



MEMOIRE

Présenté à

**L’Institut Supérieur des Sciences Appliquées et de
Technologie de Gafsa**

(Département Informatique)

En vue de l’obtention du

MASTERE PROFESSIONNEL

Expert en Cyber Sécurité

Par

Aloui Radhia

**CONCEPTION ET VERIFICATION DE LA
COHERENCE D'UNE POLITIQUE DE SECURITE
DANS UN RESEAU LOCAL (CAS DE DRT_GAFSA)**

Soutenu le 06 / 06 /2023, devant le jury composé de

M. **MIRAOUI Moez** *Président*

M. **IBRAHMI Rabaa** *Rapporteur*

Mme. **AL YAOUI Nouha** *Encadreur*

A.U : 2022 – 2023

Dédicace

C'est un moment de plaisir de dédier ce modeste travail:

A l'Homme de ma vie, mon exemple éternel, mon soutien moral et source de joie et de bonheur, celui qui s'est toujours sacrifié pour me voir réussir, que Dieu te garde dans ton vaste paradis, à toi mon père.

A ma source de motivation, à ce qui n'a cessé de me soutenir, m'encourager et me guider tout au long de ma vie, à ma mère, que le Dieu la préserve et l'accorde une lange vie jusqu'à ce qu'elle me voit répondre à ses attentes.

A mon frère Kamel pour ses conseils, aide et encouragement.

A mes chères sœurs

Qui m'ont toujours aidée à dépasser les moments le plus difficiles, je vous souhaite tout le bonheur du monde et le succès. Que Dieu vous protège mes chères.

A mes frères

Qui m'ont toujours soutenu et poussé à donner le meilleur de moi-même.

Je vous porte tous un grand respect.

Je dédie également ce travail à mes amis et spécialement Souha et Taïssir pour leur soutien contenu, leur aide précieuse et leur amour.

Remerciements

Avant tout, je remercie, Dieu le tout puissant qui m'a donné la volonté, le courage et la patience et qui a guidé mes pas vers le droit chemin durant mes années d'études.

Mes estimes et ma profonde reconnaissance sont adressées particulièrement à Madame « Alyaoui Nouha » mon excellente encadrante pour son soutien, ses remarques directives et le temps qu'elle a consacré pour assurer l'encadrement de ce travail.

J'ai vous exprimé mon estime et mon profond respect

Du côté de DRT_Gafsa, je tiens à remercier Madame « Dhaouadi Moufida » pour sa disponibilité, ses conseils précieux et pour la confiance qu'elle a su m'accorder.

Je tiens à remercier sincèrement les membres de jury qui me font le grand honneur d'évaluer ce travail.

Mes vifs remerciements vont également à tous mes enseignants de l'ISSAT particulièrement à Monsieur « Fakhet Walid » pour sa générosité et la grande patience dont il a su faire preuve malgré son charge académique et professionnelle.

Enfin, je tiens à témoigner mes sincère remerciements à toutes les personnes qui ont contribué de près ou de loin au bon déroulement de mon stage et l'élaboration de ce modeste travail.

Sommaire

Liste des abréviations	6
<i>Liste des figures</i>	8
<i>List des tableaux</i>	9
<i>INTRODUCTION GENERALE</i>	1
Chapitre 1 : Présentation de DRT_Gafsa	3
1. Introduction	4
2. Présentation de société d'accueil.....	4
2.1. Tunisie Télécom	4
2.2. Les missions du Groupe	4
2.3. Organisation Fonctionnelle.....	5
2.4. Problématique.....	5
3. Conclusion.....	6
Chapitre 2 : La Sécurité Informatique.....	7
1. Introduction	8
2. La sécurité informatique.....	8
3. Besoins de la sécurité informatique.....	8
4. Menaces.....	9
5. Attaques.....	9
5.1. Les différents types d'attaques	9
5.2. Attaque d'accès	9
5.3. Attaque de modification	10
5.4. Attaque de saturation.....	11
5.5. Attaque de répudiation	12
6. Les Différents cibles d'attaque	13
7. Qu'est-ce qu'un Hacker ?	14
8. Les types de hackers.....	15
9. Application des analyses avancées : Solution SIEM.....	16
9.1. SIEM	16
9.2. Quelques solutions SIEM	17
10. Intérêt d'un SOC	18
10.1. Définition d'un SOC.....	18
10.2. Objectif d'un SOC.....	18
11. Conclusion.....	19

Chapitre3 :	20
Présentation de l'outil SPLUNK.....	20
1. Introduction	21
2. Présentation du SPLUNK.....	21
2.1. Définition et objectif du Splunk	21
2.2. Écosystème Splunk.....	21
2.3. Licences Splunk	21
2.4. Les avantages de Splunk :	23
3. Les Composants du Splunk	23
3.1. Forwarder.....	24
3.2. Indexeur.....	24
3.3. Search head.....	24
4. Que peut indexer Splunk ?	25
5. Fonctionnement de Splunk	26
5.1. Données d'entrée :	26
5.2. Analyseur :	27
5.3. Indexation.....	27
5.4. Recherche	27
6. Processus d'indexation.....	28
6.1. Phase d'entrée.....	29
6.2. Phase d'analyse	29
6.3. Phase d'indexation.....	29
7. VMware.....	29
8. Kali Linux.....	30
9. Sandbox	30
9.1. L'outil App-Any-Run	31
9.2. L'outil URL scan	32
9.3. VirusTotal	32
10. Conclusion.....	33
Chapitre 4 :	34
Application du Splunk.....	34
1. Introduction	35
2. Présentation du système proposé.....	35
2.1. Environnement matériel	35
2.2. Environnement logiciel	36
3. Mise en œuvre de la solution.....	37

3.1.	Installation de Splunk Entreprise.....	37
3.2.	Récupération des logs.....	40
4.	Configuration de la réception des Syslog sur Splunk	49
5.	Configurer le collecteur d'événements HTTP dans Splunk	52
6.	Création des alertes	56
7.	Tentative d'attaque par PyPhisher	59
8.	Les sandbox.....	63
8.1.	App Any Run.....	63
8.2.	URLScan	64
8.3.	VirusTotal	65
9.	Blocage de l'attaque phishing	66
10.	Conclusion.....	67
	<i>Conclusion Générale</i>	68
	<i>Bibliographie</i>	69
	<i>Résumé</i>	70

Liste des abréviations

ADSL : Asymetric Digital Subscriber Line

ARP : Address Resolution Protocol

API : Application Programming Interface

DRT_Gafsa : Direction Régional de Tunisie Télécom Gafsa

DOS : Denial Of Service

DDOS : Distributed Denial Of Service

DNS : Domaine Name System

DHCP : Dynamic Host Configuration Protocol

ICMP : Internet Control Message Protocol

IP : Internet Protocol

IoT : Internet of Things

JSON : JavaScript Object Notation

LDAP : Lightweigh Directory Access Protocol

MAC : Media Access Control

OSSIM : Open Source Security Information Management

PUP : Potentially Unwanted Program

SI : Système Informatique

SOC : Security Operations Center

SQL : Structured Query Language

SMS : Short Message Service

SIEM : Security Information Event Management

SIM : Security Information Management

SEM : Security Event Management

SNMP : Simple Network Management Protocol

TCP : Transmission Control Protocol

UDP : User Datagram Protocol

UF : Universal Forwarder

URL : Uniform Ressource Locator

VSAT : Very Small Aperture Termina

Liste des figures

Figure 1: Logo de la société Tunisie télécom	4
Figure 2: Organigramme Général du Groupe Tunisie Télécom [1]	5
Figure 3: Les différentes cibles d'attaque [9].....	13
Figure 4: Les Types de Hackers	14
Figure 5: Système de License de splunk	23
Figure 6: Principaux composants de splunk	25
Figure 7: Les différentes catégories d'indexation.....	26
Figure 8: Fonctionnalités de splunk.....	28
Figure 9: Logo VMware.....	30
Figure 10: Logo Kali Linux	30
Figure 11: La sandbox ANY.RUN	31
Figure 12: Interface URL scan	32
Figure 13: Interface utilisateur de VirusTotal	33
Figure 14: Topologie de l'infrastructure	35
Figure 15: Installation Splunk	37
Figure 16: : Création d'un compte administrateur.....	38
Figure 17: Panneau récapitulatif de l'installation.....	38
Figure 18: Étape d'installation de splunk	39
Figure 19: Interface utilisateur du splunk.....	39
Figure 20: Interface de Splunk Entreprise	40
Figure 21: Configurer la réception sur l'indexeur splunk	41
Figure 22: Configurer la transmission sur l'indexeur Splunk.....	41
Figure 23: Installer Splunk Universal Forwarder.....	42
Figure 24: Création d'un compte d'administrateur	42
Figure 25: Configurer serveur de déploiement	43
Figure 26: Configurer l'écoute sur l'indexeur	43
Figure 27: Fin de l'installation	44
Figure 28: Importer les données	45
Figure 29: La classe serveur.....	46
Figure 30: : Sélection des logs d'événements.....	46
Figure 31: Chois du l'index	47
Figure 32: Recherche des logs	48
Figure 33: Exporté des logs.....	49
Figure 34: Exporté des Syslog	50
Figure 35: Récupération des Syslog	51
Figure 36: Activation de collecteur d'évènement http	52
Figure 37: Evènement http : Paramètres d'entrée avancée	53
Figure 38: Création d'un jeton Event Collector	54
Figure 39: : La requête JSON.....	55
Figure 40: Evènement Hello world	56
Figure 41: Requête de recherche	57
Figure 42: Création d'alerte connection	58
Figure 43: Alerta de la tentative de connection	59

Figure 44: Installation python3.....	60
Figure 45: installation des outils de git.....	60
Figure 46: exécution PyPhisher	61
Figure 47: Choisir l'option Facebook	61
Figure 48: URL malicieux	62
Figure 49: Données de la victime	63
Figure 50: L'analyse de l'URL avec ANY_RAN.....	64
Figure 51: L'analyse de l'URL avec URLScan.....	65
Figure 52: L'analyse de l'URL avec VirusTotal	66

Liste des tableaux

Tableau 1: Caractéristiques techniques.....	36
---	----

INTRODUCTION GENERALE

La sécurité informatique est devenue un enjeu important pour les entreprises. Les systèmes d'informations sont d'une importance primordiale, leur protection est donc une caractéristique nécessaire. De manière générale, la sécurité des systèmes d'information consiste à protéger les ressources de l'organisation afin qu'elles soient utilisées dans le contexte prévu. Cependant, de nouveaux problèmes émergents aujourd'hui autorisent les utilisateurs malveillants d'accéder à ces ressources et de lancer des attaques à partir de diverses sources.

Il est nécessaire pour une entreprise de développer des outils pour la surveillance proactive. Ces outils fournissent un système d'alerte immédiat dès qu'un dysfonctionnement ou une menace d'intrusion est détecté alors les problèmes potentiels sont identifiés avant qu'ils ne surviennent. Les utilisateurs reçoivent des informations concises leur permettant l'étude des incidents. L'évolutivité de l'infrastructure informatique est également prévue.

DRT_Gafsa est une société de télécommunications qui offre une large gamme de services pour les particuliers et les entreprises. Elle dispose d'un réseau étendu et local via de fibres optiques. Il est donc important pour l'entreprise de mettre en place des mesures de sécurité solides pour protéger leurs données et leurs systèmes.

C'est dans ce cadre que s'inscrit notre travail qui consiste à la mise en place d'une solution SIEM (Security Information and Event Management) pour l'entreprise DRT_Gafsa. Au cours de ce projet, nous allons nous intéresser à l'étude et la mise en place d'une solution Splunk.

Le présent mémoire est organisé de la façon suivante :

- Le premier chapitre est consacré à la présentation de l'entreprise de Direction Régionale de Tunisie Telecom DRT_Gafsa
- Le deuxième chapitre présente des généralités sur la sécurité informatique, allant de la généralité sur les menaces, en passant par les applications des analyses avancées, la définition de SOC et leur objectif. Nous allons également étudier l'importance de la sécurité informatique.
- Le troisième chapitre présente la solution SPLUNK dont lequel ses composants et son fonctionnement seront décrits.

- Le dernier chapitre est consacré au déploiement de la solution SIEM choisie (SPLUNK). Les différentes étapes à suivre pour la bonne installation et la configuration de cette dernière ont été exploités.

Chapitre 1 : Présentation de DRT_Gafsa

1. Introduction

Les réseaux se développent en fonction de leurs caractéristiques et besoins. Ils deviennent aujourd’hui une infrastructure indispensable dans tous les domaines de la vie. Cependant, les menaces et les attaques sur les réseaux prennent de nouvelles mises à jour représentant les pires ennemis de cette technologie de ces derniers. Pour cela, la sécurité des communications est devenue une préoccupation importante des utilisateurs et des entreprises. Dans ce chapitre nous présentons l’entreprise de Direction Régionale de Tunisie Telecom DRT_Gafsa. Nous nous discutons également le problématique de notre stage.

2. Présentation de société d'accueil

2.1. Tunisie Télécom

Tunisie Télécom est un opérateur de télécommunications qui a comme objectif de renforcer l'infrastructure des télécommunications en Tunisie et tend à améliorer le taux de couverture sur ses réseaux fixe et mobile.

Sa politique de diversification des services lui a permis d'offrir à ses clients une gamme de services au niveau de la téléphonie fixe, de la téléphonie mobile (LTE, UMTS...), et transmission par satellite (VSAT) et l'ADSL.

Avec près de 7 millions d'abonnés, le groupe s'intéresse aujourd'hui aux valeurs de proximité, de fiabilité et d'accessibilité en visant une meilleure qualité de service à travers de ses 120 agences commerciales, ses multiples centres d'appels et ses différents points de vente.



Figure 1: Logo de la société Tunisie télécom

2.2. Les missions du Groupe

Le Groupe “Tunisie Télécom” est chargé d’un ensemble d’opérations, parmi lesquelles on cite :

- L’installation, l’exploitation et l’entretien des réseaux publics de télécommunications.
- La contribution et la participation au développement des études et des recherches scientifiques liées au secteur des télécommunications.

2.3. Organisation Fonctionnelle

L'organigramme actualisé le 16/02/2023 du Tunisie Telecom est le suivant :

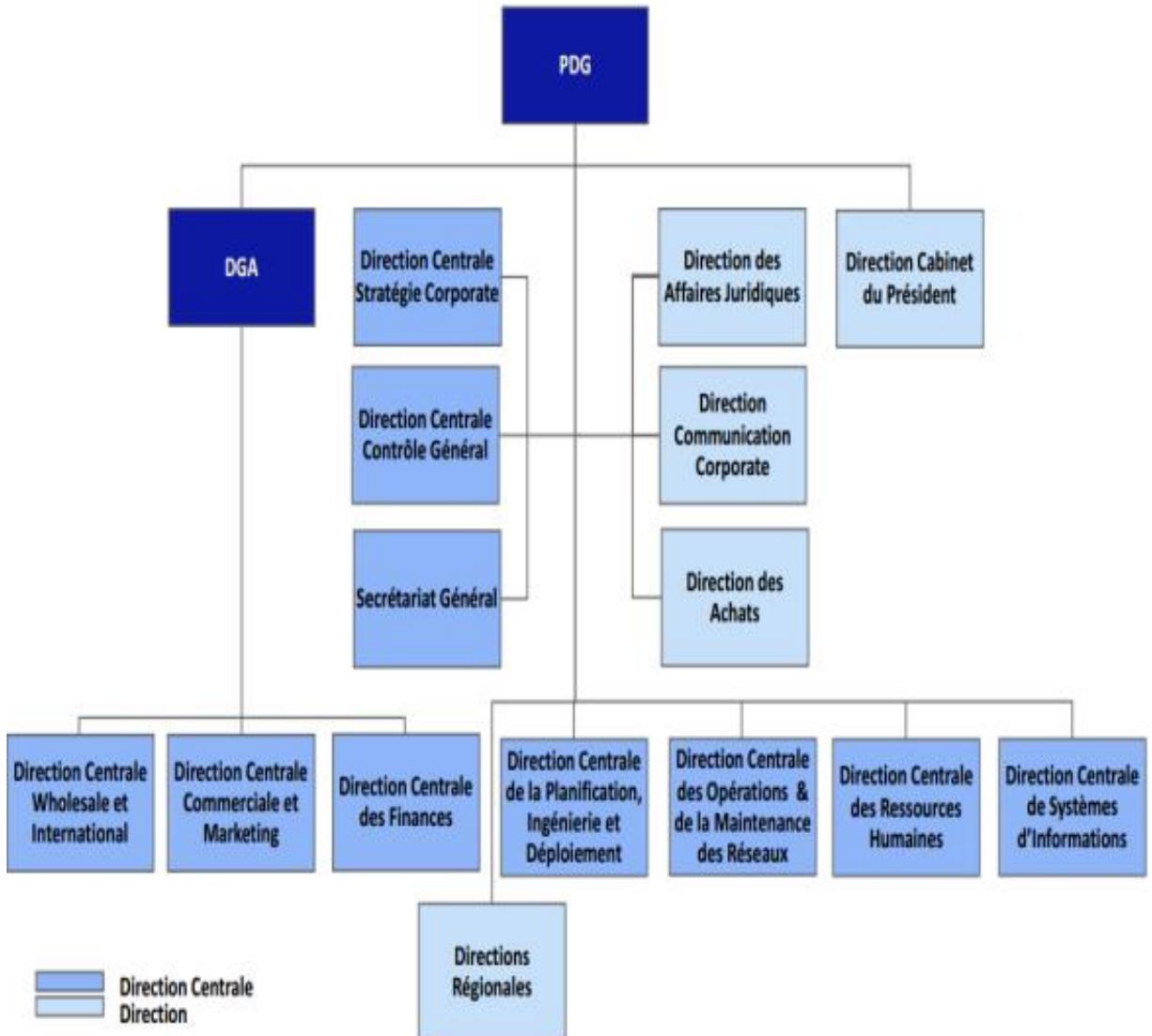


Figure 2: Organigramme Général du Groupe Tunisie Télécom [1]

2.4. Problématique

L'entreprise de Direction Régionale de Tunisie Telecom DRT_Gafsa utilise encore l'antivirus client-serveur Kaspersky. Bien que Kaspersky ait de nombreuses fonctionnalités et avantages, il présente également quelques inconvénients et limites potentiels en matière de sécurité informatique : Préoccupations en matière de confidentialité. Il peut avoir un impact sur les performances des systèmes, en particulier sur les ordinateurs plus anciens ou moins puissants.

Kaspersky possède une base de données de signatures de logiciels malveillants étendue et utilise des algorithmes sophistiqués pour détecter les menaces. Par contre, plusieurs logiciels malveillants peuvent s'échapper de sa détection.

Il est à noter également que la protection de Kaspersky dépend de la mise à jour régulière du logiciel, donc si les mises à jour ne sont pas effectuées régulièrement, les nouvelles menaces pourraient ne pas être détectées et la protection pourrait être compromise.

Nous n'oubliions pas une étape importante pour assurer la sécurité informatique au niveau de l'entreprise, c'est la nécessité de gestion des journaux. Comme les journaux enregistrent toute action prise sur un réseau, leur volume risque d'être très important, au point où il devient très difficile de les gérer et donc, de les exploiter facilement.

De tous ces problèmes, le besoin d'une solution sécurisée qui automatise l'exploitation des logs tout en fournissant plus de visibilité sur le système, est né. Et le SIEM est la réponse à ce besoin. Notre application de supervision doit offrir donc plus de simplicité d'utilisation, plus d'efficacité mais aussi plus de visibilité, elle devra non seulement tenir compte des problèmes actuels mais également être capable d'évoluer facilement et efficacement au rythme des besoins.

A la fin de notre travail, nous devons mettre en place une solution qui permet d'assurer le Monitoring en temps-réel, créer et envoyer une notification d'alerte, identifier les problèmes de sécurité dès que possible aussi de centraliser, analyser et visualiser les sources de données pour vérifier les menaces.

3. Conclusion

Ce chapitre fait l'objectif de la présentation de l'entreprise ainsi qu'aux besoins de la DRT Gafsa. Le chapitre suivant s'intéresse de la sécurité informatique et leurs objectifs, les différents types d'attaque ainsi que l'intérêt du SOC.

Chapitre 2 : La Sécurité Informatique

1. Introduction

Les réseaux se développent en fonction de leurs caractéristiques et besoins. Ils deviennent aujourd’hui une infrastructure indispensable dans tous les domaines de la vie. Cependant, les menaces et les attaques sur les réseaux prennent de nouvelles mises à jour représentant les pires ennemis de cette technologie de ces derniers. Pour cela, la sécurité des communications est devenue une préoccupation importante des utilisateurs et des entreprises.

2. La sécurité informatique

La sécurité informatique protège l’intégrité des technologies de l’information comme les systèmes, les réseaux et les données informatiques contre les attaques, les dommages ou les accès non autorisés. Pour préserver leur compétitivité dans le contexte de la transformation numérique, les entreprises doivent comprendre comment adopter des solutions de sécurité informatique qui sont intégrées dès la phase de conception.

3. Besoins de la sécurité informatique

La sécurité est essentielle pour la protection de trois caractéristiques critiques des systèmes et de l’information qu’ils traitent et maintiennent, à savoir [2] :

- **Disponibilité** : assure que l’information et les systèmes soient accessibles et utilisables par les parties autorisées aux moments où elles en ont besoin.
- **Confidentialité** : assure que l’information soit protégée contre toute divulgation accidentelle ou malveillante aux parties non autorisées.
- **Intégrité** : assure que l’information et les systèmes soient protégés contre toute modification ou destruction accidentelle ou malveillante.

