



# RAPPORT DE STAGE

**Benoît DOUBLE**

03/06/24

05/07/24

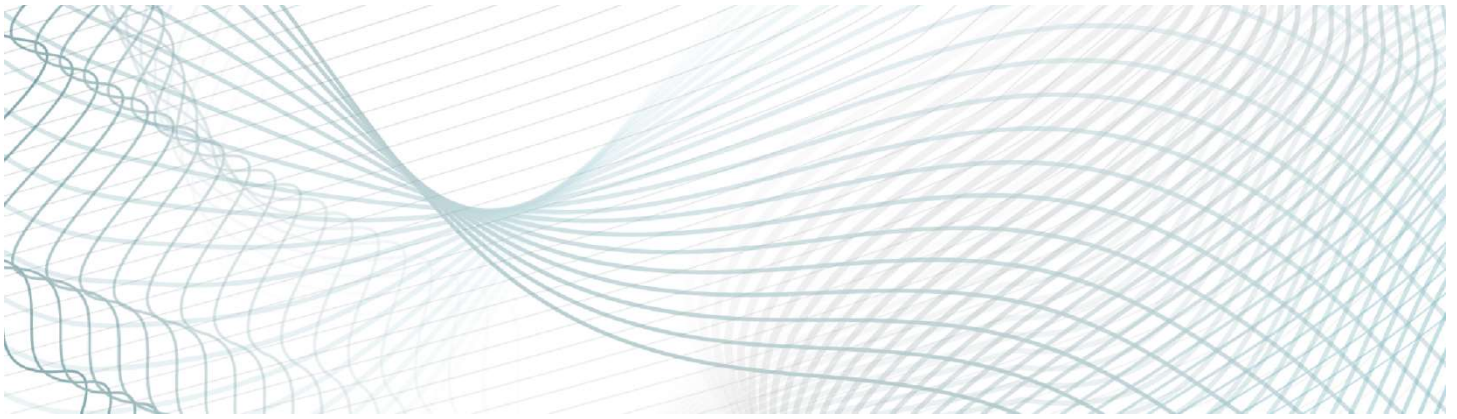
—

SIO-SISR

2023-2024

—

Mr Langloy



## REMERCIEMENTS

---

Tout d'abord, je remercie chaleureusement Mr. Anis Djerrah, mon maître de stage, pour son encadrement bienveillant et ses conseils avisés. Grâce à lui, j'ai pu découvrir de nombreuses facettes de la cybersécurité et développer des compétences essentielles dans ce domaine.

Je remercie également Mr. Laurent Double, responsable de l'équipe de Francheville, ainsi que tous les membres de cette équipe pour leur accueil chaleureux, leur disponibilité et leur soutien tout au long de mon stage. Leur expertise et leur patience m'ont beaucoup appris et m'ont permis de m'intégrer rapidement au sein de l'équipe.

Un grand merci à l'alternant Kalontas Mermer pour sa collaboration sur le projet IPAM. Travailler ensemble sur ce projet a été une expérience très instructive et agréable.

Enfin, je remercie Securitas Technology pour m'avoir offert cette opportunité de stage et pour m'avoir permis de découvrir un environnement de travail stimulant et enrichissant. Ce stage a été une étape importante dans ma formation et a confirmé mon intérêt pour le domaine de l'informatique et de la cybersécurité.

Je repars de cette expérience avec de nouvelles compétences, des souvenirs précieux et une motivation renforcée pour poursuivre ma carrière dans ce domaine passionnant.

---

# Table des matières

SECURITAS TECHNOLOGY .....	4
A. L'entreprise.....	4
B. La place de l'informatique dans l'entreprise .....	4
C. L'EQUIPE .....	5
Les projets.....	6
IPAM .....	6
Introduction à IPAM .....	6
Contexte et Importance de l'IPAM .....	6
Objectifs et Bénéfices de l'Utilisation de l'IPAM .....	6
La Mission .....	7
Ajout des Sous-Réseaux et des VLANs .....	7
Importation des Plages IP en CSV .....	8
Configuration NAT .....	8
Mise à Jour Dynamique .....	9
Réalisation de la Documentation.....	9
Communication avec les Employés .....	9
Conclusion.....	9
PENTEST .....	10
Introduction .....	10
1. Préparation et Planification du Pentest .....	10
2. Mise en Place de l'Environnement de Pentest.....	10
3. Réalisation du Pentest.....	11
Conclusion .....	12
VEILLE CYBER.....	12
Introduction .....	12
1. Mise en Place de la Veille Technologique.....	13
2. Processus de Veille et Réponse aux Vulnérabilités.....	15
Conclusion.....	15
Conclusion .....	16
Annexes.....	17

## INTRODUCTION

Dans le cadre de mon stage de fin d'année de mon BTS SIO1 option SISR, j'ai rejoint les équipes du service IT Monitoring de Securitas Technology sur une période d'un mois. Tout au long de ce stage, j'ai été encadré par une équipe qui m'a permis de découvrir certaines facettes du monde de l'IT et celui du travail. J'ai donc été affecté à plusieurs missions, assisté à plusieurs réunions et formations. J'ai été supervisé par Mr Anis Djerrah, qui m'a permis notamment de découvrir la cybersécurité.



