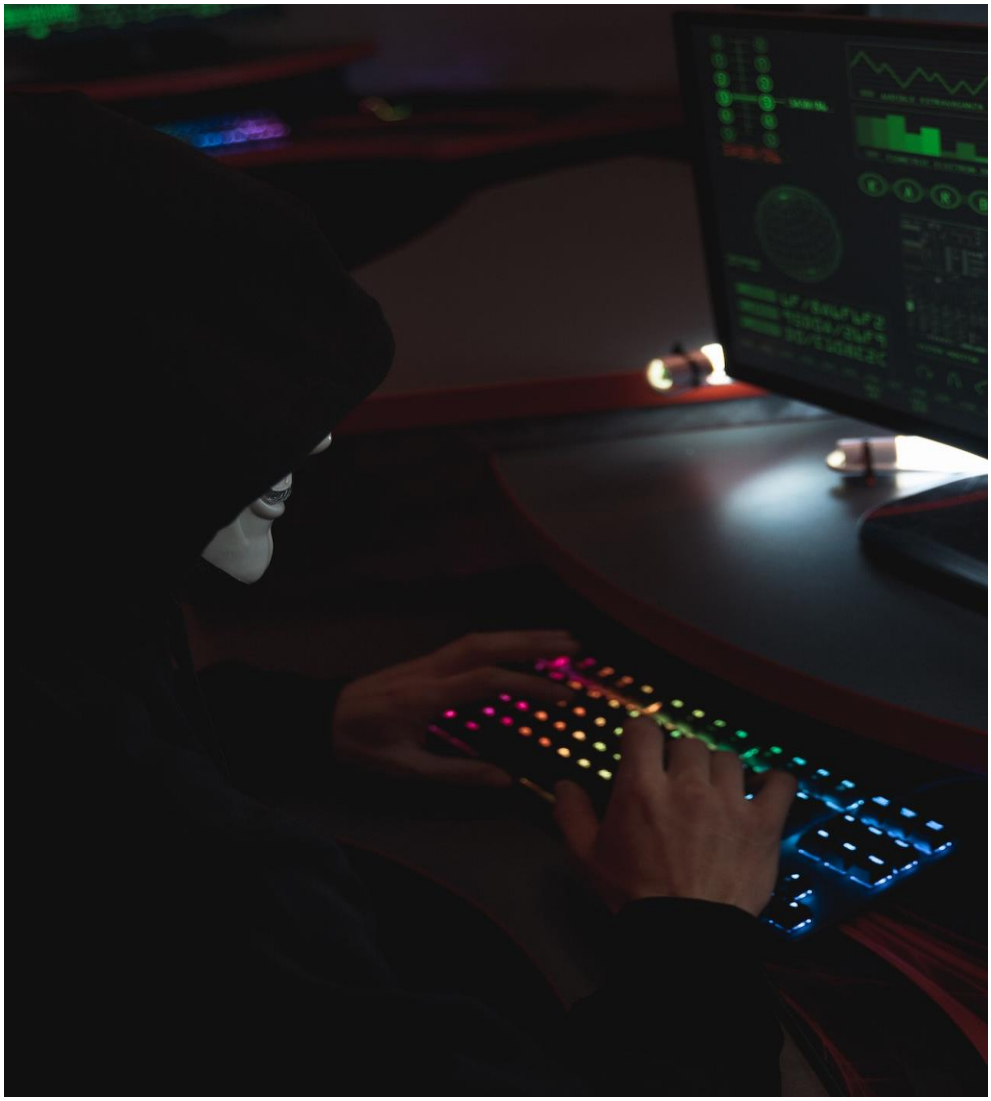


Projet validation des acquis finaux

Lucie ASCENZIO DE ESTEVE

Younes CHBADA

13/07/2023

Crédit photo : Photo de Tima Miroshnichenko: https://www.pexels.com/fr-fr/photo/personne-lumieres-saisir-etre-assis-5380633/

Contexte et problématique

Une entreprise de taille moyenne, Piggy Bank Corporation, opère dans le secteur des services financiers et traite un grand volume de données sensibles. Récemment, l'entreprise a connu une augmentation des incidents de sécurité, notamment des tentatives de phishing, des attaques par ransomware et des fuites de données. Ces incidents ont entraîné des perturbations des opérations commerciales, des pertes financières et une atteinte à la réputation de l'entreprise.

Pour se prémunir, ils souhaitent approfondir leurs connaissances sur ce genre d'attaque.

Pour se faire, ils font appel à une jeune équipe de SOC.

Voici les différentes tâches que vous aurez à effectuer :

- Vous devrez définir et documenter des chemins d'attaques cohérents.
- Vous ferez ensuite une présentation des outils d'aide à la détection que vous utilisez (présentation de l'outil, règles de détection, journalisation etc).
- Vous montrerez ensuite l'efficacité et la performance de ces outils en simulant une attaque complexe. Cette attaque sera évidemment une simulation, et devra être mise en place à l'aide d'outil de simulation comme caldera, ART …

Par la suite vous effectuerez un rapport détaillé de l'attaque (type d'attaque, son fonctionnement, l'attaquant, la cible, porte d'entrée, son fonctionnement, etc.) et vous mettrez en évidence l'importance d'un SOC dans une organisation.

Introduction

Notre objectif est de comprendre en détail les scénarios d'attaques mis en évidence dans le contexte précédemment exposé afin d'aider l'entreprise à renforcer sa posture de sécurité et à se prémunir contre les menaces croissantes qui pourraient compromettre la confidentialité, l'intégrité et la disponibilité de ses données sensibles.

Dans un souci de cohérence vis-à-vis du contexte nous examineront en particulier les scénarios de phishing, d'attaque par ransomware et de fuite de données.

Nous identifierons pour chaque scénario les étapes clés de l'attaque, les acteurs impliqués et les impacts potentiels (réels ou supposés) sur les opérations commerciales, les finances et la réputation de l'entreprise.

Nous fournirons ensuite des recommandations et des mesures de sécurité préventives pour aider Piggy Bank Corporation à se prémunir contre ces menaces.

Notre approche se concentre sur une combinaison de mesures techniques, de bonnes pratiques en matière de sensibilisation à la sécurité et de processus de réponse aux incidents pour assurer une protection globale contre les attaques potentielles.

Comprendre les risques associés à ces scénarios d'attaques permettra à l'entreprise d'être proactives face aux menaces qui pèsent sur elle et de s'y préparer au mieux avec une équipe SOC capable d'y faire face.

En fournissant une analyse approfondie des chemins d'attaques cohérents, nous contribuons à renforcer la posture de sécurité globale de l'entreprise et à protéger ses actifs les plus précieux.

Note : Les scénarios d'attaques présentés ci-dessous sont basés sur des situations hypothétiques et ont été conçus pour illustrer les différentes méthodes d'attaques potentielles. Ils ne représentent pas des événements réels ayant affecté Piggy Bank Corporation.

I) Définition et documentation des chemins d’attaques

La présente section vise à fournir une analyse approfondie des scénarios d'attaques potentielles auxquelles Piggy Bank Corporation pourrait être confrontée. Ces scénarios ont été identifiés dans le cadre de notre évaluation de la sécurité de l'entreprise et se basent sur les tendances actuelles des cybermenaces et les vulnérabilités spécifiques du secteur financier.

1) Scénario de phishing :

Le scénario de phishing implique des attaquants qui envoient des e-mails frauduleux à des employés en se faisant passer pour une entité légitime, les incitant à divulguer leurs informations d'identification sensibles, telles que leurs noms d'utilisateurs et leurs mots de passe. L'objectif est d'obtenir un accès non autorisé aux systèmes internes de l'entreprise et de voler des informations confidentielles.

Étapes :

1. Les attaquants envoient un e-mail aux employés, prétendant provenir d'une institution financière connue et demandant la vérification des informations d'identification.
2. Les e-mails frauduleux contiennent un lien vers un site web de phishing soigneusement conçus, ressemblant à s'y méprendre à celui de l'institution financière légitime.
3. Les employés trompés cliquent sur le lien et accèdent au faux site web, où ils sont invités à saisir leurs informations d'identification.
4. Les attaquants récupèrent les informations d'identification fournies par les employés.
5. Les attaquants utilisent ces informations volées pour accéder aux systèmes internes et voler des données sensibles.

Impacts potentiels :

- Vol de données confidentielles, y compris les informations financières des clients.
- Compromission des comptes utilisateurs internes.
- Perturbation des opérations commerciales et perte de confiance des clients.
- Risque de fraude et de vols d'identité.

2) Scénario d'attaque par ransomware :

L'attaque par ransomware implique des attaquants qui utilisent des logiciels malveillants pour chiffrer les fichiers sur les systèmes, empêchant ainsi l'accès aux données. Les attaquants exigent ensuite une rançon en échange de la clé de déchiffrement, menaçant de supprimer définitivement les données si la rançon n'est pas payée.

Étapes :

1. Les attaquants diffusent un fichier malveillant via des sites web compromis ou des pièces jointes d'e-mails.
2. Un employé télécharge et exécute le fichier infecté ou ouvre la pièce jointe malveillante.
3. Le ransomware se déploie sur le système de l'employé, se propageant rapidement aux autres machines et serveurs du réseau interne.
4. Le ransomware chiffre les fichiers sur les systèmes infectés via une clé de chiffrement unique, rendant les données inaccessibles.
5. Les attaquants affichent une demande de rançon, exigeant le paiement dans une cryptomonnaie spécifique en échange de la clé de déchiffrement, si la rançon n'est pas payée dans le délai imparti, ils menacent de supprimer définitivement les données.

Impacts potentiels :

- Inaccessibilité des données essentielles pour les opérations commerciales.
- Perturbation des services et perte de productivité.
- Perte de données et coûts de récupération élevés.
- Risque de dommages à la réputation de l'entreprise.

3) Scénario de fuite de données :

Le scénario de fuite de données implique des attaquants qui exploitent les vulnérabilités dans les applications web ou les systèmes de Piggy Bank Corporation pour accéder à une base de données contenant des informations sensibles. Les attaquants exfiltrent ensuite ces données cherchant à se faire discret pour ne pas être détectés, ce qui peut entraîner des conséquences graves pour l'entreprise et ses clients.

Étapes :

1. Les attaquants identifient une vulnérabilité dans une application web utilisée ou dans ses systèmes internes.
2. À l'aide d'outils automatisés ou de techniques d'ingénierie sociale, les attaquants exploitent la vulnérabilité et obtiennent un accès non autorisé au réseau de l'entreprise.
3. Les attaquants font de la reconnaissance à travers le réseau, recherchant des bases de données contenant des informations sensibles.
4. Une fois qu'ils ont localisé une base de données appropriée, les attaquants extraient discrètement les données confidentielles tachant de ne pas alerter les systèmes de sécurité (cherchent à être sous les seuils de détections).
5. Les données volées sont exfiltrées vers un serveur contrôlé par les attaquants à l'extérieur du réseau de Piggy Bank Corporation.