A côté de ces caractéristiques de bases nous rencontrons également les composantes suivantes :

- **Authentification** : assure l’identification d’un individu, d’une entité mais également l’origine de l’information ou encore d’une opération effectuée sur celle-ci.
- **Autorisation** : assure le contrôle du type d’activités ou d’informations qu’une personne ou entité est autorisée à effectuer ou accéder.
- **Non-répudiation** : assure le fait qu’une personne ou entité ne puisse nier avoir effectué une activité. Dans le domaine du courriel, l’irrévocabilité est utilisée pour assurer que le destinataire ne pourra nier avoir reçu l’information, et assurer que l’expéditeur de la source de l’information ne peut nier avoir envoyé l’information.

4. Menaces

La menace désigne l'exploitation d'une faiblesse de sécurité par un attaquant, qu'il soit interne ou externe à l'entreprise. La probabilité qu'un événement exploite une faiblesse de sécurité est généralement évaluée par des études statistiques, même si ces derniers sont difficiles à réaliser.

- **Menaces graves** : Il s'agit de menaces classiques capables d'effectuer par elles-mêmes des actions destructrices et illégales (suppression et vol de données, pannes de réseau, etc.) au sein du système. Ces menaces incluent les logiciels traditionnellement connus sous le nom de Malware. Ce sont des vers, des virus et des chevaux de Troie.
- **Menaces mineures** : Ces menaces sont considérées comme moins dangereuses, mais peuvent être utilisées par des tiers pour effectuer des actions malveillantes. De plus, la présence de menaces même mineures dans le système démontre sa vulnérabilité. Les experts en sécurité informatique décrivent de telles menaces comme des logiciels "gris" (graywares) ou des "logiciels potentiellement non sollicités" (PUP - Programmes Potentiellement Indésirables), qui sont les types de logiciels suivants : adwares, dialers, canulars, riskwares et hacktools [3].

5. Attaques

Dans ce qui suit, nous présenterons les différents types d'attaques

5.1. Les différents types d'attaques

Il existe un grand nombre d'attaques permettant à une personne mal intentionnée de s'approprier des ressources, de les bloquer ou de les modifier. Certaines requièrent plus de compétences que d'autres, en voici quelques-unes.

5.2. Attaque d'accès

Une attaque d'accès est une tentative d'accès à l'information par une personne non autorisée. Ce type d'attaque concerne la confidentialité de l'information, par exemple : Sniffing, chevaux de Troie, porte dérobée, injection SQL et craquage de mot de passe....

- Sniffing : L'écoute du réseau ou le Sniffing est une technique qui consiste à analyser le trafic réseau.
- Ce type d'attaque est utilisé par les pirates informatiques pour obtenir des mots de passe. Grâce à un logiciel appelé renifleur de paquets (Sniffer), qui permettre d'intercepter tous les paquets qui circulent sur un réseau même ceux qui ne sont pas destinés (aux pirates).

- Balayage de port : L'attaque par balayage de port (Ports Scanning) permet à découvrir la liste des ports de communication exploitables (ouverts, fermés et filtrés). Grâce à cette technique, les attaquants peuvent trouver des ports ouverts et attaquent les services qui s'exécutent sur ces ports. Les détails liés au réseau tels que l'adresse IP, l'adresse MAC, le routeur, la passerelle de filtrage, les règles de pare-feu... peuvent être connus par cette attaque. Il existe diverses techniques de balayage de ports qui sont le balayage TCP, UDP, SYN, FIN, ACK, etc.
- Attaque par injection SQL : L'injection SQL est devenue un problème courant qui affecte les sites Web exploitant des bases de données. Elle se produit lorsqu'un malfaiteur exécute une requête SQL sur la base de données via les données entrantes du client au serveur. Des commandes SQL sont insérées dans la saisie du plan de données (par exemple, à la place du nom d'utilisateur ou du mot de passe) afin d'exécuter des commandes SQL prédéfinies. Un exploit d'injection SQL réussi peut lire les données sensibles de la base de données, modifier (insérer, mettre à jour ou supprimer) les données de la base de données, exécuter des opérations d'administration de la base de données (par exemple la fermer), récupérer le contenu d'un fichier spécifique, et, dans certains cas, envoyer des commandes au système d'exploitation.
- Le craquage de mots de passe : Cette technique consiste à essayer plusieurs mots de passe afin de trouver le bon. Elle peut s'effectuer à l'aide d'un dictionnaire des mots de passe les plus courants (et de leur variantes), ou par la méthode de brute force (toutes les combinaisons sont essayées jusqu'à trouver la bonne). Cette technique longue et fastidieuse, souvent peu utilisée à moins de bénéficier de l'appui d'un très grand nombre de machines.

5.3. Attaque de modification

Une attaque de type « modification » consiste, pour un attaquant, à tenter de modifier des informations. Ce type d'attaque est dirigé contre l'intégrité de l'information, par exemple : virus, vers et chevaux de Troie

- Virus : Ce type de menaces informatiques se caractérise par sa capacité à introduire son code dans le code d'exécution d'autres logiciels. Cette pénétration porte le nom d'infection. Dans la plupart des cas, le fichier infecté devient lui-même porteur du virus et le code introduit n'est plus conforme à l'original. La majeure partie des virus est conçue pour détériorer ou détruire les données du système.

- Vers : Tout comme les virus, ils sont capables de s'auto répliquer et de diffuser leurs copies, mais n'affectent pas d'autres logiciels ni fichiers (ils n'ont pas besoin des fichiers host pour se répandre). Les vers pénètrent dans un ordinateur via un réseau mondial ou local (souvent via une pièce jointe dans un email) et ils envoient massivement leurs propres copies à d'autres ordinateurs du réseau.
- Chevaux de Troie : Ce type de logiciels malicieux n'est pas capable de s'auto répliquer ni d'infecter d'autres logiciels. Les Chevaux de Troie se substituent à des programmes très utilisés, effectuent les mêmes actions qu'eux ou en imitent le fonctionnement. Dans le même temps, ils effectuent des actions malveillantes dans le système (suppriment ou endommagent des fichiers ou des données, envoient les données confidentielles de l'utilisateur) ou donnent aux pirates un accès à l'ordinateur pour, par exemple, porter atteinte au propriétaire de l'ordinateur touché.

5.4. Attaque de saturation

Les attaques par saturation sont des attaques informatiques qui consistent à envoyer des milliers de messages depuis des dizaines d'ordinateurs, dans le but de submerger les serveurs d'une société, de paralyser pendant plusieurs heures son site Web et d'en bloquer ainsi l'accès aux internautes. Cette technique de piratage assez simple à réaliser est jugée comme de la pure malveillance. Elle ne fait que bloquer l'accès aux sites, sans en altérer le contenu. Il existe différente attaque par saturation : Flooding, le TCP-SYN Flooding, ...

- Attaques par déni de service (DoS) et par déni de service distribué (DDoS) : Une attaque par déni de service submerge les ressources d'un système afin que ce dernier ne puisse pas répondre aux demandes de service. En général, le déni de service va exploiter les faiblesses de l'architecture d'un réseau ou d'un protocole. Une attaque DDoS vise elle aussi les ressources d'un système, mais elle est lancée à partir d'un grand nombre d'autres machines hôtes infectées par un logiciel malveillant contrôlé par l'attaquant.[4]
- Attaque TCP SYN flood : La machine de l'attaquant inonde de demandes de connexion la petite file d'attente de traitement du système cible, mais elle ne réagit pas lorsque le système cible répond à ces demandes. Le système cible se met alors à temporiser en attendant la réponse de la machine de l'attaquant, ce qui fait planter le système ou le rend inutilisable lorsque la file d'attente de connexion se remplit.
- Attaque Smurf : Cette attaque implique d'usurper une adresse IP et d'utiliser l'ICMP pour saturer de trafic un réseau cible. Cette méthode d'attaque utilise des demandes d'écho

ICMP ciblant des adresses IP de diffusion. Ces demandes ICMP proviennent d'une adresse usurpée.

5.5. Attaque de réputation

La réputation est une attaque contre la responsabilité. Autrement dit, la réputation consiste à tenter de donner de fausses informations ou de nier qu'un événement ou une transaction se soient réellement passé. Par exemple l'homme de milieu, IP Spoofing, Phishing...

➤ L'homme de milieu (Man In the Middle) : le système attaquant s'impose dans le chemin de communication entre deux autres systèmes.

Il s'agit généralement une attaque contre les protocoles de réseau (IP, ARP, DNS, DHCP...) qui entraîne une mauvaise orientation du trafic.

L'attaquant peut ensuite écouter, modifier ou encore bloquer la communication.

➤ IP Spoofing : Les intrus utilisent IP Spoofing pour convaincre un système qu'il est en communication avec une entité connue de confiance afin de fournir l'intrus avec un accès au système.

Usurpation d'adresse IP implique la modification d'un paquet au niveau de TCP, qui est utilisé pour attaquer les systèmes connectés à Internet qui offrent divers services TCP/IP. L'attaquant envoie un paquet avec une adresse IP source de, un hôte connu de confiance au lieu de sa propre adresse IP source à un hôte cible. L'hôte cible peut accepter le paquet et agir sur elle. Il existe des variantes car le *Spoofing* peut se faire aussi sur des adresses e-mail, des serveurs DNS ...

➤ Attaques phishing : L'hameçonnage consiste à envoyer des e-mails qui semblent provenir de sources fiables dans le but d'obtenir des informations personnelles ou d'inciter les utilisateurs à faire quelque chose. Cette technique combine ingénierie sociale et stratagème technique. Elle peut impliquer une pièce jointe à un e-mail, qui charge un logiciel malveillant sur votre ordinateur. Elle peut également utiliser un lien pointant vers un site Web illégitime qui vous incite à télécharger des logiciels malveillants ou à transmettre vos renseignements personnels. [5]

- **Spear phishing** : ces messages électroniques sont envoyés à des personnes spécifiques au sein d'une organisation, généralement des titulaires de comptes à haut privilège.

- **Smishing** : à l'aide de messages SMS, les attaquants incitent les utilisateurs à accéder à des sites malveillants depuis leur smartphone.

- **Vishing** : les attaquants utilisent un logiciel de changement de voix pour laisser un message disant aux victimes ciblées qu'elles doivent appeler un numéro où elles peuvent être escroquées.

6. Les Différents cibles d'attaque

Une "attaque informatique" ou "cyberattaque" est un acte délibéré et malveillant qui utilise un réseau informatique pour endommager des informations ou ses processeurs. Cette dernière à plusieurs cibles [9].



Figure 3: Les différentes cibles d'attaque [9]

Attaque sur les réseaux : De nombreux protocoles réseau ont historiquement été implémentés sans le concept de sécurité. Les éléments d'un système d'information est nécessaire pour cela il communique à travers plusieurs canaux configurés. Les canaux secrets sont des canaux de communication possibles, mais ils ne doivent pas être utilisés comme canaux de communication lors de la conception de système. Par conséquent, les canaux secrets peuvent envoyer des informations sans l'autorisation ou la connaissance du propriétaire de l'information ou de l'administrateur réseau.

Attaques sur le système d'exploitation : Les services de l'infrastructure étant fournis au-dessus du système d'exploitation, plusieurs attaques impliquent leur exploitation. Par conséquent, un système d'exploitation non maintenu ou obsolète en est souvent la principale raison. De plus, les vulnérabilités récemment découvertes mais non corrigées sont une tactique courante utilisée par les attaquants.

Attaques sur les applications et les logiciels : Les applications présentent souvent des vulnérabilités qui peuvent être causées par une mauvaise exécution. Cette mise en œuvre

inadéquate peut être causée par une négligence lors des étapes d'analyse et de conception de la sécurité, un manque de compétences/de sensibilité des développeurs, des problèmes de synchronisation et un manque de tests de sécurité pendant le développement ou la mise en œuvre. Les experts en sécurité发现 de nombreuses vulnérabilités logicielles et des pirates.

7. Qu'est-ce qu'un Hacker ?

Un hacker est une personne très intelligente avec des compétences techniques qui utilise ces connaissances pour chercher et exploiter les failles de sécurité informatique d'un système afin de pouvoir récupérer un accès non autorisé à voler des informations confidentielles faire des modifications....

Il existe **différents types de hackers** qui utilisent leurs compétences de différentes manières, certains sont éthiques et d'autres malveillants, certains cherchent à protéger les systèmes, d'autres cherchent à les compromettre. La définition exacte de ce qu'est un hacker, un pirate ou encore un cybercriminel varie en fonction **du contexte et des motivations**.



Figure 4: Les Types de Hackers

8. Les types de hackers

- **Les White Hat Hackers**

Ce sont les bons Hackers qui permettent de protéger les systèmes informatiques des entreprises. Lorsque ces hackers confrontent des failles, ils permettent de les corriger ou bien les signaler aux éditeurs des logiciels. [6].

- **Les Grey Hat Hacker**

C'est la personne la plus floue, c'est à dire parfois elle est éthique et parfois non. Ils trouvent le plaisir de déjouer les systèmes de sécurité informatique pour avoir une idée sur leur capacité.

Ce type de hacker, n'applique pas leurs connaissances pour des raisons malveillantes. Par exemple, lorsqu'il déjoue le système informatique d'une entreprise, il leur donne un minimum de temps pour qu'elle puisse corriger la faille et récupérer son système.[6]

- **Les Blacks Hat Hackers**

Ce sont les cybercriminels qui possèdent une mauvaise intention. Ils ont pour but l'exploitation de leurs compétences et connaissances pour de mauvaises raisons. Ils font exprès de nuire aux systèmes informatiques des entreprises à travers différentes méthodes comme par exemple l'escroquerie, le vol de données, l'espionnage...

- **Script Kiddies**

Les Script Kiddies sont des mineurs qui n'ont pas une connaissance complète du processus de piratage. Ils essayent de pirater le système, les réseaux ou les sites Web avec des scripts d'autres hackers. L'intention derrière le piratage est simplement d'attirer l'attention.

- **Green Hat Hackers**

Les pirates au chapeau vert sont des types de pirates qui apprennent les ficelles du piratage. Ils sont légèrement différents des Script Kiddies en raison de leur intention qui est de s'efforcer et d'apprendre à devenir des hackers à part entière. Ils recherchent des occasions d'apprendre auprès de pirates expérimentés.

- **Blue Hat Hackers**

Les Blue Hat Hackers sont des types de hackers similaires aux Script Kiddies. L'intention d'apprendre est absente. Ils utilisent le piratage comme une arme pour gagner en popularité auprès de leurs semblables.

Ils utilisent le piratage pour régler leurs comptes avec leurs adversaires. Les Blue Hat Hackers sont dangereux en raison de l'intention derrière le piratage plutôt que de leurs connaissances.

- **Red Hat Hackers**

Red Hat Hackers sont les types de hackers qui ressemblent aux hackers blancs. Les pirates au chapeau rouge ont l'intention d'arrêter l'attaque des pirates au chapeau noir. La différence entre les hackers Red Hat et les hackers white Hat est en train de pirater par intention reste la même. Les hackers Red Hat sont assez impitoyables lorsqu'ils traitent avec des hackers Black Hat ou contrecarrent les logiciels malveillants. Les hackers Red Hat continuent d'attaquer et peuvent finir par devoir remplacer l'ensemble du système mis en place.

- **Suicide Hackers**

Les hackers suicides sont ceux qui visent à détruire les infrastructures critiques pour une "cause" et n'ont pas peur de la prison ou de tout autre type de punition.

- **State sponsored hackers**

Les pirates sponsorisés par l'état sont recrutés par les gouvernements pour accéder aux données secrètes d'autres gouvernements.

- **Hacktivist**

Les activistes pénètrent dans les systèmes gouvernementaux ou d'entreprise en signe de protestation. Ils utilisent leurs compétences pour promouvoir un agenda politique ou social. Les cibles sont généralement des agences gouvernementales ou de grandes entreprises.

9. Application des analyses avancées : Solution SIEM

9.1. SIEM

SIEM est un système centralisé qui offre une visibilité totale sur l'activité du réseau. Il assimile et parcourt un grand volume de données en quelques secondes pour détecter et signaler les comportements inhabituels. Il génère ensuite des alertes de sécurité lorsqu'il identifie des problèmes potentiels et il nous permet ainsi de réagir aux menaces en temps réel et il aide à la surveillance et la conformité de la sécurité et de l'activité des utilisateurs.

SIEM est aussi connu comme système d'analyse de la sécurité (Big Data), système de renseignement sur les cybermenaces. Il est composé de deux concepts qui sont : SEM (gestion des événements de sécurité) et le SIM (gestion des informations de sécurité).

- **SEM**

Il traite les données des journaux et des événements des dispositifs de sécurité systèmes et applications en temps réel pour assurer la sécurité la surveillance, la corrélation des événements et les réponses aux incidents. SIEM soutient les activités de surveillance des menaces externes et internes de l'organisation de la sécurité informatique et améliore la gestion des incidents [7].

- **SIM**

Il fournit la gestion des journaux, la collecte, la création des rapports et analyse les données des systèmes hôtes et des applications, des périphériques réseau et de sécurité. Il prend en charge les rapports de conformité réglementaire, la gestion interne des menaces et surveillance de l'accès aux ressources. SIM s'occupe l'utilisateur privilégié et les activités des surveillances de l'accès aux ressources, ainsi que les besoins des rapports de l'audit internet les organismes de conformité [7].

Les SIEM utilisent des étapes de récupération, analyse et gestion de l'information, qui consiste la collecte, la normalisation, l'agrégation, la corrélation, le reporting et la réponse.

9.2. Quelques solutions SIEM

Il existe plusieurs solutions qui sont proposées par plusieurs en-têtes. Certaines sont payantes parce qu'elles sont propriétaires comme SPLUNK, SolarWinds, IBM QRadar, McAfee et LogRhythm, d'autres sont libres ou gratuites (open Source) comme OSSIM, SIEMonster, ELK et Graylog.

Avant de déterminer la solution qui convient à notre projet, nous allons faire une brève présentation de certaines solutions, notamment IBM QRadar, McAfee, ELK, LogRhythm, SPLUNK.

IBM QRadar : QRadar SIEM consolide les données d'événement de source de journal à partir de milliers de périphériques distribués et de points de terminaison d'application sur le réseau. Il effectue immédiatement des activités de normalisation et de corrélation sur les données brutes pour différencier les menaces réelles des faux positifs.

McAfee : McAfee Enterprise Security Manager offre une visibilité en temps réel sur le monde extérieur (données sur les menaces, sources de réputation et statut de vulnérabilité) et une vue des systèmes, des données, des risques et des activités au sein de l'entreprise.

ELK (Elasticsearch Logstash Kibana) : Pile ELK (ELK Stack) est une collection de trois produits open-source : Elasticsearch, Logstash et Kibana.

Ils sont tous développés, gérés et maintenus par la société Elastic. C'est une plateforme de gestion centralisée de logs qui intègre plusieurs technologies ensemble dans le but de permettre aux utilisateurs d'utiliser des données provenant de n'importe quelle source, quel que soit leur format, et de rechercher, analyser et visualiser ces données en temps réel.

LogRhythm : C'est une plate-forme d'entreprise qui associe de manière transparente, la gestion des journaux, la surveillance de l'intégrité des fichiers et l'analyse des machines, aux analyses d'hôte et de réseau, au sein d'une plate-forme unifiée de renseignements de sécurité. Il est conçu pour faire face à un paysage en constante évolution de menaces et de défis, avec une suite complète d'outils haute performance pour la sécurité, la conformité et les opérations.

SPLUNK : Logiciel pour suivre et analyser des données machine, Splunk (produit) collecte, indexe et met en corrélation des données en temps réel dans des archives consultables, permettant la génération de graphiques, de rapports, d'alertes, de tableaux de bord et d'infographies.

10. Intérêt d'un SOC

10.1. Définition d'un SOC

Le **Security Operations center, SOC**, désigne dans une entreprise l'équipe en charge d'assurer la sécurité de l'information.

Le SOC est une plateforme permettant la supervision et l'administration de la sécurité du système d'information au travers d'outils de collecte, de corrélation d'événements et d'intervention à distance. Le SIEM (Security Information Event Management) est l'outil principal du SOC puisqu'il permet de gérer les événements d'un SI.

10.2. Objectif d'un SOC

L'objectif d'un SOC est de détecter, analyser et remédier aux incidents de cybersécurité à l'aide de solutions technologiques et d'un ensemble de démarches. Ils surveillent et analysent l'activité sur les réseaux, les serveurs, les terminaux, les bases de données, les applications, les sites Web et autres systèmes, à la recherche de signaux faibles ou de comportements anormaux qui pourraient être le signe d'un incident ou d'un compromis en matière de sécurité. Le SOC doit veiller à ce que les incidents de sécurité potentiels soient correctement identifiés, analysés, défendus, enquêtés et signalés. Les SOC sont composés, en général, d'analystes et d'ingénieurs en sécurité, ainsi que de managers supervisant les opérations de sécurité. Les capacités supplémentaires de certains SOC peuvent inclure l'analyse avancée, la cryptanalyse et l'ingénierie inverse des logiciels malveillants pour analyser les incidents.

Les équipes SOC travaillent étroitement avec les équipes d'intervention afin de s'assurer que le problème de sécurité soit bien réglé une fois qu'il a été découvert.

11. Conclusion

Dans ce chapitre, nous avons détaillé les besoins de la sécurité informatique et les différents types d'attaques. Une partie a été réservée pour la définition des hackers et leurs types. A la fin de ce chapitre, nous avons présenté quelques solutions SIEM et l'intérêt de SOC.

Chapitre3 :

Présentation de l'outil SPLUNK

1. Introduction

Ce chapitre s'agit d'une présentation de l'outil SPLUNK. Ainsi, nous détaillons son rôle et son fonctionnement, aussi le processus d'indexation. Nous allons ensuite citer quelques sandbox d'analyse des URL et des pièces jointes des mails de phishing.

2. Présentation du SPLUNK

2.1. Définition et objectif du Splunk

Le mot Splunk vient du mot spelunking (spéléologie), qui signifie explorer des grottes. Splunk peut analyser presque tous les types de données connus, y compris les données machine, les données structurées et les données non structurées. Splunk fournit des informations opérationnelles sur ce qui se passe dans une infrastructure en temps réel, ce qui facilite la prise de décision rapide.

