue Team”, cette infrastructure sera composée d’une suite logicielle complète (SIEM, IDS, Honeypot) qui servira de lab de détection de test pour la Blue Team.

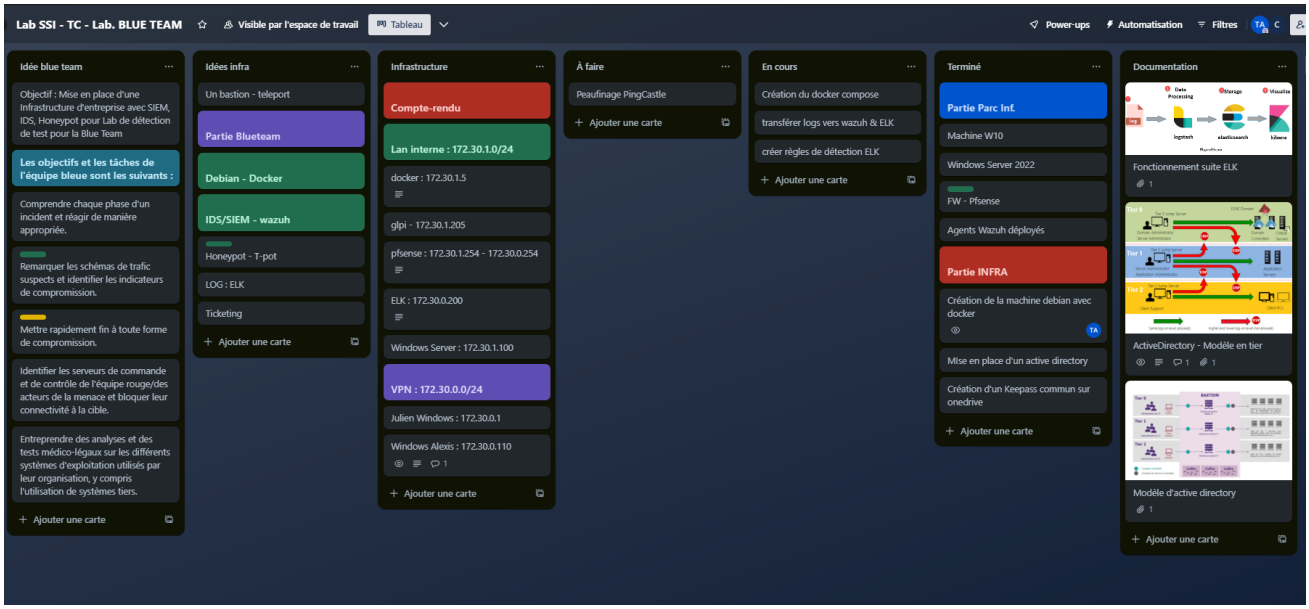
Nous avons décidé de faire ce projet principalement pour la découverte des applications open-source et de s’améliorer dans la création d’infrastructure sécurisée.

Le système d’annuaire de Microsoft (Active Directory) est prédominant sur le marché, il est important d’après nous de maximiser ces connaissances sur ce service afin de le sécuriser au mieux et contrôler les différentes surfaces d’attaques.

1.2 - Organisation du projet

Le projet sera organisé et planifié à travers un Trello, ce qui nous permettra de référencer toutes les étapes clés de notre projet, leurs progressions et quand celle-ci seront complétées.

Ce trello nous permet d’avoir une vision d’ensemble sur le projet et la direction à prendre pour sa mise en production le plus rapidement possible.



1.3 - Définition des besoins

Pour mener ce projet à bien, nous devons définir les différentes solutions applicatives que nous allons utiliser pour notre lab.

Pour définir ces applications, nous avons étudié et déterminé les outils qui composent un lab blue team.