# SECURITAS TECHNOLOGY

## A. L'entreprise

### Securitas AB :

- **Secteur d'activité** : Securitas AB est une entreprise internationale de sécurité privée. Ses services incluent la surveillance humaine, la sécurité mobile, les solutions de sécurité électronique, la sécurité des événements et des installations, ainsi que les services de consultation en sécurité.
- **Chiffre d'affaires** : En 2022, le chiffre d'affaires de Securitas AB s'élevait à environ 120 milliards de SEK (couronnes suédoises), soit environ 10,6 milliards d'euros.
- **Effectifs** : Securitas AB emploie environ 345 000 personnes dans le monde entier, ce qui en fait l'une des plus grandes entreprises de sécurité au niveau mondial.

### Securitas Technology France :

- **Secteur d'activité** : Securitas Technology France se spécialise dans les solutions de sécurité électronique, incluant les systèmes de vidéosurveillance, de contrôle d'accès, d'alarme incendie, et les solutions de sécurité intégrée.
- **Chiffre d'affaires** : Le chiffre d'affaires spécifique de Securitas Technology France n'est pas publiquement disponible, mais elle fait partie de la division technologique de Securitas AB qui représente une part significative de l'activité totale du groupe.
- **Effectifs** : En France, Securitas emploie environ 15 000 personnes, dont une partie importante travaille pour Securitas Technology France.

## B. La place de l'informatique dans l'entreprise

L'informatique joue un rôle crucial dans le fonctionnement de Securitas Technology France. Voici quelques points clés :

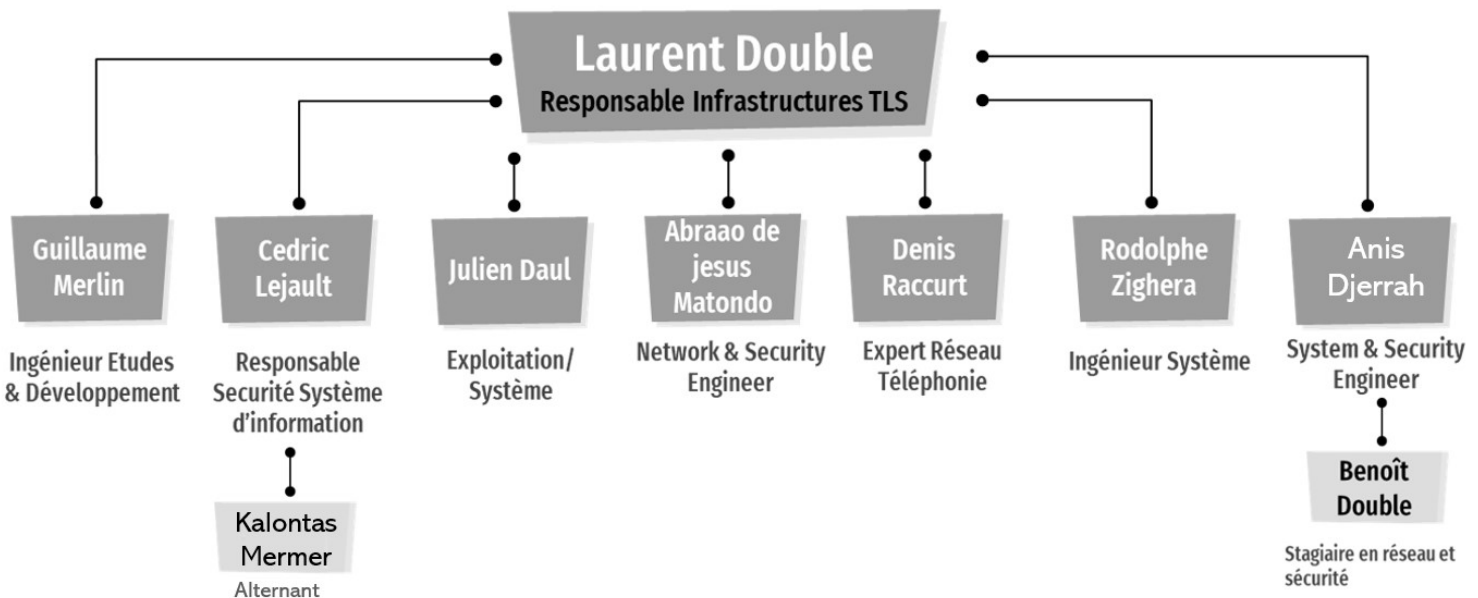
- **Systèmes de Surveillance** : La vidéosurveillance moderne repose sur des systèmes informatiques sophistiqués pour l'enregistrement, le stockage et l'analyse des images.
- **Contrôle d'Accès** : Les systèmes de contrôle d'accès utilisent des bases de données et des logiciels pour gérer les autorisations et surveiller les entrées et sorties.
- **Alarmes et Détection d'Incendie** : Ces systèmes sont intégrés à des réseaux informatiques pour une surveillance en temps réel et une réponse rapide aux incidents.