Splunk est une plateforme logicielle permettant de chercher, d'analyser et de visualiser les données générées par des machines, collectées à partir de sites web, d'applications, de capteurs, et d'appareils en tout genre. Il suffit de transférer les données sur la plateforme pour **laisser Splunk se charger de les traiter et de les transformer en informations exploitables**. Ainsi, les entreprises peuvent aisément détecter d'où viennent les éventuels problèmes techniques de leurs machines.

Splunk **surveille, signale et analyse les données machine en temps réel** et indexe les données en fonction des horodatages.[8]

2.2. Écosystème Splunk

Splunk peut récupérer n'importe quelle source de données. Soit sur le cloud ou sur des bases de données des systèmes d'exploitation des logs réseaux.

Splunk est l'une des solutions les plus riches mais aussi des plus simples avec tout type d'environnement, aussi c'est une solution à travers laquelle on peut effectuer des recherches directement du monitoring, de faire du reporting et de l'analyse ou encore de pouvoir créer des tableaux de bord bien spécifiques.

2.3. Licences Splunk

Lorsque vous saisissez des données dans Splunk, l'indexeur les indexe et les stocke sur le disque. La licence Splunk détermine la limite d'ingestion de données. Chaque instance Splunk Enterprise a besoin d'une licence qui spécifie les règles sur la quantité de données qu'elle peut indexer en une journée. Il existe différents types de licences Splunk.

- **Licence Splunk Entreprise**

La licence « standard » Splunk Enterprise spécifie le type de données indexées, disponibles à l'achat ou configurées.

- **Licence sans application**

La licence Splunk Enterprise standard a un volume d'indexation quotidien maximum dans lequel vous recevez un avertissement de violation s'il est dépassé. Si vous recevez plus de cinq avertissements en un mois, vous violez votre licence. Cela peut entraîner la désactivation de la tête de recherche Splunk. Cependant, en l'absence d'application, même si vous violez la licence, votre tête de recherche ne sera pas désactivée.

- **Licence d'essai d'entreprise**

La licence Enterprise Trial permet une indexation maximale de 500 Mo/jour. Elle expire après 60 jours et vous êtes invité à passer à la licence Splunk Enterprise standard ou à la licence gratuite.

- **Licence d'essai de vente**

La licence Enterprise Trial expire après 60 jours et a une capacité d'indexation de 500 Mo/jour. Si vous avez un projet pilote nécessitant une capacité d'indexation supérieure à 500 Mo/jour, vous pouvez contacter directement l'équipe commerciale de Splunk pour obtenir une licence.

- **Licence de développement/test**

Splunk donne accès à sa licence Dev/Test pour opérer dans un environnement hors production.

- **License gratuite**

La licence gratuite de Splunk a une capacité d'indexation allant jusqu'à 500 Mo/jour. Avec cette licence, vous ne pouvez pas effectuer de recherches distribuées, de transfert TCP/HTTP, d'alertes, de gestion des utilisateurs, de LDAP ou d'authentification par script.

- **Splunk pour les licences IoT industrielles**

Splunk fournit une licence spéciale pour l'IoT industriel qui donne accès à des ensembles d'applications spécialement conçues.

- **Licence de transitaire**

La licence Forwarder permet de transférer un nombre illimité de données. Contrairement à une licence gratuite, elle permet l'authentification. Vous n'avez pas besoin d'acheter une licence supplémentaire car elle est incluse dans Splunk.[8]

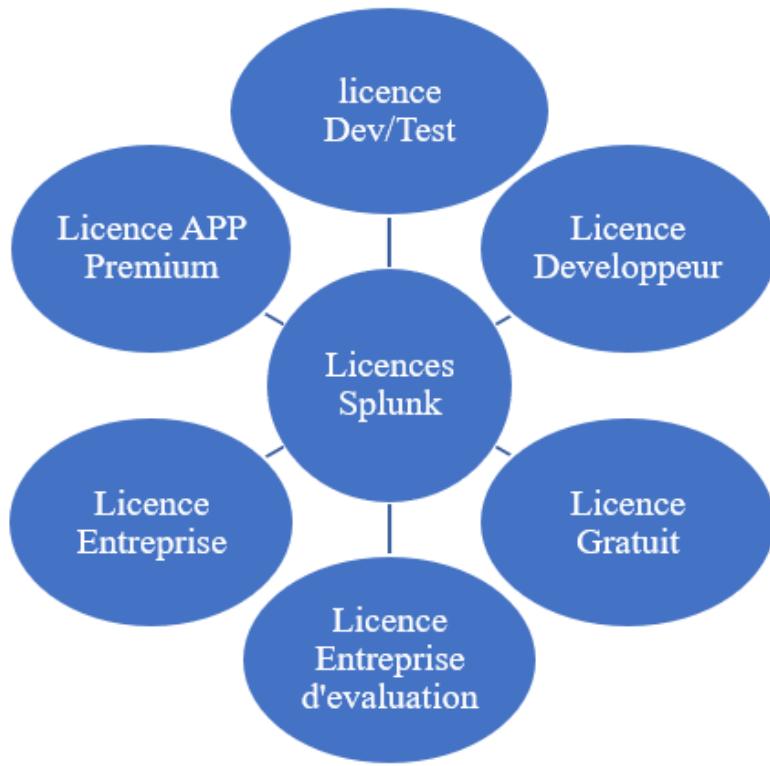


Figure 5: Système de License de splunk

2.4. Les avantages de Splunk :

Splunk offre une variété d'avantages, notamment les suivants :

- Convertit le rapport d'analyse de journal complexe en graphiques
- Prend en charge les données structurées et non structurées
- Fournit une plate-forme simple et évolutive
- Offre une architecture simple pour l'architecture la plus complexe
- Comprend les données de la machine
- Fournit des informations sur les données pour l'intelligence opérationnelle
- Surveille les données informatiques en continu

Splunk offre une flexibilité riche en fonctionnement et conviviale, mais elle a un coût élevé.

3. Les Composants du Splunk

Les principaux composants de l'architecture Splunk sont le Forwarder, l'indexeur et Search head.

3.1. Forwarder

Ce sont les agents collecteurs de logs, installés sur les systèmes d'exploitation Unix et Windows, qui collectent les journaux et les envoient à l'indexeur. Splunk propose deux types de forwarder :

- Universal Forwarder : transmet les données brutes sans aucun traitement préalable. Ceci est plus rapide et nécessite moins de ressources sur l'hôte, mais entraîne l'envoi d'énormes quantités de données à l'indexeur.
- Heavy Forwarder : effectue l'analyse et l'indexation à la source, sur la machine hôte, et envoie uniquement les événements analysés à l'indexeur.

3.2. Indexeur

L'indexeur est le processus central de Splunk qui transforme les données en événements, les stocke sur le disque et les ajoute à un index.

L'indexeur crée les fichiers suivants, en les séparant dans des répertoires appelés buckets :

- Données brutes compressées
- Index pointant vers des données brutes (fichiers. TSIDX)
- Fichiers de métadonnées

L'indexeur effectue un traitement d'événement générique sur les données du journal, comme l'application d'un horodatage et l'ajout d'une source, et peut également exécuter des actions de transformation définies par l'utilisateur pour extraire des informations spécifiques ou appliquer des règles spéciales, comme le filtrage d'événements indésirables.

Dans Splunk Enterprise, vous pouvez configurer un cluster d'indexeurs avec réPLICATION entre eux, pour éviter la perte de données et fournir plus de ressources système et d'espace de stockage pour gérer de gros volumes de données.

3.3. Search head

La tête de recherche fournit l'interface utilisateur que les utilisateurs peuvent utiliser pour interagir avec Splunk. Il permet aux utilisateurs de rechercher et d'interroger les données Splunk, et s'interface avec les indexeurs pour accéder aux données spécifiques qu'ils demandent.

Splunk fournit une architecture de recherche distribuée, qui vous permet d'évoluer pour gérer de gros volumes de données et de mieux gérer le contrôle d'accès et les données géo-dispersées. Dans un scénario de recherche distribuée, la tête de recherche envoie des requêtes de recherche à un groupe d'indexeurs, également appelés homologues de recherche.

Les indexeurs effectuent la recherche localement et renvoient les résultats à la tête de recherche, qui fusionne les résultats et les renvoie à l'utilisateur.

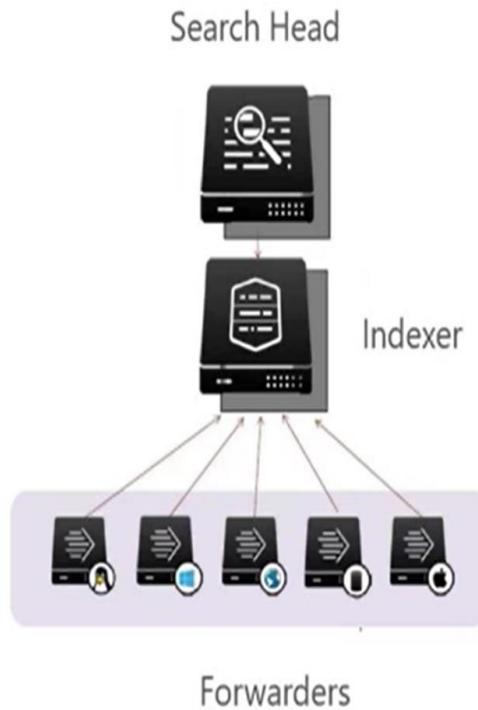


Figure 6: Principaux composants de splunk

4. Que peut indexer Splunk ?

On peut absolument indexer une grande variété de types de données provenant des sources diverses, pour pouvoir les traiter, les analyser et les présenter sur le tableau de bord ou le Dashboard que nous permettrons de prendre des bonnes décisions au bon moment.

- Avec Splunk nous pouvons tout simplement surveiller les fichiers et répertoires, des évènements réseau qui se passe par TCP et UDP ou encore de SNMP et nous pouvons aussi passer par des divers de manière plus traditionnelle c'est-à-dire avec des protocoles comme de Syslog.
- Grâce à l'Universal Forwarder, nous pouvons récupérer des sources d'informations relatives à Windows. Tout est configurables comme on les souhaite.
- Avec l'utilisation de HEC « HTTP Event Collector », nous pouvons récupérer les évènements http. C'est-à-dire aux actions qui vont être perpétrés au niveau de serveur web qui nous permet d'effectuer des analyses plus approfondies sur l'activité web de l'utilisateur au niveau de notre plateforme web. Pour pouvoir prévoir notamment des stratégies des produits, des approches ou tout simplement pour une analyse.

- Nous pouvons aussi penser à exécuter des scripts. Ces derniers permettent la recherche des informations de manière continue, plus structurée et encore plus intéressante.
- Nous avons plein de connecteurs qui nous permettent de se connecter à la base de données comme l'oracle, MySQL ou également à des solutions orientées tel que le Big Data.
- Splunk permet aussi d'avoir des approches orientées cloud permettant la contraction d'une infrastructure hybride ce qui assure l'analyse de log. Il peut être également considéré comme un outil très puissant pour la collecte.



Figure 7: Les différentes catégories d'indexation

5. Fonctionnement de Splunk

L'indexeur Splunk fonctionne d'une manière spécifiée dans une architecture définie.

Splunk offre essentiellement quatre fonctionnalités principales qui sont :

5.1. Données d'entrée :

Il s'agit de la première phase des données d'intégration. Il existe plusieurs méthodes pour importer des données dans Splunk : il peut écouter votre port, votre point de terminaison API REST, le protocole de contrôle de transmission (TCP), le protocole de datagramme utilisateur (UDP), etc., ou utiliser une entrée scriptée.

5.2. Analyseur :

La deuxième phase consiste à analyser l'entrée. Elle s'agit d'un bloc de données qui est divisé en divers événements. La taille maximale des données dans le pipeline d'analyse est de 128 Mo. Dans la phase d'analyse, vous pouvez extraire les champs par défaut, tels que le type de source.

Vous pouvez également extraire des horodatages des données, identifier la terminaison de la ligne et effectuer d'autres actions similaires. Vous pouvez aussi masquer des données sensibles mais utiles. Par exemple, si les données proviennent d'une banque et comprennent les numéros de compte d'un client, le masquage des données est essentiel. Dans la phase d'analyse, vous pouvez appliquer des métadonnées personnalisées, si nécessaire.

5.3. Indexation

Dans cette phase, l'événement est divisé en segments dans lesquels la recherche peut être effectuée. Les données sont écrites sur le disque et vous pouvez concevoir des structures de données d'indexation.

5.4. Recherche

Dans cette phase, les opérations de recherche sont effectuées sur les données d'index, et vous pouvez créer un objet de connaissance et effectuer n'importe quelle tâche ; par exemple, un rapport de ventes mensuel.

Les données d'entrée, l'analyseur et l'indexeur se trouvent tous sur une seule machine autonome. Contrairement à cela, dans un environnement distribué, les données d'entrée sont analysées vers l'indexeur ou le redirecteur lourd à l'aide de Universal Forwarder (UF), qui est un programme léger qui obtient des données dans Splunk.

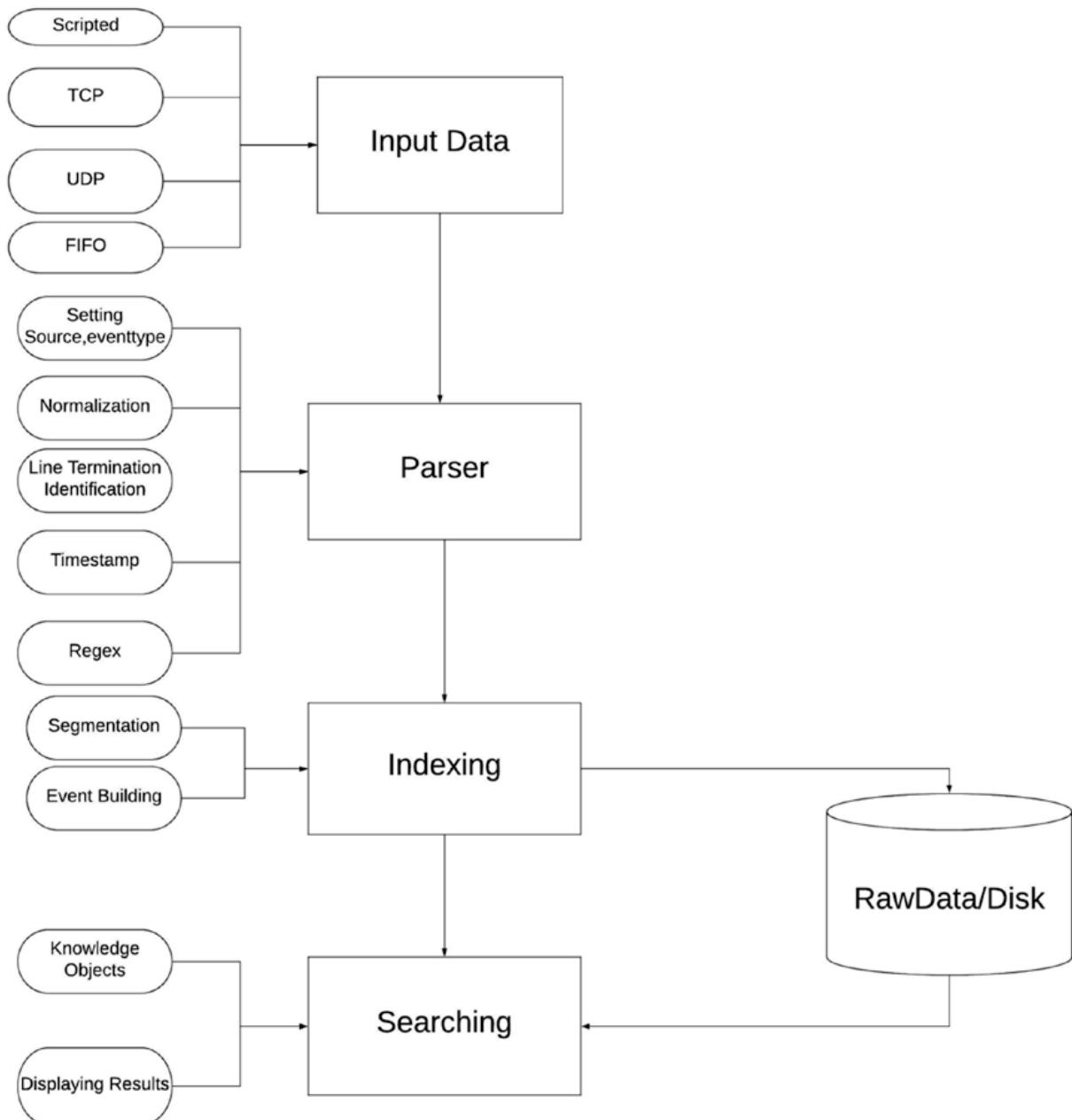


Figure 8: Fonctionnalités de splunk

6. Processus d'indexation

L'indexation sur Splunk est un processus continu qui se produit en temps réel ou à intervalles réguliers. Les données indexées peuvent être facilement recherchées, analysées et visualisées à l'aide d'outils de tableau de bord et de visualisation intégrés dans la plateforme.

Ce processus d'indexation permet aux utilisateurs de Splunk d'obtenir des informations exploitables à partir de grandes quantités de données, facilitant ainsi la prise de décision et la résolution de problèmes.

Le processus d'indexation de Splunk peut être divisé en trois phases principales : la phase d'entrée, la phase d'analyse et la phase d'indexation.

6.1. Phase d'entrée

La première phase du processus d'indexation de Splunk est la phase d'entrée. Au cours de laquelle, les données sont collectées à partir de différentes sources telles que des fichiers journaux, des bases de données, des flux de données, des API et des systèmes de messagerie. Splunk dispose de nombreux connecteurs pour récupérer des données à partir de ces sources et peut même être configuré pour extraire des données à partir de formats personnalisés.

6.2. Phase d'analyse

Une fois les données collectées, Splunk passe à la phase d'analyse dont il extrait des informations pertinentes à partir des données brutes. Cette phase peut inclure des étapes telles que la détection automatique du schéma, la reconnaissance des types de données et la création de champs pour les données extraites. Splunk peut également appliquer des règles et des filtres pour identifier les erreurs et les événements importants.

Cette étape permet de nettoyer les données et de les transformer en un format standardisé, facilitant ainsi la recherche et l'analyse ultérieures.

6.3. Phase d'indexation

Au cours de cette phase, Splunk indexe les données extraites dans un format optimisé pour les recherches et les analyses. Les données sont stockées dans un index, qui est organisé en partitions pour permettre une recherche et une analyse rapides. Splunk applique également des algorithmes de compression pour optimiser l'utilisation de l'espace de stockage.

7. VMware

VMware Workstation est une technologie de virtualisation qui permet de créer des machines virtuelles sur un ordinateur physique. Cela signifie que vous pouvez exécuter plusieurs systèmes d'exploitation différents sur le même ordinateur, sans qu'ils n'interfèrent les uns avec les autres.

VMware est très populaire dans le monde de l'informatique et est utilisé par de nombreuses entreprises pour déployer des applications et des serveurs.

Par conséquent, il est compatible avec la plupart des systèmes d'exploitation sans avoir besoin d'exigences matérielles particulières.



Figure 9: Logo VMware

8. Kali Linux

Kali Linux est une distribution Linux open source basée sur Debian. Il est publié le 13 mars 2013, la version finale a succédé à Back Track.

Kali Linux est une distribution Linux spécialisée dans la sécurité informatique et les tests de pénétration. Elle est conçue pour les professionnels de la sécurité informatique et les chercheurs en sécurité, mais elle peut également être utilisée par les étudiants et les amateurs de sécurité informatique pour apprendre et pratiquer les techniques de piratage éthique. Kali Linux contient de nombreux outils de piratage et de test de pénétration pré-installés, ainsi que des outils de forensique numérique.



Figure 10: Logo Kali Linux

9. Sandbox

Aujourd’hui, les sandboxes deviennent le moyen le plus rapide et le plus simple d’avoir une vue d’ensemble de la menace et de détecter la plupart des malwares.

Les sandboxes vont pouvoir représenter à la base des solutions extrêmement intéressantes qui permet de pouvoir simuler un espace cloisonné dans lequel on va pouvoir exécuter un malware et analyser ces différentes actions.

Ces sandboxes tentent de reproduire l'environnement ciblé le plus fidèlement possible, mais de légères différences permettent de le distinguer d'un environnement réel. Cela peut être la présence d'une interface réseau virtuelle par exemple. Un malware peut alors savoir s'il s'exécute sur une machine virtuelle ou une sandbox en cherchant ces différences et changer son exécution.[9]

On peut retrouver différents exemples de sandbox :

9.1. L'outil App-Any-Run

ANY.RUN est un outil de détection, de surveillance et de recherche des cybermenaces en temps réel. Le sandbox interactif en ligne est une excellente solution pour réduire le temps d'analyse. Un processus de travail facile, une interface ergonomique et des rapports d'analyse détaillés.

La sandbox donne accès au laboratoire de logiciels malveillants avec un grand nombre d'outils différents disponibles en une seconde.

La sandbox Any-Run permet de présenter de nombreux aspects des tests, tels que la création de nouveaux processus, les fichiers ou URL potentiellement suspects ou malveillants ainsi que l'activité du registre, les requêtes réseau et bien plus encore, ce qui permet de tirer des conclusions pendant l'exécution de la tâche sans avoir à attendre le rapport final. [10]



Figure 11: La sandbox ANY.RUN

9.2. L'outil URL scan

L'URL scan est un service Web autonome qui accepte l'entrée de la requête d'URL via une liaison HTTPS sécurisée et cryptée pour rechercher les infections de fichiers par hameçonnage et malveillants. Il utilise des services Web tiers réputés pour analyser les URL et les sites Web.