Impacts potentiels :

- Vol et compromission des informations personnelles des clients.
- Risque de fraude et de vols d'identité.
- Non-conformité aux réglementations en matière de protection des données.
- Répercussions négatives sur la confiance des clients et la réputation de l'entreprise.

Pour être plus technique, voici un tableau expliquant les différentes techniques et tactiques utilisées, décrites par le site MITRE ATT&CK pour effectuer des attaques dans le cadre du phishing, de l'attaque par ransomware et de la fuite de données. Vous trouverez les références aux pages pertinentes du site MITRE ATT&CK pour chaque TTP :

Tactique	Technique	Description	Référence MITRE ATT&CK
Phishing	Spearphishing Attachment	Envoyer des courriels malveillants avec des pièces jointes contenant des logiciels malveillants pour infecter le système cible.	https://attack.mitre.org/techniques/TA1143/
Phishing	Spearphishing Link	Envoyer des courriels malveillants contenant des liens vers des sites web compromis pour piéger les utilisateurs et collecter leurs informations sensibles.	https://attack.mitre.org/techniques/TA1136/
Ransomware	Data Encrypted for Impact	Crypter les données sensibles d'un système pour causer des perturbations majeures et demander une rançon en échange de leur déchiffrement.	https://attack.mitre.org/techniques/T1486/
Ransomware	Remote File Copy	Copier des fichiers malveillants sur des	https://attack.mitre.o

		systèmes distants pour préparer une attaque par ransomware.	rg/techniques/TA0011/
Fuite de données	Exfiltration Over Alternative Protocol	Utiliser des protocoles alternatifs (par exemple, DNS, ICMP) pour exfiltrer discrètement les données volées hors du réseau de l'organisation.	https://attack.mitre.org/techniques/T1048/
Fuite de données	Exfiltration Over Command and Control Channel	Transférer les données volées vers un serveur de commande et de contrôle (C2) contrôlé par l'attaquant pour exfiltration ultérieure.	https://attack.mitre.org/techniques/T1041/

II) Présentation des outils d'aide à la détection utilisé par notre équipe SOC

Pour tester notre efficacité dans la détection d'indice de compromission dans le cadre de la simulation que nous avons choisi de mettre en place : Le scénario de la fuite de données, nous avons été amenés à utiliser les outils suivants : Wireshark, les journaux système de Windows et pour finir la solution Splunk.

Nous allons détailler les raisons de nos choix et présenter ces outils de manières concise pour pouvoir développer ensuite le déroulement de notre simulation.

1) Wireshark :

Qui dit exfiltration de données, dit activité réseau et quoi de mieux pour analyser cette activité que l'outils de prédilection de l'analyse de paquets réseaux qu'est Wireshark.

Wireshark est un outil très puissant et populaire utilisé pour l'analyse du trafic réseau. Il permet de capturer et d'inspecter les paquets de données qui circulent sur un réseau. Voici une explication brève de Wireshark et de son importance dans la détection d'une attaque visant la fuite de données :

1. Qu'est-ce que Wireshark ?

Wireshark est un logiciel libre et open-source qui offre une interface graphique conviviale pour l'analyse des paquets réseau. Il est disponible sur plusieurs plateformes (Windows, macOS, Linux) et prend en charge une grande variété de protocoles de communication.

2. L'importance de Wireshark :

Wireshark est un outil essentiel pour les professionnels de la sécurité informatique, les administrateurs réseau et les chercheurs en sécurité. Il permet de capturer et d'analyser le trafic réseau en temps réel, ce qui permet de détecter les activités suspectes, y compris les attaques visant la fuite de données.

3. Utilisation de Wireshark pour la détection d'une attaque de fuite de données :

Lorsqu'une attaque de fuite de données se produit, les attaquants peuvent exfiltrer des informations sensibles du réseau. Wireshark peut être utilisé pour détecter ces activités malveillantes en suivant ces étapes :

- **Capture du trafic** : Wireshark permet de capturer le trafic réseau en temps réel sur l'interface réseau ciblée.

- **Filtrage des paquets** : Une fois le trafic capturé, vous pouvez appliquer des filtres pour isoler les paquets pertinents en fonction des protocoles, des adresses IP source/destination, etc.

- **Analyse des flux de données** : En analysant les paquets capturés, Wireshark permet de visualiser les conversations réseau, les requêtes, les réponses et les échanges de données entre les machines.

- **Détection de comportements anormaux** : En comparant les schémas de communication normaux avec les schémas observés pendant une attaque, vous pouvez repérer des activités

suspectes, telles que l'envoi massif de données ou l'utilisation de protocoles inhabituels.

- **Identification des données exfiltrées** : En inspectant les paquets capturés, Wireshark peut vous aider à identifier les données sensibles qui sont transférées en dehors du réseau de manière non autorisée.

Wireshark est un outil extrêmement utile pour la détection précoce des attaques visant la fuite de données, permettant ainsi une réponse rapide pour limiter les dommages potentiels.

2) Les journaux système de Windows :

Notre machine cible est une machine virtuelle Windows, nous avons fait ce choix car lors de notre formation nous n'avons pas vraiment travaillé avec cette cible et nous désirions nous servir de ce TP pour nous challenger mais aussi étendre notre panel de connaissance.

Les journaux système de Windows sont des fichiers qui enregistrent les activités et les événements se produisant sur un système d'exploitation Windows.

Ils sont essentiels pour la surveillance, le dépannage et la détection des problèmes système. Voici une explication brève sur les journaux système de Windows, leur importance et leur utilisation dans la détection d'une attaque visant la fuite de données :

1. Qu'est-ce que les journaux système de Windows ?

Les journaux système de Windows sont des fichiers qui stockent des informations sur les événements liés au fonctionnement du système d'exploitation. Ils enregistrent une variété d'événements, tels que les démarrages et arrêts du système, les modifications de configuration, les erreurs, les avertissements, les activités réseau, etc.

2. L'importance des journaux système de Windows :

Les journaux système jouent un rôle crucial dans la surveillance et la maintenance des systèmes Windows. Ils permettent de :

- **Diagnostiquer les problèmes système** : Les journaux fournissent des informations détaillées sur les erreurs, les avertissements et d'autres événements liés au système, ce qui facilite le diagnostic des problèmes.

- **Surveiller l'activité système** : Les journaux permettent de suivre les activités du système en enregistrant les événements importants, ce qui facilite la détection des comportements anormaux.

- **Effectuer des audits de sécurité** : Les journaux système peuvent être utilisés pour vérifier l'intégrité du système, détecter les violations de sécurité et auditer les activités des utilisateurs.

3. Utilisation des journaux système dans la détection d'une attaque de fuite de données :

Lorsqu'une attaque de fuite de données se produit, les journaux système de Windows peuvent fournir des indices précieux pour détecter et analyser l'incident.

Voici comment ils peuvent être utilisés :

- **Analyse des journaux de sécurité** : Les journaux de sécurité contiennent des informations sur les tentatives de connexion, les modifications des privilèges d'utilisateur, les accès aux fichiers, etc. En les analysant, on peut repérer des activités suspectes, comme des accès non autorisés ou des tentatives de fuite de données.

- **Surveillance des journaux réseau** : Les journaux réseau peuvent révéler des comportements anormaux, tels que des transferts de données inhabituels, des connexions sortantes non autorisées ou des activités de communication vers des adresses IP suspectes.

- **Détection des modifications système suspectes** : Les journaux système peuvent enregistrer les modifications de configuration

du système, les installations de logiciels, les modifications du registre, etc. En identifiant des modifications inattendues ou malveillantes, on peut détecter des attaques ciblant la fuite de données.

3) Splunk :

Splunk est une plateforme de gestion des données et d'analyse opérationnelle très populaire. Elle permet d'indexer, de rechercher, d'analyser et de visualiser de vastes quantités de données générées par diverses sources. Voici une brève explication de Splunk, de son importance et de son utilisation dans la détection d'une attaque visant la fuite de données :

1. Qu'est-ce que Splunk ?

Splunk est un logiciel d'analyse de données qui collecte, indexe et analyse des données provenant de différentes sources telles que les journaux système, les événements de sécurité, les données réseau, les données d'application, etc. Il permet de traiter et d'extraire des informations significatives à partir de ces données, facilitant ainsi la prise de décisions et la résolution de problèmes.

2. L'importance de Splunk :

Splunk joue un rôle essentiel dans la gestion des données et la sécurité informatique. Voici quelques raisons pour lesquelles Splunk est important :

- **Agrégation et indexation des données** : Splunk peut collecter et indexer de grandes quantités de données provenant de sources multiples, ce qui permet une recherche rapide et efficace.

- **Recherche et analyse** : Splunk offre des fonctionnalités de recherche puissantes pour extraire des informations précieuses à partir des données collectées, permettant de détecter des schémas, des anomalies et des comportements suspects.

- **Corrélation des événements** : Splunk peut associer et corréler des événements provenant de différentes sources, facilitant ainsi la détection des attaques et des activités malveillantes.

- **Visualisation des données** : Splunk propose des fonctionnalités de visualisation et de création de tableaux de bord interactifs pour présenter les données d'une manière claire et compréhensible.

3) Utilisation de Splunk dans la détection d'une attaque de fuite de données :

Splunk peut jouer un rôle essentiel dans la détection précoce des attaques visant la fuite de données. Voici comment Splunk peut être utilisé :

- **Surveillance en temps réel** : Splunk peut être configuré pour surveiller en temps réel les événements liés à la sécurité et à la fuite de données, tels que les accès non autorisés, les transferts de données suspects, les tentatives d'exfiltration, etc.

- **Analyse des journaux et des flux de données** : Splunk permet de collecter, analyser et corréler les journaux système, les journaux réseau, les journaux de sécurité, etc., afin de détecter les activités anormales associées à une attaque de fuite de données.

- **Détection d'anomalies** : Splunk peut utiliser des algorithmes d'apprentissage automatique (machine learning) pour identifier les schémas de comportement normaux et détecter les anomalies potentielles liées à une fuite de données.

- **Gestion des incidents de sécurité** : En centralisant les données et en fournissant des fonctionnalités d'alerte et de reporting, Splunk peut faciliter la gestion des incidents de sécurité liés à une attaque de fuite de données.

Les 3 outils que nous vous avons présenté pourrons, comme vous l'avez compris grâce au point 2 de chaque présentation que nous avons faite, être utiles pour la détection des attaques que nous avons présentés en partie I et d'autres.

Une multitude d'outils existent mais dans le temps qui nous a été alloué, nous avons décidé d'utiliser ces 3 là qui nous paraissaient les plus cohérent au vu du choix de simulation que nous avons fait.