- **Gestion des Données** : L'entreprise doit gérer de grandes quantités de données sensibles, nécessitant des systèmes informatiques robustes et sécurisés.
- **Outils de Gestion** : Les opérations, les ressources humaines, les finances et la gestion des projets utilisent divers logiciels de gestion et de planification.

**Peut-elle travailler sans informatique ?** : Il est presque impossible pour Securitas Technology France de fonctionner sans informatique. Les systèmes de sécurité modernes dépendent largement de la technologie informatique pour être efficaces et réactifs. L'informatique permet l'automatisation, la surveillance en temps réel, l'analyse des données, et la gestion des incidents, ce qui est essentiel pour assurer une sécurité optimale pour leurs clients.

## C. L'EQUIPE

L'équipe à laquelle j'appartiens est divisé entre deux sites, Caluire et Francheville supervisé par Mr Laurent DOUBLE. J'ai donc tout au long de mon stage beaucoup appris aux côtés de l'équipe de Francheville, tout particulièrement mon maitre de stage Anis Djerrah (Organigramme de l'équipe de Francheville ci-dessous).



# Les projets

## IPAM

### Introduction à IPAM

Dans le cadre de mon stage, j'ai eu l'opportunité de travailler sur la gestion des adresses IP, un aspect crucial des infrastructures réseau modernes. Plus précisément, j'ai utilisé et paramétré un système de gestion des adresses IP, couramment appelé IPAM (IP Address Management).

L'IPAM est une solution logicielle qui permet de planifier, de suivre et de gérer l'espace d'adressage IP d'un réseau. Elle offre une vue centralisée sur l'allocation des adresses IP, facilitant ainsi la gestion des sous-réseaux et des plages d'adresses. Cette gestion est essentielle pour éviter les conflits d'adresses IP, optimiser l'utilisation des ressources réseau et garantir la sécurité et la performance des infrastructures IT.

### Contexte et Importance de l'IPAM

Dans les environnements réseau modernes, où les entreprises dépendent de plus en plus de technologies connectées, la gestion des adresses IP devient un défi de taille. Les dispositifs IoT, les machines virtuelles, les appareils mobiles et autres augmentent la complexité du réseau et la quantité d'adresses IP à gérer. Un outil IPAM aide à automatiser de nombreuses tâches associées à la gestion des adresses IP, réduisant ainsi les erreurs humaines et augmentant l'efficacité opérationnelle.

Avant la mise en place de IPAM, les IP étaient stockées dans de grands fichiers Excel, réparties en sous-réseaux et en sites.

### Objectifs et Bénéfices de l'Utilisation de l'IPAM

En intégrant et paramétrant un système IPAM, les objectifs principaux étaient :

- **Centralisation de la Gestion des Adresses IP** : Fournir une plateforme unique pour visualiser et administrer les adresses IP.
- **Optimisation de l'Utilisation des Adresses IP** : Assurer une allocation efficace et éviter les gaspillages ou les conflits.
- **Sécurité** : Améliorer la sécurité du réseau en détectant et en prévenant les accès non autorisés.
- **Automatisation des Tâches Répétitives** : Réduire le temps consacré à la gestion manuelle et minimiser les erreurs humaines.