Ce scanner d'URL a une interface facile à utiliser et fournit des instructions de base pour identifier les liens nuisibles. En outre, ce service Web permet le partage les résultats des tests avec d'autres membres à l'aide d'un lien partageable.[11]

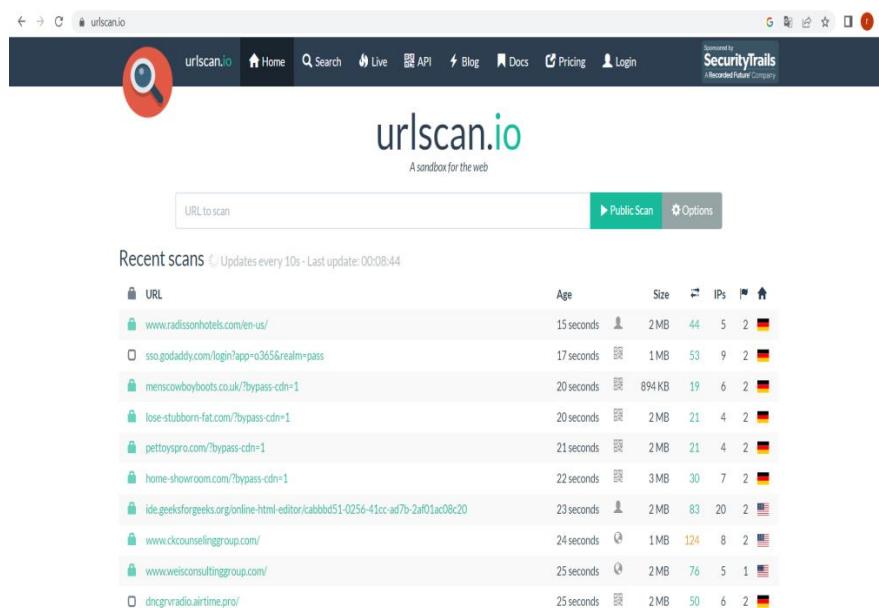


Figure 12: Interface URL scan

9.3. VirusTotal

VirusTotal utilise une méthodologie de données agrégées et complètes pour détecter les URL nuisibles et malveillantes. Entrez simplement l'URL Web cible dans le champ de saisie et cliquez sur Entrée pour effectuer une analyse du site Web. Il fournit des services API publics et privés pour les programmeurs. Ces API peuvent être utilisées pour développer un outil de vérification d'URL personnalisé sur votre site Web.

Cet outil peut examiner les hachages de fichiers, les adresses IP et les URL. Il détecte les liens et les sites Web nuisibles en recoupant tous les résultats d'analyse antivirus les plus récents des fournisseurs d'analyse d'URL avec plus de 60 autres services. Et enfin, les résultats des tests peuvent être instantanément partagés avec la communauté de la sécurité pour future référence [11].

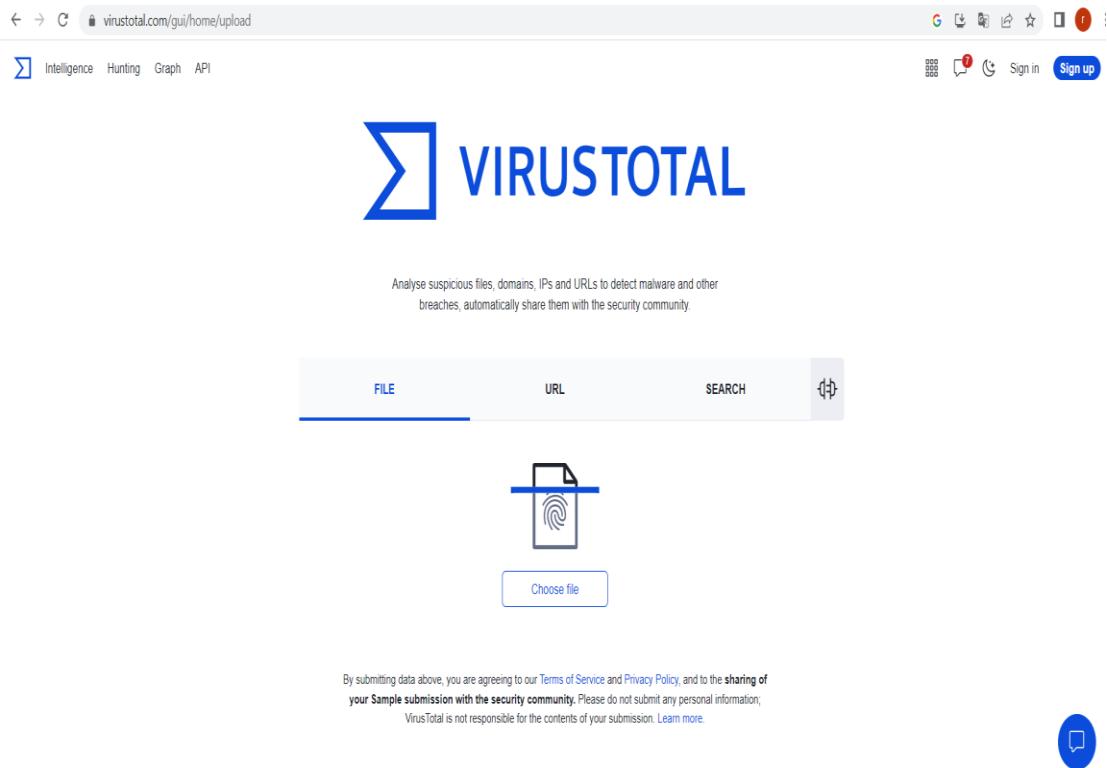


Figure 13: Interface utilisateur de VirusTotal

10. Conclusion

Tout au long de ce troisième chapitre, nous avons présenté le fonctionnement du splunk et leurs principaux composants. En deuxième lieu, nous avons présenté le processus d'indexation. Enfin, nous avons cité les outils nécessaires pour réaliser notre protocole de sécurité proposé.

Chapitre 4 :

Application du Splunk

1. Introduction

L'objectif principal de cette phase est de mettre en place la solution décrite dans le chapitre précédent. Pour ce faire, nous allons d'abord spécifier l'environnement de développement matériel et logiciel. Ensuite, nous décrivons les différentes étapes d'installation et leur mise en œuvre. Enfin, nous montrons les différentes interfaces à travers des tests pour vérifier l'efficacité et le bon fonctionnement de notre solution.

2. Présentation du système proposé

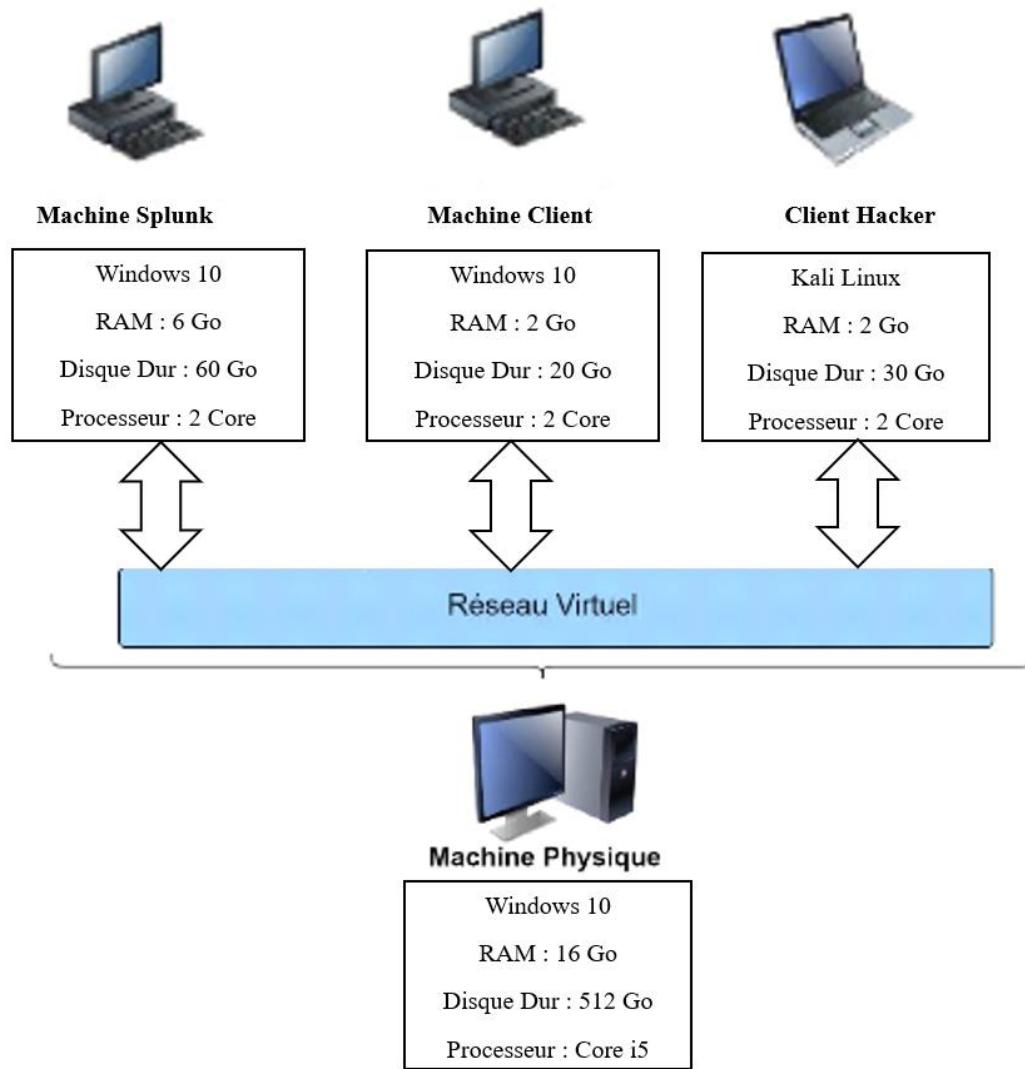


Figure 14: Topologie de l'infrastructure

Dans cette section, nous allons présenter l'environnement de développement qui est constitué de deux parties, nommés environnement matériel et environnement logiciel.

2.1. Environnement matériel

Nous avons utilisé deux ordinateurs portables qui ont les caractéristiques mentionnées dans le tableau 1.

Tableau 1: Caractéristiques techniques

	PC 1	PC2
Processeur	Intel(R) Core(TM) i5-10210U CPU @ 1.60GHz 2.11 GHz	Intel(R) Core(TM) i3-3217U CPU @ 1.80GHz 1.80 GHz
Mémoire RAM	8,00 Go	8,00 Go
Type de système	Système d'exploitation 64 bits	Système d'exploitation 64 bits
Système d'exploitation	Windows 10	Windows 10

2.2. Environnement logiciel

Une fois que nous avons bien configuré la partie matérielle, nous passerons à la configuration logicielle.

La première tâche à faire est de télécharger et installer les machines virtuelles que nous utiliserons dans notre solution.

- ✓ Nous avons téléchargé l'image de Windows 10 de version 64 sur le site officiel www.microsoft.com.

Après l'installation et la configuration de deux machines Windows sur VMWare Workstation 17 pro, nous avons commencé la mise en place de la solution splunk.

Sur une machine nommée Machine Splunk qui est caractérisée par 6 Go du RAM et de capacité de disque 60 Go, nous avons installé notre application Splunk Entreprise pour pouvoir récupérer les logs.

Au niveau de la deuxième machine Windows 10 caractérisée par 2 Go du RAM et de disque de 20 Go, nous avons installé Universal Forwarder.

- ✓ Nous avons téléchargé l'image de kali de version 64 qui est compatible avec notre machine virtuelle sur le site officiel www.kali.org pour effectuer notre test d'intrusion.

Après l'installation de kali, nous avons téléchargé PyPhisher sur le site web www.github.com. Ceci dans le but d'appliquer un test d'attaque de phishing.

Une fois tous les logiciels sont téléchargés, nous passerons à l'étape d'installation.

- ✓ Pour l'installation du Splunk Entreprise et Splunk Universal Forwarder, nous avons utilisé les e-mails professionnels :

Kamel.aloui2@tunisetelecom.tn

moufida.dhaouadi@tunisetelecom.tn

3. Mise en œuvre de la solution

3.1. Installation de Splunk Entreprise

Afin d'installer Splunk sur un serveur Windows 10, nous avons :

- Crée un compte et téléchargé le programme d'installation de Splunk à partir de la page officielle www.Splunk.com. Le programme d'installation de Windows est un fichier MSI.
- Double-cliquer sur le fichier splunk.msi pour démarrer l'installation. Le programme s'exécute et affiche le panneau du programme d'installation de Splunk Enterprise.
- Avant de cliquer sur "suivant", il faut tout d'abord cocher la case "Cochez cette case pour accepter le contrat de licence". Cela active les boutons "Personnaliser l'installation" et "Suivant" comme illustré dans la figure

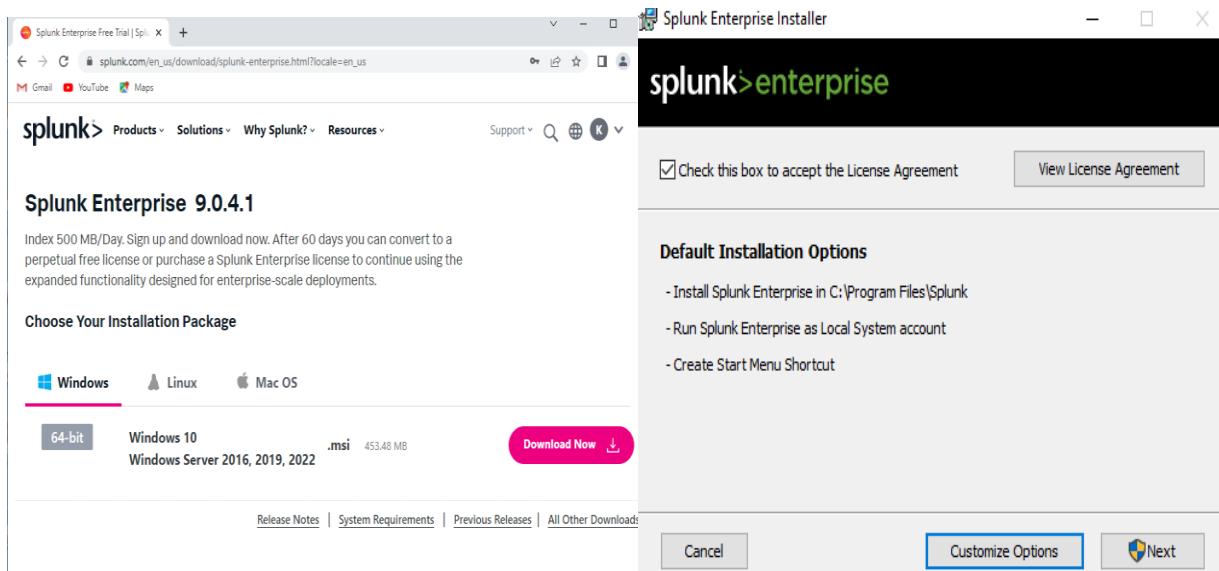


Figure 15: Installation Splunk

Le programme d'installation affiche le panneau "Informations de connexion". Nous spécifions un nom d'utilisateur et un mot de passe avant de cliquer sur "suivant".

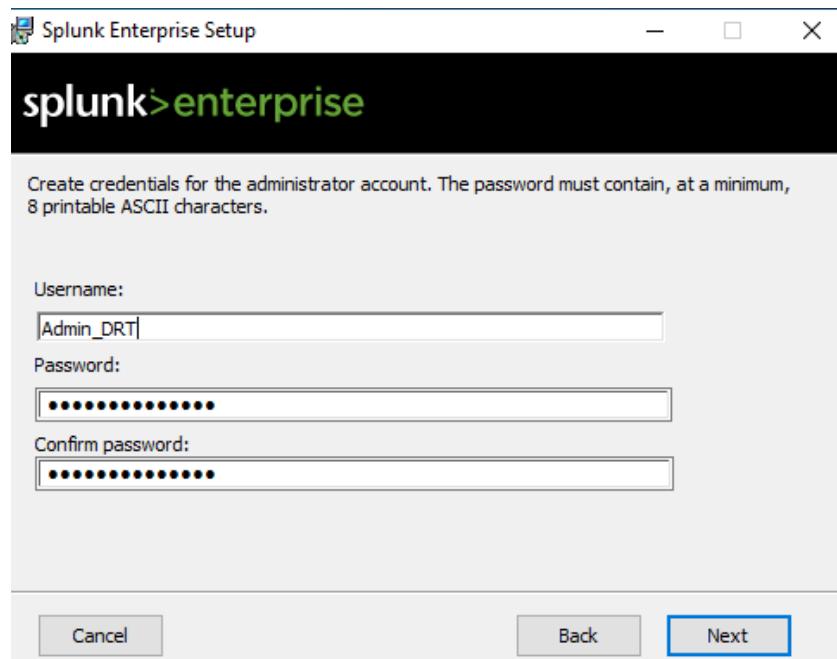


Figure 16: : Cr ation d'un compte administrateur

Ces informations seront utilis es ult rieurement pour acc der   la plate-forme SPLUNK une fois l'installation est termin e.

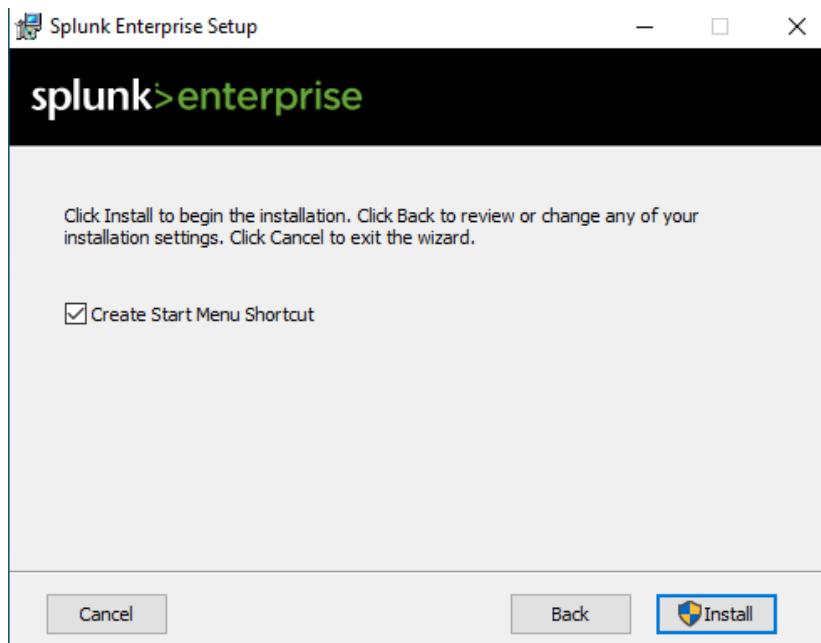


Figure 17: Panneau r  capitulatif de l'installation

Cliquons sur "Installer" pour proc der   l'installation. Le programme s'ex cute, installe le logiciel et affiche la fen tre Installation termin e. Enfin, cliquons sur "terminer". Splunk Enterprise d marre et se lance dans un navigateur.

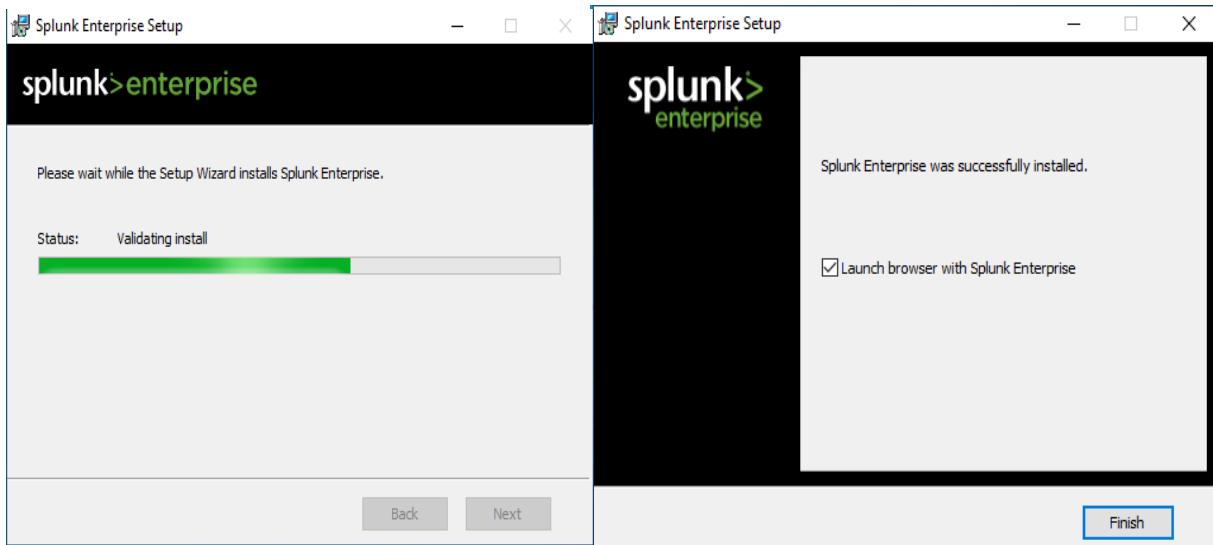


Figure 18: Étape d'installation de splunk

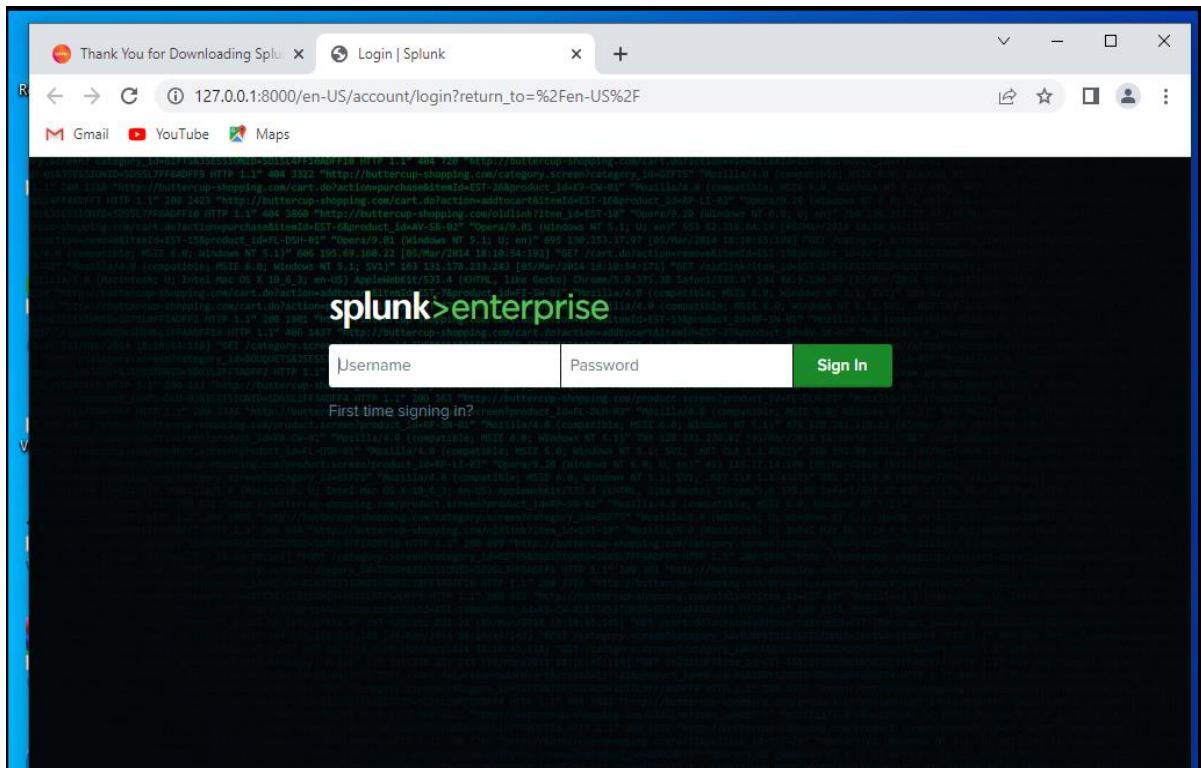


Figure 19: Interface utilisateur du splunk

Un nom d'utilisateur et un mot de passe sont requis pour accéder à l'interface de Splunk. La capture d'écran 19 montre la page d'accueil de Splunk Enterprise.