III) rapport détaillé de l'attaque simulée :

Pour réaliser cette simulation, nous avons utilisé l'outils Caldera. Caldera est un projet open-source développé par MITRE Corporation. Il fournit une plateforme de simulation qui permet aux équipes de sécurité de planifier, d'exécuter et d'analyser des scénarios d'attaques réalistes dans un environnement contrôlé. Caldera permet aux utilisateurs de modéliser les tactiques, techniques et procédures (TTP) utilisées par les attaquants pour mener à bien une attaque.

Caldera est donc l'outil idéal pour que nous mettions en place notre **scénario de fuite de données**. Il offre plusieurs avantages :

- **Évaluation de la posture de sécurité** : Caldera permet de tester la résistance des systèmes à une attaque visant une fuite de données, en répliquant les TTP utilisés par les attaquants réels.

- **Détection des vulnérabilités** : En simulant une attaque de fuite de données, Caldera peut révéler les vulnérabilités potentielles dans les défenses de sécurité existantes et aider à les corriger avant qu'un véritable incident ne se produise.

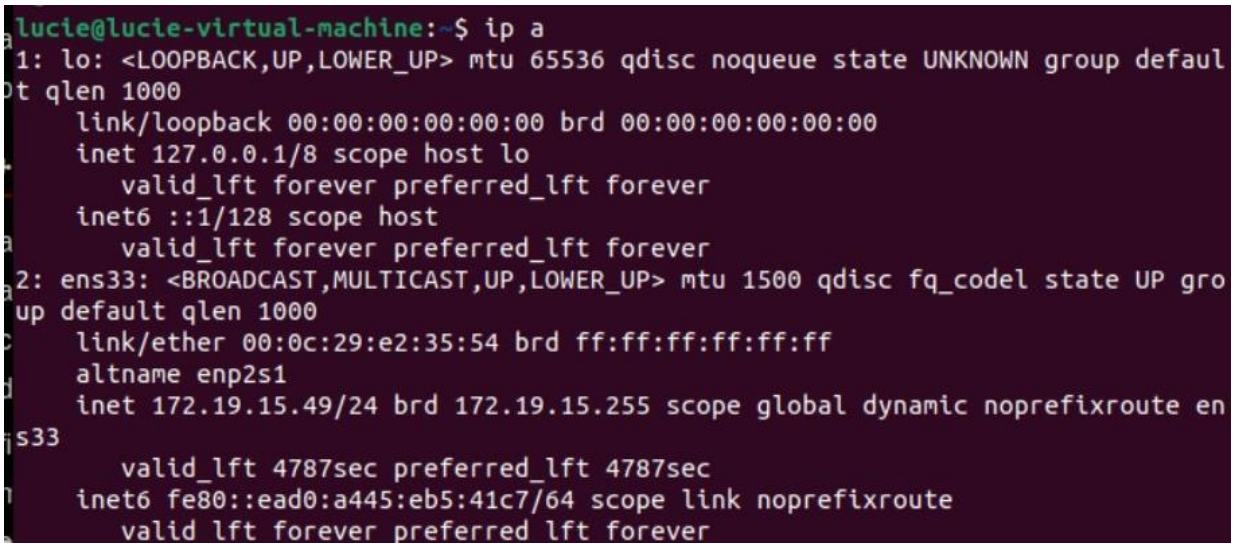
- **Validation des outils de détection** : Caldera permet de tester l'efficacité des outils de détection et des solutions de sécurité en simulant des attaques réelles, ce qui aide à améliorer la capacité de détection et de réponse aux incidents.

- **Formation et sensibilisation** : L'utilisation de Caldera permet de former les équipes de sécurité à reconnaître et à réagir aux attaques de fuite de données, tout en sensibilisant à l'importance de la sécurité des données.

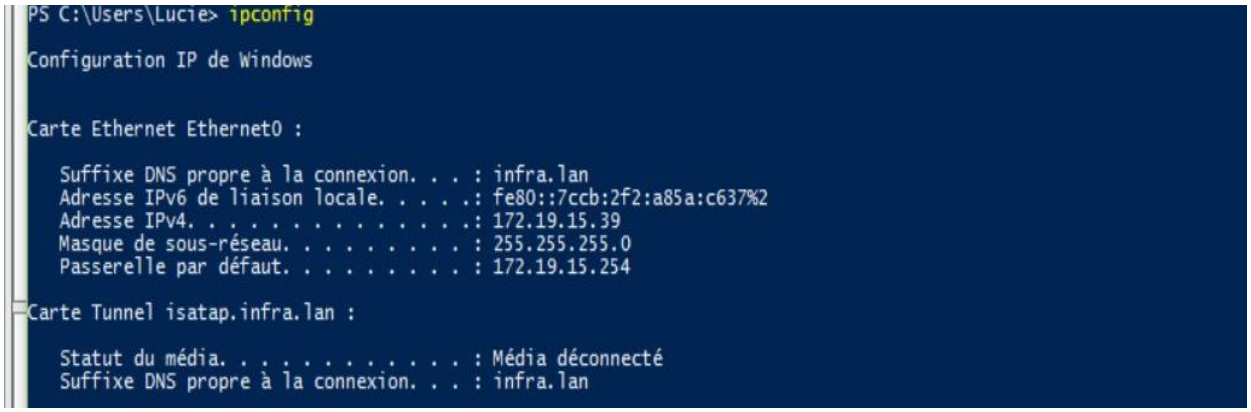
1) Mise en place et fonctionnement de l’attaque :

Nous avons décidé de partir sur l’utilisation de 2 machines virtuels.

Une machine Ubuntu qui servira d’attaquant mais aussi à recueillir les logs de la machine cible. Dont voici l’adresse IP : 172.19.15.49



Une machine Windows qui sera la machine victime vu que nous n’avons jamais réalisé d’attaque dessus nous souhaitions nous challenger.
Son adresse IP est la suivante : 172.19.15.39

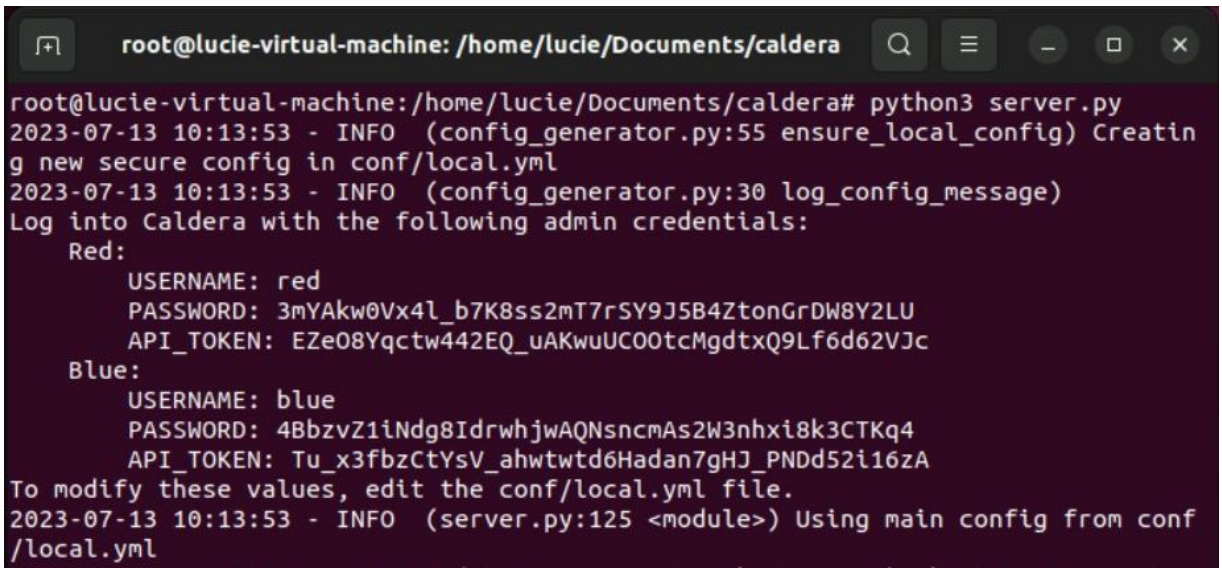


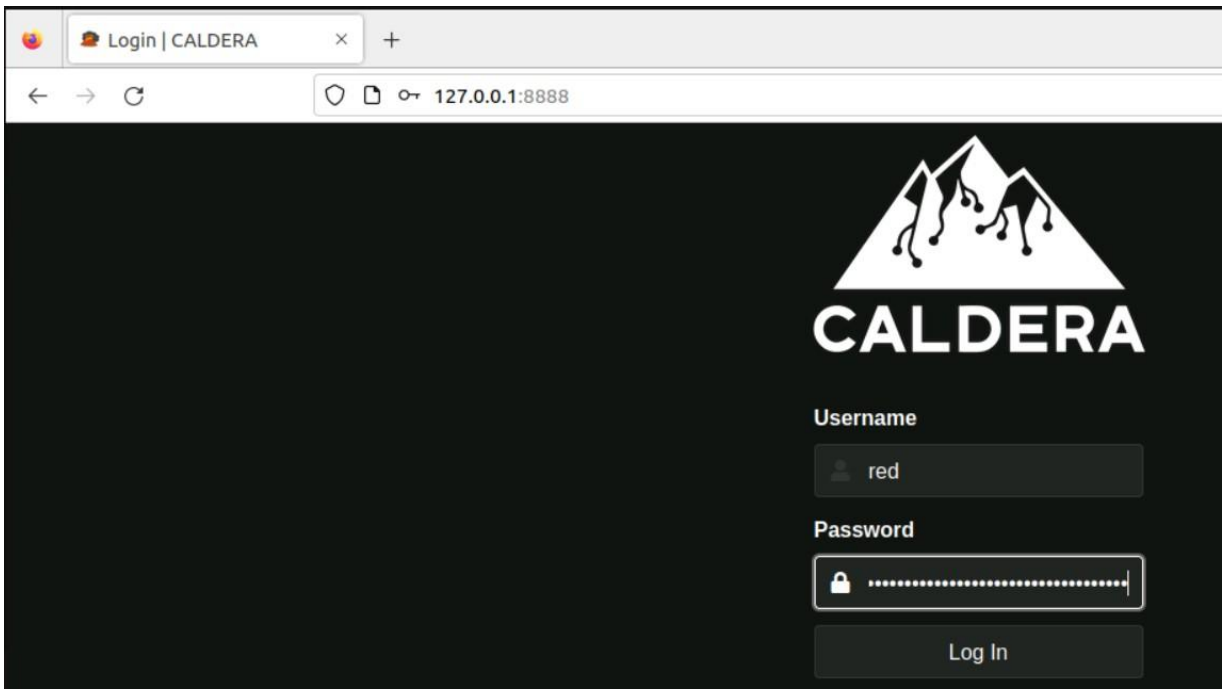
Notre objectif est de mettre en place une simulation d’extraction de données. Pour cela nous devons installer Caldera pour les raisons que nous avons développées précédemment dans le rapport.