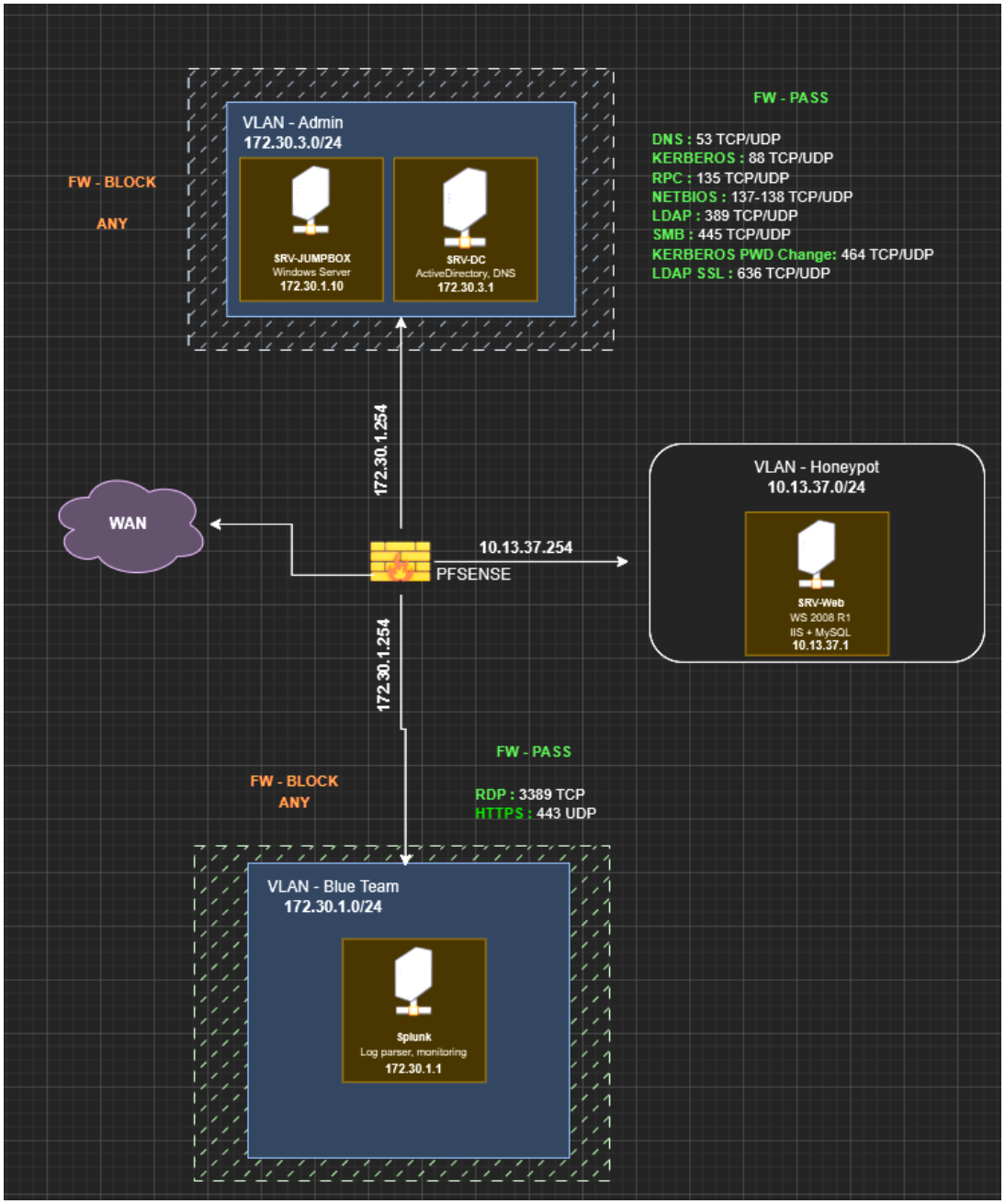
Un lab blue team, se compose principalement d'une plateforme de collecte de log et d'un SIEM/IDS pour la partie supervision, d'un honeypot pour contrer la Red Team et d'un serveur Windows qui embarquent les services "DNS","DHCP" et "Active Directory" pour notre infrastructure système et d'un firewall.