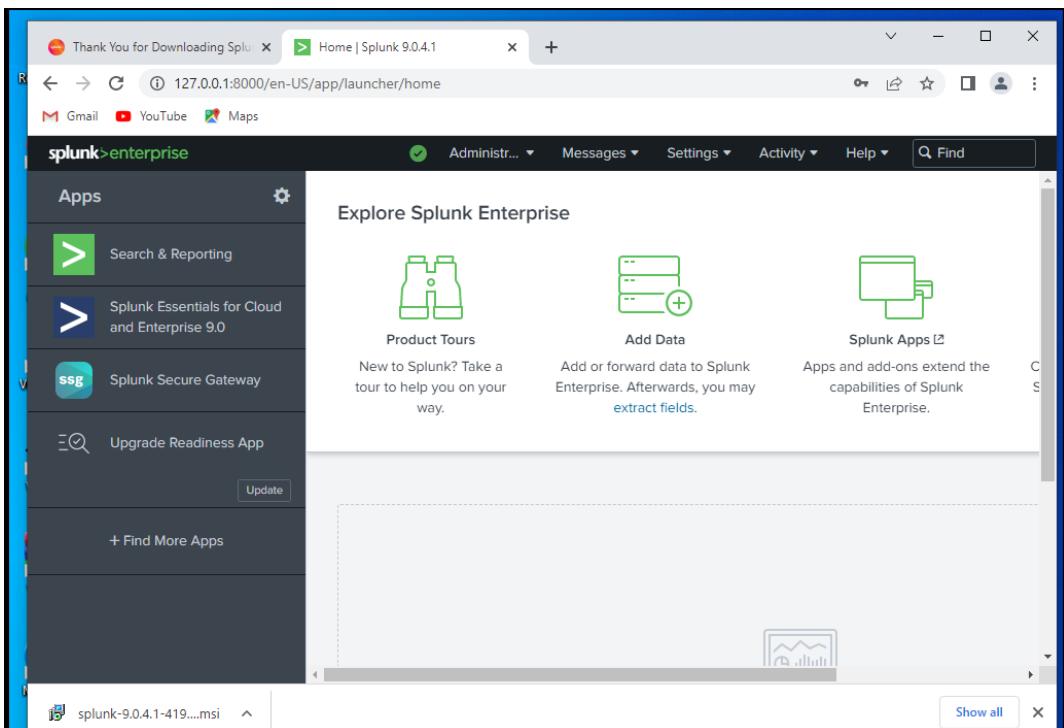


Figure 20: Interface de Splunk Entreprise

3.2. Récupération des logs

Pour collecter les fichiers logs depuis un ordinateur distant, il faut configurer l'expéditeur et le destinataire. Ce dernier est une instance Splunk qui reçoit les données.

La récupération des données sur Windows se fait en suivant les trois étapes suivantes :

a. Configuration de splunk indexer

Ce qui suit explique le processus de transfert des données vers l'indexeur splunk via splunk web :

- Accéder à l'interface web de l'indexeur splunk.
- Accéder à "Paramètres" dans la barre navigateur principale et sélectionner "Transfert et réception" dans le menu déroulant.
- Sélectionner à "configurer la réception" et cliquer sur "ajouter nouveau".
- Entrer "9997" dans écouter sur ce port. Si nous utilisons un port différent, nous devons le spécifier au niveau du forwarder.

The figure consists of two screenshots of the Splunk Enterprise web interface. The top screenshot shows the 'Add new' configuration page for receiving data. It has a form with a 'Listen on this port' field containing '9997'. Below the field is a note: 'For example, 9997 will receive data on TCP port 9997.' At the bottom are 'Cancel' and 'Save' buttons. The bottom screenshot shows the 'Receive data' list page. It displays a table with one item: '9997' in the 'Listen on this port' column, 'Enabled | Disable' in the 'Status' column, and 'Delete' in the 'Actions' column. A green button labeled 'New Receiving Port' is visible at the top right of the list page.

Figure 21: Configurer la réception sur l'indexeur splunk

Pour configurer la transmission, comme illustré sur la figure ci-dessous, nous avons :

- Cliqué sur "Paramètres" et sélectionné "Transmission et réception".
- Sélectionné "Configurer la transmission" et cliqué sur "Ajouter nouveau".
- Introduit le nom d'hôte ou l'adresse IP du serveur de déploiement et le port 9997.

The figure consists of two screenshots of the Splunk Enterprise web interface. The top screenshot shows the 'Add new' configuration page for forwarding data. It has a form with a 'Host' field containing '192.168.1.16:9997'. Below the field is a note: 'Set as host:port or IP:port. You must also enable receiving on this host.' At the bottom are 'Cancel' and 'Save' buttons. The bottom screenshot shows the 'Forward data' list page. It displays a table with one item: '192.168.1.16:9997' in the 'Host' column, 'Automatic Load Balancing' in the 'App' column, 'Enabled' in the 'Status' column, and 'Clone | Delete' in the 'Actions' column. A green button labeled 'New Forwarding Host' is visible at the top right of the list page.

Figure 22: Configurer la transmission sur l'indexeur Splunk

b. Installer et configurer Splunk Universal Forwarder

Le Universal Forwarder joue un rôle clé dans la collecte des données et l'intégration de celles-ci dans la plateforme Splunk pour une visualisation efficace des données.

Pour ce faire nous avons téléchargé le package d'installation du Splunk Universal Forwarder à partir du site web www.splunk.com et lancé le fichier .MSI en acceptant le contrat de licence et ensuite nous avons sélectionné l'emplacement d'installation du Forwarder et en cliquant sur "suivant".

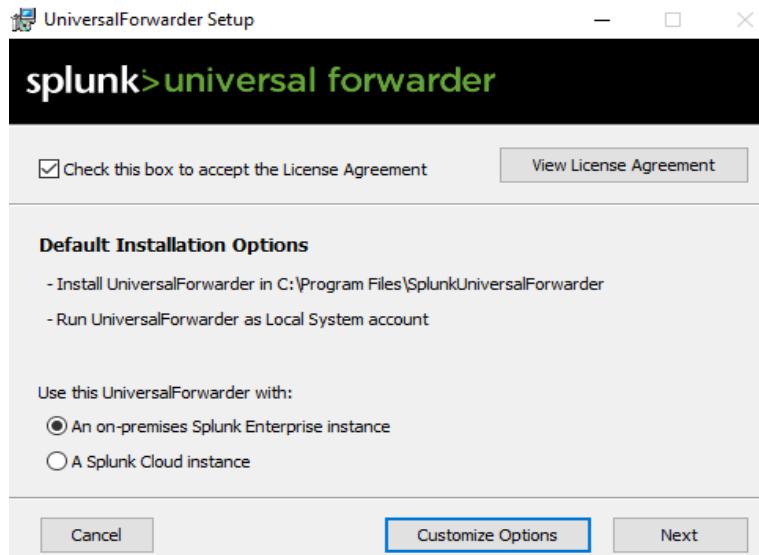


Figure 23: Installer Splunk Universal Forwarder

Par la suite, nous avons entré les informations demandées pour créer un compte administrateur.

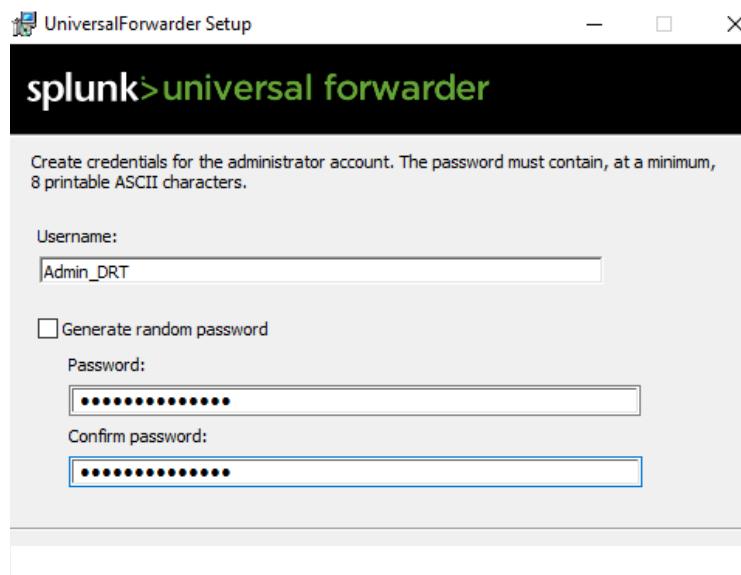


Figure 24: Crédit d'un compte d'administrateur

Universal Forwarder a besoin d'un serveur de déploiement ou d'un indexeur de réception. Pour spécifier le serveur de déploiement, nous avons indiqué le nom du serveur Splunk ou son adresse IP. Par contre, le port est laissé à sa valeur par défaut.

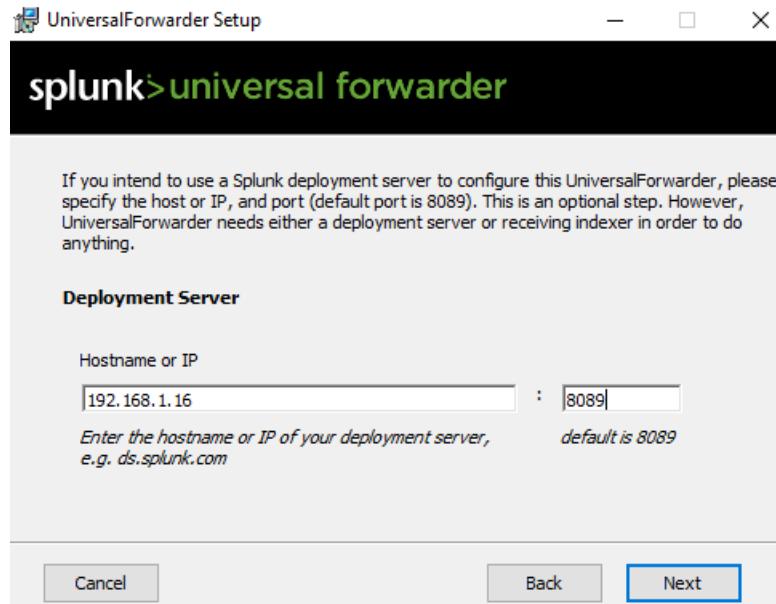


Figure 25: Configurer serveur de déploiement

Une fois que nous avons spécifié l'indexeur splunk, les données seront indexées et elles seront disponibles pour la recherche et l'analyse dans splunk.

Pour le spécifier, nous avons donné le nom ou l'adresse IP du serveur splunk. Encore une fois, le port reste à sa valeur par défaut "9997"

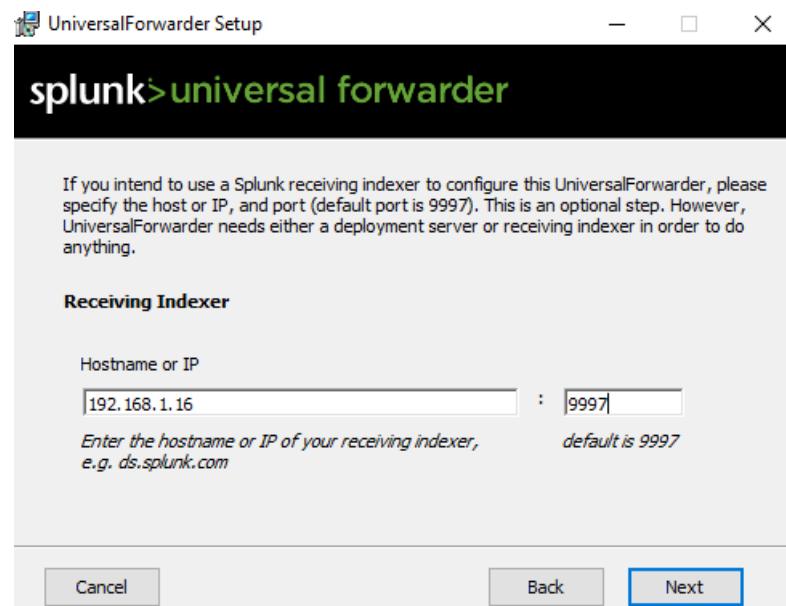


Figure 26: Configurer l'écoute sur l'indexeur

Maintenant que l'installation de splunk universel forwarder est terminée, la connectivité entre la machine distante (cliente) et le serveur splunk est assurée.

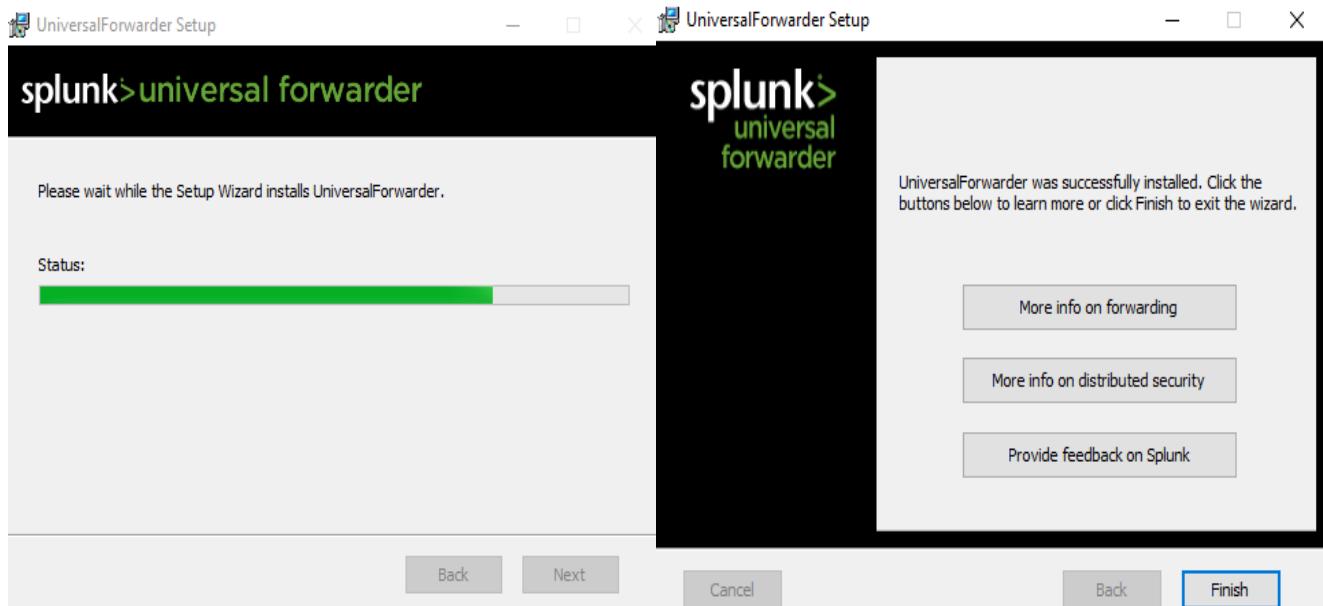
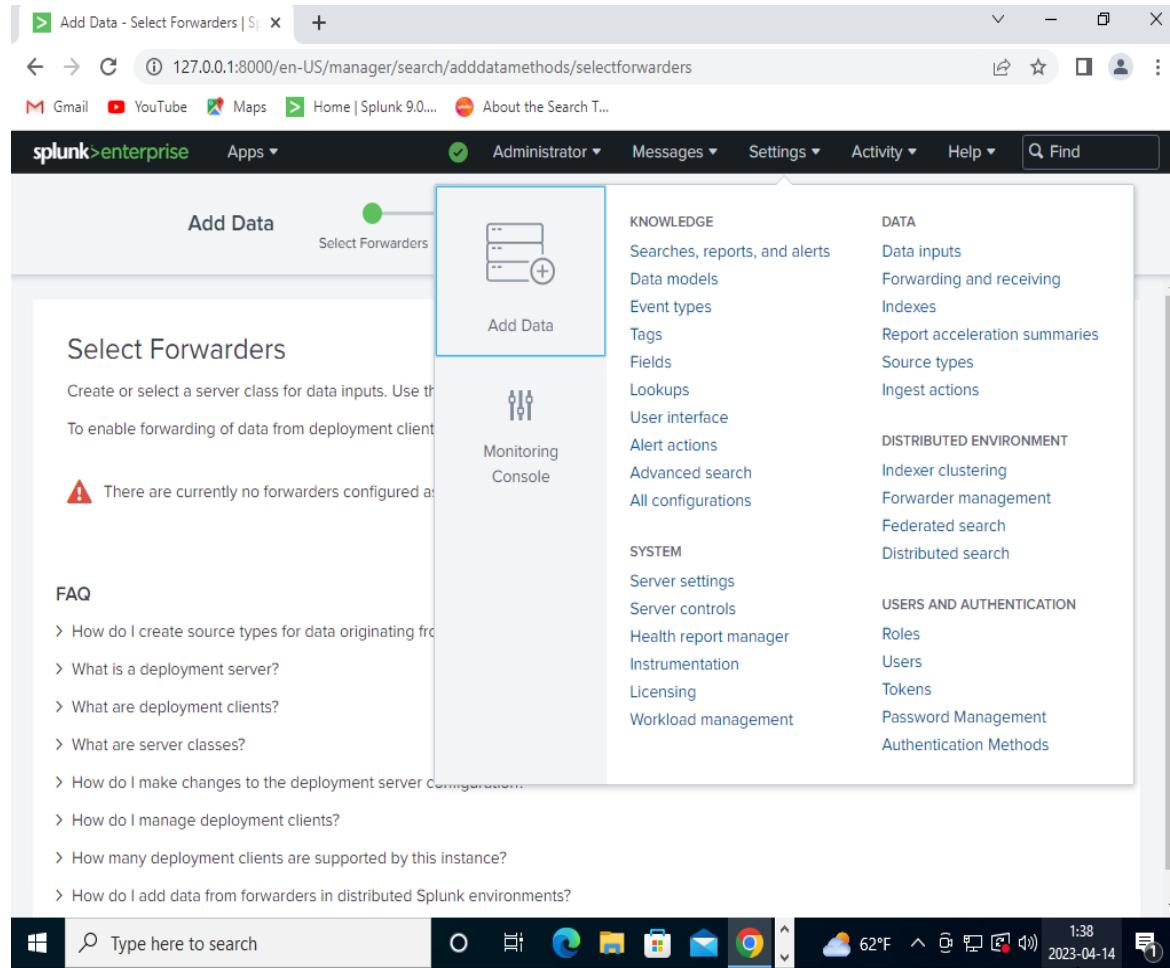


Figure 27: Fin de l'installation

c. Collecte des logs

Un log représente tout simplement un horodatage et une donnée Data. C'est l'un des traces d'action sur une machine ou application, et chacun va pouvoir interpréter ce dernier comme il le souhaite selon son expérience, ses compétences et son angle d'analyse.

Pour collecter les données journaux, nous avons accédé à "Paramètres", sélectionné "Ajouter des données", puis cliqué sur "Transmettre".



