

6560 Esplanade Ave Suite 204, Montréal, Québec H2V 4L5

COURS : GARANTIE DE SECURITE, TESTS ET VALIDATION

Projet Final : Détection d'Attaques avec Splunk

Le cas du phishing ou hameçonnage

Etudiant :

Wilfridy Lormero

Enseignant :

M . Raouf Ouni

SESSION D'AUTOMNE 2025

Table des matières

Introduction.....	2
I. Problématique	3
II. Objectifs du projet.....	4
1. Objectif général	4
2. Objectifs spécifiques.....	4
III. Contexte et justification	4

IV.	Cadre théorique.....	5
1.	Le phishing.....	5
2.	La surveillance de sécurité	5
3.	Splunk	5
V.	Méthodologie	5
VI.	Mise en place de l'environnement contrôlé	6
1.	Installation de Splunk Enterprise.....	7
2.	Installation du redirecteur Splunk sur Windows10.....	10
3.	Configuration de Splunk Enterprise	13
4.	Communication entre le redirecteur et l'instance Splunk Enterprise.....	14
5.	Création des alertes dans Splunk Enterprise.....	19
6.	Création de tableau de bord dans Splunk	24
7.	Installation et configuration de la machine d'attaque(Phishing).....	27
a)	Kali Linux.....	27
b)	Installation.....	27
c)	Préparation de l'attaque avec Pyphishing.....	28
8.	Quelques simples requêtes SPL (Search Processing Language) dans Splunk.....	31
	Conclusion	33
	Annexes	34

Introduction

La multiplication des cyber-menaces, et en particulier des attaques de phishing, représente aujourd’hui un défi majeur pour la sécurité des systèmes d’information. Exploitant la vulnérabilité humaine, le phishing demeure l’un des vecteurs d’attaque les plus efficaces pour obtenir un accès non autorisé ou dérober des informations sensibles.

Dans ce contexte, la mise en place de mécanismes de surveillance et de détection performants constitue une nécessité pour les organisations. Ce projet s'inscrit dans cette perspective en simulant une attaque de phishing dans un environnement contrôlé, afin d'analyser les traces laissées par l'attaque et d'évaluer l'efficacité d'un système de détection basé sur la plateforme **Splunk**.

L'objectif est de développer une compréhension pratique des techniques de détection, de renforcer les compétences en analyse de logs et en configuration d'alertes, et d'acquérir une expérience concrète en gestion d'incidents au sein d'un cadre proche de celui d'un centre opérationnel de sécurité (SOC).

I. Problématique

Dans un environnement numérique où les attaques de phishing sont de plus en plus fréquentes et sophistiquées, comment mettre en place un système de détection efficace, basé sur Splunk, permettant d'identifier rapidement une tentative de compromission et de déclencher une réponse adaptée dans un contexte opérationnel réaliste ?

II. Objectifs du projet

1. Objectif général

Mettre en place un système de détection et de surveillance permettant d'identifier une attaque de phishing simulée à l'aide de la plateforme Splunk.

2. Objectifs spécifiques

- Simuler une attaque de phishing dans un environnement contrôlé.
- Collecter, analyser et interpréter les logs générés par l'attaque.
- Configurer des tableaux de bord Splunk pour visualiser les événements pertinents.
- Définir et mettre en place des alertes de sécurité adaptées.
- Évaluer la capacité du système à détecter l'attaque et à déclencher une réponse.
- Développer des compétences pratiques en surveillance de la sécurité et en gestion d'incidents.

III. Contexte et justification

Les organisations modernes dépendent fortement de leurs systèmes d'information pour assurer la continuité de leurs activités. Cette dépendance s'accompagne d'une exposition accrue aux cyber-menaces, dont le phishing représente l'un des risques les plus critiques. Les conséquences d'une attaque réussie peuvent être graves : vol de données, compromission de comptes, propagation de malwares, pertes financières ou atteinte à la réputation.

Face à ces enjeux, les entreprises investissent dans des solutions de surveillance avancées telles que Splunk, qui permettent de collecter, corrélérer et analyser de grandes quantités de données issues des systèmes d'information. La maîtrise de ces outils constitue aujourd'hui une compétence essentielle pour les professionnels de la cyber-sécurité.

Ce projet répond donc à un double besoin :

1. Comprendre les mécanismes d'une attaque de phishing, de sa conception à son exécution.
2. Développer une expertise pratique dans l'utilisation de Splunk pour la détection et la réponse aux incidents.

IV. Cadre théorique

1. Le phishing

- Technique d'ingénierie sociale visant à tromper un utilisateur.
- Utilise généralement des courriels frauduleux, des liens malveillants ou des pages web falsifiées.
- Objectifs : vol d'identifiants, installation de malwares, accès non autorisé.

2. La surveillance de sécurité

- Processus continu visant à détecter des comportements anormaux.
- Repose sur la collecte et l'analyse de logs provenant de différentes sources.
- Constitue le cœur des activités d'un SOC.

3. Splunk

- Plateforme SIEM (Security Information and Event Management).
- Permet l'ingestion, l'indexation et la visualisation de données en temps réel.
- Fonctionnalités clés :
 - recherche avancée (SPL),
 - tableaux de bord,
 - alertes automatisées,
 - corrélation d'événements.

V. Méthodologie

La méthodologie adoptée pour ce projet se déroule en plusieurs étapes :

Étape 1 : Préparation de l'environnement

- Mise en place d'un environnement contrôlé (machine victime, serveur Splunk, serveur d'attaque).
- Configuration des sources de logs pertinentes.

Étape 2 : Simulation de l'attaque de phishing

- Conception d'un courriel frauduleux ou d'une page de phishing.
- Envoi du message à la machine cible.
- Observation du comportement de l'utilisateur simulé.

Étape 3 : Collecte et analyse des logs

- Récupération des journaux générés par l'attaque.
- Analyse des événements clés : clics, connexions, exécutions, anomalies.

Étape 4 : Configuration de Splunk

- Indexation des logs.
- Création de requêtes SPL pour identifier les traces de l'attaque.
- Mise en place de tableaux de bord de visualisation.

Étape 5 : Mise en place d'alertes

- Définition de seuils et de conditions de détection.
- Configuration d'alertes automatisées dans Splunk.

Étape 6 : Évaluation et interprétation

- Vérification de la capacité du système à détecter l'attaque.
- Analyse des résultats et identification des limites.

VI. Mise en place de l'environnement contrôlé

Pour réaliser la simulation de phishing, un environnement contrôlé a été mis en place. Il se compose de deux machines Windows 10 jouant le rôle de postes victimes, (sur lesquelles est installé) ou sera installé un redirecteur Splunk, d'un serveur Windows Server 2019 utilisé pour l'installation de Splunk (Entreprise), (ainsi que) d'un serveur d'attaque basé sur Kali Linux ; le tout dans un environnement virtuel sur VMware. Cette configuration isolée permet de reproduire un scénario réaliste tout en garantissant la sécurité et la maîtrise des interactions entre l'attaquant, les machines ciblées et l'outil de détection.

1. Installation de Splunk Enterprise

Après l'installation de notre environnement virtuel VMware et l'installation de notre serveur Windows serveur 2019, nous passons à l'installation de Splunk Enterprise dans Windows serveur 2019 (en) suivant les étapes (suivantes):

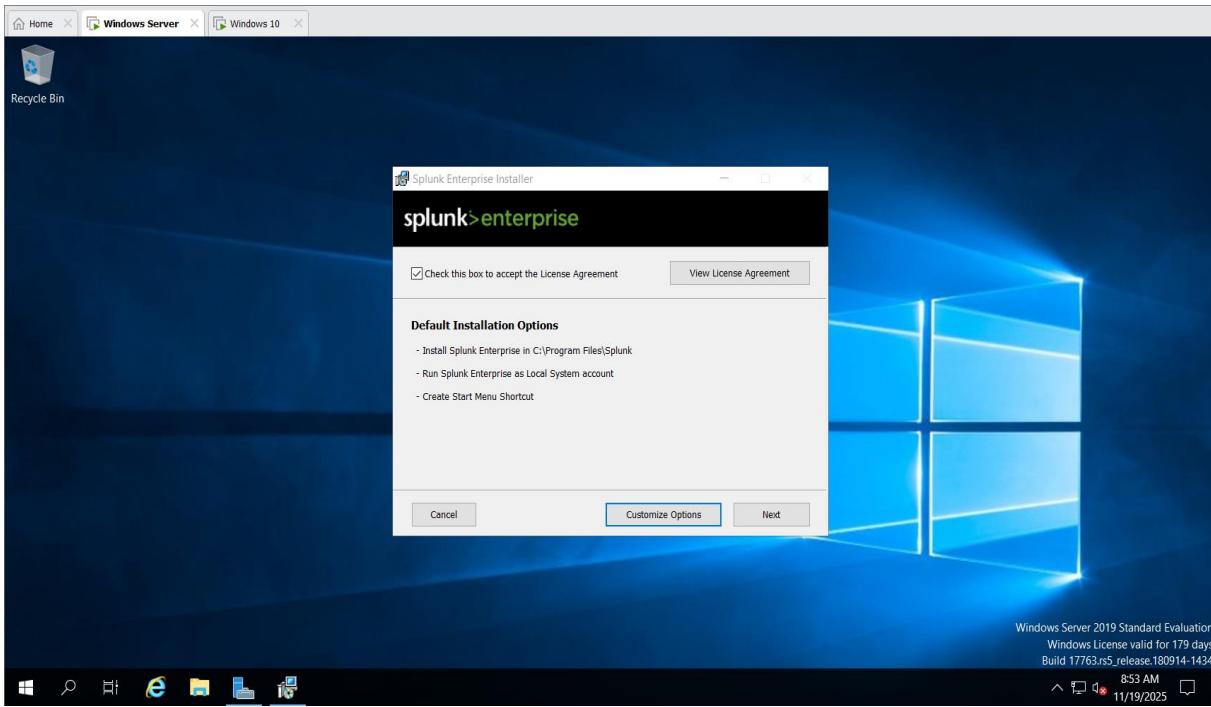
Accédez à la page de téléchargement de Splunk: Visitez le site officiel de Splunk à l'adresse, <https://www.splunk.com/> et cliquez sur "Free Splunk" dans le coin supérieur droit.

Création d'un compte: Si vous n'êtes pas connecté ou si vous n'avez pas de compte associé à Splunk, vous devrez créer un compte.

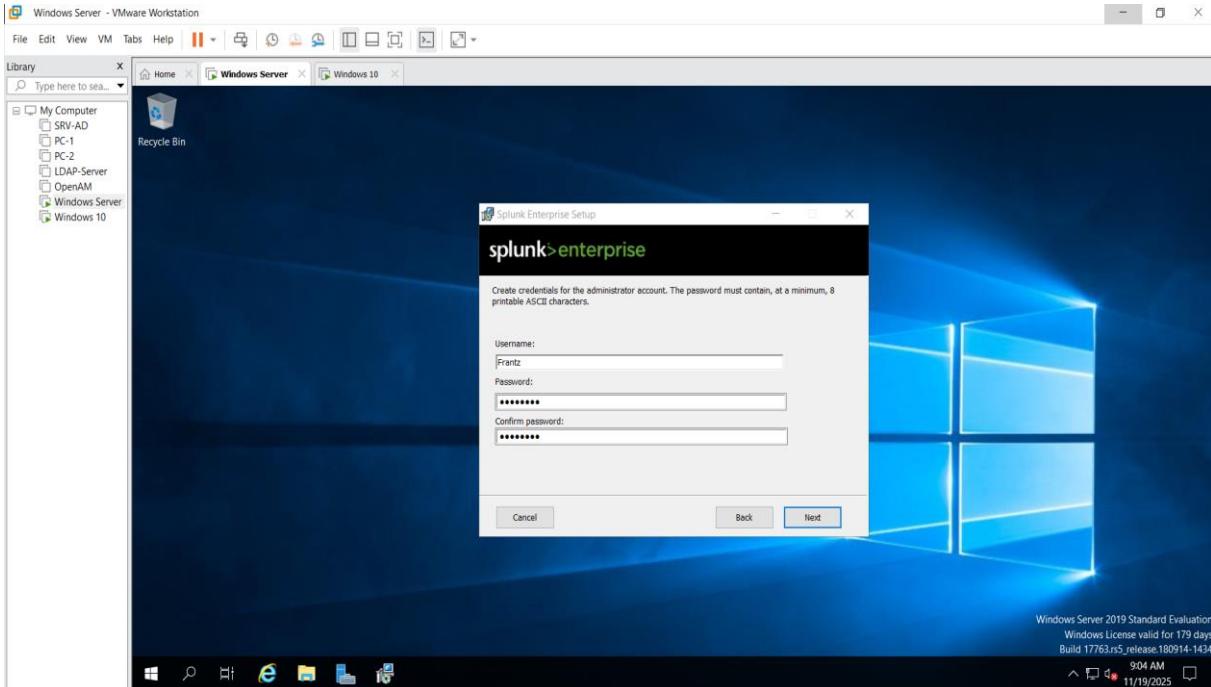
Téléchargement du package: Sous l'onglet Windows, cliquez sur le bouton '**téléchargement**' selon la configuration de votre machine.

Exécution du package: Une fois le package téléchargé, exécuter le pour commencer l'installation.