## La Mission

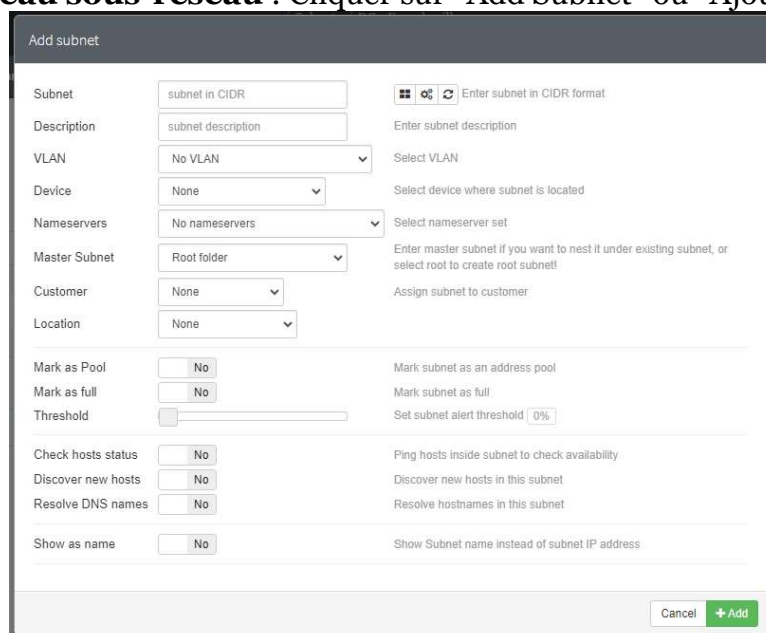
Le service It-Monitoring de Securitas est divisé en sept sites, le périmètre concerné par le projet est de quatre sites : Francheville, Ivry sur Seine, Bar-le-Duc et Vitrolles. La mise en place de IPAM m'a été attribué ainsi qu'à l'alternant Kalontas Mermer.

J'ai donc eu à m'occuper des sites de Francheville et de Bar-le-Duc. De plus par la suite j'ai eu à configurer du NAT sur IPAM et des circuits pour les opérateurs. J'ai fini ce projet en réalisant la documentation et en officialisant la transition.

## Ajout des Sous-Réseaux et des VLANs

Pour chaque site, des sous-réseaux et des VLANs ont été ajoutés simultanément dans l'interface IPAM. Les informations nécessaires étaient extraites de fichiers Excel fournis. Voici le processus détaillé :

1. **Accéder à l'interface IPAM** : Se connecter à l'interface web du logiciel IPAM.
2. **Naviguer vers la section des sous-réseaux** : Cliquer sur l'onglet ou le menu dédié à la gestion des sous-réseaux.
3. **Ajouter un nouveau sous-réseau** : Cliquer sur "Add Subnet" ou "Ajouter un sous-réseau".



The screenshot shows the 'Add subnet' form with the following fields and options:

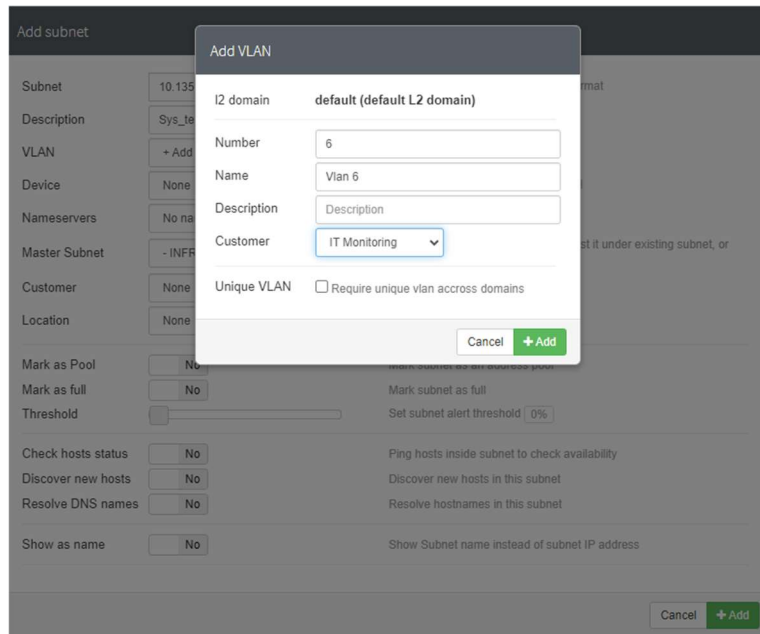
- Subnet: Input field with placeholder 'subnet in CIDR' and a help icon.
- Description: Input field with placeholder 'subnet description'.
- VLAN: Dropdown menu with 'No VLAN' selected.
- Device: Dropdown menu with 'None' selected.
- Nameservers: Dropdown menu with 'No nameservers' selected.
- Master Subnet: Dropdown menu with 'Root folder' selected.
- Customer: Dropdown menu with 'None' selected.
- Location: Dropdown menu with 'None' selected.
- Mark as Pool:  No
- Mark as full:  No
- Threshold: Slider set to 0%
- Check hosts status:  No
- Discover new hosts:  No
- Resolve DNS names:  No
- Show as name:  No

Buttons: Cancel, +Add

4. **Remplir les informations nécessaires** : Saisir l'adresse du sous-réseau, le masque de sous-réseau, et d'autres détails pertinents tels que la description ou les commentaires.