Or get data in with the following methods

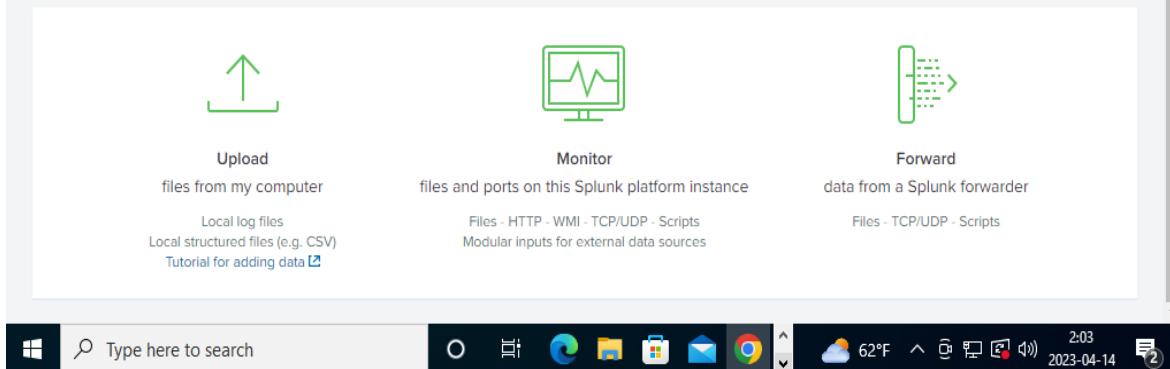


Figure 28: Importer les données

Parmi la liste des machines clientes qui s'affichent, nous avons choisi celles dont nous permettons de récupérer les logs, puis nous avons spécifié le nom de la classe serveur qui regroupe plusieurs hôtes, et enfin nous cliquons sur Suivant pour continuer la configuration.

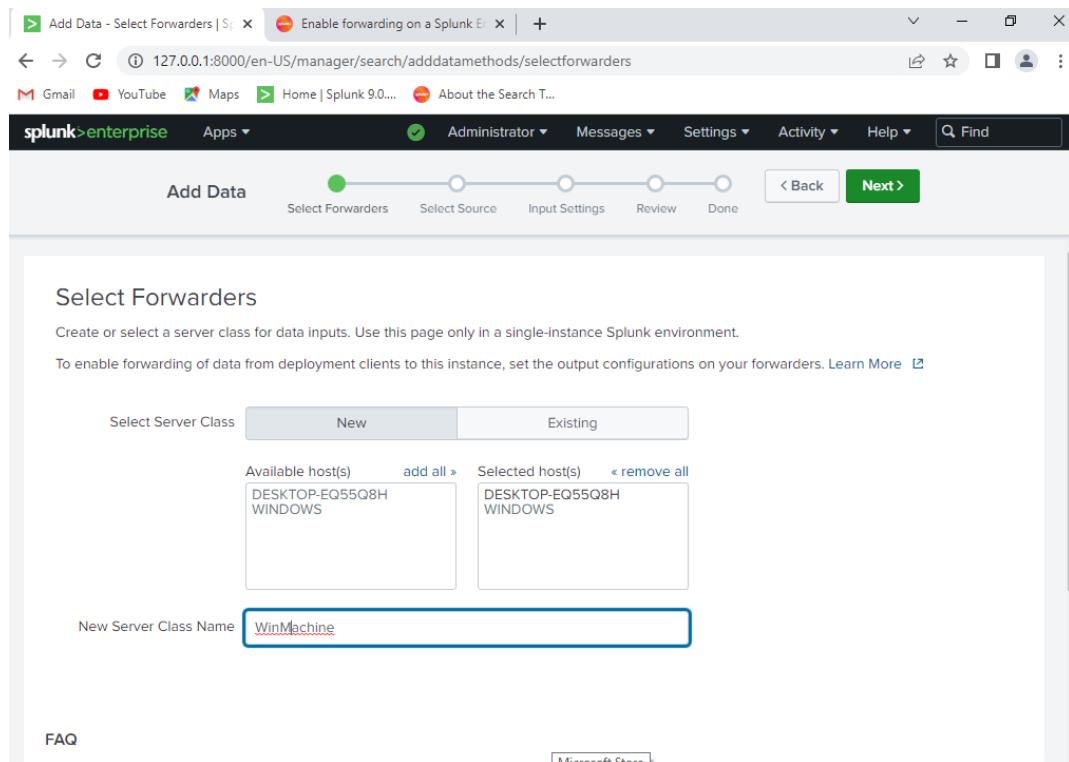


Figure 29: La classe serveur

En deuxième lieu, nous avons cliqué sur les fichiers journaux que nous souhaitons analyser "Logs d'évènements locaux". Puis, nous avons sélectionné tous les événements que nous souhaitons les indexer et en cliquant sur "suivant".

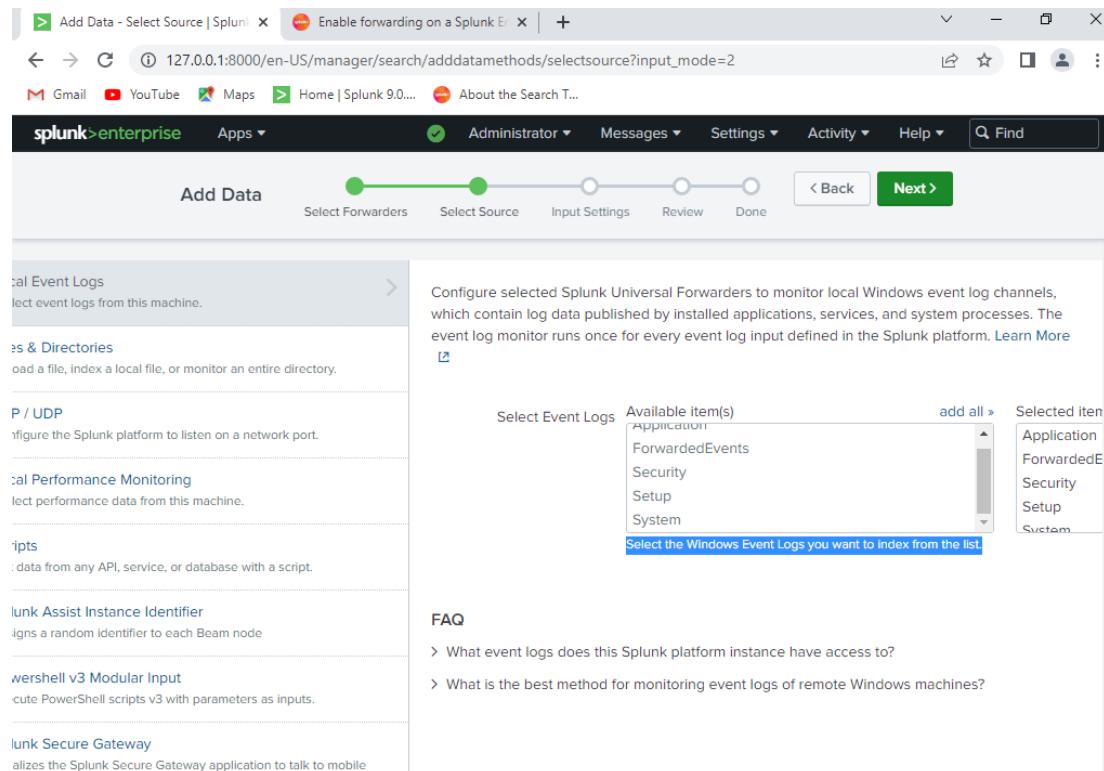
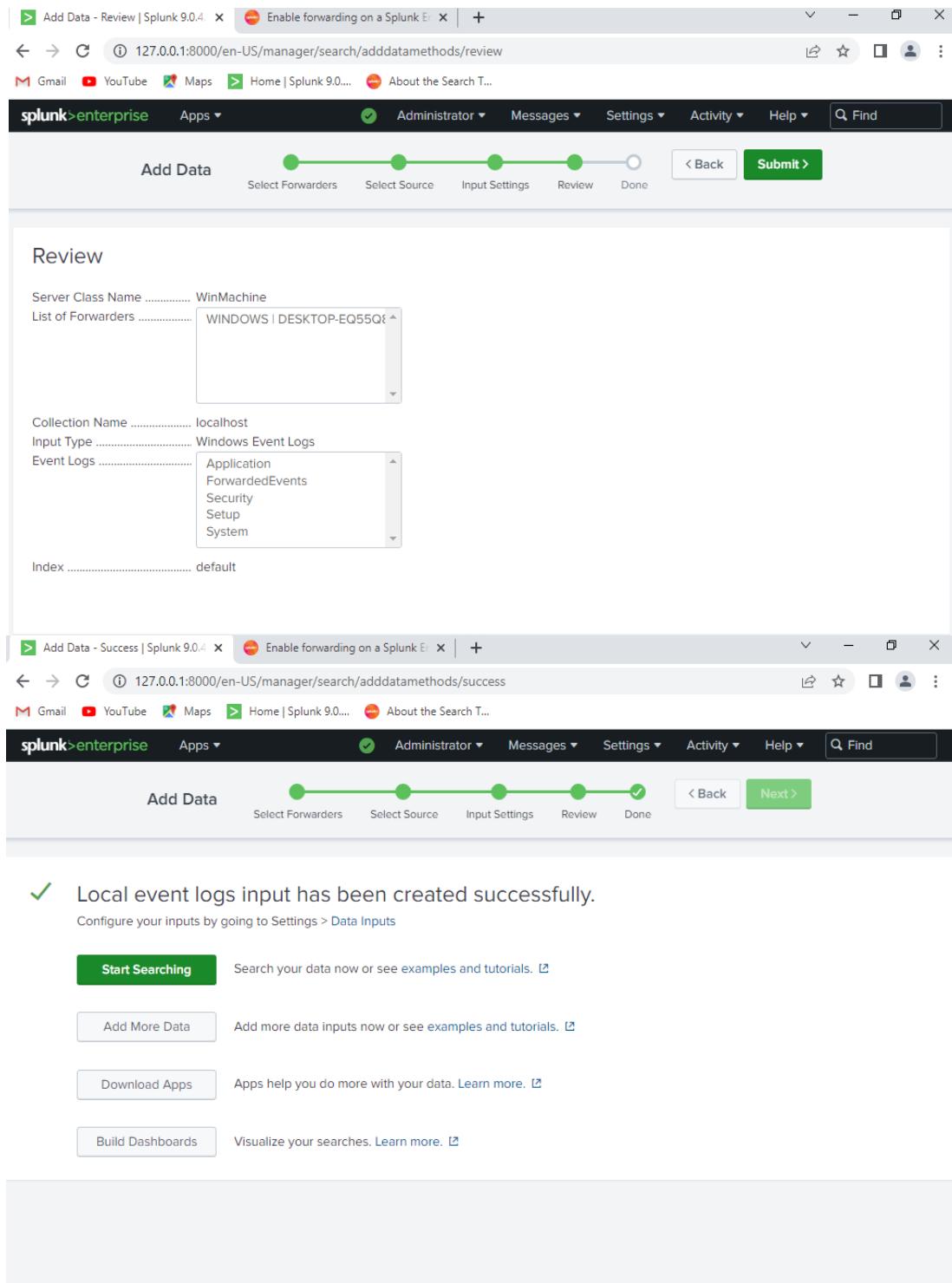


Figure 30: : Sélection des logs d'événements

Sur le champ index, nous avons sélectionné "Default" qui est l'index par défaut utilisé pour toutes les données qui ne sont pas explicitement routées vers un index spécifique. Dans cette étape, nous pouvons créer un nouvel indexeur. Pour ce faire, il suffit de cliquer sur "créer un nouvel index", ensuite il suffit d'entrer le nom.

Figure 31: Chois du l'index

Le résumé des paramètres d'entrée s'affiche. En cliquant sur "Lancer la recherche", des logs devraient apparaître dans Splunk.

*Figure 32: Recherche des logs*

Une fois les logs s'affichent dans Splunk, nous pouvons effectuer des traitements dessus. Comme nous le voyons dans la figure suivante :

The screenshot shows the Splunk web interface. At the top, there's a navigation bar with tabs like 'Search | Splunk 9.0.4.1', 'Enable forwarding on a Splunk E...', and a search bar containing the URL '127.0.0.1:8000/en-US/app/search/search?q=search%20*&display.page.search.mode=smart&dispatch.sampled=false'. Below the bar are links to 'Gmail', 'YouTube', 'Maps', 'Home | Splunk 9.0...', and 'About the Search Test...'. The main area has a table titled 'Event' with columns 'Time' and 'Event'. One event is listed: '4/14/23 2:38:41.000 AM' with details like LogName=Security, EventCode=4672, EventType=0, ComputerName=DESKTOP-EQ55Q8H, SourceName=Microsoft Windows security auditing, Type=Information, RecordNumber=9150, Keywords=Audit Success, TaskCategory=Special Logon, OpCode=Info, and Message=Special privileges assigned to new logon. Below the event table is a 'Subject:' section with fields for Security ID (S-1-5-18), Account Name (SYSTEM), Account Domain (NT AUTHORITY), and Logon ID (0x3E7). Another section for 'Privileges' lists SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, and SeLoadDriverPrivilege. At the bottom, a 'Data Summary' section shows a table for 'Sources (4)'. The table has columns 'Source', 'Count', and 'Last Update'. It lists four sources: WinEventLog:Application (1,689 events, last updated 4/14/23 12:16:09.000 PM), WinEventLog:Security (8,070 events, last updated 4/14/23 12:23:05.000 PM), WinEventLog:Setup (45 events, last updated 4/14/23 2:38:00.000 AM), and WinEventLog:System (2,949 events, last updated 4/14/23 12:03:24.000 PM).

Source	Count	Last Update
WinEventLog:Application	1,689	4/14/23 12:16:09.000 PM
WinEventLog:Security	8,070	4/14/23 12:23:05.000 PM
WinEventLog:Setup	45	4/14/23 2:38:00.000 AM
WinEventLog:System	2,949	4/14/23 12:03:24.000 PM

Figure 33: Exporté des logs

4. Configuration de la réception des Syslog sur Splunk

Dans cet exemple, nous allons montrer comment renvoyer les logs vers splunk. Dans ce cas, nous avons renvoyé les logs d'un Palo-Alto vers Splunk. Nous choisissons le chemin : Paramètres -> Données -> Entrée de Données -> Entrées Locales.

Sur la ligne UDP, nous cliquons sur Ajouter nouveau.

Par la suite, nous devons saisir les paramètres que nous avons tapé sur notre équipement. Nous utilisons Syslog UDP et le port 514 et nous cliquons sur Suivant.

Nous allons maintenant paramétriser l'entrée. Pour cela nous allons sélectionner une SourceType. Si elle n'existe pas dans la liste cliquer sur Nouveau. Dans cet exemple nous avons créé une étiquette Palo-Alto.

Dans Context de l'app, nous avons laissé la valeur par défaut Search & reporting (search).

Dans Hôte, idem nous avons laissé la valeur par défaut IP.

Dans Index, nous avons sélectionné, l'index par défaut "Testindex" qui est un index utilisé pour les tests et les développements.

The screenshot displays the Splunk Enterprise interface for adding a new data source. The process is divided into four steps: Select Source, Input Settings, Review, and Done. The current step is 'Input Settings'.

Input Settings Step:

- Configure this instance to listen on any TCP or UDP port to capture data sent over the network (such as syslog). Learn More
- Port: 514 (Example: 514)
- Source name override: optional host:port
- Only accept connection from: optional example: 10.1.2.3, !badhost.splunk.com, *.splunk.com

Source type Step:

- Select: Palo-Alto
- Source Type Category: Custom
- Source Type Description: (empty)

App context Step:

- App Context: Search & Reporting (search)

Host Step:

- Method: IP, DNS, Custom (selected)
- Host field value: DESKTOP-EQ55Q8H

Index Step:

- Index: testindex (selected)
- Create a new index: (button)

Taskbar:

- Type here to search
- Icons for File, Internet Explorer, File Explorer, Mail, Google Chrome, Settings, Help, Cloud, Weather (78°F), Date (2023-04-25), Time (4:13)

Figure 34: Exporté des Syslog

Le résumé de nos paramètres d'entrée s'affiche, ensuite nous avons cliqué sur Lancer la recherche.

The screenshot shows two main parts of the Splunk interface:

- Add Data - Review Step:** A browser window titled "Add Data - Review" with the URL "127.0.0.1:8000/en-US/manager/launcher/adddatamethods/review". The navigation bar includes "splunk>enterprise" and "Apps". The "Add Data" process is shown with four steps: "Select Source" (green), "Input Settings" (green), "Review" (green), and "Done" (gray). The "Review" step is active. Below the steps, the configuration details are listed:
 - Input Type UDP Port
 - Port Number 514
 - Source name override N/A
 - Restrict to Host N/A
 - Source Type Palo-Alto
 - App Context search
 - Host DESKTOP-EQ55Q8H
 - Index testindex
- New Search Page:** A search interface with the query "source='udp:514' host='DESKTOP-EQ55Q8H' index='testindex' sourcetype='Palo-Alto'". The results section shows "0 events (before 4/25/23 4:17:47:00 AM)" and "No Event Sampling". The visualization tab is selected, showing the message "Events (0)". Below the visualization, it says "No results found.".

Collection Type	Count	Action
Remote event log collections	1	+ Add new
Files & Directories	13	+ Add new
Local performance monitoring	0	+ Add new
Remote performance monitoring	0	+ Add new
HTTP Event Collector	0	+ Add new
TCP	0	+ Add new
UDP	1	+ Add new

Figure 35: Récupération des Syslog

5. Configurer le collecteur d'événements HTTP dans Splunk

Le HEC est un moyen flexible et puissant permettant la collecte des données à partir de sources http. Il peut être utilisé par une variété de cas d'utilisation, tel que la surveillance des performances, la collecte de données d'utilisation et de trafic et l'analyse des logs [12].

- Activer le collecteur d'événements http sur Splunk Entreprise**

Pour configurer le HEC pour recevoir des événements dans splunk web :

Dans la console splunk, dans le menu "Paramètre" nous avons cliqué sur "Saisies des données".

Sous "Entrées locales" nous avons cliqué sur "Collecteur d'évènement HTTP", ensuite dans le coin supérieur droit, nous avons cliqué sur "Paramètres globaux".

Dans la boite de dialogue "Modifier les paramètres globaux" en regard de " tous les joutons" nous avons sélectionné sur "Activé ", après nous avons sélectionné "json" comme type de source et pour index, nous choisissons "main". Le port est laissé à la valeur par défaut et nous avons cliqué sur "Enregistrer".

All Tokens	Enabled	Disabled
Default Source Type	_json ▾	
Default Index	main ▾	
Default Output Group	None ▾	
Use Deployment Server	<input type="checkbox"/>	
Enable SSL	<input checked="" type="checkbox"/>	
HTTP Port Number ?	8088	

Cancel **Save**

Figure 36: Activation de collecteur d'évènement http

- **Créer un jeton Event Collector sur Splunk Enterprise**

Pour obtenir un jeton du collecteur d'événements HTTP, dans le coin supérieur droit de la page "Collecteur d'évènement HTTP" nous avons cliqué "Nouveau jeton", ensuite nous avons saisir un nom et une description pour le jeton (option par défaut), puis en cliquant sur "Suivant".

Sur la page "Paramètres d'entrées" nous avons sélectionné le type source "Automatique" et nous avons ajouté l'index principal aux index autorisés, nous avons sélectionné "main" et "testindex" et puis nous avons cliqué sur "Réviser" et en passant à l'écran suivant.

Input Settings
Optionally set additional input parameters for this data input as follows:

Source type
The source type is one of the default fields that the Splunk platform assigns to all incoming data. It tells the Splunk platform what kind of data you've got, so that the Splunk platform can format the data intelligently during indexing. And it's a way to categorize your data, so that you can search it easily.

Select Allowed Indexes
Available item(s) add all > Selected item(s) < remove all
Selected item(s): main, testindex
Select indexes that clients will be able to select from.
Default Index: main
Create a new index

Figure 37: Evènement http : Paramètres d'entrée avancée

La page résumée qui va représenter tous les paramètres que nous avons définie est affichée. Nous avons vérifié nos informations, l'option "Activer l'accusés de réception de l'indexeur" est définie sur "Non" et que "Index autorisés "inclut l'index principal.

Lorsque en cliquant sur Soumettre, un jeton généré, nous avons copié la valeur de jeton affiché par splunk web et nous avons collé dans un autre document pour référence ultérieure.

The figure consists of three screenshots of the Splunk 9.0.4 web interface:

- Screenshot 1: Add Data - Review**
This screenshot shows the "Review" step of the "Add Data" process. It displays the configuration for a new token input. Key details include:
 - Input Type:** Token
 - Name:** test HTTP
 - Source name override:** N/A
 - Description:** N/A
 - Enable indexer acknowledgment:** No
 - Output Group:** N/A
 - Allowed indexes:** main
testindex
 - Default index:** main
 - Source Type:** Automatic
 - App Context:** launcher
- Screenshot 2: Add Data - Success**
This screenshot shows the success message after the token was created. It includes a link to "Configure your inputs by going to Settings > Data Inputs". The token value is displayed as a highlighted blue box: `3b393937-f47b-4fff-9376-681de258e25d`.
- Screenshot 3: HTTP Event Collector**
This screenshot shows the "HTTP Event Collector" page under "Data Inputs". It lists the newly created token:

Name	Actions	Token Value	Source Type	Index	Status
test HTTP	Edit Disable Delete	3b393937-f47b-4fff-9376-681de258e25d	main		Enabled

Figure 38: Création d'un jeton Event Collector

- **Exemple d'envoi de données vers HEC avec une requête JSON**

Exemple d'envoi de données vers HEC avec une requête http. L'exemple suivant envoie une requête HTTP POST au HEC sur le port 8088 et utilise HTTP pour le transport. Cet exemple utilise la commande curl pour générer la requête JSON.

Lorsque vous faites une requête JSON pour envoyer des données à HEC, vous devez spécifier la clé "event" dans la commande.

L'en-tête HTTP d'autorisation pour HEC nécessite le mot-clé "Splunk" avant le jeton HEC.



```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.19045.2728]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>curl -k http://localhost:8088/services/collector -H "Authorization:Splunk 3b393937-f47b-4fff-9376-681de258e25d" -d "{\"sourcetype\": \"trial\", \"event\":\"hello world!\\"}"
{"text":"Success", "code":0}
C:\Windows\system32>
```

Figure 39: : La requête JSON

Nos données sont envoyées à splunk.