- Installation de Caldera et récupération des identifiants :

Ici, après installation, nous obtenons des identifiants pour nous connecter à Caldera sur le port qui lui est affilié par défaut, le port 8888.

Nous choisissons les identifiants Red car il s'agit de mettre en place une attaque donc nous utilisons cet outil pour du Red Teaming.





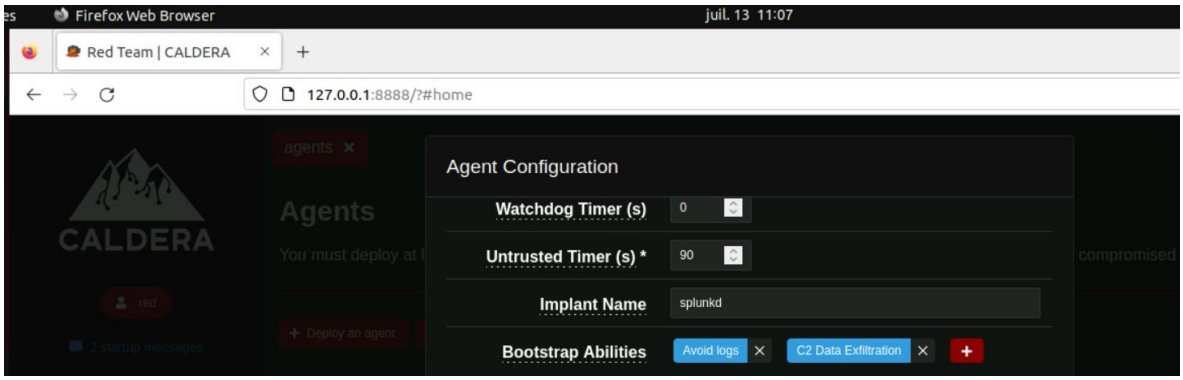
- Installation de Splunk :

En parallèle nous lançons l'installation de Splunk qui nous servira dans la suite de notre simulation. Notamment dans un but de détection.

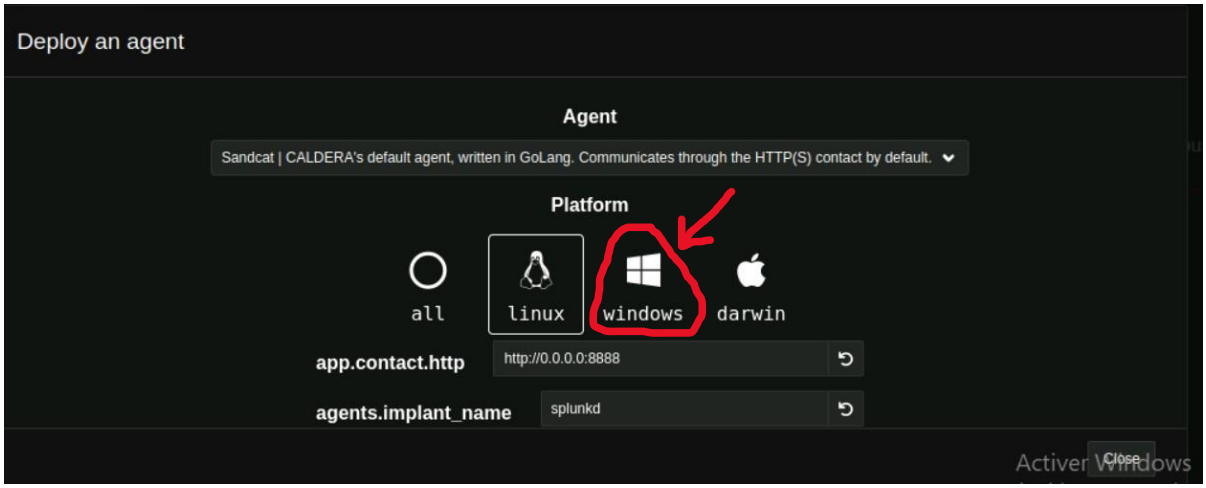
- Mise en place du schéma que nous avons imaginé :

Pour se faire nous devons créer sur Caldera un agent que l'on va lancer sur notre machine Windows afin de simuler que nous avons une main sur la machine cible.

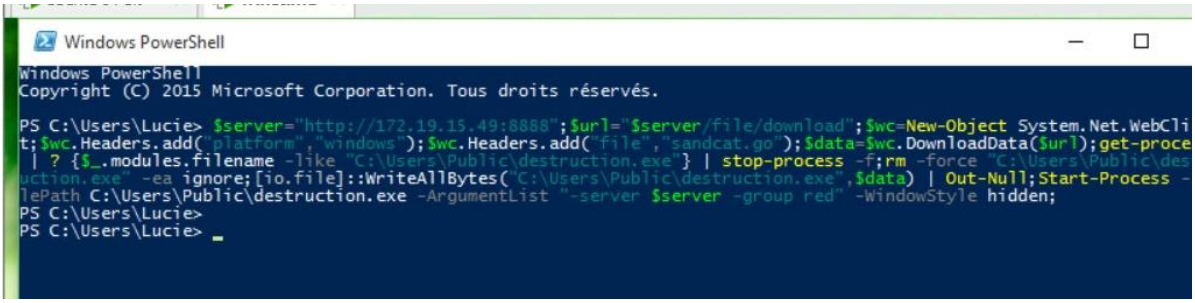
Avant toute attaque il faut de la reconnaissance et créer une porte d'entrer pour pouvoir faire des opérations sur une machine. C'est ce que va simuler cet agent.



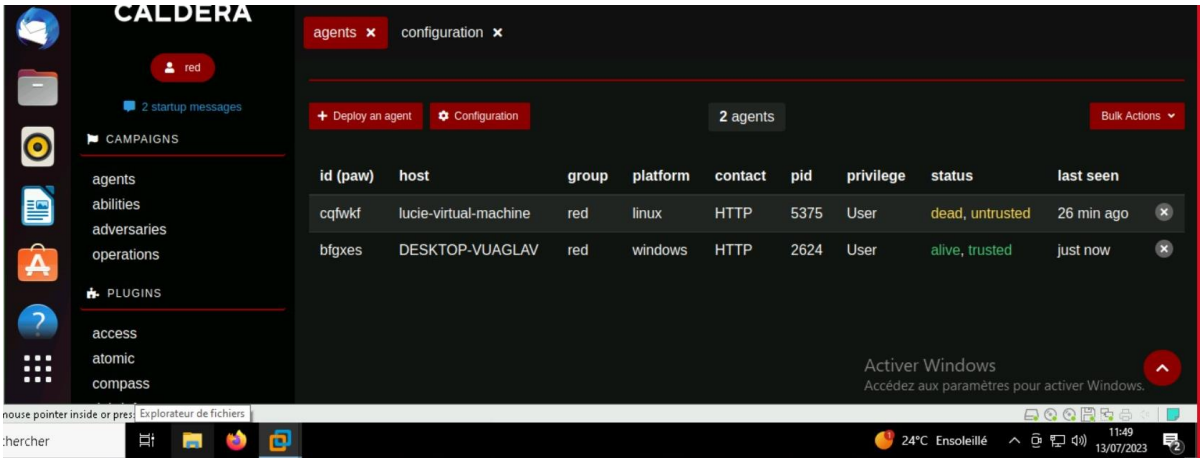
Après avoir créé l'agent il faut le déployer, nous visons un environnement Windows donc on sélectionne la plateforme Windows.



Une fois ceci fait nous copions le premier script mis à disposition par Caldera afin de l'insérer dans un invite de commande PowerShell de notre Windows victime afin de l'exécuter et rendre notre agent actif.