5. **Créer les VLANs associés** : Pendant l'ajout du sous-réseau, configurer les VLANs associés en utilisant les informations des fichiers Excel.



## Importation des Plages IP en CSV

Pour faciliter l'importation des plages IP, celles-ci ont été formatées en fichiers CSV. Cela a permis une intégration rapide et sans erreurs dans l'IPAM. Le processus d'importation était le suivant :

1. **Préparation des fichiers CSV** : Créer des fichiers CSV contenant les plages IP avec les colonnes nécessaires telles que l'adresse IP, le masque de sous-réseau, et les descriptions.
2. **Importation dans IPAM** : Utiliser la fonction d'importation de l'interface IPAM pour charger les fichiers CSV et créer automatiquement les entrées de plages IP.

## Configuration NAT

La configuration NAT (Network Address Translation) a été essentielle pour permettre la communication entre différents réseaux internes et externes. Voici comment cette configuration a été effectuée :

1. **Accéder à l'interface de configuration NAT** : Depuis l'interface IPAM, naviguer vers la section dédiée à la gestion NAT.
2. **Ajouter une nouvelle règle NAT** : Cliquer sur "Add NAT" ou "Ajouter une règle NAT".
3. **Configurer la règle NAT** : Saisir les informations telles que les adresses IP source et destination, les ports concernés, et le type de traduction (statique ou dynamique).



Name	Type	Translation	Device	Src Port	Dst Port	Description
FRC	Destination	None	FRC-	/	/	32000 TCP ; 3001 UDP ; ATS8550

# Mise à Jour Dynamique

Pour rendre les configurations plus dynamiques, une mise à jour régulière des plages IP et des règles NAT a été mise en place. Cela permet d'adapter rapidement les configurations aux besoins changeants du réseau :

1. **Surveiller les changements de réseau** : Utiliser des outils de monitoring pour détecter les changements dans l'utilisation des adresses IP et les besoins en NAT.
2. **Mettre à jour les configurations** : Importer régulièrement des fichiers CSV mis à jour ou utiliser les fonctionnalités de mise à jour automatique de l'IPAM pour maintenir une configuration actuelle et dynamique.

## Réalisation de la Documentation

Une documentation complète a été rédigée pour accompagner la mise en place du système IPAM. Cette documentation inclut les procédures d'installation, les configurations réalisées, ainsi que les bonnes pratiques pour la gestion future. (Première page en annexe page 18).

## Communication avec les Employés

Un mail a été envoyé aux employés pour les informer de la mise en production du nouveau système IPAM. Ce mail comprenait des instructions sur l'utilisation du système et les contacts pour le support.

Chers collègues,

Nous avons le plaisir de vous informer

que la mise en production de notre nouvelle solution de gestion des adresses IP (IPAM) :

Cette nouvelle solution IPAM permettra une gestion centralisée et optimisée de notre infrastructure réseau. Voici quelques points clés concernant cette mise en production :

1. **Amélioration de la Gestion des Adresses IP** :
  - o Allocation dynamique des adresses IP.
  - o Suivi en temps réel de l'utilisation des adresses IP.
  - o Réduction des conflits d'adresses IP et des erreurs de configuration.
2. **Sécurité et Conformité** :
  - o Renforcement des contrôles d'accès et de la gestion des autorisations.
  - o Conformité avec les normes et les meilleures pratiques en matière de sécurité réseau.

Nous vous remercions de votre coopération et de votre compréhension durant cette période de transition pour ne plus utiliser les fichiers Excel avec lesquelles vous êtes habitués.

Nous sommes convaincus que cette nouvelle solution apportera des bénéfices significatifs à notre organisation et améliorera notre efficacité opérationnelle.

N'hésitez pas à nous faire part de vos questions ou de vos préoccupations.

Merci à [@Benoit Double](#) et [@Kalontas Mermer](#) pour le travail effectué !

## Conclusion

La mise en place du système IPAM a été une étape importante pour améliorer la gestion des adresses IP chez Securitas. Ce projet a permis de centraliser les informations, d'optimiser l'utilisation des

ressources réseau et d'assurer une meilleure sécurité. La documentation détaillée et la communication avec les employés ont facilité la transition vers ce nouveau système.

# PENTEST

## Introduction

Dans le cadre de mon stage au sein du service IT-Monitoring de Securitas, j'ai été chargé de réaliser un test d'intrusion (pentest) pour évaluer la sécurité de l'infrastructure réseau de l'entreprise. Cette partie du rapport détaille les étapes suivies, les outils utilisés et les résultats obtenus lors de cette mission de pentest.