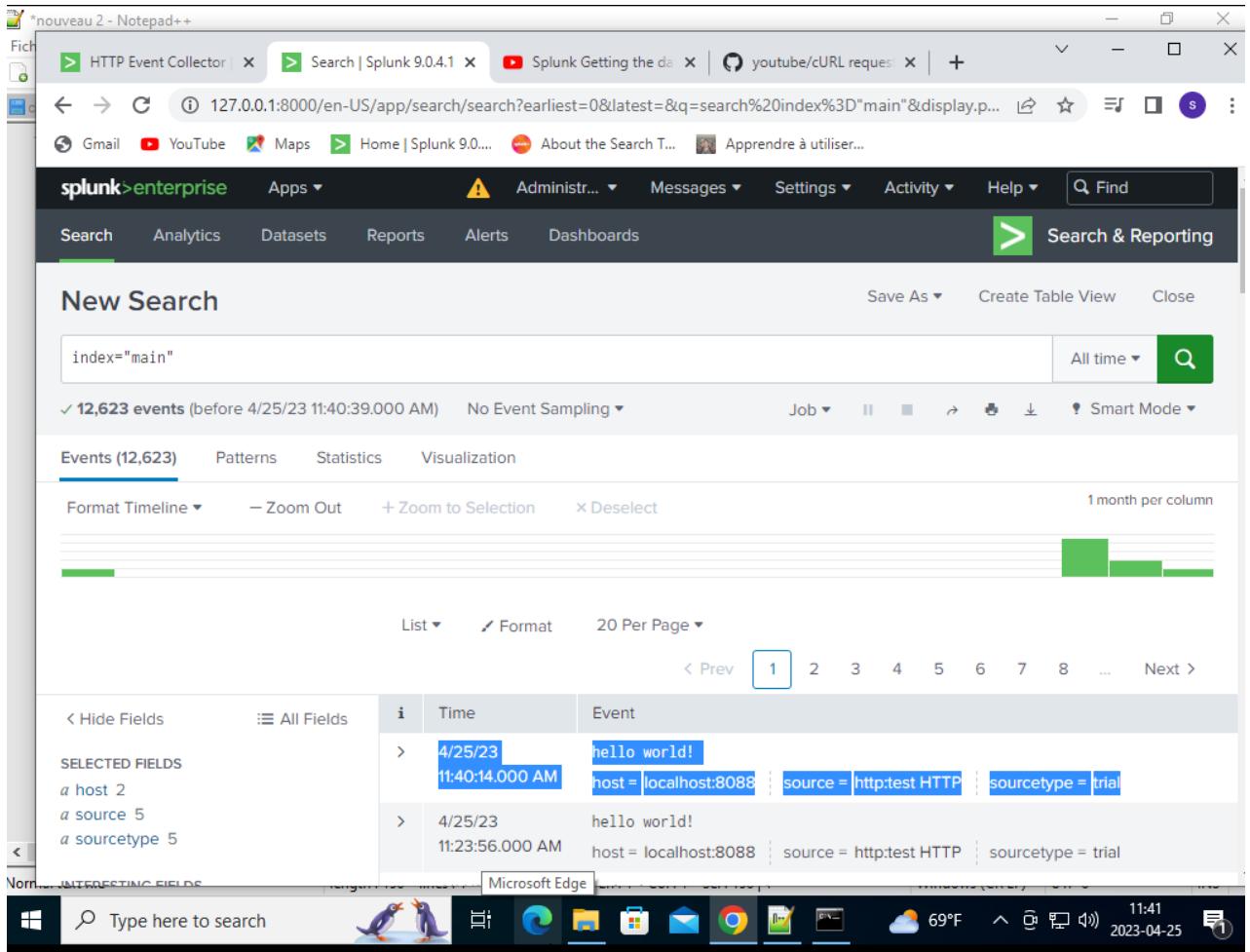


Figure 40: Evènement Hello world

6. Crédation des alertes

Nous avons utilisé les alertes pour surveiller et répondre à des événements spécifiques. Les alertes se déclenchent lorsque les seuils d'alerte définis pour une métrique sur une entité ou un groupe répondent à des conditions spécifiques. Voici les étapes pour créer une alerte dans Splunk :

En premier lieu, nous avons dirigé dans le "Paramètres" et ensuite, dans l'onglet "Paramètres de serveur", nous paramétrons la messagerie.

Ensuite, dans la page Recherche, nous avons entré la chaîne de recherche « index="_audit" action="login attempt" info="failed" » :

- ✓ index="_audit" : concerne les données audit de splunk notamment des recherches effectuées ou encore les modifications qui ont été faites au niveau privilèges, fichiers et notamment l'authentification.
- ✓ action="login attempt" : l'action d'authentification.
- ✓ info="failed" : l'authentification qui n'a pas réussi

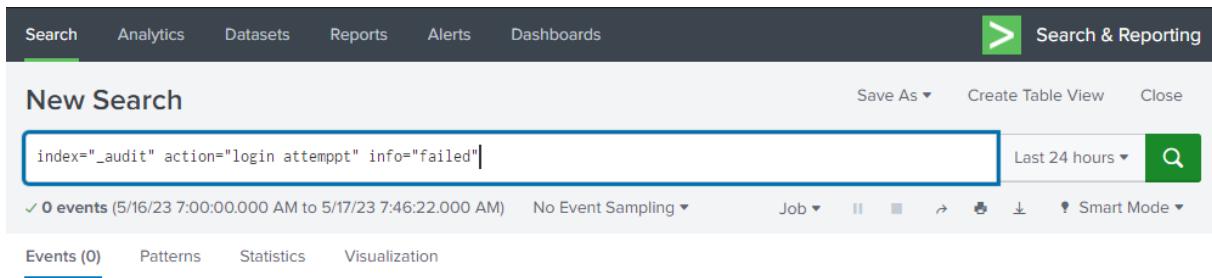


Figure 41: Requête de recherche

Pour créer une alerte, nous avons sélectionné "Enregistrer sous", puis nous avons sélectionné "Alerte" relativement à cette requête.

L'écran suivant s'affichera dans lequel nous pouvons entrer des détails supplémentaires.

Nous l'avons nommé "tentative de connection". Nous sélectionnons par la suite le type d'alerte en temps réel avec une expiration en 24 minutes.

Ensuite, nous avons déclenché l'alerte, il s'agit de la section qui détermine la manière dont les utilisateurs sont informés de cette alerte. Dans l'objet et le corps de l'e-mail pour ajouter de la spécificité à l'alerte. Par exemple, les champs objet et corps sont préremplis avec du texte qui utilise le jeton *name*. Une fois que nous avons enregistrée l'alerte, nous pouvons apporter des modifications aux autorisations.

Save As Alert

When triggered

Send email

To: aloui.radhia2011@gmail.com

Priority: Highest

Subject: Splunk Alert: \$name\$

The email subject, recipients and message can include tokens that insert text based on the results of the search. [Learn More](#)

Message: The alert condition for '\$name\$' was triggered.

Include:

- Link to Alert
- Link to Results
- Search String
- Trigger Condition
- Trigger Time
- Allow Empty Attachment
- Inline Table
- Attach CSV
- Attach PDF

Type: [HTML & Plain Text](#) [Plain Text](#)

Add to Triggered Alerts [Remove](#)

Search Analytics Datasets Reports Alerts Dashboards [Search & Reporting](#)

Tentative de connection

Enabled: Yes. Disable

App: search

Permissions: Private. Owned by admin_drt. [Edit](#)

Modified: Apr 25, 2023 2:50:16 AM

Alert Type: Real-time. [Edit](#)

Trigger Condition: Number of Results is > 0 in 1 minute. [Edit](#)

Actions: 2 Actions [Edit](#)

[Add to Triggered Alerts](#)

[Send email](#)

Figure 42: Création d'alerte connection

Pour voir les alertes en temps réel, nous sommes allés dans "Activité" ensuite "Alertes déclenchées", suite à quelques tentatives, on peut voir l'alerte qui a été remontée.

The screenshot shows the Splunk interface with the title 'Triggered Alerts - Splunk'. The URL is 127.0.0.1:8000/en-US/alerts/search. The top navigation bar includes links for Gmail, YouTube, Maps, Home | Splunk 9.0..., and About the Search T... The main search bar has 'Search & Reporting (search)' selected. The alert table lists six entries, each showing a timestamp, the type of alert ('Tentative de connection'), the app ('search'), the type ('Real-time'), severity ('High'), mode ('Digest'), and actions ('View results', 'Edit search', 'Delete'). The table is sorted by time.

	Time	Fired alerts	App	Type	Severity	Mode	Actions
<input type="checkbox"/>	2023-04-25 03:15:48 Pacific Daylight Time	Tentative de connection	search	Real-time	High	Digest	View results Edit search Delete
<input type="checkbox"/>	2023-04-25 03:15:33 Pacific Daylight Time	Tentative de connection	search	Real-time	High	Digest	View results Edit search Delete
<input type="checkbox"/>	2023-04-25 03:15:25 Pacific Daylight Time	Tentative de connection	search	Real-time	High	Digest	View results Edit search Delete
<input type="checkbox"/>	2023-04-25 03:15:00 Pacific Daylight Time	Tentative de connection	search	Real-time	High	Digest	View results Edit search Delete
<input type="checkbox"/>	2023-04-25 03:14:34 Pacific Daylight Time	Tentative de connection	search	Real-time	High	Digest	View results Edit search Delete
<input type="checkbox"/>	2023-04-25 03:14:34 Pacific Daylight Time	Tentative de connection	search	Real-time	High	Digest	View results Edit search Delete

Select All | None Selected alerts [Delete](#)

Figure 43: Alerte de la tentative de connection

7. Tentative d'attaque par PyPhisher

L'attaque par phishing est une forme d'attaque informatique qui vise à tromper les utilisateurs en se faisant passer pour une entité légitime afin d'obtenir des informations sensibles, telles que des identifiants de connexion, des informations financières ou des données personnelles. L'objectif principal de cette attaque est de manipuler les victimes pour qu'elles divulguent volontairement ces informations confidentielles. La victime ne saura pas que les informations d'identification qu'elle saisira iront dans la main de la personne malveillante au lieu du serveur authentique. Donc, pour effectuer le Phishing Ethically, nous avons utilisé l'outil PyPhisher, qui est développé en langage Python et prend en charge diverses plateformes sociales authentiques comme Facebook, Snapchat, etc. [14]

Pour installer l'outil PyPhisher sur Kali :

L'approche suivante permet l'installation de python3 « sudo apt install git python3 php openssh-client -y » et « sudo » pour le droit d'administration.

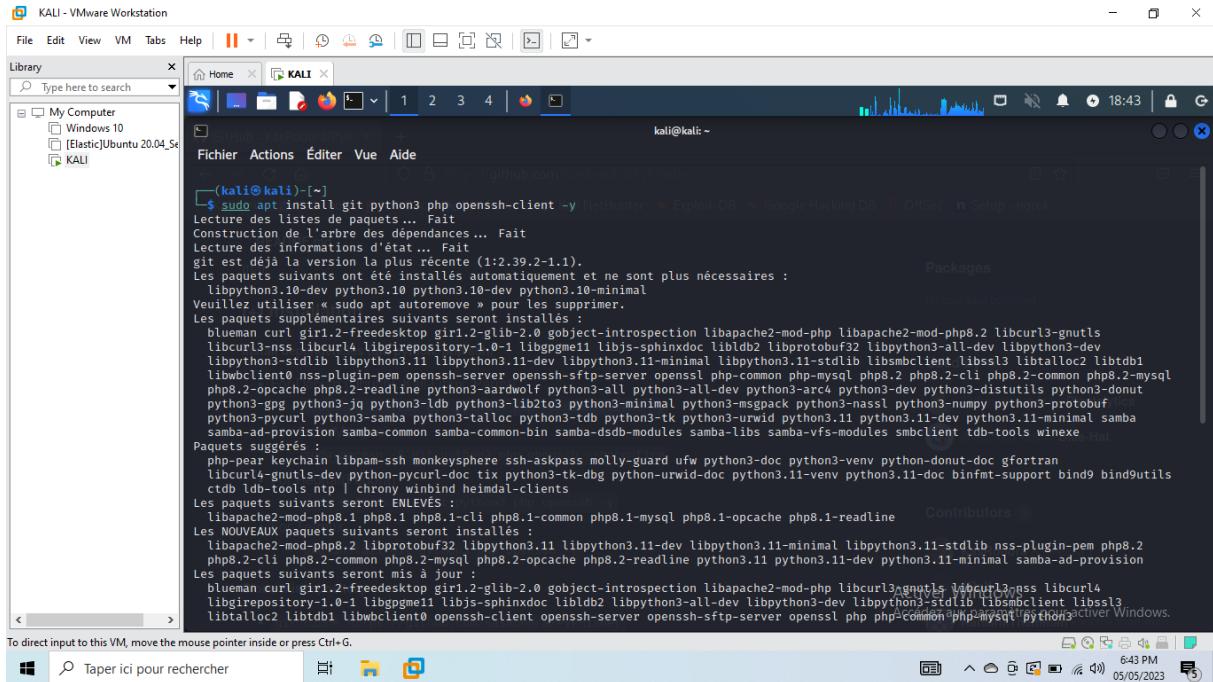


Figure 44: Installation python3

Ici, nous allons cloner l'outil PyPhisher à partir de la plate-forme GitHub. Nous avons utilisé la commande cd ci-dessous pour accéder au répertoire PyPhisher qui a été créé après le clonage de l'outil PyPhisher.

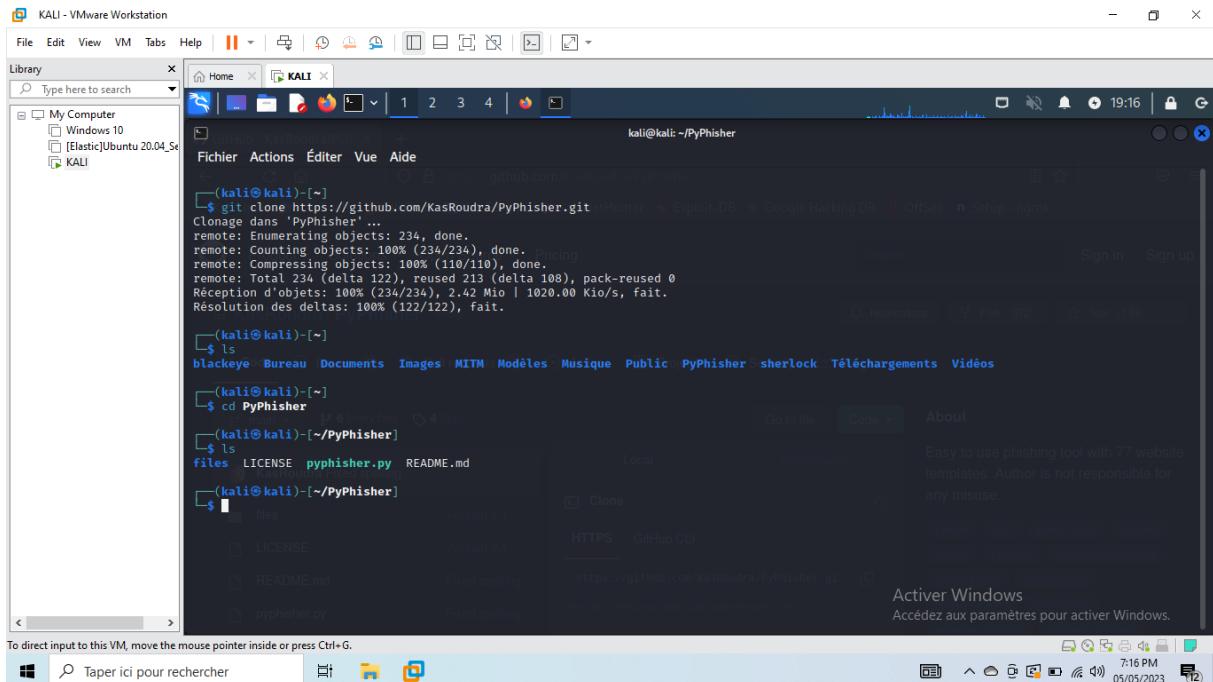


Figure 45: installation des outils de git

Pour vérifier l'installation, nous exécutons la commande « `python3 phphisher.py` ».

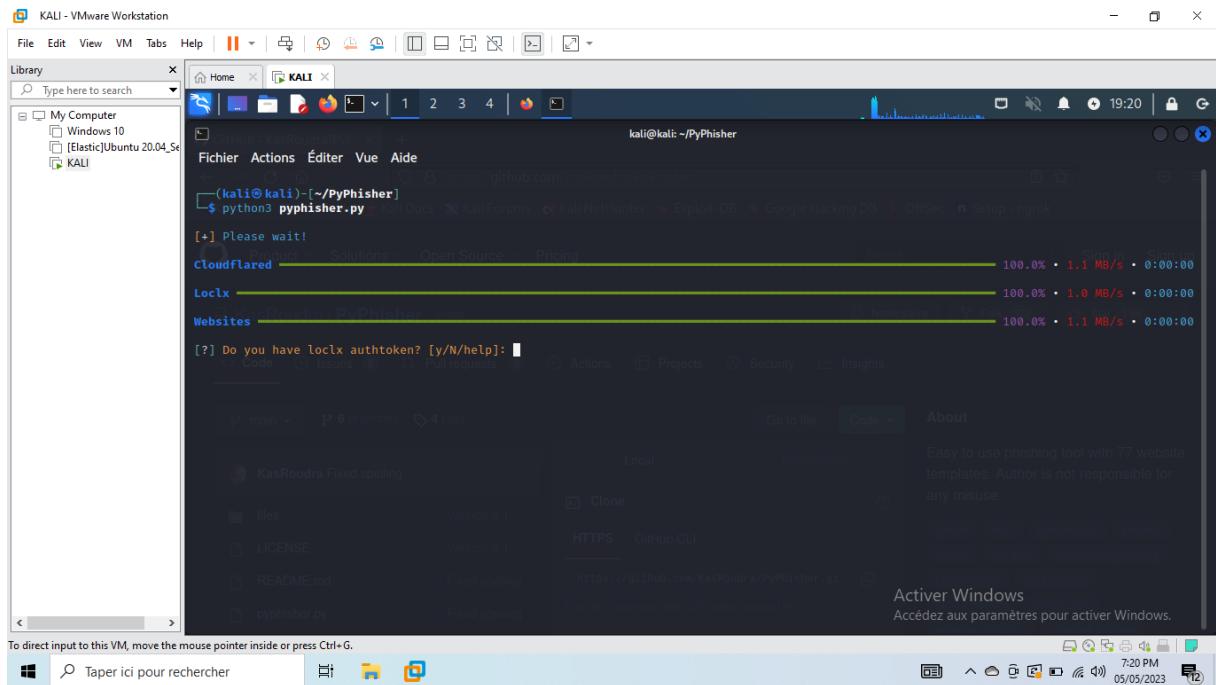


Figure 46: exécution PyPhisher

Maintenant et en utilisant cet outil, nous effectuerons une attaque de phishing avec usurpation de Facebook.

Tout d'abord, nous choisissons l'option qui correspond au Facebook comme l'indique la figure suivante :

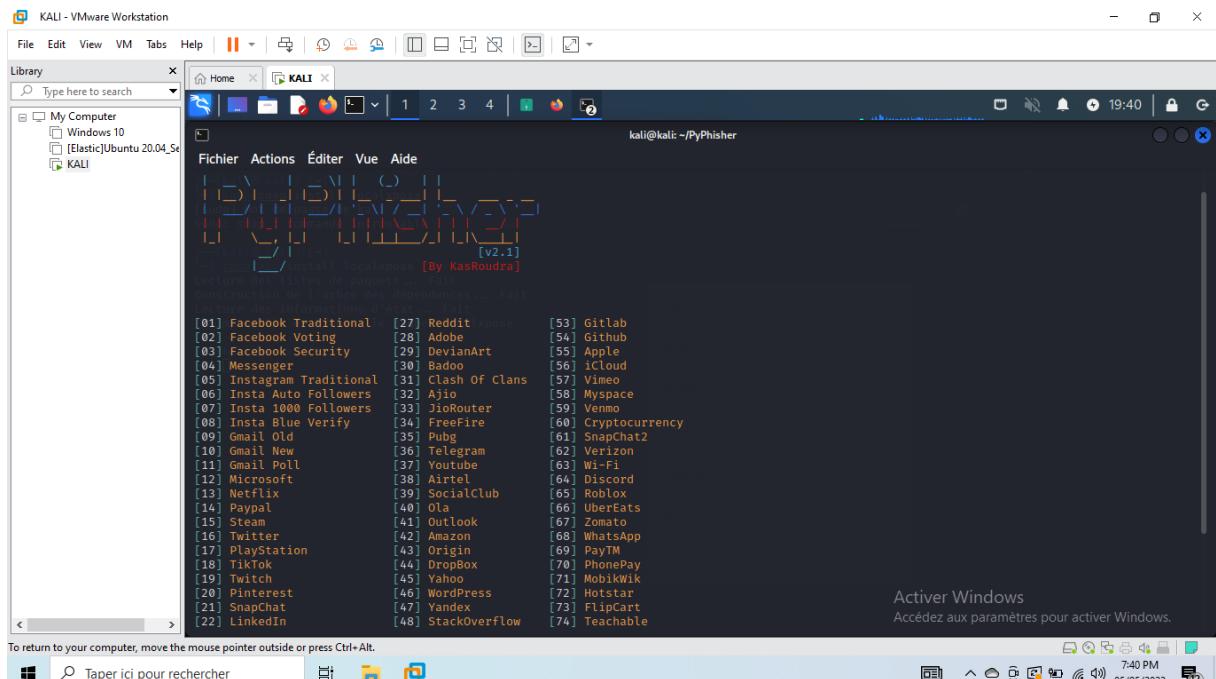


Figure 47: Choisir l'option Facebook

Et voilà, quatre URL malicieux s'affichent sur le terminal avec lesquelles nous allons effectuer l'attaque.