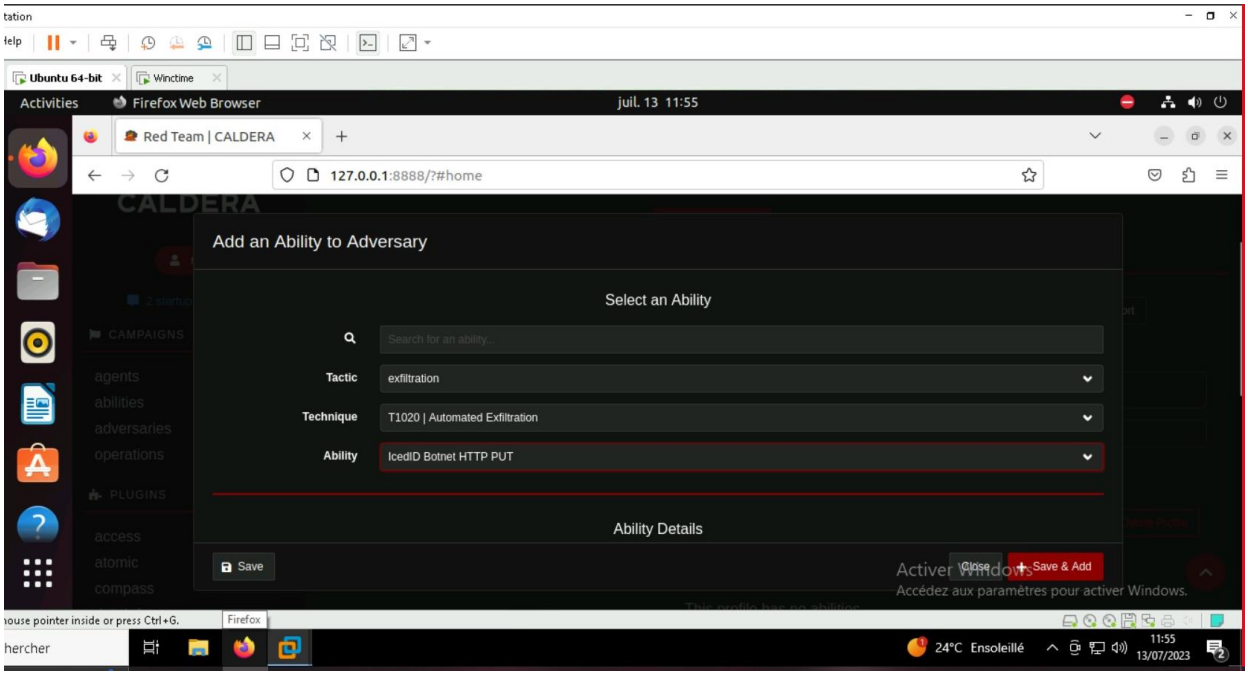


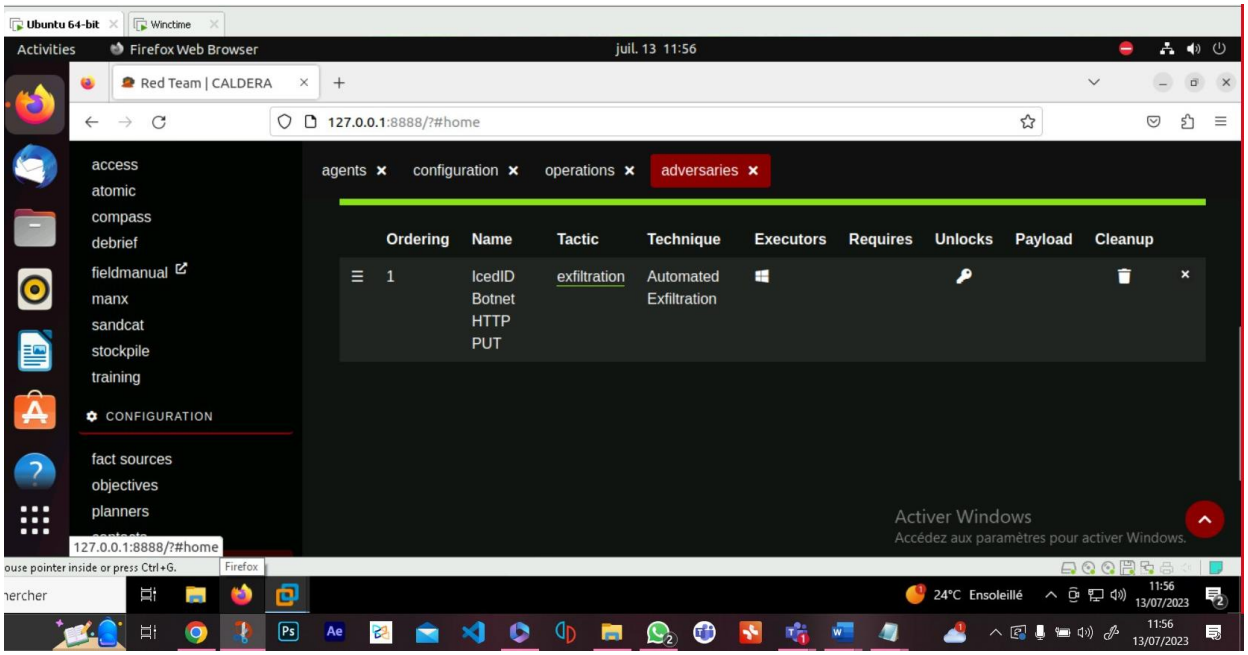
Une fois ceci fait, nous vérifions que notre agent est bien actif, c'est le cas comme vous pouvez le voir ci-dessous.



Maintenant que nous avons la main sur notre Windows, nous allons créer notre attaquant.

Vu que nous avons développé quelques TTP pour l'exfiltration précédemment, nous décidons afin de montrer un exemple différent des précédents, de choisir une technique d'attaque qui n'est pas parmi celles que nous avons mentionnés comme l'illustre la création de notre adversaire ci-dessous.





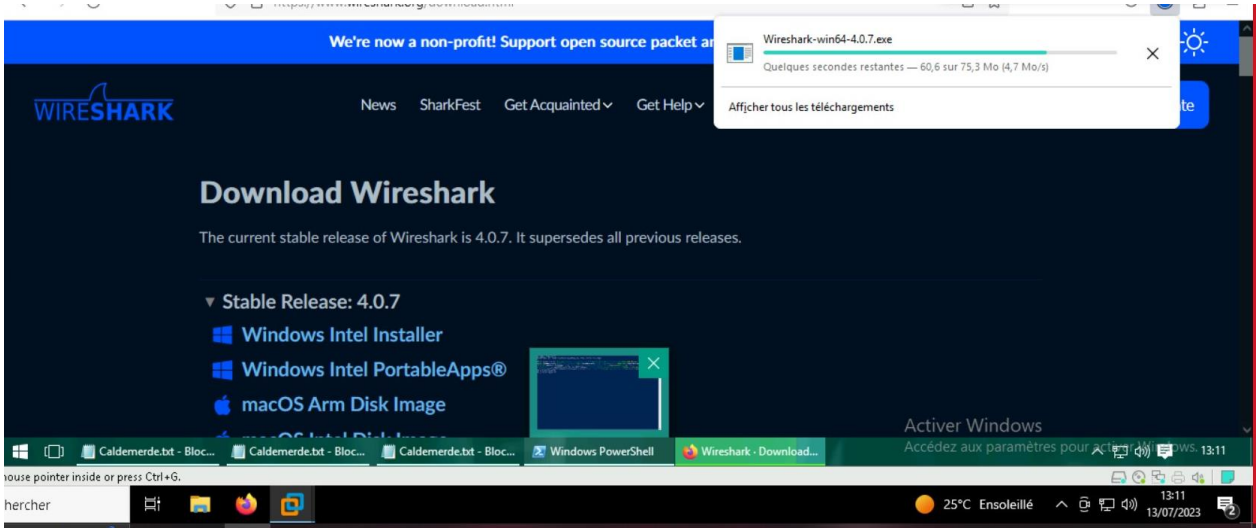
Notre adversaire maintenant crée reste à lancer l'attaque et vérifier si l'attaque est bien en cours et détectable par les outils de détection que nous avons sélectionnés.

2) Mise en place des outils de surveillance et détection de l'anomalie :

- Téléchargement de Wireshark sur notre machine Windows :

Nous avons décidé que le moyen le plus rapide de détecter de l'exfiltration sur la machine corrompue était d'user de Wireshark.

Nous installons donc cet outil sur notre Windows :

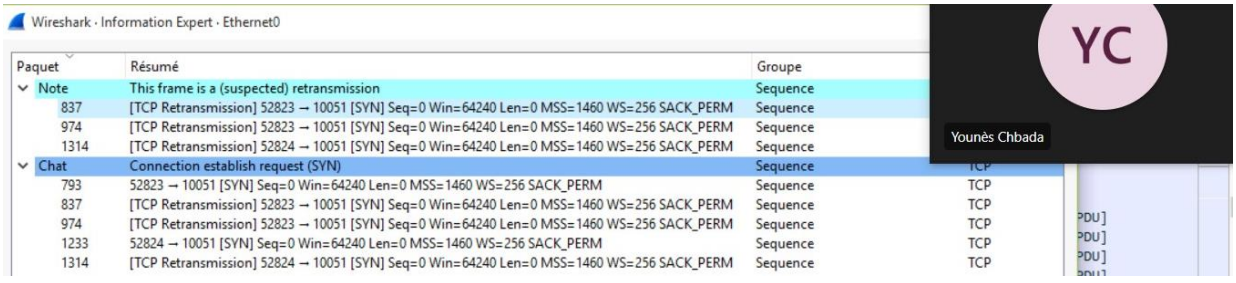


Une fois ceci fait nous commençons à nous servir de l'outils pour trouver des indices nous permettant de recueillir des preuves d'une activité malveillante.

Nous réalisons une capture du trafic réseau à l'aide de Wireshark et nous avons trouvé la preuve que nous cherchions et eu la confirmation que notre attaque s'est bien déroulé ! Voici ce que nous avons pu trouver :

1. Notre premier réflexe : regarder l'expert info.

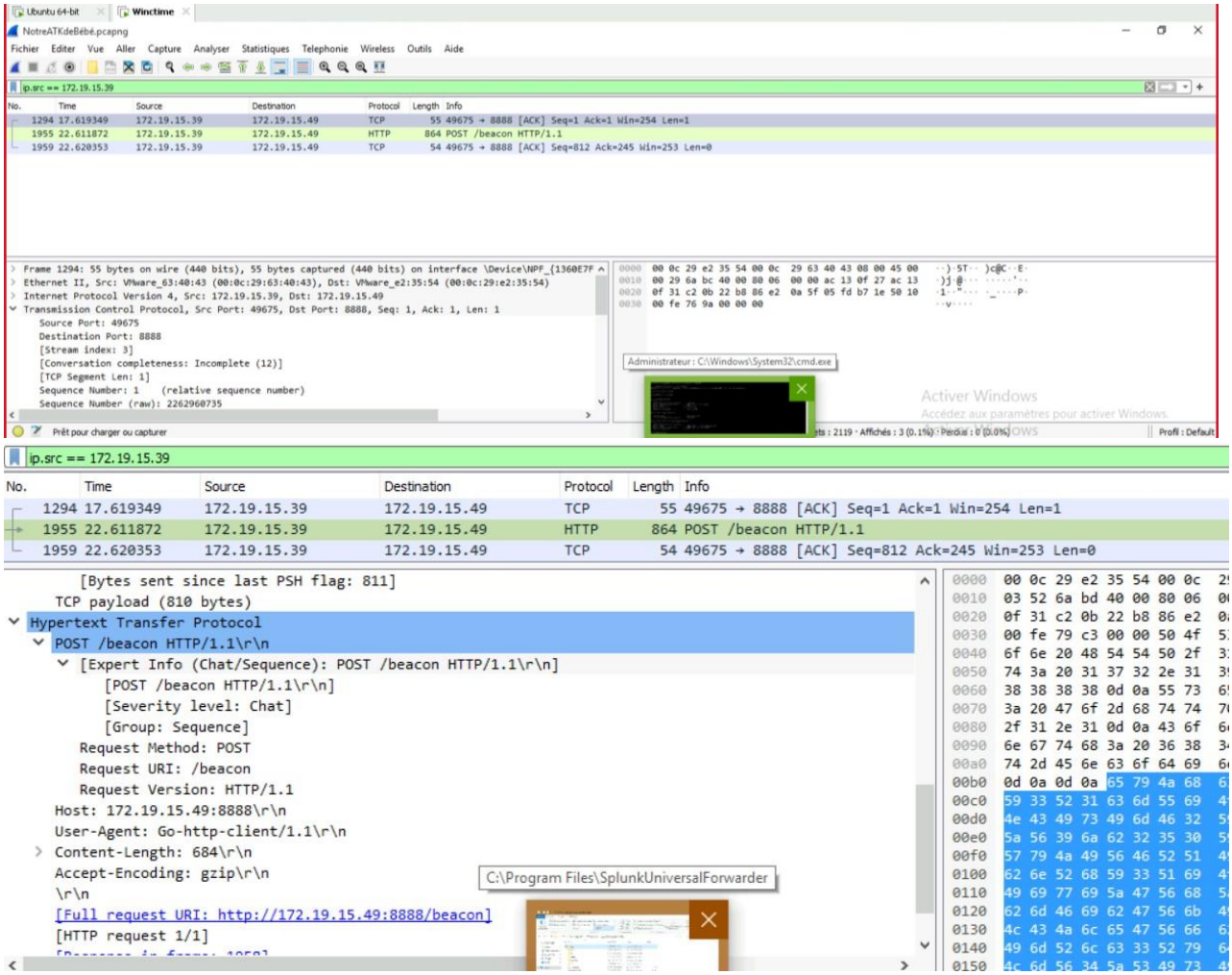
Ici on nous voyons déjà qu'il y une retransmission suspecte comme l'indique l'expert