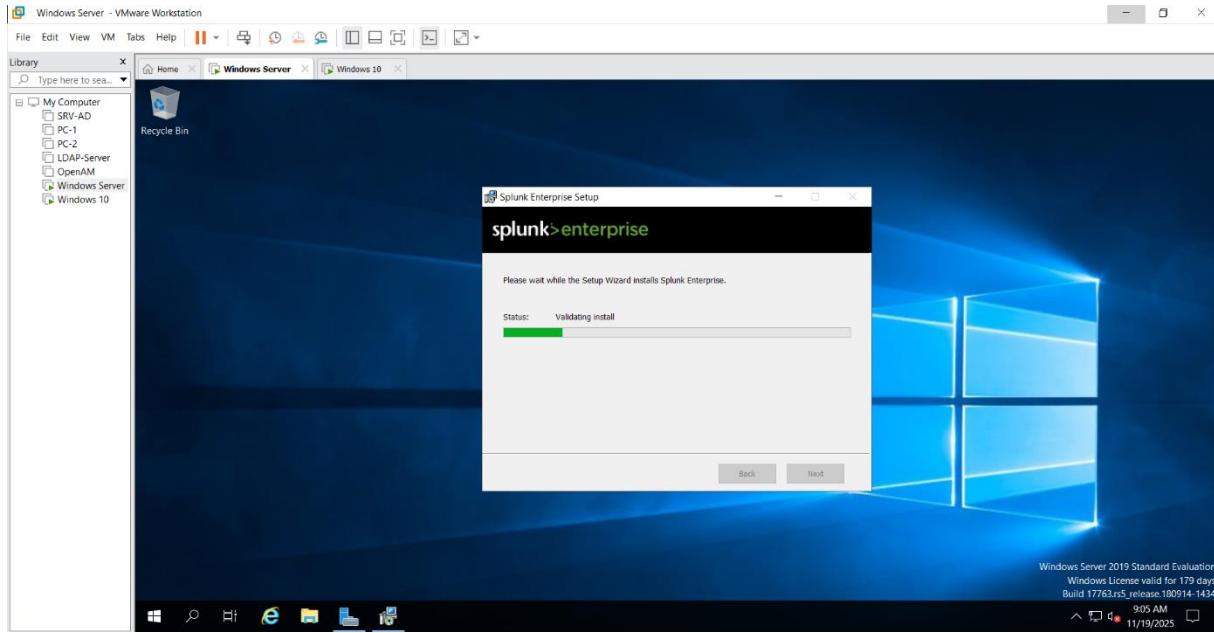
On obtient la fenêtre suivante :



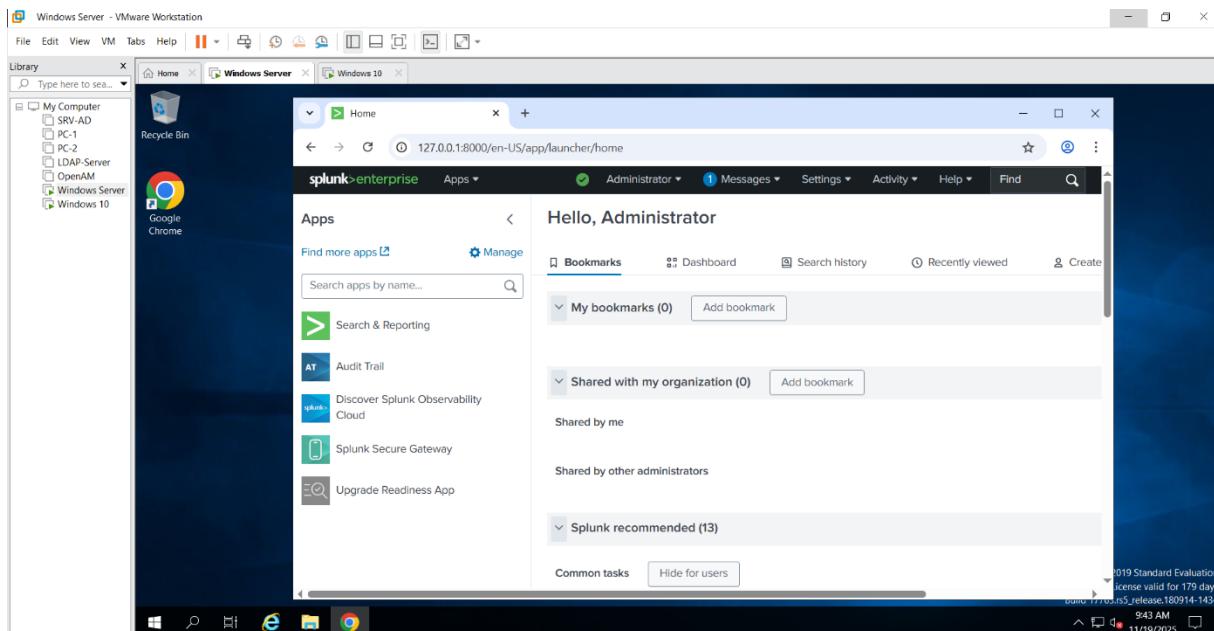
Après avoir coché la case d'acceptation du contrat de License et laissé les options par défaut, on continue sur suivant pour créer un compte tout en respectant les exigences liées au mot de passe



Ensuite sur suivant pour commencer l'installation de splunk Enterprise.



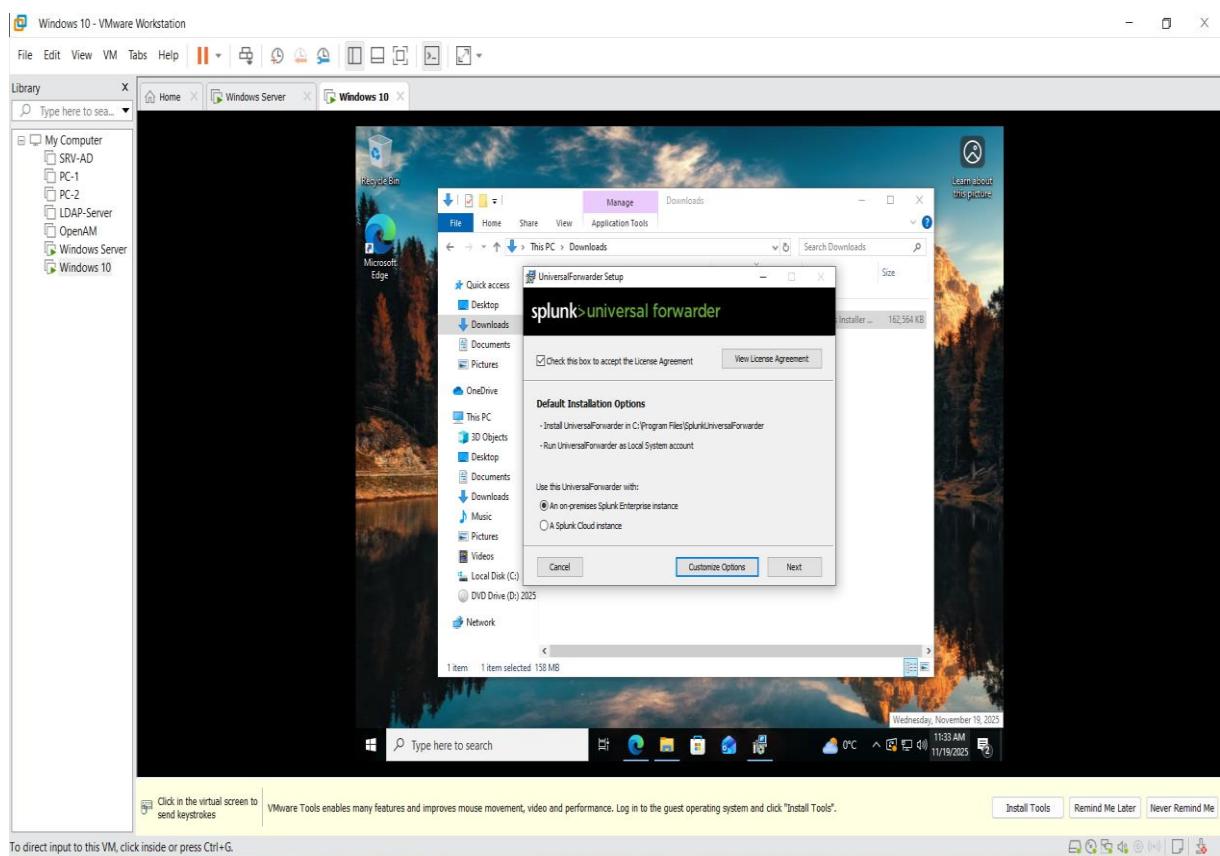
Une fois l'installation terminée, on clique sur le bouton terminer et on lance Splunk Enterprise à partir de notre navigateur de préférence à l'exception d'**internet explorer** non supporté. Vu que Splunk Enterprise est installé sur le serveur, Splunk Web est configuré par défaut pour n'écouter que sur l'adresse : 127.0.0.1 et le port utilisé par Splunk Web est 8000. Donc dans le navigateur on entrera l'adresse 127.0.0.1:8000 pour y accéder.



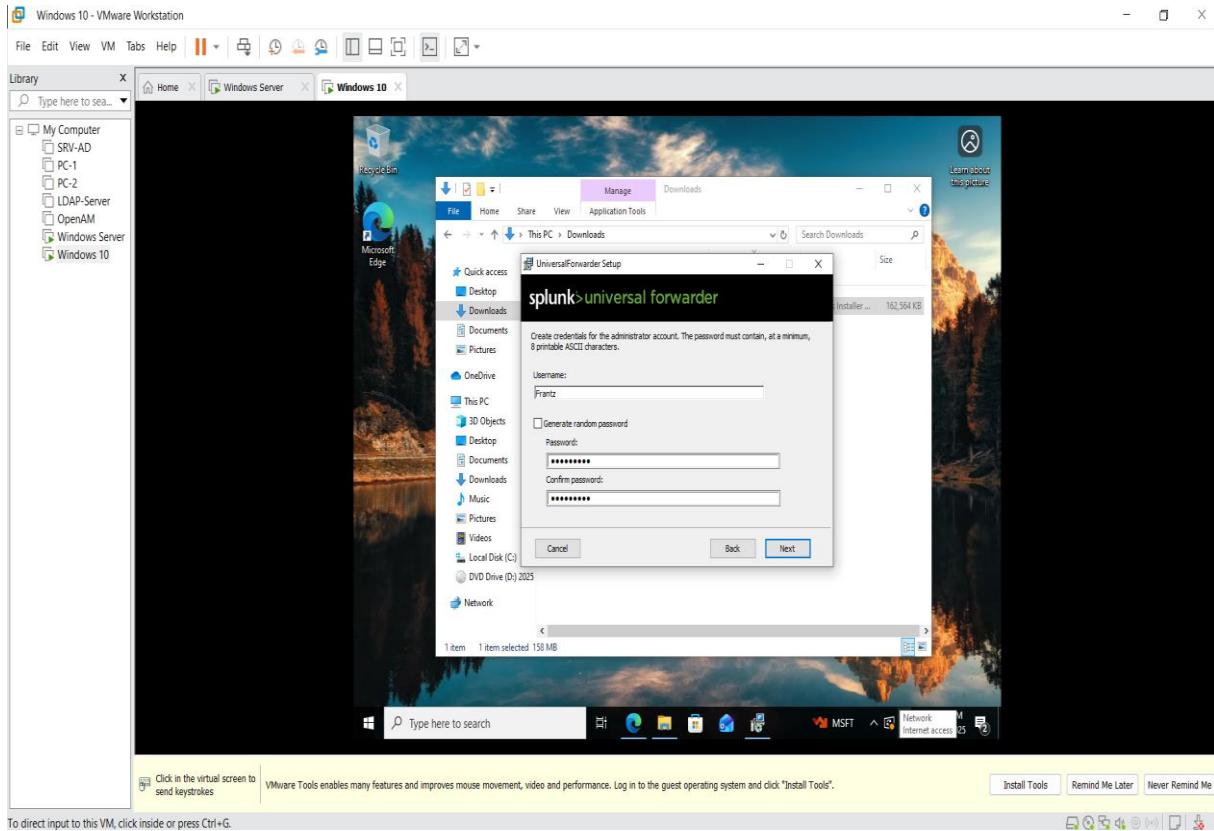
2. Installation du redirecteur Splunk sur Windows10

Après l'installation de nos machines cibles Windows 10, il est question d'installer des redirecteurs Splunk qui pourront collecter et envoyer des données de ces machines vers le serveur Splunk central ; en gros les redirecteurs récupèrent les logs d'application, les événements système, les logs de sécurité, etc.