## 1. Préparation et Planification du Pentest

### 1.1. Formation et Recherche

Pour me familiariser avec les concepts et les techniques de pentest, j'ai suivi plusieurs vidéos pédagogiques et visité des sites spécialisés en sécurité informatique. Ces ressources m'ont permis de comprendre les différentes phases d'un pentest, les outils à utiliser et les meilleures pratiques en la matière.

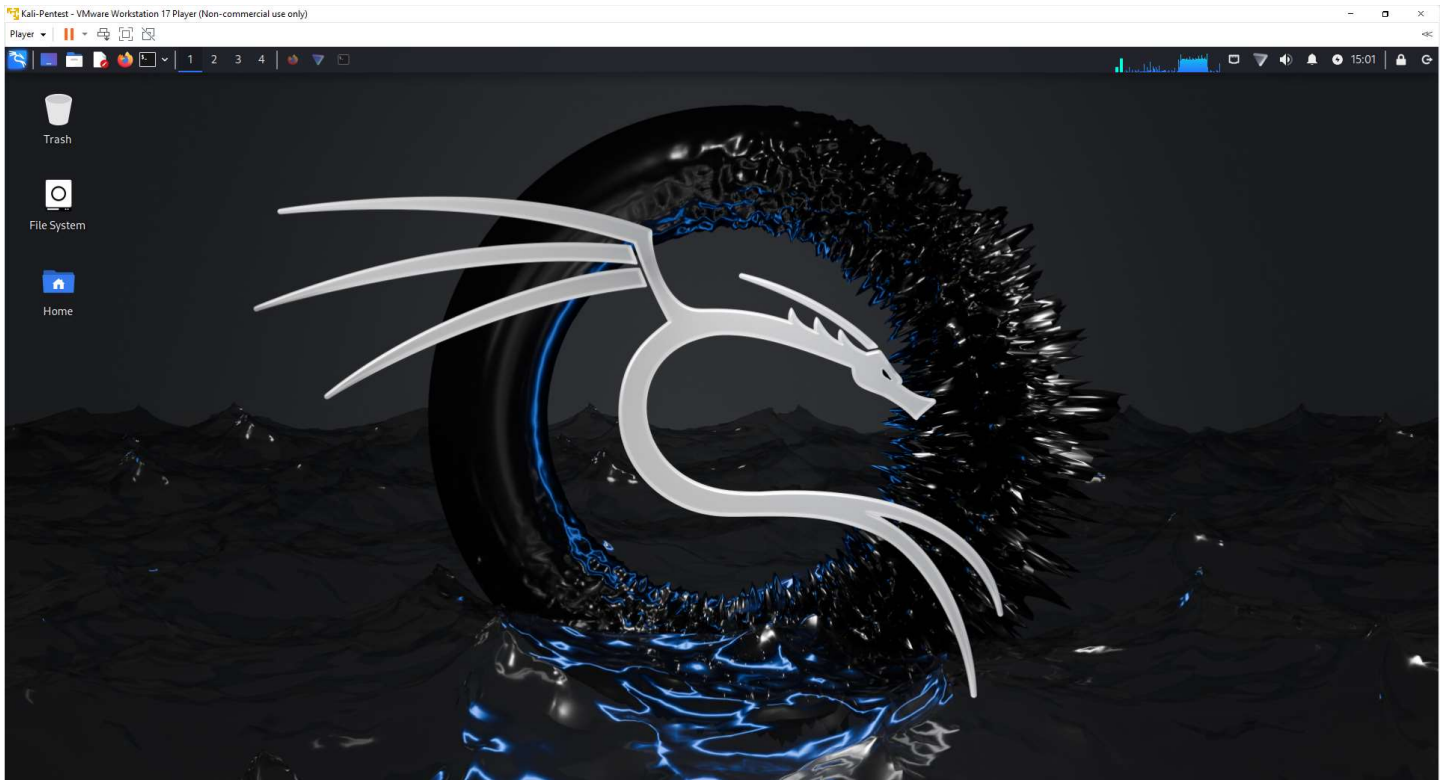
### 1.2. Rédaction du Contrat de Pentest

Avant de commencer le pentest, j'ai rédigé un contrat de pentest pour définir clairement le périmètre de l'opération, les règles à respecter et les adresses IP et FQDN (Fully Qualified Domain Name) concernés. Ce document a été essentiel pour obtenir l'approbation des parties prenantes et garantir que le pentest se déroule dans un cadre légal et éthique. (Disponible en annexe)

## 2. Mise en Place de l'Environnement de Pentest

### 2.1. Installation de Kali Linux

Pour réaliser le pentest, j'ai installé une machine virtuelle (VM) Kali Linux. Kali Linux est une distribution Linux spécialisée dans les tests de sécurité et le pentest, offrant une large gamme d'outils préinstallés.