2. Maintenant il faut préciser si c'est bien à cause de notre machine attaquante

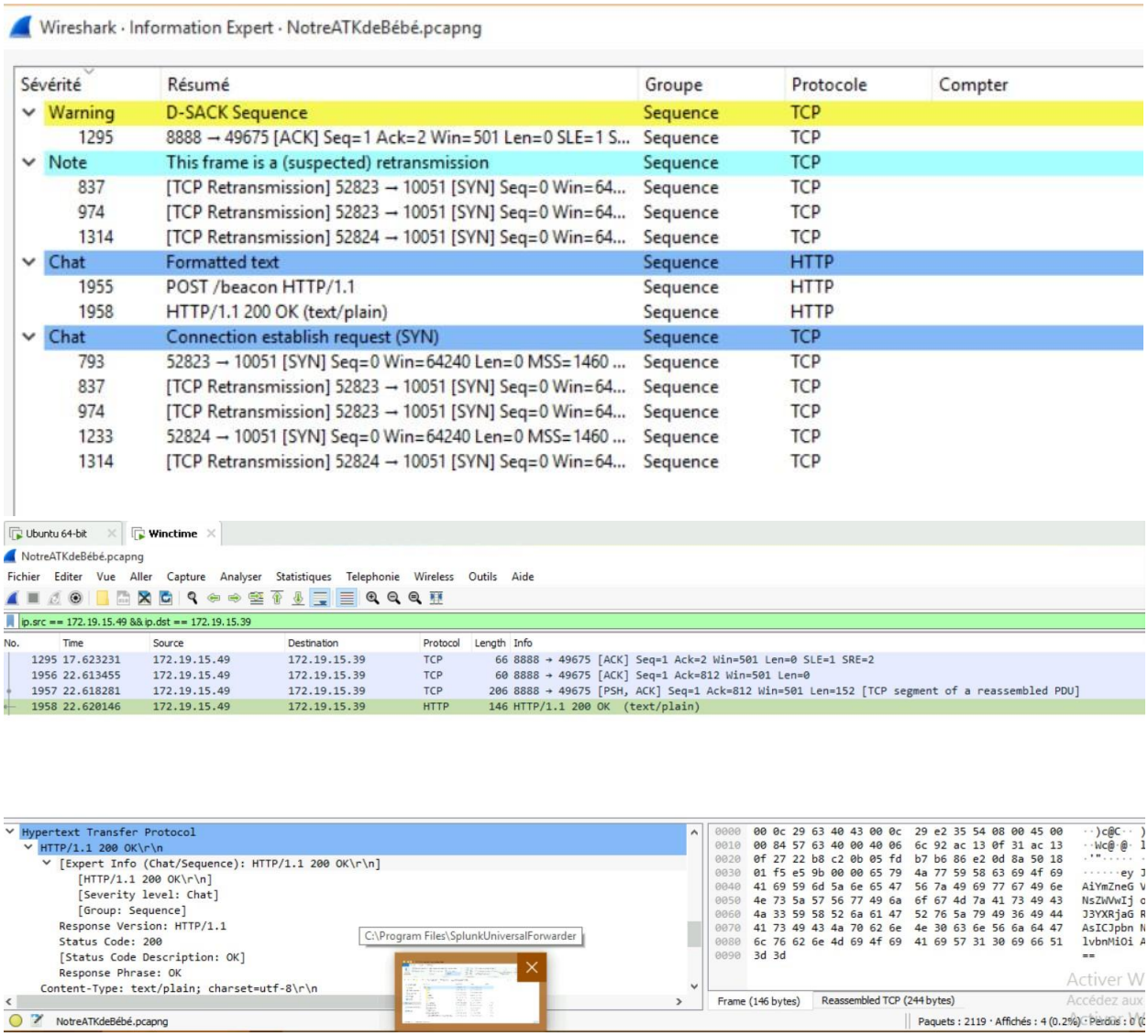
Pour se faire nous allons appliquer un filtre avec pour IP source de notre victime afin de vérifier s'il y a bien une communication avec notre machine Ubuntu attaquante.

Voici ce que nous obtenons :



BINGO ! Voici ce que nous obtenons ! Une communication via TCP qui entre temps donne lieu à un envoi de données (méthode POST) par notre victime vers notre machine attaquante via le protocol HTTP !

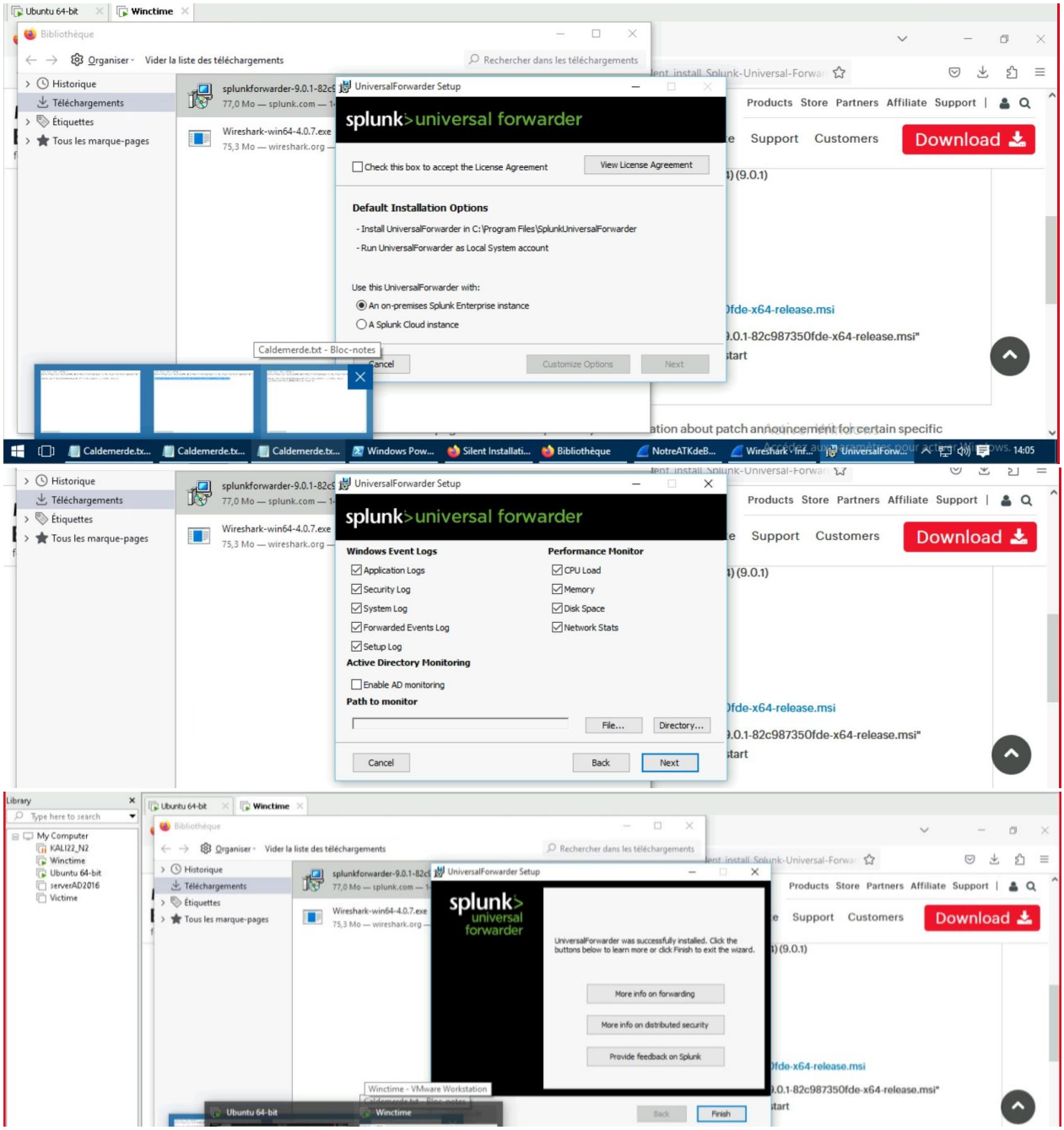
On a maintenant la confirmation que notre attaque s'est bien déroulée mais aussi que l'outil Wireshark à bien tenu ses promesses car il a pu détecter cette communication suspecte entre les deux machines.



On remarquera que la communication s'est passée sans encombre car en appliquant un filtre cette fois avec l'IP source étant l'attaquant et l'IP destination la victime on a un code 200 qui signifie une connexion avec succès. Ci-joint au présent rapport vous notre fichier Pcap.

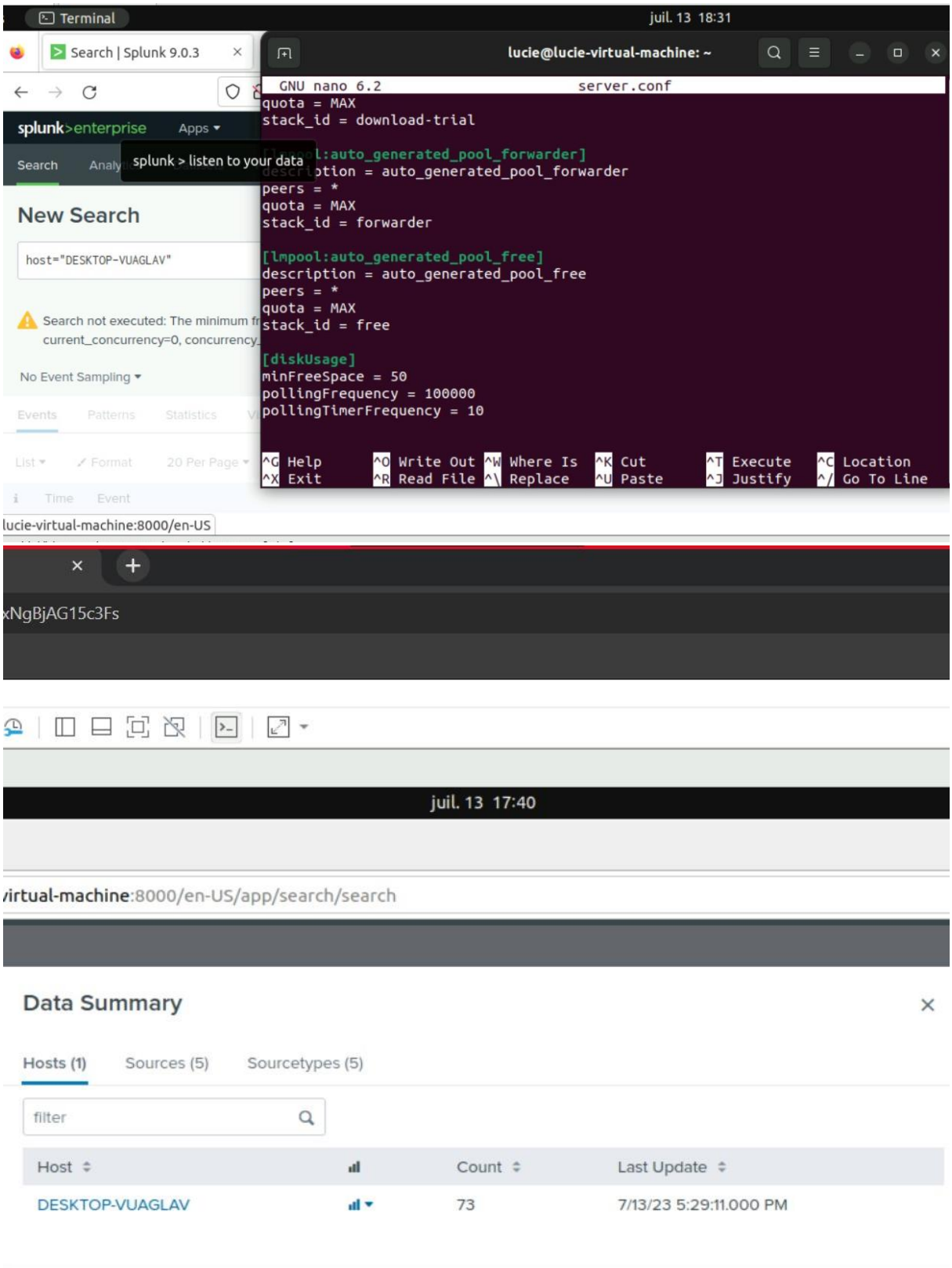
- Maintenant que nous avons vérifiés que ça marche, il faut faire remonter les logs à notre machine Ubuntu dans Splunk :

Nous avons téléchargé l'Universal Forwarder sur notre Windows et l'avons paramétré afin de récupérer nos logs.