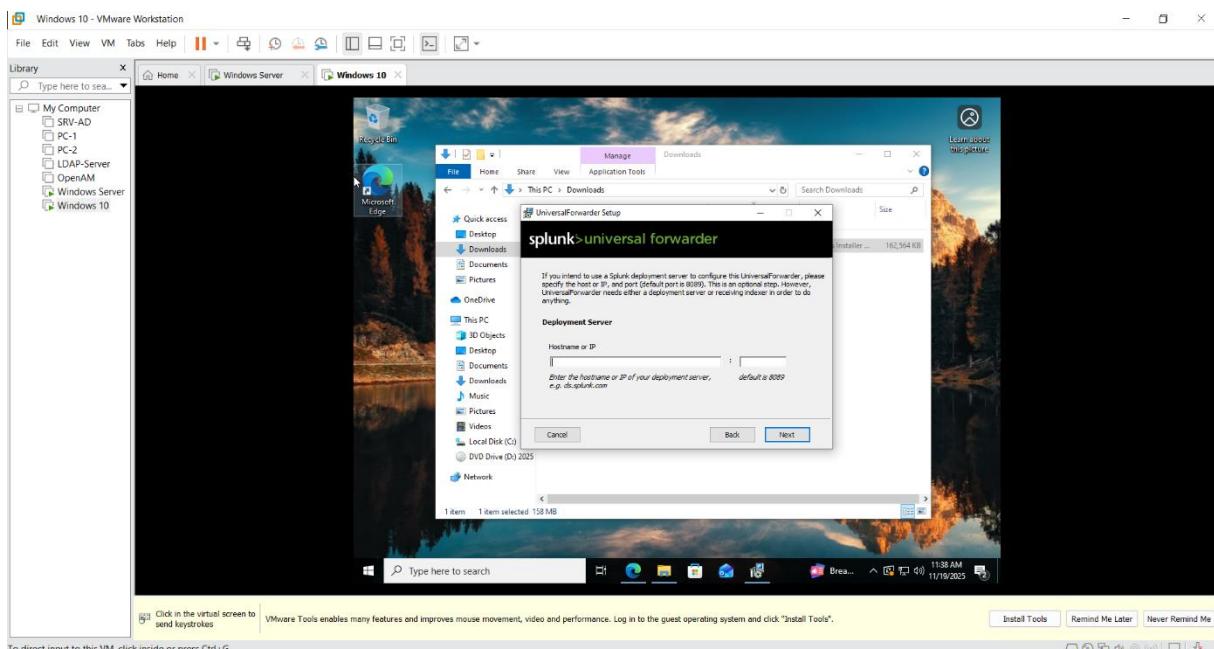
Après le téléchargement sur https://www.splunk.com/Fr_fr/Download, on lance l'exécutable et on obtient cette fenêtre



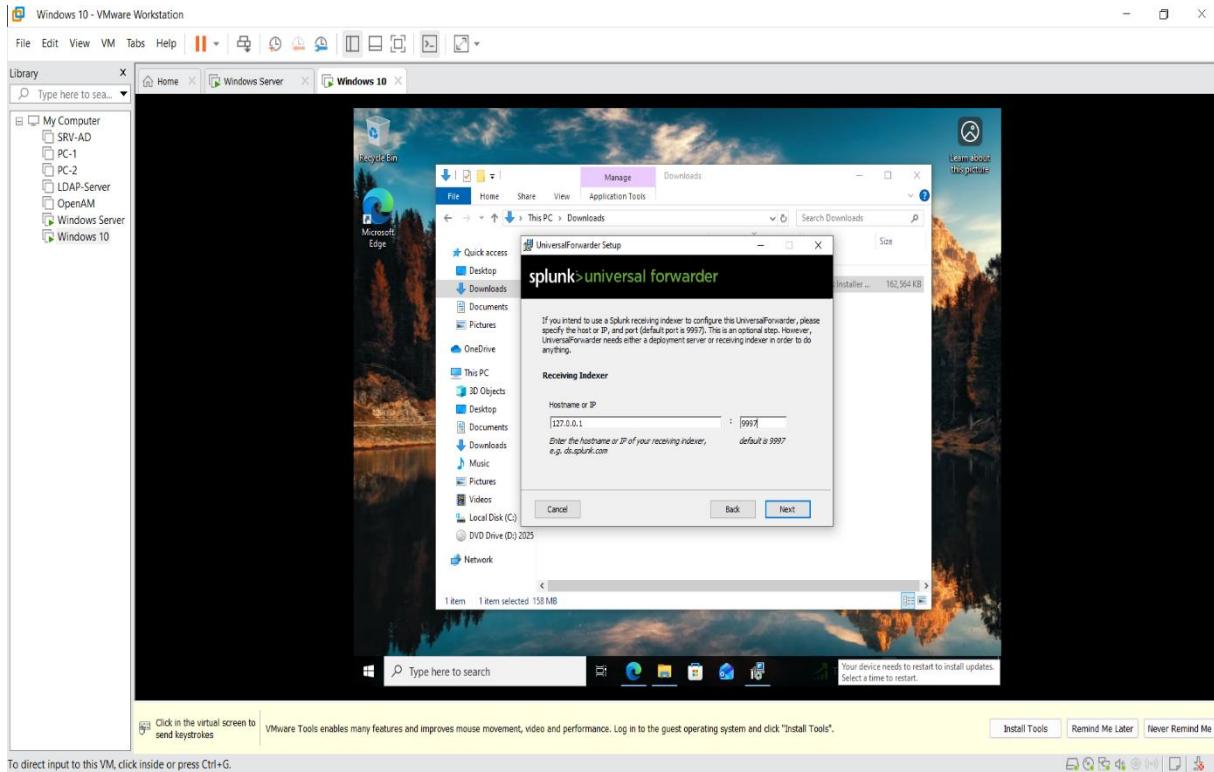
Après avoir coché pour accepter le contrat de licence, on crée un compte administrateur et un mot de passe avec les exigences liées à ce dernier.



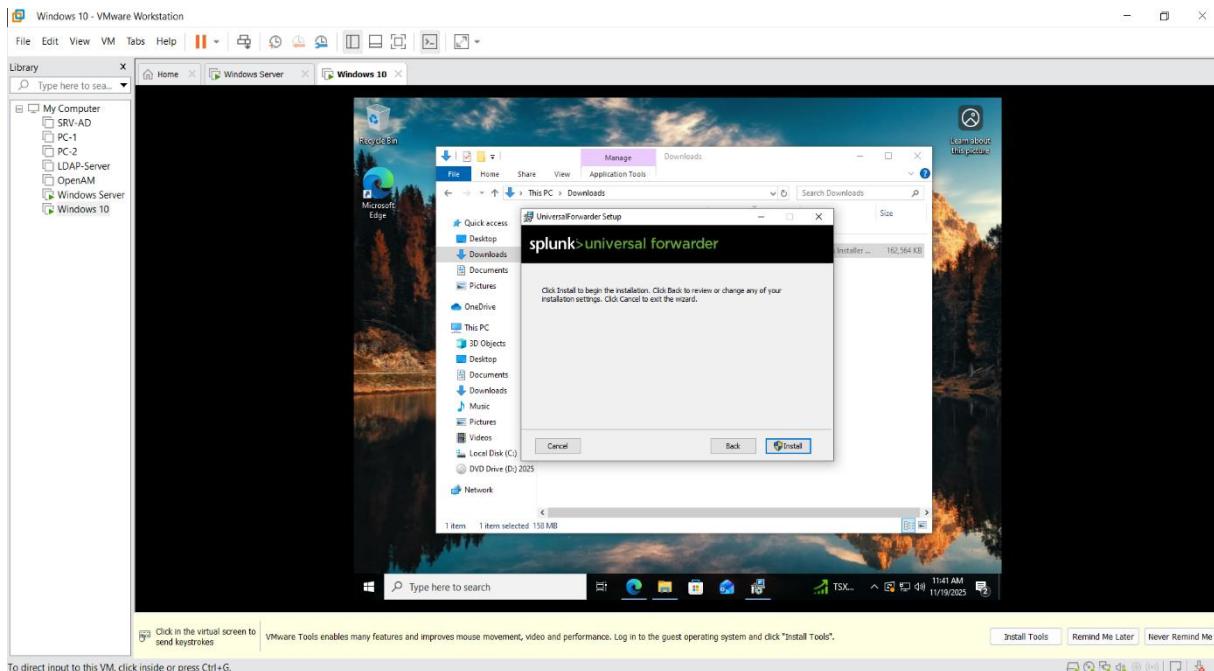
Ensuite on entre l'adresse du serveur de déploiement et le port par défaut 8089 ou pas.



On entre l'adresse du serveur Splunk qui reçoit les données envoyées par les redirecteurs et le port par défaut : 9997.

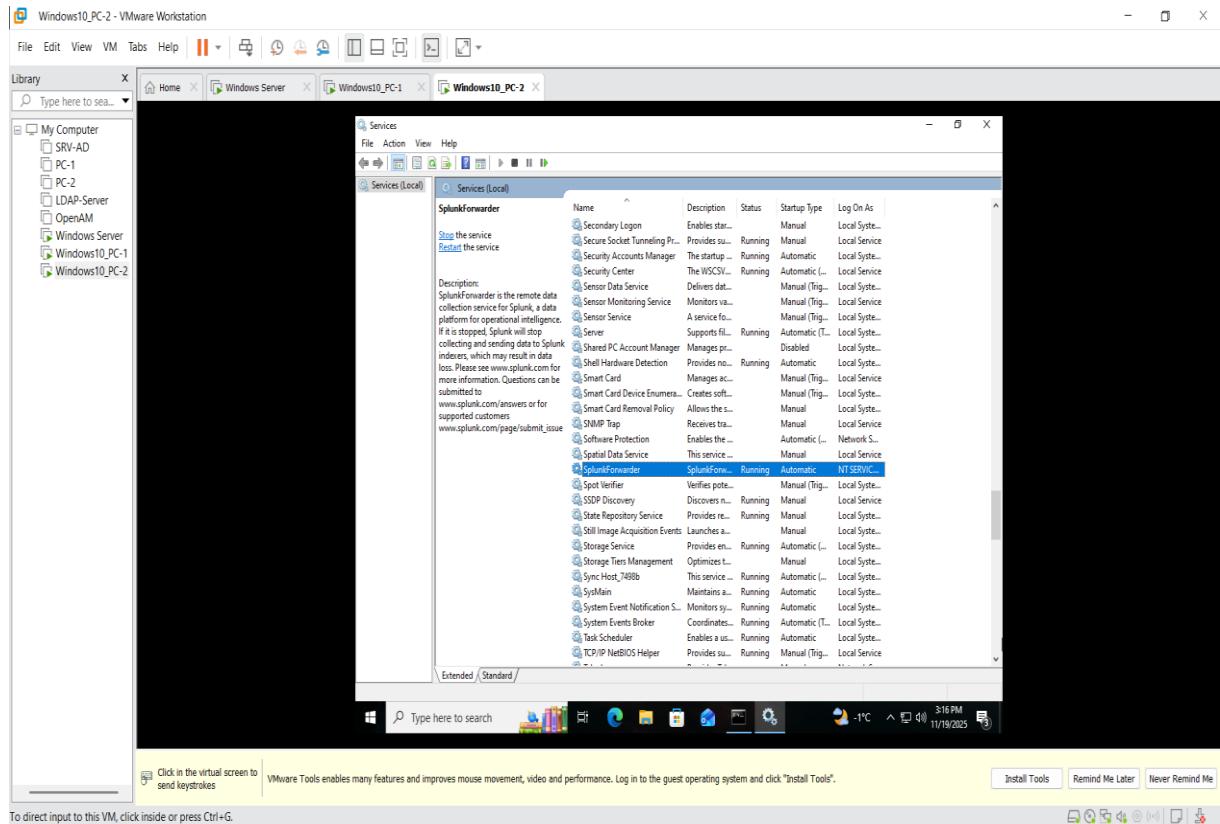


On clique sur suivant puis sur installer pour commencer l'installation.



Après l'installation, on clique sur finir ; on pourra vérifier les configurations faites dans : **C:\Programmes Files\SplunkUniversalForwarder\etc\system\local\outputs.conf**. Ensuite on va dans services Windows grâce à la commande en mode administrateur dans l'invite de commande services.msc et on recherche SplunkForwarder Service et on le redémarre.

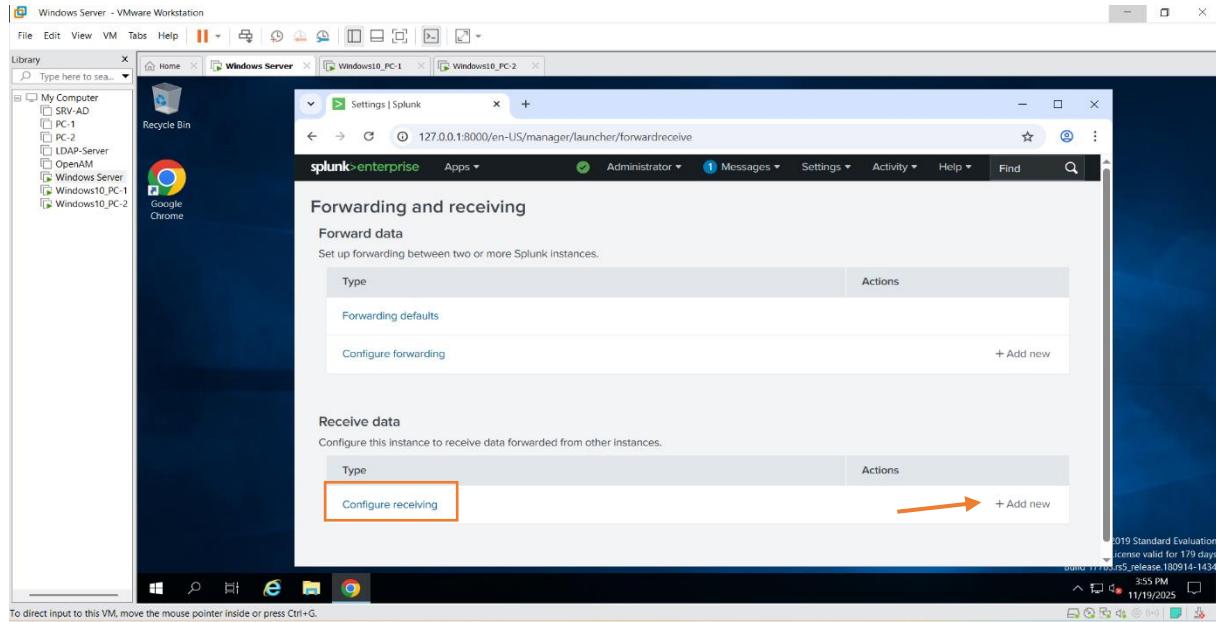
On s'assure qu'il est : **En cours d'exécution** et le type de démarrage : **Automatique**, pour chaque windows10