## 2.2. Utilisation de Proton VPN

Afin de sécuriser ma connexion et de masquer mon adresse IP, j'ai installé et configuré Proton VPN sur la VM Kali Linux. Cela a permis de protéger mon identité et d'assurer que mes activités de pentest ne soient pas détectées et bloquées par des mesures de sécurité réseau.

## 2.3. Installation de Nessus

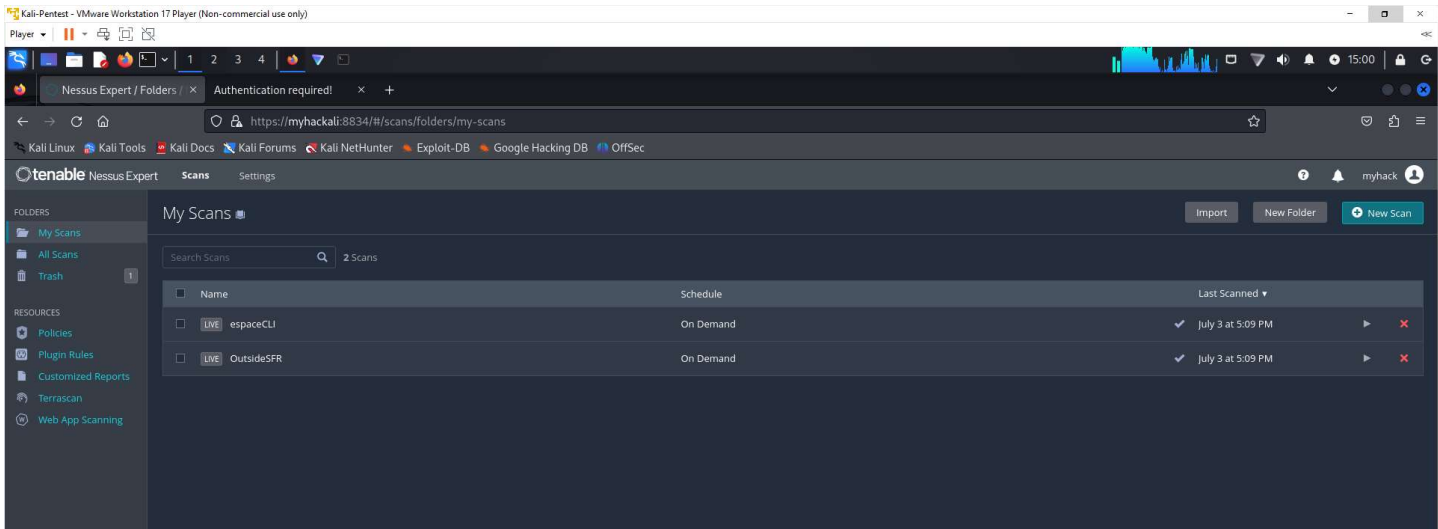
Pour effectuer des analyses de vulnérabilités, j'ai installé Nessus, un scanner de vulnérabilités puissant et polyvalent. Nessus permet de détecter une large gamme de failles de sécurité dans les systèmes informatiques.

# 3. Réalisation du Pentest

## 3.1. Utilisation de Nessus

Avec Nessus, j'ai réalisé des scans de vulnérabilités sur les systèmes identifiés lors des scans de sous-réseaux. Nessus a fourni des rapports détaillés sur les failles de sécurité détectées, classées par niveau de criticité (Annexes p 20).

1. Configuration des Scans : Définition des cibles, des types de scans et des politiques de scan.
2. Analyse des Résultats : Examen des vulnérabilités détectées et évaluation de leur impact potentiel sur la sécurité de l'infrastructure.



## 3.2. Recherches Google Dorks

En complément des scans techniques, j'ai effectué des recherches Google Dorks pour vérifier si des informations sensibles ou des failles de sécurité concernant Securitas Technology étaient disponibles en ligne. Les Google Dorks sont des requêtes avancées permettant de trouver des informations spécifiques sur les moteurs de recherche.

1. Utilisation de Requêtes Avancées : Formulation de requêtes spécifiques pour identifier des pages web potentiellement vulnérables ou des informations confidentielles exposées.
2. Analyse des Résultats : Vérification et documentation des résultats obtenus pour évaluer leur pertinence et leur impact sur la sécurité de l'entreprise.

## Conclusion

La réalisation du pentest pour Securitas a permis de mettre en évidence plusieurs points forts et vulnérabilités de l'infrastructure réseau. Les scans de sous-réseaux et les analyses de vulnérabilités effectuées avec Nessus ont fourni une vue détaillée des systèmes en place et des failles potentielles. Les recherches Google Dorks ont également permis d'identifier des informations sensibles accessibles en ligne. Ce projet a été une opportunité précieuse pour renforcer la sécurité de l'entreprise et améliorer ma compréhension des techniques de pentest.