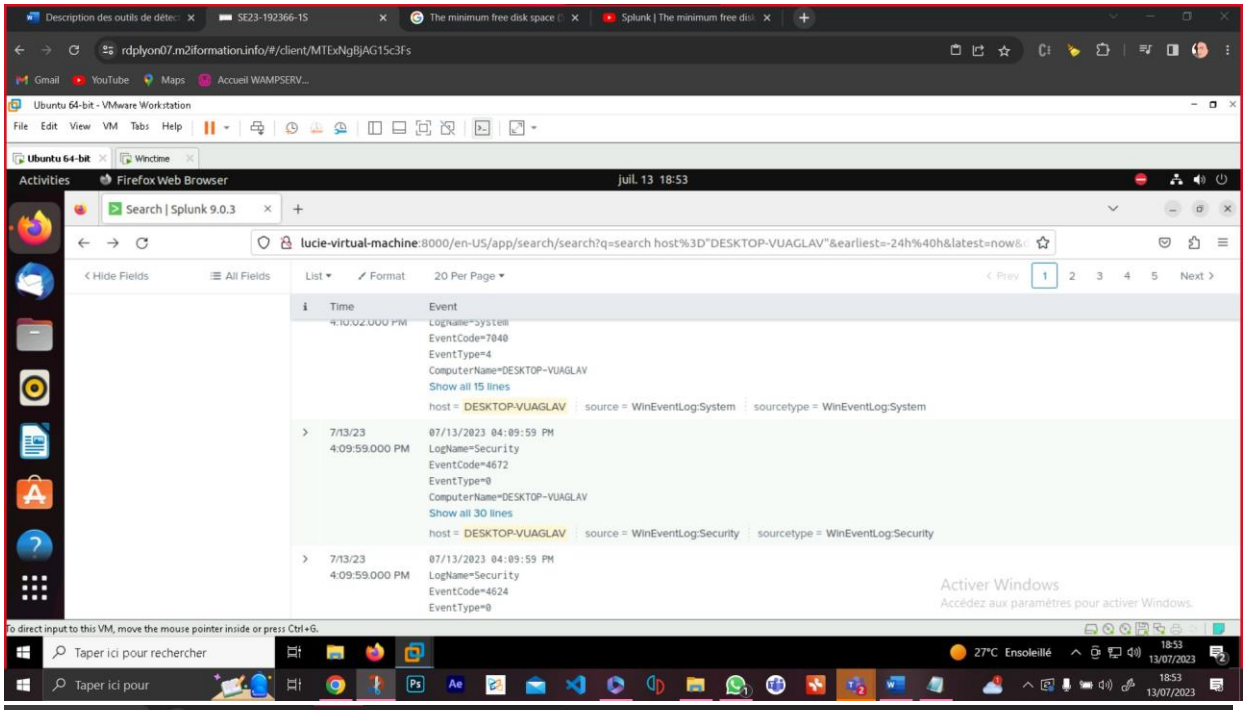


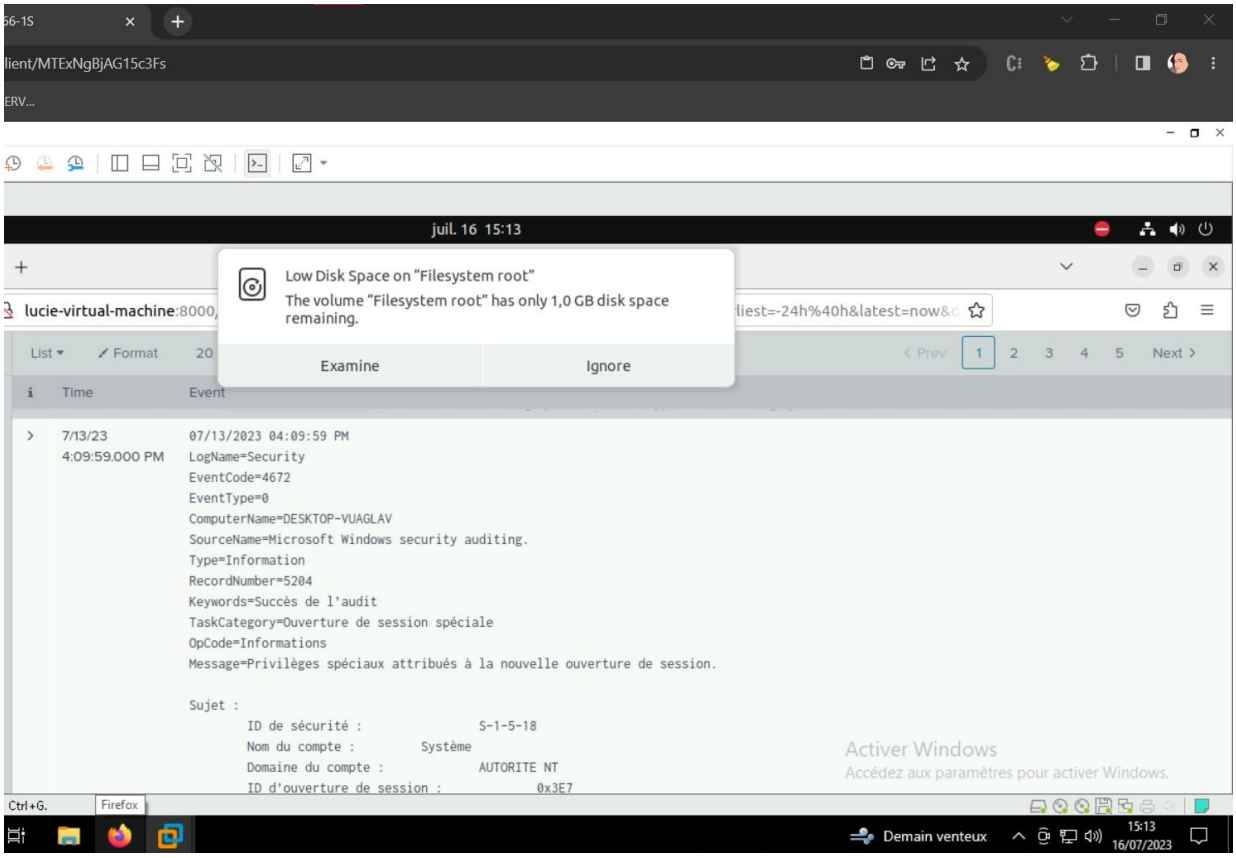
Nous avons dû faire des modifications en ligne de commande pour paramétrer le forwarder et faire la connexion sur le port 9997.

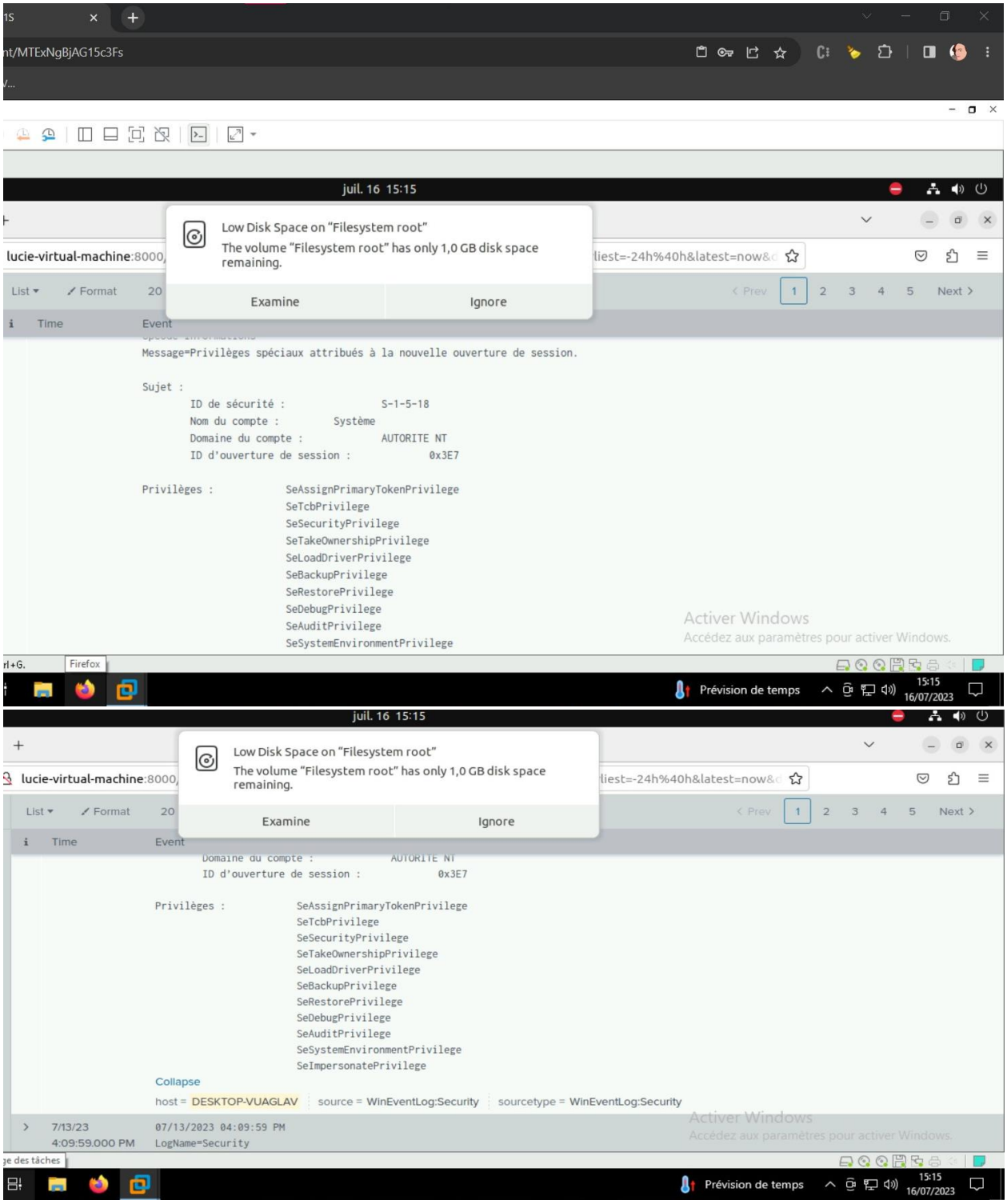
Après ces modifications nous avons eu un souci de mémoire que nous avons résolu en modifiant le fichier server.conf



Nous avons après avoir redémarré Splunk pu enfin accéder à nos logs que voici.