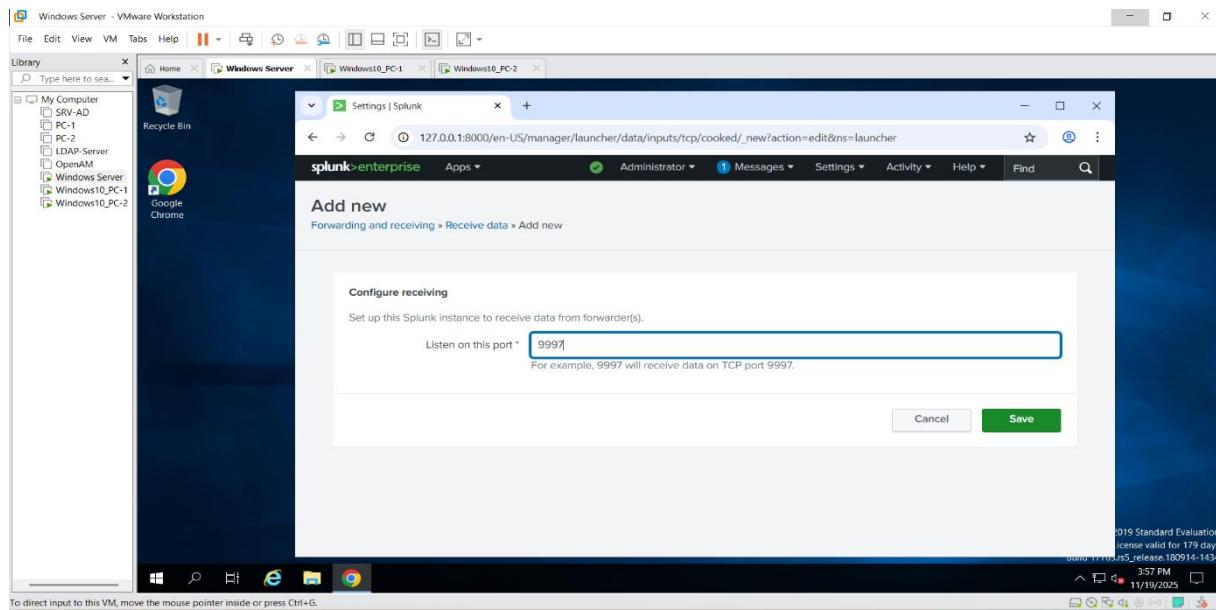
3. Configuration de Splunk Enterprise

Après l'installation de Splunk Enterprise et des redirecteurs Splunk dans les machines windows10, il faut configurer Splunk Enterprise pour qu'il puisse recevoir les données provenant des redirecteurs.

Dans Splunk, on va dans Setting->Forwarding and receiving et on configure l'instance qui recevra les données provenant des autres instances. On clique sur + Add new



On ajoute le port d'écoute par lequel l'instance Splunk recevra les données du redirecteur : 9997 et on enregistre.



4. Communication entre le redirecteur et l'instance Splunk Enterprise

Le redirecteur et Splunk Enterprise ne communiquent pas encore, il est essentiel d'assurer la compatibilité et la bonne communication entre le redirecteur et l'instance Splunk Enterprise, c'est pour cela que l'ajout d'**extension Splunk** pour Microsoft Windows va permettre de définir des sources de données spécifiques, de normaliser les données, d'appliquer des

extractions de champs, et de garantir que les données envoyées sont bien interprétées par le serveur.

Etapes d'installation

- Aller sur le site : <https://splunkbase.splunk.com>
- Télécharger l'extension Splunk Add-ons for Microsoft Windows
- Installer l'extension : pour cela, on va dans le gestionnaire des applications installer des applications à partir d'un fichier et on va chercher le fichier qu'on vient de télécharger, ensuite on le charge. Une fois l'installation terminée on pourra le voir au niveau des applications installées dans Splunk Enterprise et vérifier qu'il est bien activé
- Configurer les entrées de données
 - Activer des entrées prédéfinies pour collecter des données dans notre cas : les journaux ou évènements (Applications, Sécurité et Système) au niveau du redirecteur dans le fichier

C:\Program Files\SplunkUniversalForwarder\etc\apps\Splunk_TA_windows\local

```
##### OS Logs #####
[WinEventLog://Application]
disabled = 0
start_from = oldest
current_only = 0
checkpointInterval = 5
RenderXml=false
```

```
[WinEventLog://Security]
disabled = 0
start_from = oldest
current_only = 0
evt_resolve_ad_obj = 1
checkpointInterval = 5
```

```
blacklist1 = EventCode="4662" Message="Object  
Type:(?!\\s*groupPolicyContainer)"  
  
blacklist2 = EventCode="566" Message="Object  
Type:(?!\\s*groupPolicyContainer)"  
  
renderXml=false
```

[WinEventLog://System]

```
disabled = 0  
  
start_from = oldest  
  
current_only = 0  
  
checkpointInterval = 5  
  
renderXml=false
```

[WinEventLog://Microsoft-Windows-PrintService/Operational]

```
disabled = 1  
  
start_from = oldest  
  
current_only = 0  
  
checkpointInterval = 5
```

Il est à noter qu'on a installé Sysmon sur le redirecteur et crée l'index correspondant dans Splunk Enterprise, car il permet de collecter des événements détaillés, comme les créations de processus, les connexions réseau, les modifications de fichiers, etc. En envoyant ces données vers splunk, on obtient une analyse approfondie de la sécurité et la performance du système

[WinEventLog://Microsoft-Windows-Sysmon/Operational]

```
disabled = 0  
  
index = sysmon  
  
renderXml=false
```

Après on fait un enregistrement du fichier et on redémarre le service SplunkForwarder.

- Création des indexes correspondants dans Splunk Enterprise

Dans Splunk, on va dans **settings->indexes->New index** et on donne un nom significatif selon les règles de nommage pour les journaux ou évènements configurés dans le redirecteur ; les autres options de configurations restent inchangées et en enregistre.

The screenshot shows the Splunk 10.0.2 interface for managing indexes. On the left, there's a list of existing indexes. In the center, a modal window titled "New Index" is open, showing the configuration for a new index named "win_system". The "General Settings" tab is active. The "Index Name" field is filled with "win_system". The "Index Data Type" section has "Events" selected. The "Home Path", "Cold Path", and "Thawed Path" fields are all marked as optional. At the bottom of the modal, there are "Save" and "Cancel" buttons, with "Save" being the active button.

This screenshot is identical to the one above, showing the "New Index" dialog for "win_system". The only difference is the timestamp at the bottom right of the interface, which is now 2:46 PM on 11/25/2025.

The screenshot shows the Splunk Enterprise web interface. In the top navigation bar, there are tabs for Home, Windows Server, Windows10_PC-1, and Windows10_PC-2. The main content area is titled 'Indexes' and shows a list of existing indexes. A modal window titled 'New Index' is open, prompting for index settings. The 'General Settings' tab is selected, showing fields for 'Index Name' (set to 'win_security'), 'Index Data Type' (set to 'Events'), and 'Home Path' (set to 'optional'). Below this, there are fields for 'Cold Path' and 'Thawed Path', both also set to 'optional'. At the bottom of the modal are 'Save' and 'Cancel' buttons.

On redémarre le serveur Splunk

The screenshot shows a Windows Command Prompt window titled 'Administrator: Command Prompt'. The user runs the command 'C:\Program Files\Splunk\bin>splunk.exe restart'. The output shows the Splunk service stopping, then starting again. The log message indicates that all preliminary checks passed. A message box at the bottom right says 'Your session has expired. Log in to return to the system.'

The screenshot shows a Windows Command Prompt window titled 'Administrator: Command Prompt'. The user runs the command 'C:\Program Files\Splunk\bin>splunkd'. The output shows the Splunk daemon starting (pid 2988) and waiting for the web server to become available. A message box at the bottom right says 'Your session has expired. Log in to return to the system.'

On peut voir que Splunk Entreprise communique déjà avec les redirecteurs Windows 10

Data Summary

Hosts (2) Sources (3) Sourcetypes (3)

filter

Source	Count	Last Update
WinEventLog:Application	3,025	11/25/25 1:59:15.000 PM
WinEventLog:Security	30,262	11/25/25 2:46:06.000 PM
WinEventLog:System	2,603	11/25/25 1:38:17.000 PM

Et à partir de la recherche sur Splunk, on peut voir les indexes qui ont été créés et les événements qui commencent à être transmis.

The screenshot shows the Splunk Enterprise search interface. The search bar at the top contains the query "index='win'". Below the search bar, a results table displays 16,86 events. The first event listed is from 11/28/25 at 9:27:25.666 AM, with details including LogName=Security, EventCode=4672, EventType=0, ComputerName=DESKTOP-NCLQ4MM, and host=DESKTOP-NCLQ4MM. The interface includes various navigation and filtering options like "Format", "Show: 20 Per Page", and "View: List". On the left, there are sections for "SELECTED FIELDS" (host, source, sourcetype) and "INTERESTING FIELDS" (Event, LogName, EventCode, EventType, ComputerName, host). The bottom of the screen shows the Windows taskbar with icons for File Explorer, Task View, Start, Edge, Google Chrome, File Explorer, and Task View again.

5. Création des alertes dans Splunk Enterprise

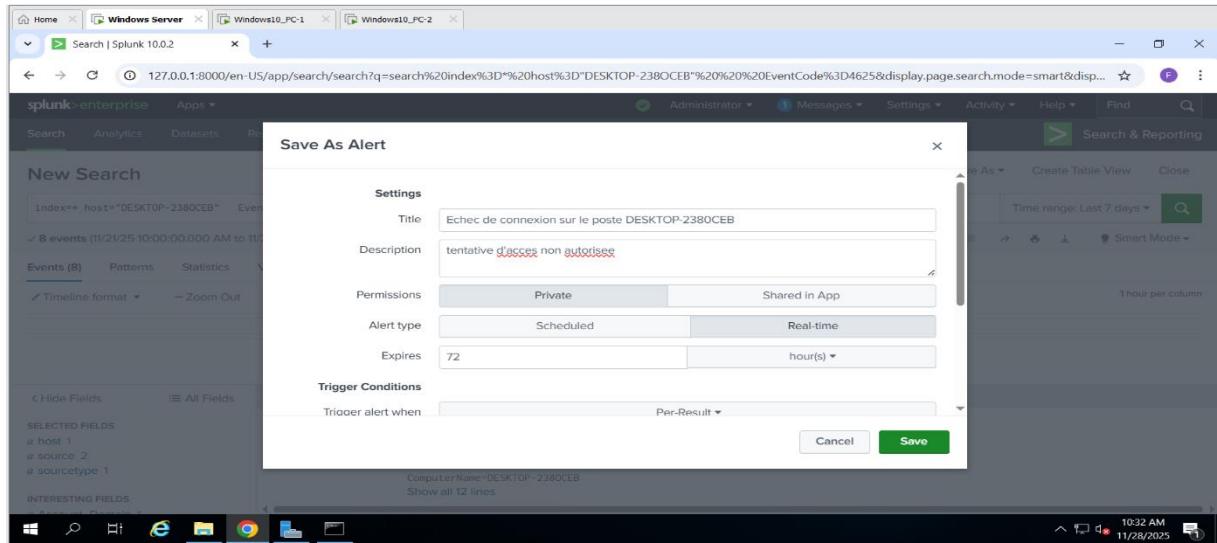
La création d'alertes dans Splunk permet de transformer les recherches en véritables mécanismes de surveillance automatisés. Au lieu de consulter manuellement les tableaux de bord ou des rapports, Splunk peut nous avertir dès qu'un événement critique se produit, qu'un seuil est dépassé ou qu'un comportement anormal est détecté. Dans notre projet nous allons créer deux alertes splunk, une qui enverra un courriel suite à une tentative d'accès non autorisée à un poste Windows 10 à l'équipe SOC level 1 et une autre qui va créer un fichier

dans lequel on aura les détails sur la tentative d'accès non autorisée sur un autre poste Windows 10.

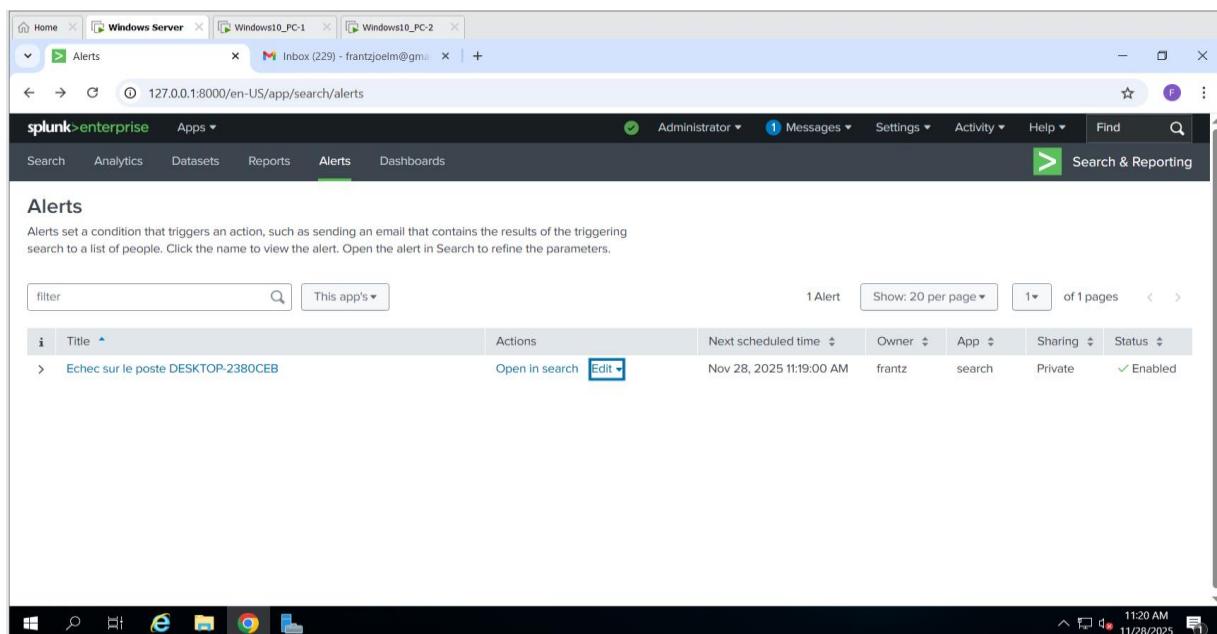
- Alerte qui enverra un courriel

Dans Splunk Enterprise on va dans :

Setting -> Searches, reports, and alerts -> New Alert, et on entre les informations dans les champs en fonction de nos attentes.