La mise en place d'autres solutions étaient envisageables mais par manque de temps, nous n'avons pas pu les mettre en place.

Nous avons songé à ajouter un scanner de vulnérabilité, un bastion pour le contrôle d'accès ou encore à une jumpbox afin de ne pas travailler directement depuis notre contrôleur de domaine.

2. Infrastructure réseau

2.1 - Schéma réseau



2.2 - Mise en place de la solution

Pour mettre en place une infrastructure sécurisée côté réseau, un cloisonnement réseau doit être réalisé. Pour réaliser une gestion des sous-réseaux et un contrôle des flux réseaux, nous sommes partis sur la solution gratuite **Pfsense**.
À travers cette application, nous allons pouvoir contrôler les entrées et sorties, faire notre cloisonnement réseau et permettre à nos sous-réseaux de communiquer entre eux.

2.3 - Fonctionnement local et distant

Comme indiqué dans notre schéma réseau, notre infrastructure sera décomposée en 3 sous-réseaux.

VLAN – Honeypot : 13.37.0.0/24
VLAN – Administration : 172.30.3.0/24
VLAN – Blue Team : 172.30.0.0/30

Les interfaces du Pfsense seront :

VLAN – Honeypot : 13.37.0.254
VLAN – Administration : 172.30.1.254
VLAN – Honeypot : 172.30.0.254

2.4 - Problématiques rencontrés

Malgré la simplicité et l'accessibilité de Pfsense, celle-ci reste une solution gratuite.
A de mainte fois, nous avons eu des problématiques avec la mise en place des sous-réseaux, les interconnexions entre nos deux cartes réseaux pour faire fonctionner nos VM.

Ce sont des problématiques inhérentes à notre infrastructure, si nous avions une infrastructure cloud ou physique avec des switchs, routeurs... L'infra aurait plus de stabilité.

2.5 - Axe d'amélioration(s) - Réseau

Nous aurions souhaité davantage pousser la configuration réseau, et faire la mise en place de règles de pare-feu avancées, par exemple.

De plus, limiter les plages IP du VLAN Admin ou du VLAN Honey-Pot afin de laisser des adresses IP libres sans réseaux. Il aurait fallu configurer ces VLANs avec un masque en 29 pour avoir 6 adresses IP libres et ainsi, nous permettre de prendre uniquement ce qui est nécessaire.

3. Infrastructure système

3.1 - Mise en place de la solution

L'équipe Blue Team protège les systèmes informatiques contre les attaques. Leur mission consiste à superviser le réseau, identifier les problèmes de sécurité, répondre aux incidents, améliorer la sécurité et instruire les utilisateurs sur les pratiques de sécurité appropriées.

Pour répondre à ces besoins nous avons sélectionné plusieurs applications.

Splunk – Pour la partie récupération Log et traitement. (faisant office également d'IDS)
Un ActiveDirectory – Un annuaire dédié Blue Team
Honeypot - Composé d'un Windows Server 2008 R2

Ces machines seront déployées à travers d'un script Vagrant et Ansible, afin d'automatiser leur configuration avec pour objectif de rendre ce Lab prêt à l'usage.

3.2 - Fonctionnement

Pour mettre en place ce lab, nous avons utilisé la solution applicative Vagrant qui permet le déploiement rapide de nos machines, il sera couplé à Ansible pour les serveurs Windows.

L'architecture du programme repose sur un fichier Vagrantfile qui instancie nos machines virtuelles (VMs) tout en configurant leur réseau, leur RAM, le nombre de CPU et leur nom.

Ensuite, pour personnaliser nos machines, nous exécuterons des commandes shell ou winrm pour installer les paquets ou applications requis.

Concernant la connectivité réseau, ces machines seront interconnectées via un pare-feu/routeur pfSense, comme décrit dans la section sur le réseau.