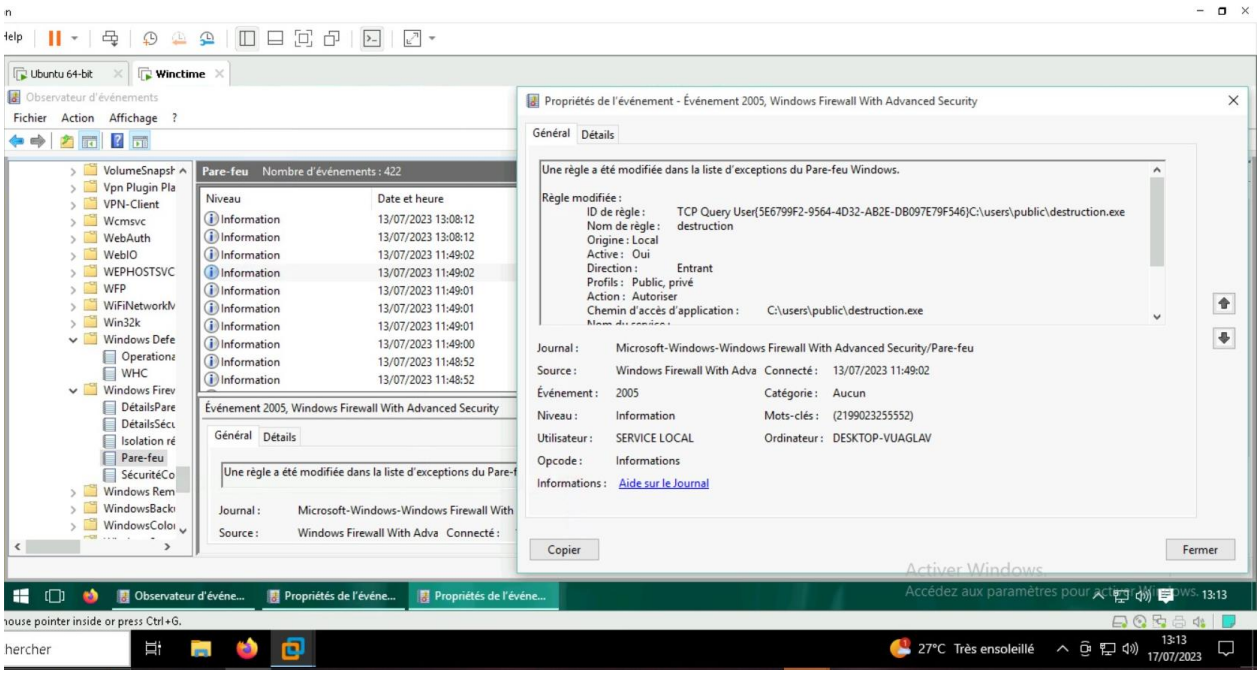

Description des outils de déte
SE23-192366-1S
The minimum free disk space
Splunk | The minimum free disk
rdplyon07.m2iformation.info/#/client/MTExNgBjAG15c3Fs
Gmail
YouTube
Maps
Accueil WAMPSERV...
Ubuntu 64-bit - VMware Workstation
File Edit View VM Tabs Help
Ubuntu 64-bit
Winctime
Activities
Firefox Web Browser
juil. 13 18:53
Search | Splunk 9.0.3
lucie-virtual-machine:8000/en-US/app/search/search?q=search host%3D"DESKTOP-VUAGLAV"&earliest=-24h%40h&latest=now&
Hide Fields
All Fields
List
Format
20 Per Page
Prev 1 2 3 4 5 Next
Time
Event
EventCode=7040
EventType=4
ComputerName=DESKTOP-VUAGLAV
Show all 15 lines
host = DESKTOP-VUAGLAV source = WinEventLog:System sourcetype = WinEventLog:System
7/13/23
4:09:59.000 PM
07/13/2023 04:09:59 PM
LogName=Security
EventCode=4672
EventType=0
ComputerName=DESKTOP-VUAGLAV
Show all 30 lines
host = DESKTOP-VUAGLAV source = WinEventLog:Security sourcetype = WinEventLog:Security
7/13/23
4:09:59.000 PM
07/13/2023 04:09:59 PM
LogName=Security
EventCode=4624
EventType=0
Activer Windows
Accédez aux paramètres pour activer Windows.
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Taper ici pour rechercher
27°C Ensoleillé
18:53
13/07/2023


juil. 16 15:13
Low Disk Space on "Filesystem root"
The volume "Filesystem root" has only 1,0 GB disk space remaining.
Examine
Ignore
lucie-virtual-machine:8000,
liest=-24h%40h&latest=now&
List
Format
Prev 1 2 3 4 5 Next
Time
Event
7/13/23
4:09:59.000 PM
07/13/2023 04:09:59 PM
LogName=Security
EventCode=4672
EventType=0
ComputerName=DESKTOP-VUAGLAV
SourceName=Microsoft Windows security auditing.
Type=Information
RecordNumber=5204
Keywords=Succès de l'audit
TaskCategory=Ouverture de session spéciale
OpCode=Informations
Message=Privilèges spéciaux attribués à la nouvelle ouverture de session.
Sujet :
ID de sécurité : S-1-5-18
Nom du compte : Système
Domaine du compte : AUTORITE NT
ID d'ouverture de session : 0x3E7
Activer Windows
Accédez aux paramètres pour activer Windows.
Ctrl+G.
Firefox
Demain venteux
15:13
16/07/2023



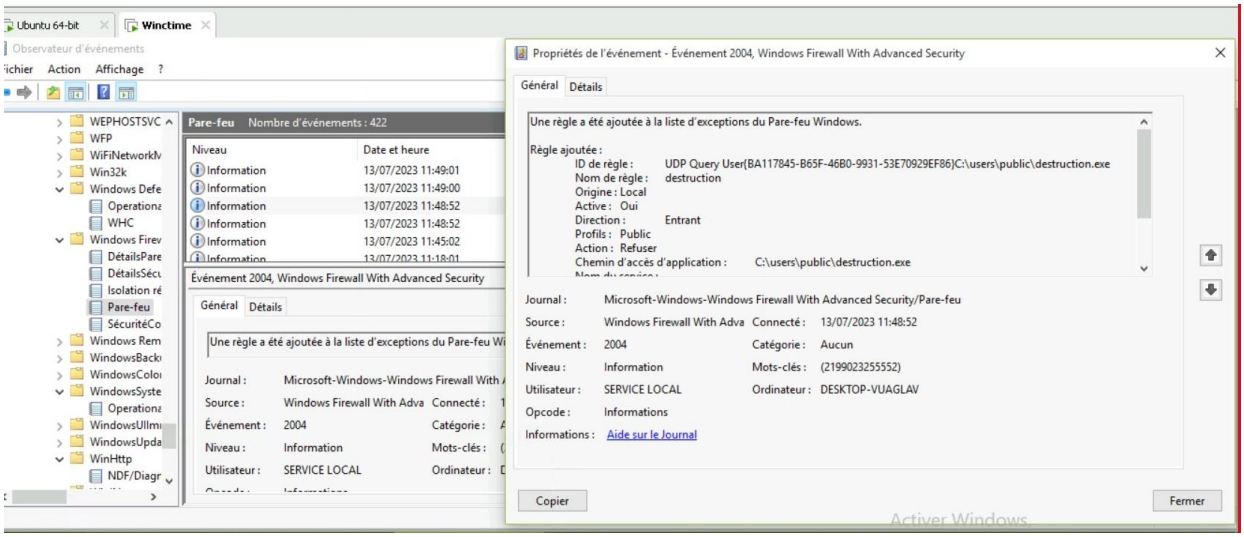
On voit que l'on récupère bien les logs du journal d'événement Windows cependant comme nous avons effectué une remontée de log après l'attaque, la machine n'a pas récupéré ce qui est antérieur à l'installation du forwarder. Notre machine virtuelle manquant d'espace je ne peux pas refaire la manipulation.

Je vais donc user des journaux d'évènement Windows pour illustrer mon propos.



Ici on peut voir que la connexion TCP que l'on décèle dans Wireshark est bien visible dans les logs du pare-feu Windows.

Il y a eu aussi une modification dans les règles de Pare-feu :



Notre agent est bien en place et comme le prouve la capture Wireshark, il y a bien exfiltration de données.

Conclusion

Un SOC (Security Operations Center) est d'une importance capitale dans une organisation telle que Piggy Bank Corporation.
Il permet une détection proactive des menaces, une réponse rapide aux incidents de sécurité, la prévention des pertes financières, la protection de la réputation de l'entreprise, ainsi qu'une amélioration continue de la sécurité.

Un SOC assure une surveillance constante du système d'information, les SOC analystes apportent une analyse approfondie et mènent des actions proactives. En résumé un SOC renforce la posture de sécurité globale de l'entreprise et contribue à la protection de ses actifs les plus précieux.

Si nous devions refaire cette manipulation nous apporterions des modifications dans l'exécution des tâches notamment :

Nous installerions d'abord le forwarder sur la Windows pour être sûre de capturer ce qu'il se passe sur la Victime durant l'attaque dans Splunk. Nous ne savions pas qu'installer le Forwarder après la manipulation serait un problème car nous n'en avions jamais installé mais cela nous a permis de nous améliorer et d'apprendre.

Nous ferions en sorte d'activer certains journaux Windows qui permettrait d'avoir une vue encore plus précise de ce qui se déroules lors de l'attaque. Quand nous sommes allés dans les journaux pour illustrer ce que nous aurions dû trouver sur Splunk, nous avons vu que certaines journalisations peut être utiles n'étaient pas activées de base comme celle-là : Les Logs HTTP.