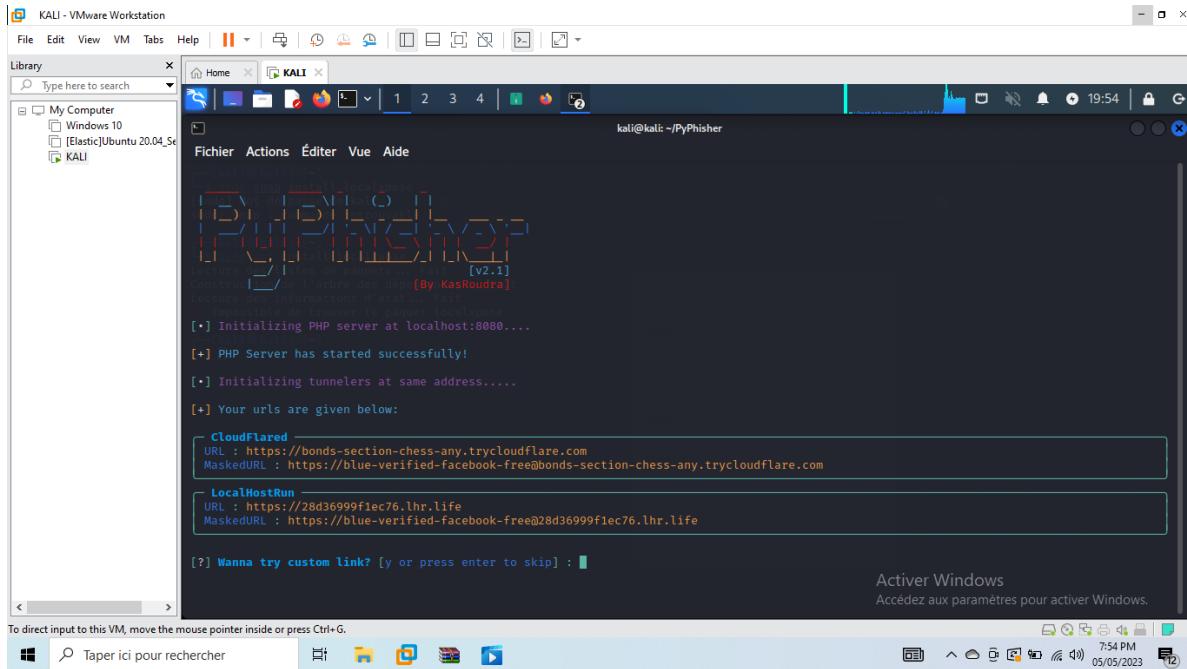


Figure 48: URL malicieux

Par la suite, lorsque nous avons entré les informations d'identification sur le phishing, les informations d'identification saisies sont capturées par l'outil PyPhisher.

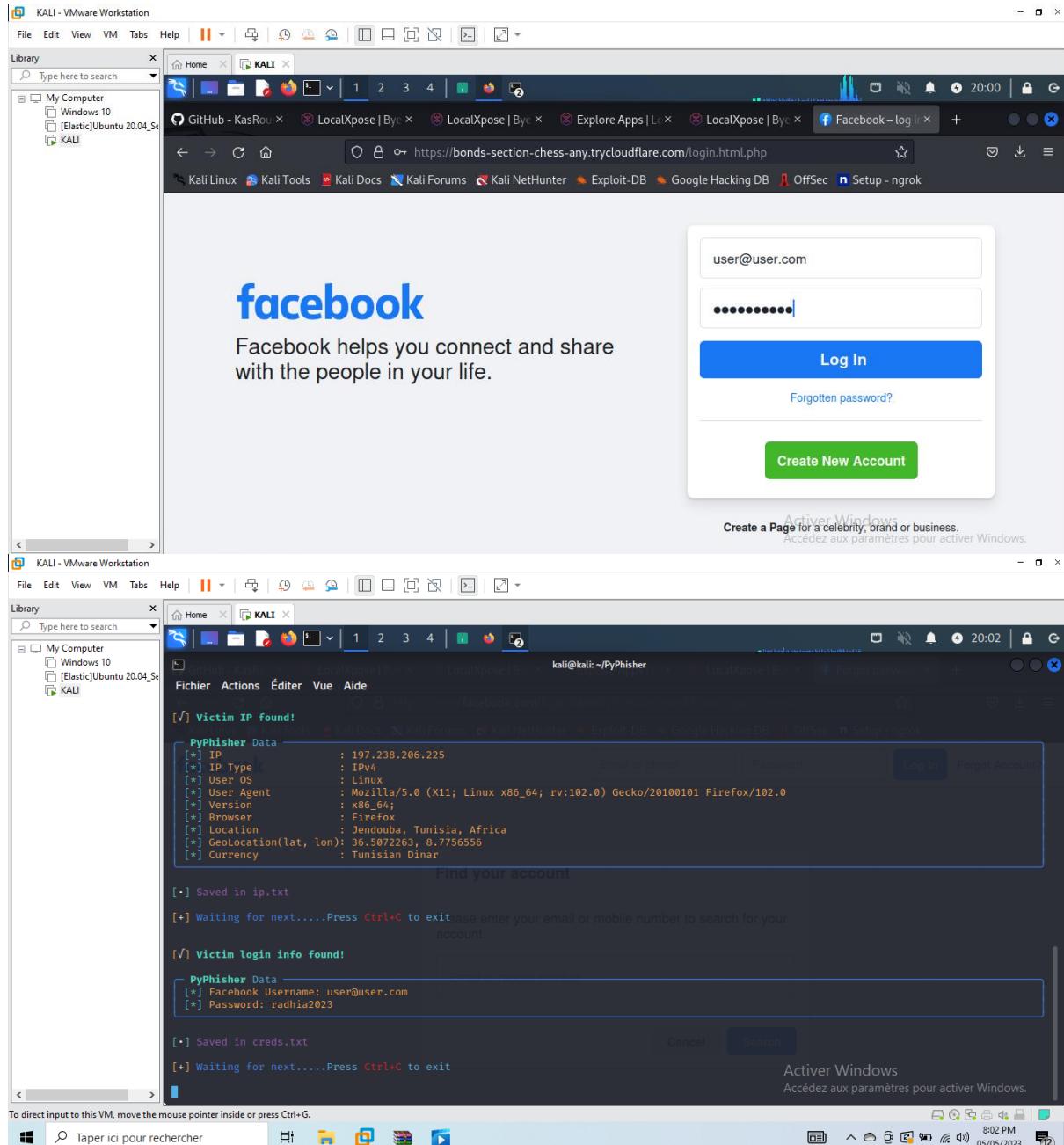


Figure 49: Données de la victime

8. Les sandbox

8.1. App Any Run

Suite à la création d'un compte au niveau du plateforme Any Run, nous avons cliqué sur « new task » et nous avons spécifié l'url. Ensuite, nous avons cliqué sur « run a public task », c'est-à-dire que les tâches que nous pouvons exécuter peuvent être accessibles à tout le monde.

Ce dernier va pouvoir analyser et notamment ce dernier présente une activité malicieuse ou pas.

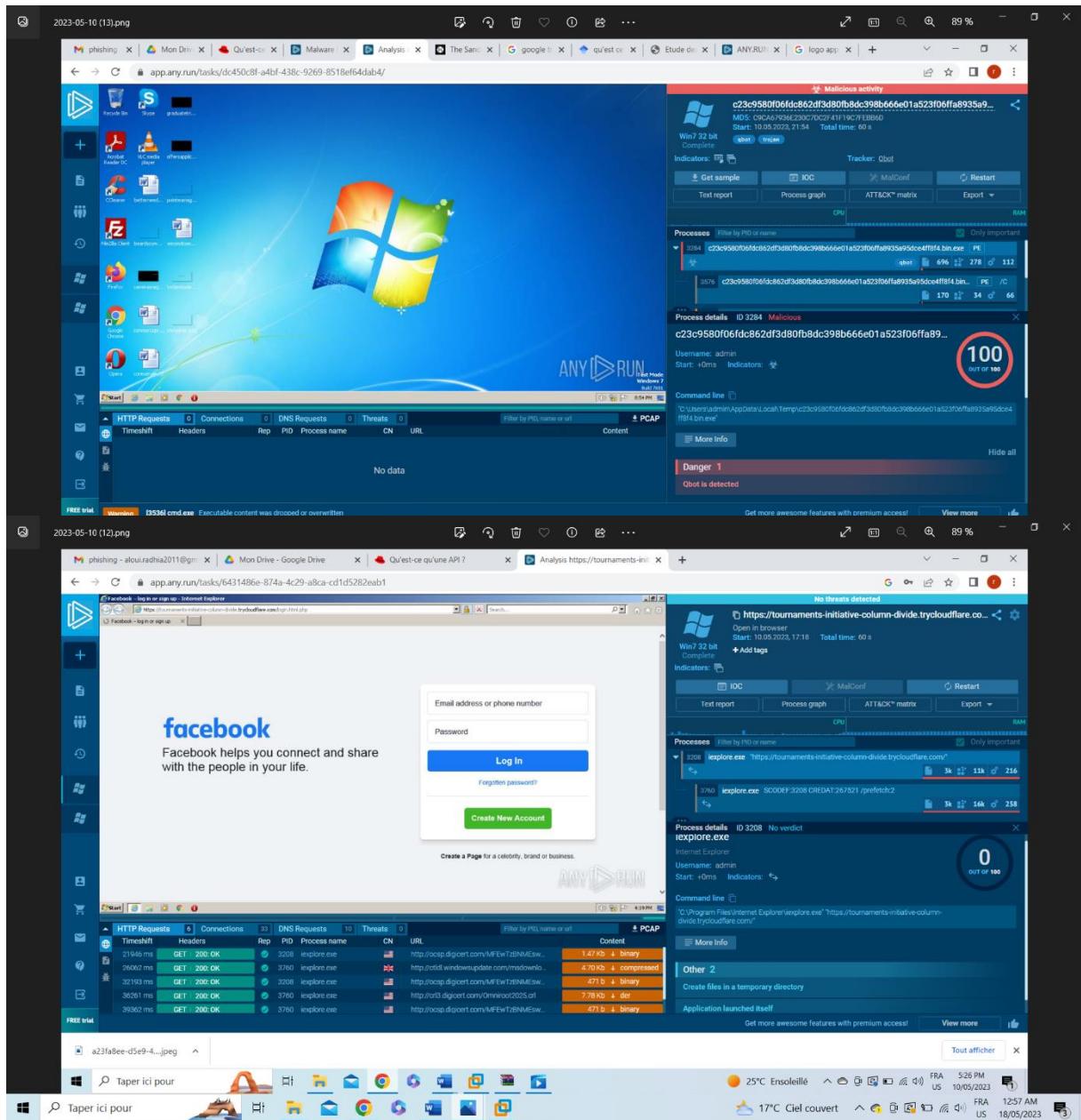


Figure 50: L'analyse de l'URL avec ANY_RAN

8.2. URLScan

URLScan nous fournit une interface sandbox afin de pouvoir analyser des domaines de manière très détaillée et de déterminer certains indicateurs qui nous permettent de déterminer si l'il s'agit d'une attaque de phishing ou pas.

Pour ce faire, dans la recherche, nous avons copié l'URL malicieux puis nous cliquons sur « Public Scan ».

Après une navigation sur la plateforme, certains scripts seront lancés et une récolte des informations aura lieu. Ceci nous permettra de déterminer si on est devant un mail malicieux ou une page malicieuse.

The figure consists of two side-by-side screenshots of the URLScan.io website. Both screenshots show the analysis of the URL <https://auction-cafe-opening-reflects.trycloudflare.com>.

Top Screenshot (Main Analysis View):

- Summary:** This section provides an overview of the website's activity. It states that the website contacted 3 IPs in 2 countries across 2 domains to perform 47 HTTP transactions. The main IP is 104.17.123.55, located in US and belongs to CLOUDFLARENET. The main domain is auction-cafe-opening-reflects.trycloudflare.com. TLS certificate: Issued by Cloudflare Inc ECC CA-3 on April 28th 2023. Valid for: a year.
- urLscan.io Verdict:** Potentially Malicious.
- Live information:** Google Safe Browsing: No classification for auction-cafe-opening-reflects.trycloudflare.com. Current DNS A record: 104.17.123.55 (AS13335 - CLOUDFLARENET, US).
- Screenshot:** A preview of the website showing a Facebook login page.
- Page URL History:** Shows the URL <https://auction-cafe-opening-reflects.trycloudflare.com/>.

Bottom Screenshot (Detailed View):

- Domain & IP information:**

IP/ASNs	IP Detail	Domains	Domain Tree	Links	Certs	Frames
8	104.17.123.55	13335 (CLOUDFLARENET)				
1	2a03:2880:f083:9:face:b00c:0:3	32934 (FACEBOOK)				
47		3				
- Detected technologies:** PHP (Programming Languages).
- Page Statistics:**

Requests	HTTPS	IPv6	Domains	Subdomains
47	19 %	50 %	2	2
3	2	185 kB	726 kB	0
IPs	Countries	Transfer	Size	Cookies

Figure 51: L'analyse de l'URL avec URLScan

8.3. VirusTotal

Avec VirusTotal, nous pouvons voir si un fichier téléchargé ou un Url sont dangereux ou pas. Pour ce faire, il suffit juste de cliquer sur URL. Ensuite, nous cliquons sur « search », nos URL seront analysées et nous aurons la réponse.

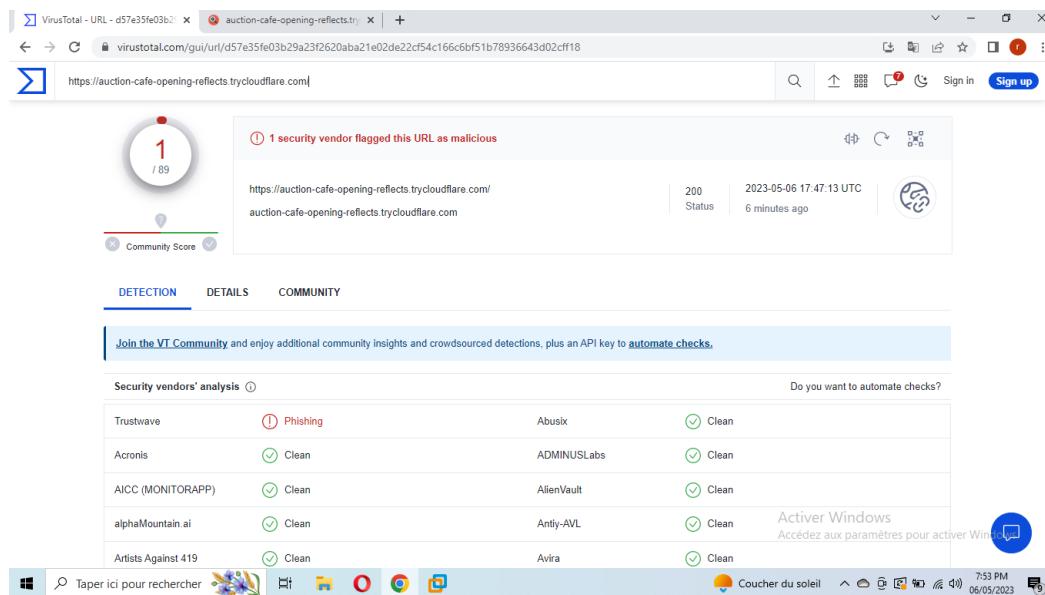


Figure 52: L'analyse de l'URL avec VirusTotal

9. Blocage de l'attaque phishing

Le blocage du phishing est une mesure de sécurité essentielle pour protéger les utilisateurs et les organisations contre les attaques de phishing. Il est important de noter que bien que ces mesures de blocage soient efficaces, les attaquants cherchent constamment de nouvelles façons de contourner les systèmes de sécurité. Par conséquent, il est essentiel de maintenir une veille continue de la sécurité, de mettre à jour régulièrement les logiciels et les systèmes de sécurité, et d'adopter une approche en couches pour une protection complète contre le phishing et d'autres attaques.

Il existe plusieurs méthodes et outils utilisés pour bloquer efficacement le phishing. Voici quelques-unes des approches couramment utilisées :

- **Filtres de courrier indésirable** : Les fournisseurs de messagerie et les services de sécurité utilisent des filtres de courrier indésirable pour identifier les e-mails suspects et les marquer comme tels, voire les bloquer complètement. Ces filtres analysent diverses caractéristiques des e-mails, telles que l'expéditeur, le contenu, les liens et les pièces jointes, afin de déterminer leur légitimité.
- **Listes de réputation d'adresses URL et d'expéditeurs** : Les solutions de sécurité utilisent des listes de réputation d'adresses URL et d'expéditeurs pour identifier les sites web et les expéditeurs associés au phishing. Ces listes sont régulièrement mises à jour en fonction des signalements et des analyses de sécurité, permettant ainsi de bloquer les connexions aux sites web malveillants et les e-mails provenant de sources non fiables.

- **Analyse comportementale** : Certaines solutions de sécurité utilisent des techniques d'analyse comportementale pour détecter les signes de phishing. Elles examinent les schémas de comportement des e-mails, des sites web ou des applications suspectes, et les comparent à des modèles de comportement connus du phishing. Cela permet de repérer des anomalies et d'identifier les attaques potentielles.
- **Éducation et sensibilisation** : Outre les mesures techniques, il est essentiel de sensibiliser les utilisateurs aux techniques de phishing et de les éduquer sur les bonnes pratiques en matière de sécurité. Les programmes de formation à la cybersécurité peuvent aider les utilisateurs à identifier les signes de phishing, à éviter de cliquer sur des liens suspects et à être prudents lorsqu'ils partagent des informations sensibles en ligne.
- **Signalement et blocage collaboratif** : Les utilisateurs peuvent signaler les e-mails de phishing, les sites web suspects et les expéditeurs non fiables aux fournisseurs de services et aux communautés de sécurité. Ces rapports aident à identifier les nouvelles menaces de phishing et à mettre à jour les mesures de blocage pour protéger les autres utilisateurs.

10. Conclusion

Tout au long de ce dernier chapitre, nous avons installé Splunk Entreprise et Splunk Universal Forwarder. La configuration a également eu lieu. Ensuite, nous avons surveiller les journaux sur un Windows distant et nous avons créé une approche pour écouter un port UDP de type Syslog. Puis, nous avons configuré le collecteur d'évènement http et nous avons créé un exemple d'alerte pour une tentative de connexion. Enfin, nous avons réalisé une tentative d'attaque de phishing et nous avons présenté quelques outils pour bloquer efficacement ce type d'attaque.

Conclusion Générale

Avec le nombre croissant de menaces de sécurité sur Internet, les entreprises doivent investir dans des solutions de sécurité robustes pour protéger leur infrastructure réseau. L'une de ces solutions est SPLUNK, qui fournit une plate-forme complète pour analyser les données de sécurité provenant de différentes sources. Ce dernier est conçu pour être très flexible et peut être utilisé pour analyser différents types de données de sécurité. L'objectif de ce rapport est de fournir une analyse approfondie de la solution de sécurité SPLUNK et de son utilisation pour l'analyse de la sécurité du réseau.

Cette solution va permettre une analyse dynamique de ces événements selon des règles construites et stockées, ce qui va aider majoritairement dans la facilitation de la supervision de la sécurité du système en offrant la possibilité de la recherche rapide et la filtration de ces évènements. A la fin de chaque analyse, un ensemble des alertes peut être ajouté et affiché.

D'une façon générale ce projet nous a été très bénéfique car nous avons enrichi nos connaissances sur les deux plans : théorique et pratique, et nous pouvons dire que les objectifs fixés au début ont été atteints.

Bibliographie

- [1] <https://www.tunisetelecom.tn>
- [2] Sécurité informatique : risques, stratégies et solutions : échec au cyber-roi
- [3]https://download.geo.drweb.com/pub/drweb/unix/doc/HTML/ControlCenter/fr/dw_8_app_a_threat_types.htm
- [4]<https://blog.netwrix.fr/2018/07/04/les-10-types-de-cyberattaques-les-plus-courants>
- [5] <https://www.proofpoint.com/fr/threat-reference/phishing>
- [6] <https://www.novahoster.tn>
- [7]https://www.novell.com/docrep/documents/yuufbom4u2/gartner_magic_quadrant_siem_report_may2011.pdf
- [8] Splunk Certified Study Guide: Prepare for the User, Power User, and Enterprise Admin Certification. ‘Deep Mehta’
- [9] Etude des malwares évasifs : conception, protection et détection Cédric Herzog
- [10] Petites entreprises et sécurité informatique : un mariage de raison ?
- [11] <https://geekflare.com/fr/best-url-scanners>
- [12]https://docs.splunk.com/Documentation/Splunk/9.0.4/Data/UsetheHTTPEventCollector#Configure_HTTP_Event_Collector_on_Splunk_Enterprise
- [13] <https://quick-tutoriel.com/creer-des-sources-de-donnees-dans-splunk>
- [14] <https://www.geeksforgeeks.org/pyphisher-simple-python-tool-for-phishing>

Résumé

Le rapport donne un aperçu de SPLUNK, de son architecture et de ses fonctionnalités dont le but de sécuriser le DRT télécom de Gafsa.

Dans ce projet, nous proposons une solution pour l'analyse des enregistrements data et sécurité en format de fichiers et logs en temps réel du SI. Cette solution nous permet une analyse dynamique à des événements http. Grâce à HEC nous pouvons surveiller le trafic web, détecter les anomalies et identifier les attaques.

Mots clés : Sécurité, Splunk, SIEM, Logs, Indexation, Alert, Piratage, phishing, PyPhisher

Abstract

The report provides an overview of SPLUNK, its architecture and its functionalities, the aim of which is to secure the Gafsa telecom DRT.

In this project, we propose a solution for the analysis of data and security records in file format and real-time IS logs. This solution allows us a dynamic analysis at http events. Thanks to HEC we can monitor web traffic, detect anomalies and identify attacks.

Keywords: Security, Splunk, SIEM, Logs, Indexing, Alert, Hacking, phishing, PyPhisher