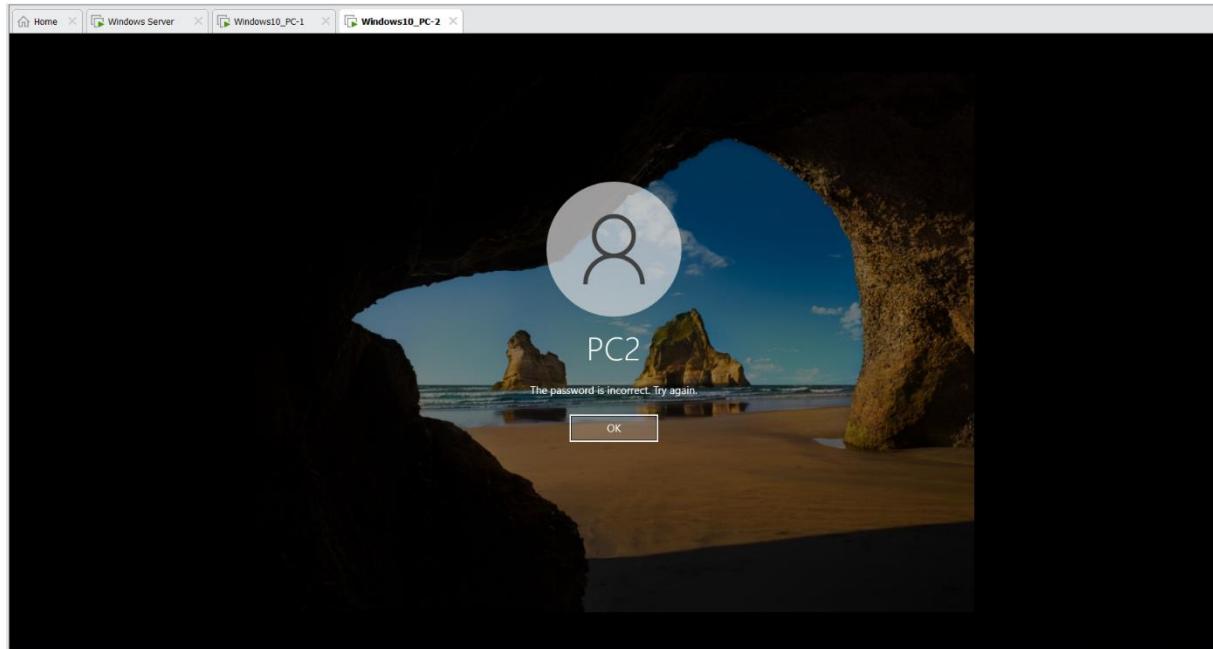


Ensuite on enregistre l'alerte qu'on peut modifier au besoin

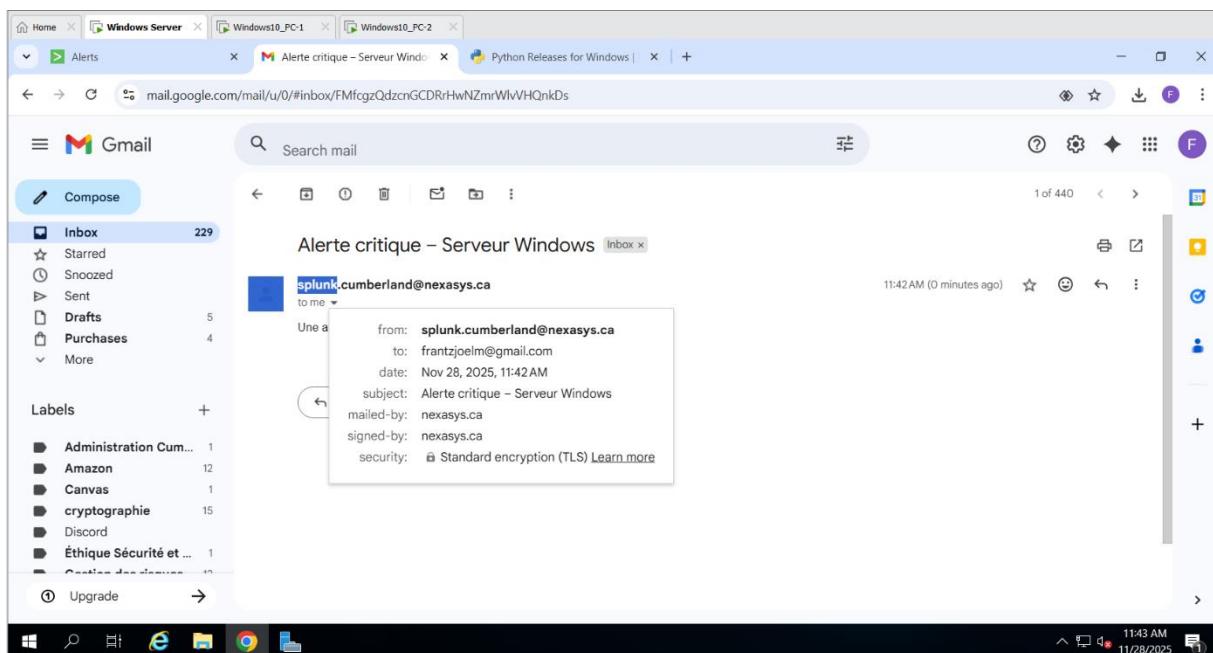


Test du fonctionnement de l'alerte

Un utilisateur légitime ou pas essaye de se connecter au poste DESKTOP-23380CEB et entre les mauvais identifiants : **échec de la connexion !**

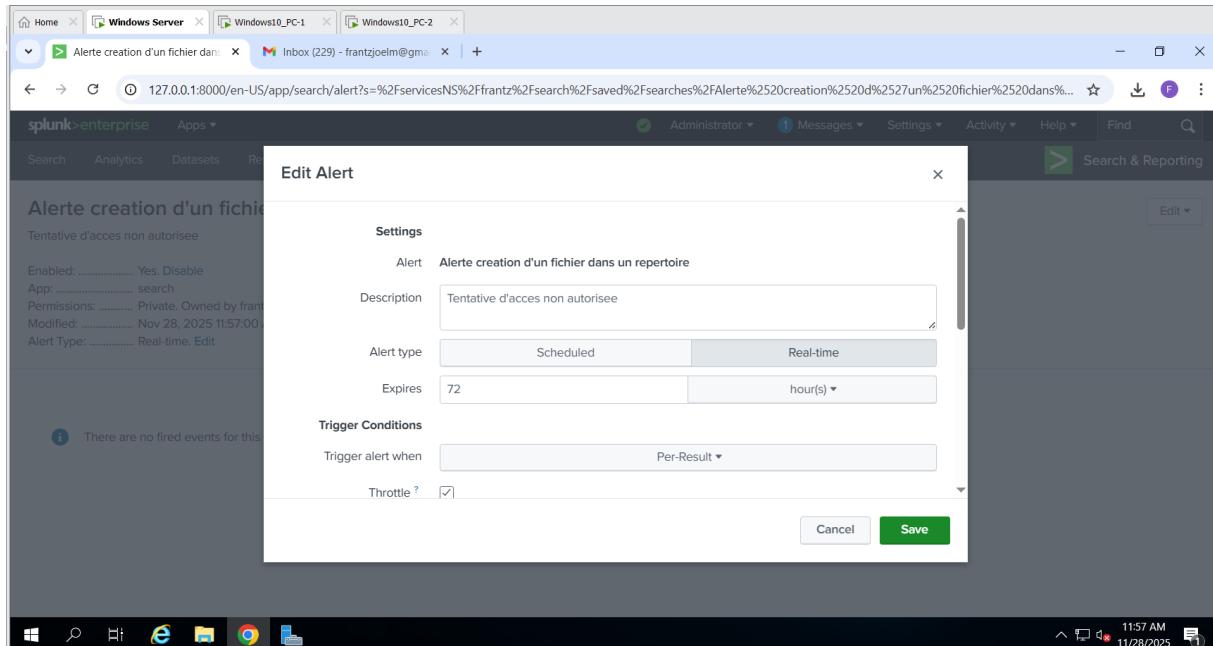


Immédiatement le l'équipe Soc L1 reçoit un courriel d'une alerte critique provenant du serveur de messagerie : une tentative de connexion est en cours. Ce qui permet à l'équipe Soc L1 de faire une vérification ciblée.



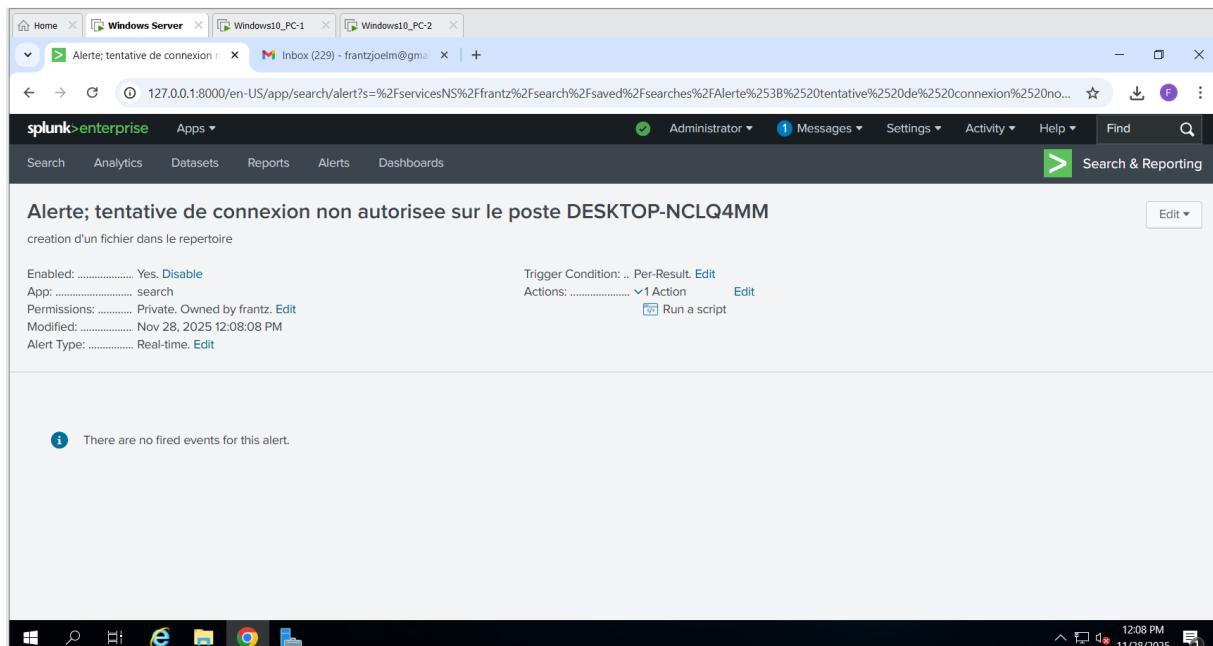
➤ Alerte qui va créer un fichier

On va suivre le même processus de création d'une alerte comme précédemment pour l'alerte qui envoie un courriel. Mais le nom et la description de l'alerte seront différents.



The screenshot shows the Splunk Enterprise web interface. A modal window titled "Edit Alert" is open. The alert is named "Alerte creation d'un fichier dans un repertoire". The description is "Tentative d'accès non autorisée". The alert type is "Scheduled". The expiration time is set to 72 hours. The trigger condition is "Per-Result". The "Throttle?" checkbox is checked. At the bottom right of the modal, there are "Cancel" and "Save" buttons. The background shows the Splunk search interface with various tabs like Home, Windows Server, and a search bar.

On enregistre et visualise l'alerte créée.