Une fois notre infrastructure opérationnelle, un domaine et un service Active Directory sont déployés sur le contrôleur de domaine, permettant l'authentification sur les machines dans ce domaine mais aussi à l'avenir un possible modèle en tier et faire de l'authentification LDAP via le serveur.

Enfin, toutes ces machines seront surveillées par un serveur Splunk, qui centralisera les journaux et les actions des utilisateurs.

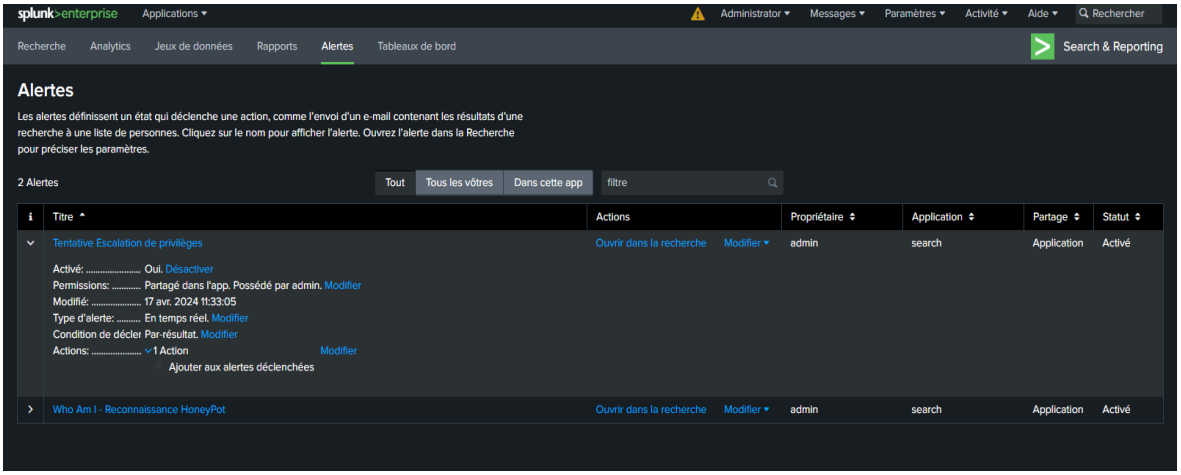
Nous avons choisi l'outil « **Splunk Entreprise** » pour surveiller l'activité de nos systèmes.
Splunk est une solution de « **Big Data** » servant à gérer ainsi qu'à analyser de grands volumes de données.

Elle est principalement utilisée pour collecter, indexer, surveiller en temps réel et analyser les données provenant de plusieurs sources (serveurs, applications, journaux réseaux et systèmes, etc..). Il est également possible de créer des tableaux de bord interactifs et des visualisations afin de mieux interpréter et comprendre les données collectées.

A noter que Splunk peut être aussi utilisé en dehors du domaine de la cybersécurité. On pourrait par exemple dans une entreprise vendant des chaussures, suivre le volume des ventes des produits.