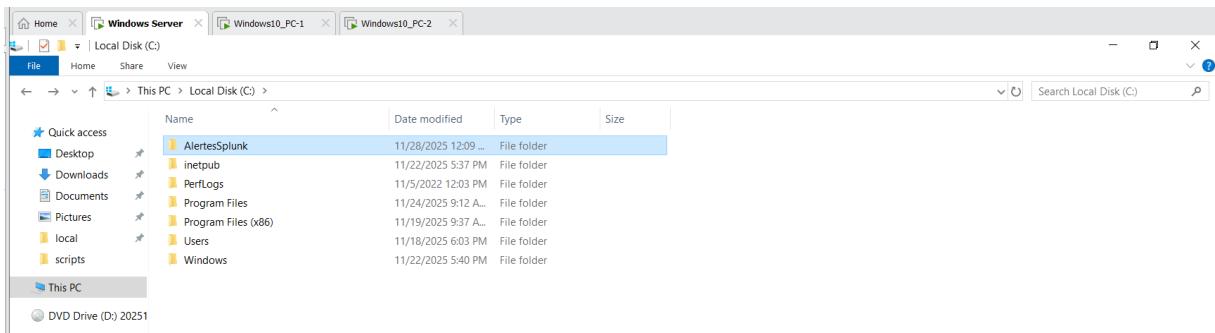
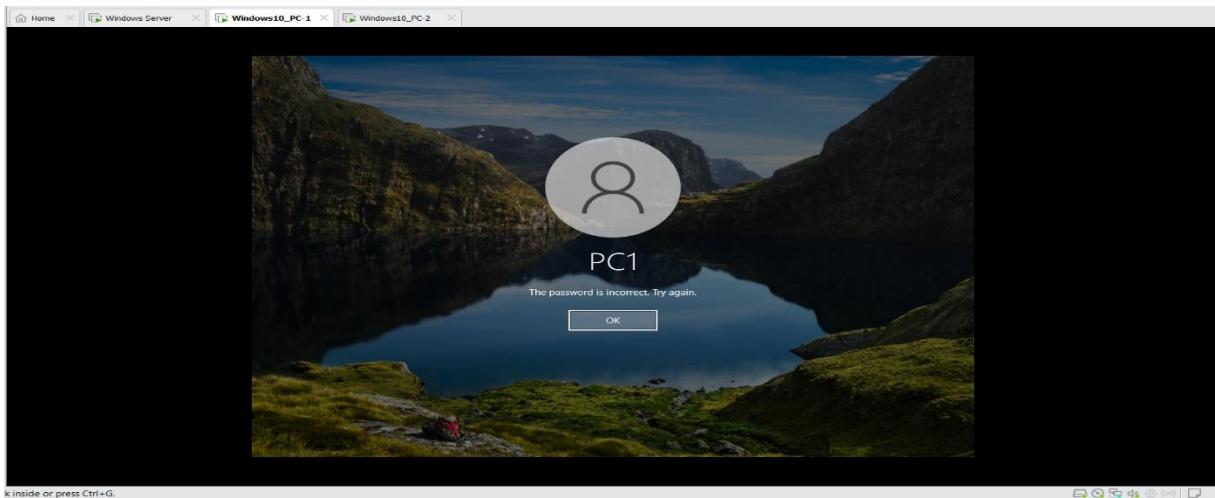


The screenshot shows the Splunk Enterprise web interface. A modal window titled "Alerte; tentative de connexion non autorisée sur le poste DESKTOP-NCLQ4MM" is open. It displays the alert configuration: "Trigger Condition: ... Per-Result, Edit" and "Actions: ... v1 Action, Edit, Run a script". The alert is enabled and was modified on Nov 28, 2025 at 12:08:08 PM. The message "There are no fired events for this alert." is displayed. The background shows the Splunk search interface with various tabs like Home, Windows Server, and a search bar.

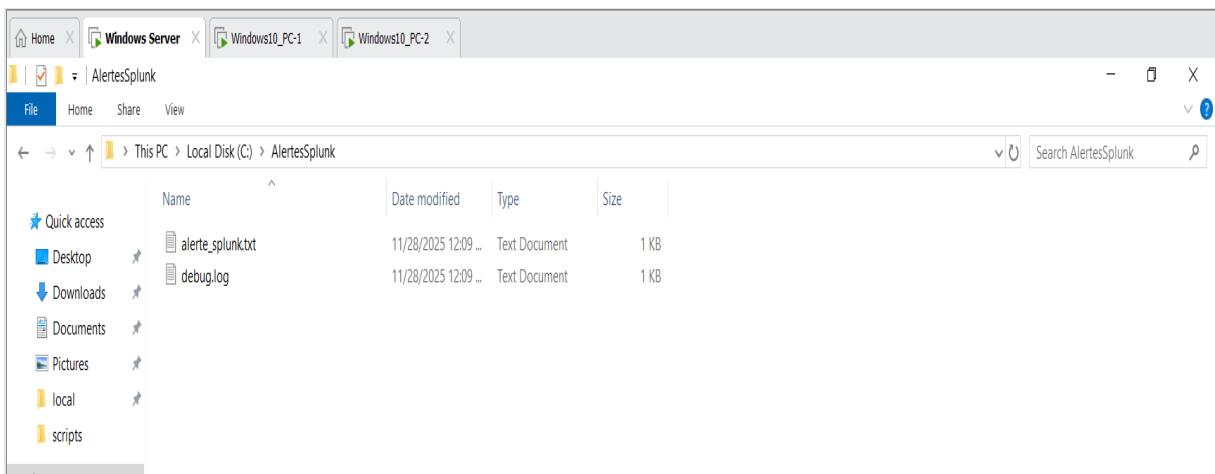
Test du fonctionnement de l'alerte

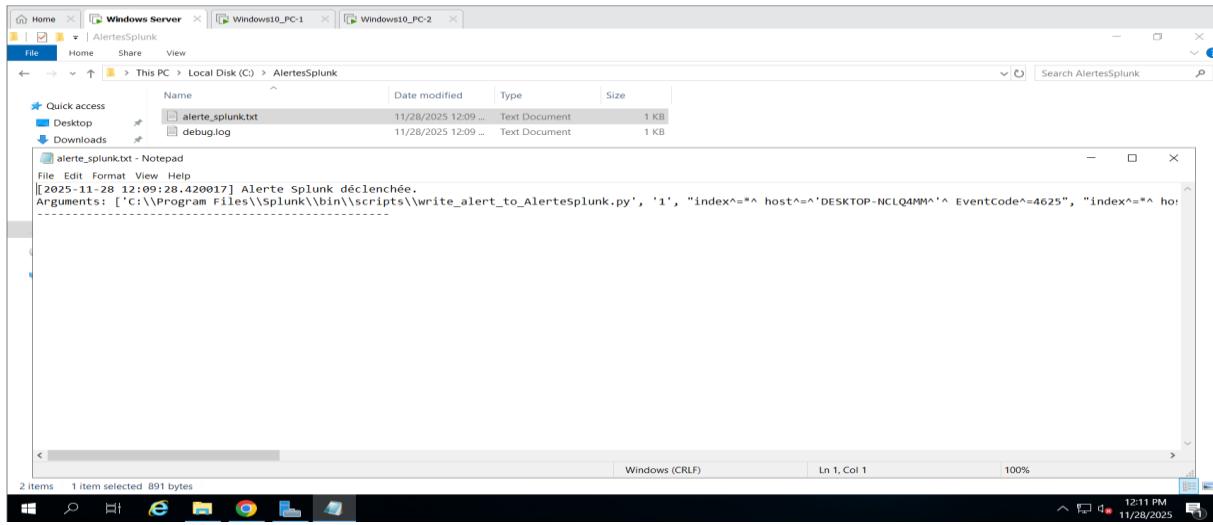
Un utilisateur légitime ou pas essaye de se connecter au poste DESKTOP-NCLQ4MM et entre les mauvais identifiants : **échec de la connexion !**

Un fichier.**.txt** est généré immédiatement dans un dossier « **Alertes Splunk** » créé à cet effet, dans lequel l'équipe SOCL1 pourra avoir les détails de la tentative de connexion non autorisée.



Et on pourra le consulter et voir les détails de l'alerte.





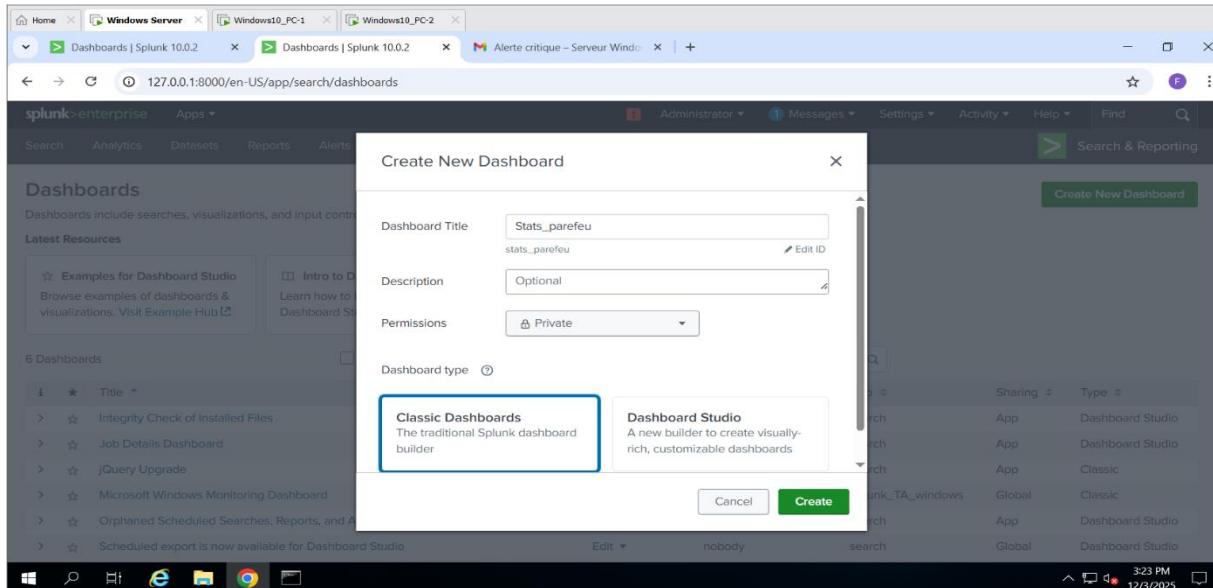
6. Création de tableau de bord dans Splunk

Les tableaux de bord dans Splunk Enterprise sont des interfaces visuelles qui permettent de transformer vos données brutes en informations claires, exploitables et faciles à interpréter. Ils jouent un rôle essentiel dans la surveillance, l'analyse et la prise de décision au sein d'un environnement technique ou métier.

Pour créer un tableau de bord dans Splunk Enterprise on va dans :

Search and Reporting -> Dashboards -> Create New Dashboard

On donne un nom à notre tableau de bord : **Stats_parfeu** et on choisit le type classique



On ajoute une entrée : **Time** qui me permettra de choisir le moment où on reçoit les données et un bouton : **Submit** pour valider mon entrée.

The screenshot shows the Splunk interface for editing a dashboard. At the top, there are tabs for 'Home', 'Windows Server', 'Windows10_PC-1', 'Windows10_PC-2', and 'Edit: Stats_parefeu | Splunk 10.0...'. The main area is titled 'Stats_parefeu' with the sub-section 'No description'. A search bar at the top of the dashboard panel has the query 'Since Dec 2, 2025 3:00 PM'. To its right is a green 'Submit' button. Below the search bar is a message 'No results found.'. The bottom right corner of the screen shows the Windows taskbar with icons for Start, Search, Task View, File Explorer, Edge, and Chrome, along with the date and time (12/3/2025, 3:49 PM).

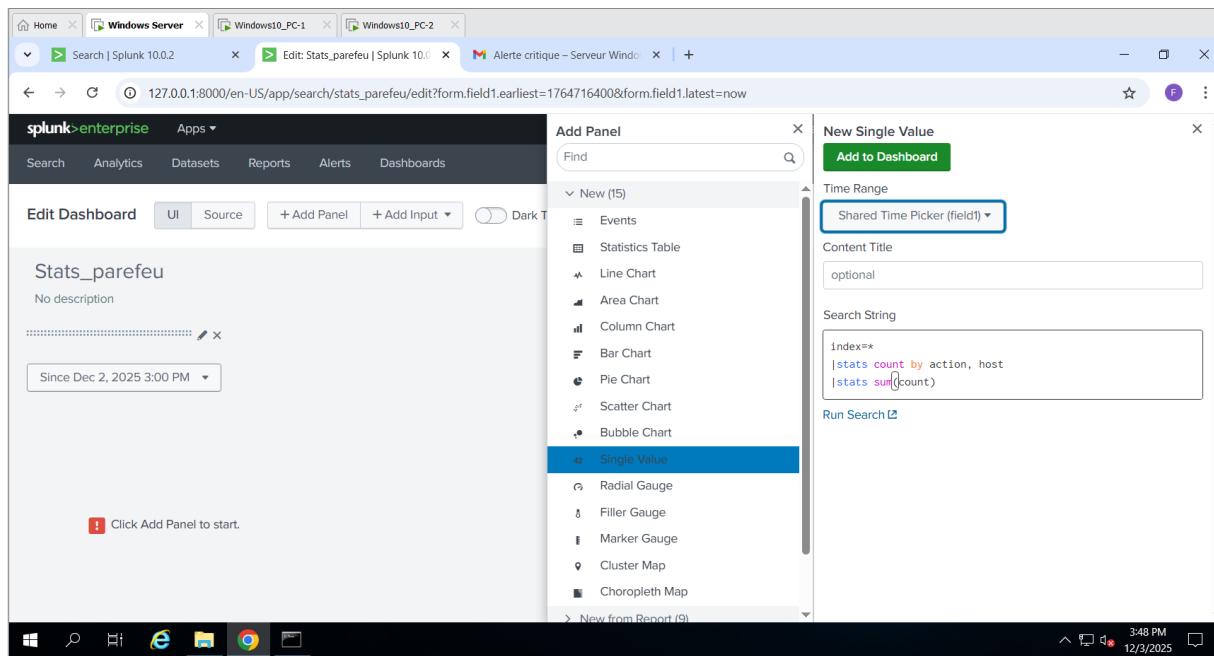
Ensuite on va chercher les données dont on souhaite voir dans mon tableau de bord

The screenshot shows the Splunk search interface with the search bar containing the query 'q=search%20index%3D*&display.page.search.mode=smart&dispatch.sample_ratio=1&workload_pool=&earliest=0&latest=&sid=17...'. The results table is titled 'action' and shows the following data:

Values	Count	%
success	48,568	97.49%
read	651	1.307%
allowed	247	0.496%
modified	244	0.49%
failure	36	0.072%
logoff	31	0.062%
created	28	0.056%
stopped	10	0.02%
deleted	2	0.004%

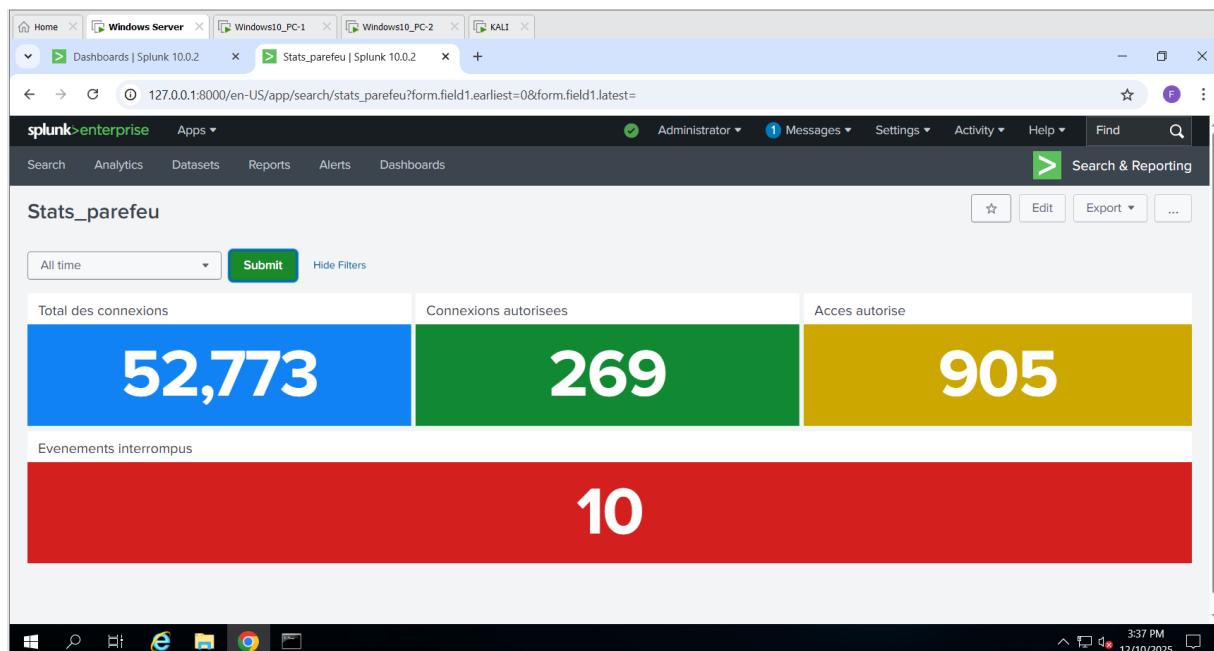
The interface also shows a timeline format at the top left and various navigation and filtering options.

Dans notre cas on utilisera : **Success** ; **Allowed** ; **Stopped** ; **Read** ensuite on ajoutera des panneaux et la requête SPL qui permet de visualiser toutes les entrées qui ont réussies



On fera ainsi pour toutes les actions dont on veut avoir un aperçu en temps réel dans notre tableau de bord.

Le rendu de notre tableau de bord après quelques manipulations sur le choix des couleurs nous donne l'aperçu ci-dessous. On pourra afficher notre tableau de bord au démarrage de splunk Enterprise et le rafraîchir selon la période souhaitée.



7. Installation et configuration de la machine d'attaque(Phishing)

a) Kali Linux

Kali Linux est une distribution Linux spécialement conçue pour les tests d'intrusion, l'audit de sécurité et l'analyse de vulnérabilités. Utilisée par les professionnels de la cyber-sécurité comme par les étudiants, elle regroupe en un seul système plus de 600 outils dédiés à l'évaluation et au renforcement de la sécurité informatique.

À quoi sert Kali Linux ?

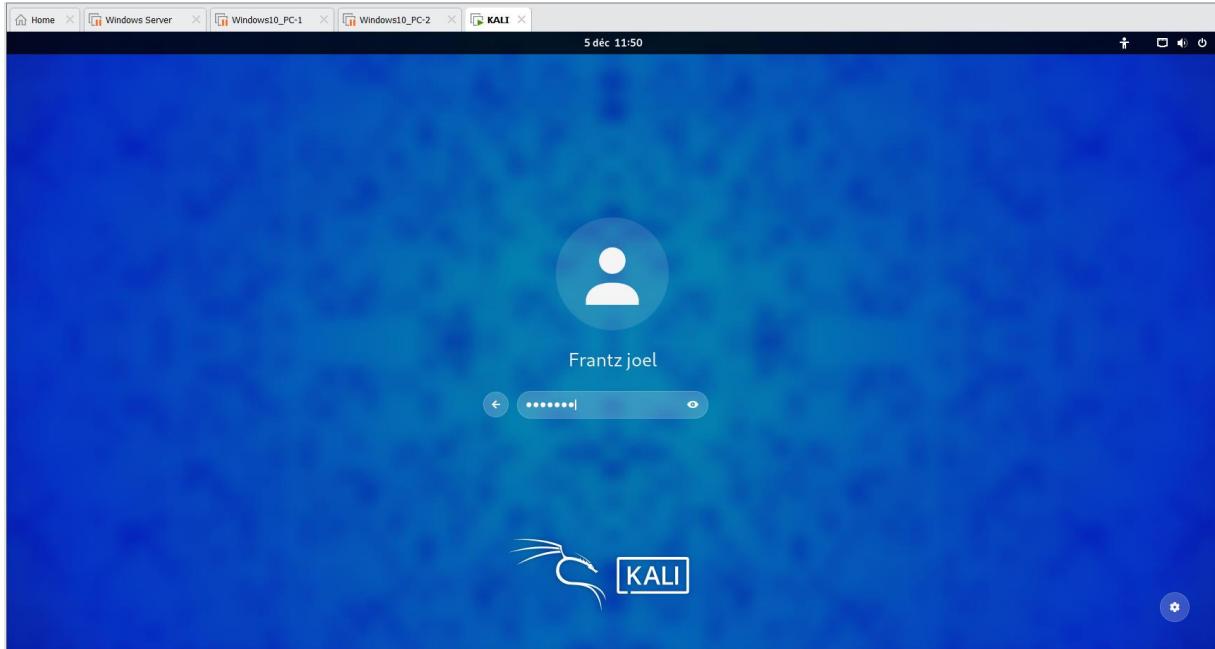
- **Tester la sécurité d'un réseau ou d'un système**
- **Identifier des failles** avant qu'elles ne soient exploitées
- **Analyser le comportement d'applications** ou de services
- **Former aux techniques de cyber-sécurité** dans un cadre contrôlé

b) Installation

A partir du site officiel <https://kali.org/get-kali/>, on accès à la page de téléchargement des images ISO, images pour machines virtuelles.



L'installation prend quelques minutes, après on entre les identifiants de connexion et on accède à kali en mode graphique qui a été notre choix pour ce projet. Mais qui peut être aussi installé et utilisé en ligne de commande.



c) Préparation de l'attaque avec Pyphishing

PyPhishing est un outil open-source utilisé dans des **contextes d'apprentissage et de simulation** pour comprendre les mécanismes des attaques par hameçonnage (phishing). Il permet de reproduire, dans un environnement contrôlé, les techniques couramment utilisées pour des attaques.

Pourquoi utiliser PyPhishing dans notre projet ?

- **Comprendre les techniques d'ingénierie sociale** utilisées dans les campagnes de phishing.
- **Analyser le comportement des systèmes** lorsqu'ils sont exposés à des tentatives d'hameçonnage.
- **Observer la génération de logs** sur les machines Windows et leur transmission vers un serveur Splunk.
- **Améliorer la détection et la réponse** en configurant des alertes, tableaux de bord et corrélations dans Splunk.

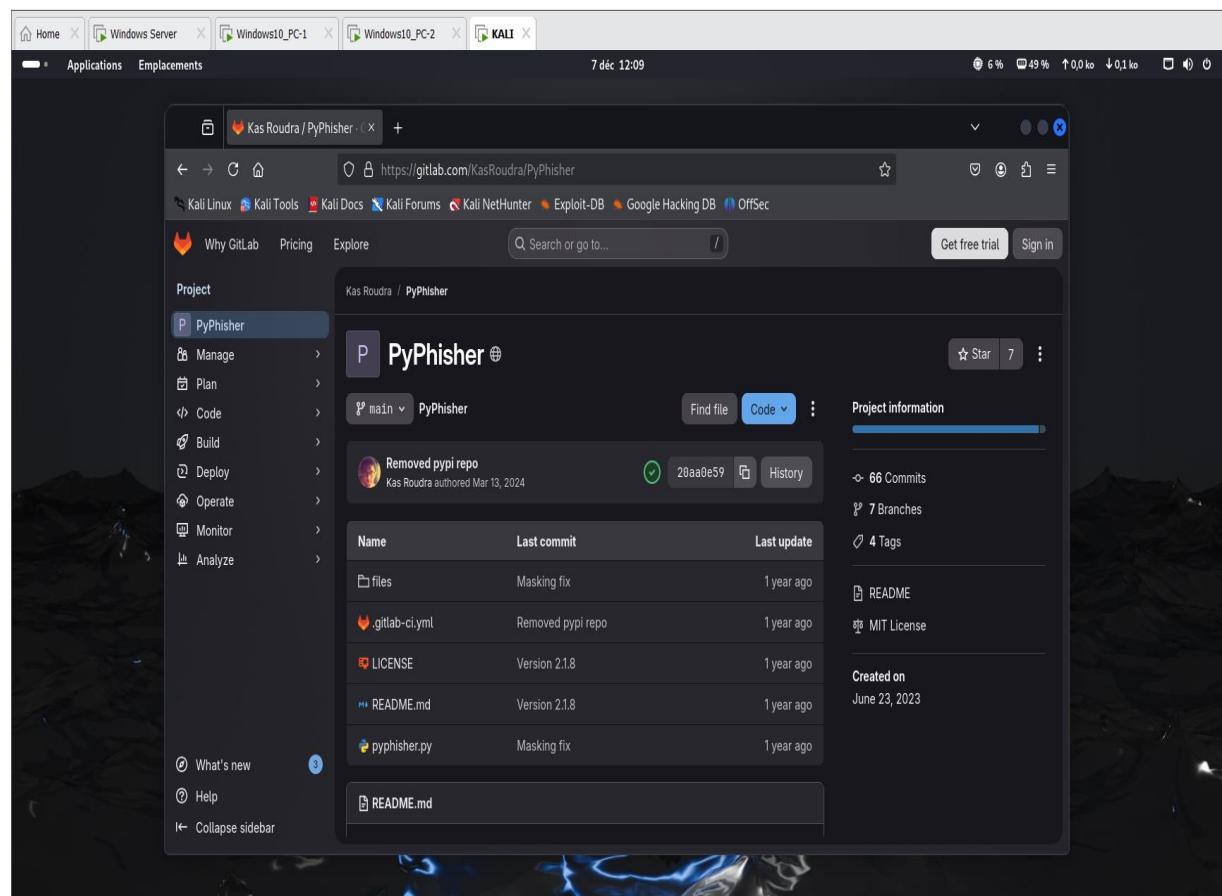
Rôle dans un environnement avec Kali Linux et Splunk

Dans ce projet :

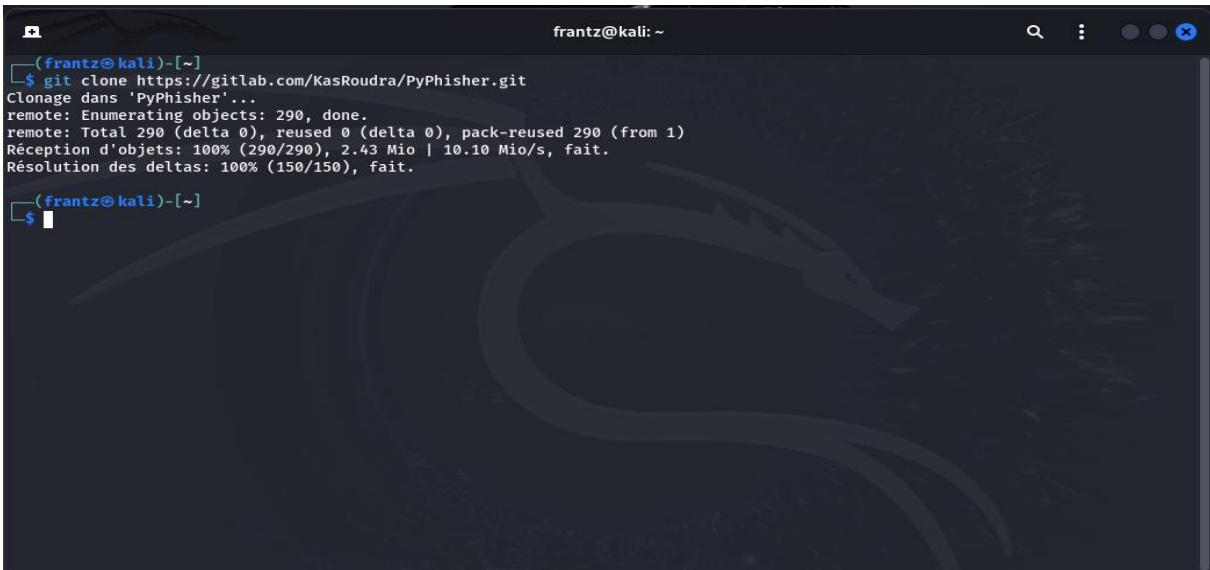
- **Kali Linux** sert de plateforme d'expérimentation pour exécuter des outils de simulation d'attaque.
- **Les machines Windows 10**, équipées de redirecteurs Splunk, envoient leurs journaux au serveur Splunk.
- **Splunk** permet ensuite d'analyser les traces laissées par les activités simulées, d'identifier les indicateurs de compromission et de tester des mécanismes de détection.

Pour obtenir PyPhishing on se rend sur :

<https://gitlab.com/KasRoudra/PyPhsing> ; on appuie sur **Code** et on va copier le lien en dessous
Clone with HTTPS : <https://gitlab.com/KasRoudra/PyPhsing>



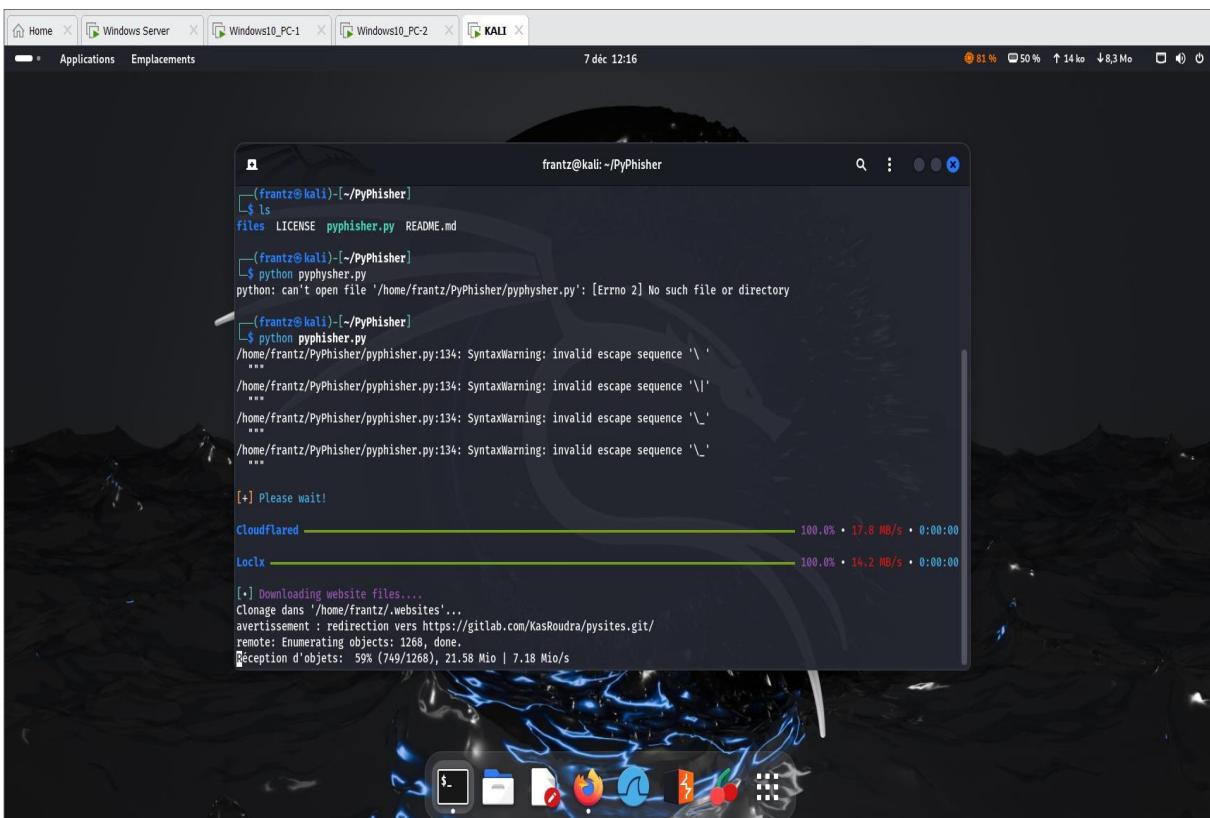
Ensute, on ouvre le terminal sur kali et on entre :



```
(frantz@kali)-[~]
$ git clone https://gitlab.com/KasRoudra/PyPhisher.git
Clonage dans 'PyPhisher'...
remote: Enumerating objects: 290, done.
remote: Total 290 (delta 0), reused 0 (delta 0), pack-reused 290 (from 1)
Récception d'objets: 100% (290/290), 2.43 Mio | 10.10 Mio/s, fait.
Résolution des deltas: 100% (150/150), fait.

(frantz@kali)-[~]
$
```

Et après, on cherche les fichiers présents dans **/PyPhisher** avec la commande **ls**. Avec la commande **python pyphisher.py** on installe et configure notre environnement d'attaque contrôlé



```
(frantz@kali)-[~/PyPhisher]
$ ls
files LICENSE pyphisher.py README.md

(frantz@kali)-[~/PyPhisher]
$ python pyphisher.py
python: can't open file '/home/frantz/PyPhisher/pyphisher.py': [Errno 2] No such file or directory

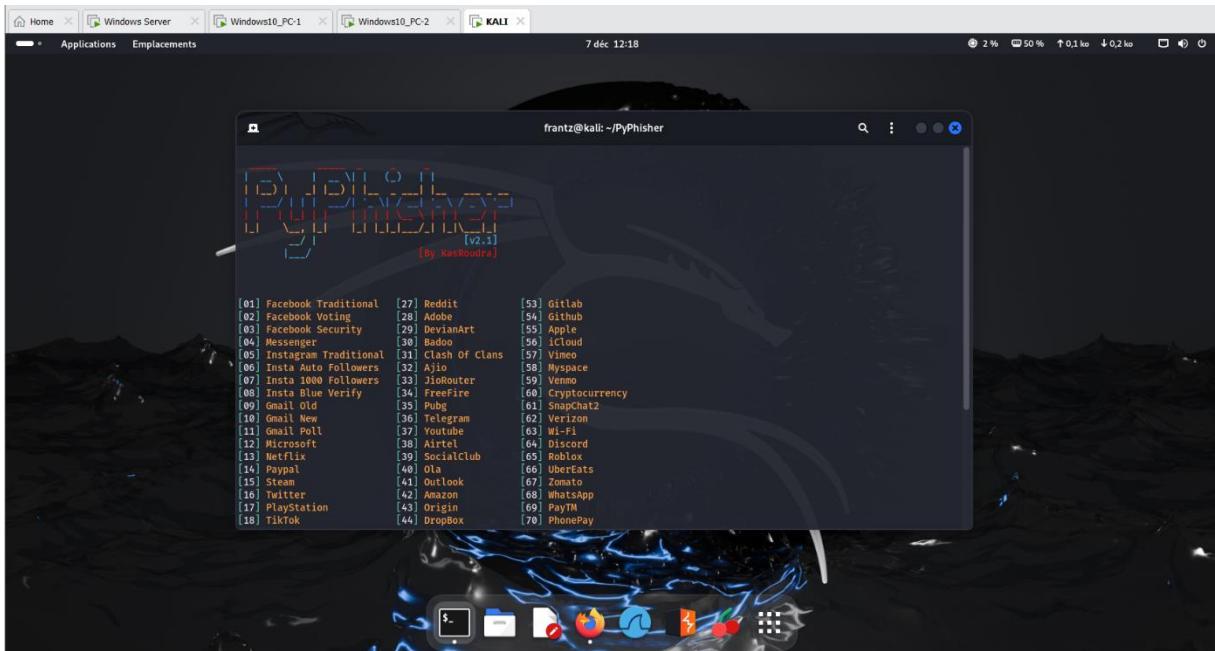
(frantz@kali)-[~/PyPhisher]
$ python pyphisher.py
/home/frantz/PyPhisher/pyphisher.py:13: SyntaxWarning: invalid escape sequence '\'
...
/home/frantz/PyPhisher/pyphisher.py:13: SyntaxWarning: invalid escape sequence '\\'
...
/home/frantz/PyPhisher/pyphisher.py:13: SyntaxWarning: invalid escape sequence '\\'
...
/home/frantz/PyPhisher/pyphisher.py:13: SyntaxWarning: invalid escape sequence '\\'
...

[*] Please wait!

Cloudflare ━━━━━━━━━━━━━━ 100.0% • 17.8 MB/s • 0:00:00
Loclx ━━━━━━━━━━━━ 100.0% • 14.2 MB/s • 0:00:00

[*] Downloading website files...
Clonage dans '/home/frantz/websites'...
avertissement : redirection vers https://gitlab.com/KasRoudra/pysites.git/
remote: Enumerating objects: 1268, done.
Récception d'objets: 59% (749/1268), 21.58 Mio | 7.18 Mio/s
```

Et on a ce rendu ; maintenant on peut simuler une attaque en suivant les instructions.



8. Quelques simples requêtes SPL (Search Processing Language) dans Splunk

Les requêtes SPL (Search Processing Language) constituent le cœur de Splunk. Elles permettent d'explorer, filtrer, analyser et corrélérer les données collectées par la plateforme. Grâce à SPL, il devient possible de transformer des millions d'événements bruts en informations exploitables pour la supervision, la sécurité ou l'analyse opérationnelle.

À quoi sert SPL ?

- Rechercher des événements dans les index Splunk
- Filtrer et extraire des champs pour mieux comprendre les données
- Créer des statistiques (comptages, moyennes, tendances)
- Construire des visualisations pour les tableaux de bord
- Déetecter des anomalies ou attaques via des corrélations avancées
- Automatiser la surveillance grâce aux alertes basées sur des requêtes

Pourquoi SPL est essentiel ?

Parce qu'il donne la capacité de :

- comprendre ce qui se passe dans un système,
- détecter des comportements suspects,
- alimenter des Dashboards dynamiques,
- et soutenir les équipes SOC dans leurs investigations.

Lister les forwarders vus dans les logs internes

```
index=_internal sourcetype=splunkd component=Metrics group=per_host_thruput  
| stats latest(_time) AS lastSeen BY host  
| eval lastSeen=strftime(lastSeen, "%Y-%m-%d %H:%M:%S")  
| sort host
```

Événements par redirecteur et par action

```
index=* host=*  
| stats count BY host, action  
| sort host, -count
```

Événements Windows classés par EventCode

```
index=wineventlog host=*  
| stats count BY host, EventCode  
| sort host, -count
```

Au-delà des recherches de base, Splunk offre également des requêtes SPL beaucoup plus complexes qui permettent d'explorer les données en profondeur. Grâce à des commandes avancées, à l'analyse de logs structurés en XML, ou encore à l'intégration directe dans des tableaux de bord dynamiques, il devient possible de construire de véritables mécanismes d'investigation et de supervision. Ces requêtes avancées ouvrent la voie à des corrélations plus riches, à une détection plus fine des anomalies et à une compréhension plus complète des environnements surveillés. Elles constituent ainsi un levier essentiel pour tirer pleinement parti de la puissance de Splunk.

Conclusion

La mise en place de cet environnement contrôlé, composé d'un serveur Splunk sous Windows Server 2019, de deux machines Windows 10 configurées comme cibles et d'une machine Kali Linux utilisée pour simuler des actions offensives, a permis de créer un véritable laboratoire d'apprentissage en cyber-sécurité. Ce cadre isolé et maîtrisé a offert la possibilité d'étudier en profondeur les mécanismes d'une attaque de phishing, depuis son exécution jusqu'à son impact sur les systèmes et les traces qu'elle laisse dans les journaux.

Grâce à l'intégration des redirecteurs Splunk sur les machines Windows, l'ensemble des événements générés, qu'ils proviennent des logs système, sécurité, application ou encore de Sysmon, ont pu être collectés, centralisés et analysés. L'utilisation de requêtes SPL a permis de mieux comprendre le comportement des machines face à une tentative d'hameçonnage et d'identifier les indicateurs de compromission pertinents. La création de tableaux de bord et d'alertes a renforcé cette visibilité en offrant une supervision claire, dynamique et orientée détection.

Ce projet a ainsi démontré l'importance d'un environnement de test réaliste pour appréhender les techniques d'attaque et les capacités de défense. Il a permis de développer une approche méthodique, combinant observation, analyse et corrélation, tout en mettant en lumière la puissance de Splunk comme outil d'investigation et de surveillance. Au final, cette démarche contribue à renforcer les compétences nécessaires pour comprendre, détecter et analyser des scénarios de compromission dans un contexte sécurisé et pédagogique.

Annexes

Références et sites consultés pour la réalisation du projet

➤ Documentation officielle Splunk

- Splunk Documentation — *Search Processing Language (SPL)*
<https://docs.splunk.com/Documentation/Splunk/latest/Search>
- Splunk Enterprise — *Forwarders & Deployment Server*
<https://docs.splunk.com/Documentation/Forwarder>
- Splunk Enterprise — *Dashboards & Visualizations*
<https://docs.splunk.com/Documentation/Splunk/latest/Viz>

➤ Sysmon et Windows Event Logging

- Microsoft Sysmon (Sysinternals) — Documentation officielle
<https://learn.microsoft.com/sysinternals/downloads/sysmon>
- Microsoft Windows Event Logging — Event IDs
<https://learn.microsoft.com/windows/security/threat-protection/auditing/event-logs>

➤ Ressources communautaires utiles

- Splunk Community & Answers <https://community.splunk.com>
- Reddit r/Splunk (discussions techniques) <https://www.reddit.com/r/Splunk>
- GitHub (exemples de configurations Sysmon, dashboards Splunk, etc.)
<https://github.com>