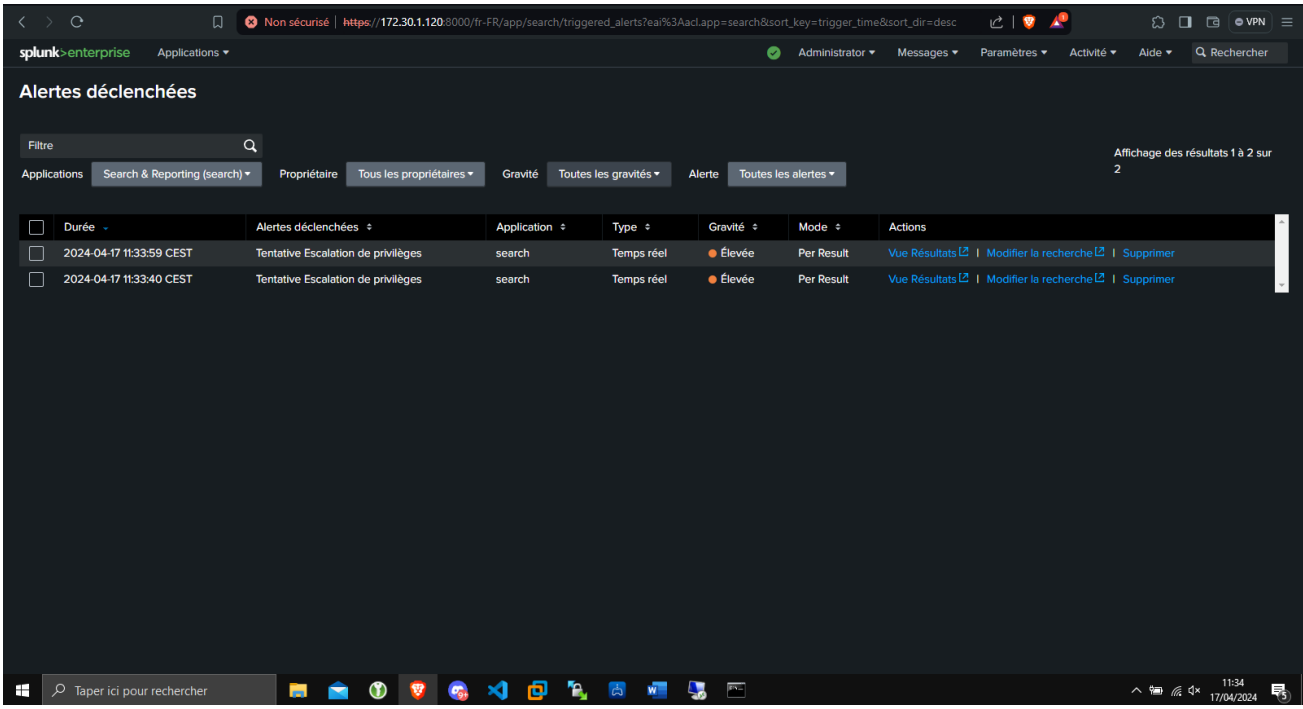
Nous avons décidé d'utiliser Splunk comme un outil de sécurité informatique afin d'améliorer la détection des menaces, mais aussi pour pouvoir faire de la réponse à incident.

Nous y avons également rajouté quelques règles de détection permettant de détecter en temps réel des comportements dangereux afin de mieux réagir en cas d'attaque et ainsi, améliorer la résilience de nos systèmes.



(Règles de détection mises en place)

Dès qu'un certain comportement dit « suspect » est détecté par les règles de détection, une alerte est créée dans l'onglet « Alertes déclenchées ».
Dans un premier temps, l'analyste détermine s'il s'agit d'un faux-positif, ou alors d'un vrai positif.
Dans un second temps, il fait les actions nécessaires pour résoudre l'incident.



(Alertes déclenchées)

A noter qu'il est possible de définir une action précise lors du déclenchement d'une alerte : par exemple, un script qui s'exécute lors du déclenchement.

3.3 - Problèmes rencontrés

Bien que Vagrant offre des avantages considérables en matière de déploiement, d'accessibilité et de disponibilité, nous avons rencontré plusieurs problèmes d'interopérabilité entre Vagrant / Ansible.

3.4 - Axe d'amélioration(s) - Système

Comme pour la partie réseau, nous pouvons davantage forcer sur la sécurisation système, Modèle en tier sur l'ActiveDirectory via un script HardenAD, la mise en place d'outils supplémentaires sur le serveur JumpBox...

On pourrait aussi avancer sur la configuration de Splunk, etc.

4 - Conclusion

Ce projet nous permis d'accroître nos connaissances et découvrir ces différentes solutions et leurs mises en place.

Nous aurions apprécié avoir plus de temps pour la mise en place de sécurisation et tenter de jouer avec le HoneyPot.