# VEILLE CYBER

## Introduction

Au cours de mon stage au sein du service IT-Monitoring de Securitas, une de mes premières tâches a été de mettre en place un système de veille technologique. Cette mission avait pour objectif de suivre en temps réel les nouvelles vulnérabilités et menaces potentielles pouvant affecter les infrastructures de l'entreprise. Ce rapport détaille les outils utilisés, les processus mis en place, et les résultats obtenus.

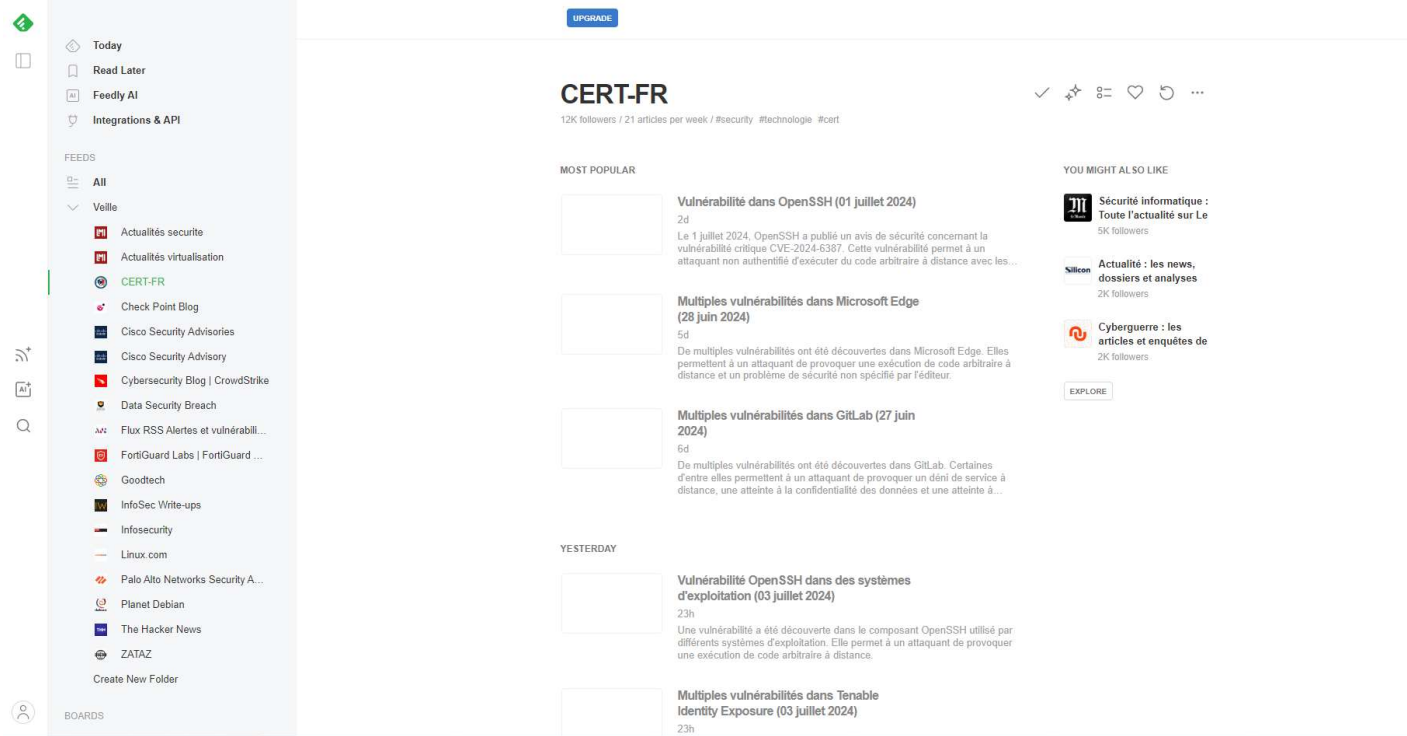


# 1. Mise en Place de la Veille Technologique

## 1.1. Création d'un Compte Feedly

Pour centraliser et organiser les informations pertinentes, j'ai créé un compte sur Feedly, une plateforme de curation de contenu. Feedly permet de suivre des flux RSS de différentes sources, ce qui facilite la collecte et la gestion des informations.

- **Abonnement à des Médias Pertinents :** J'ai sélectionné et suivi des médias spécialisés en sécurité informatique, tels que Threatpost, Dark Reading, et les blogs de fournisseurs de solutions de sécurité comme Cisco et Palo Alto Networks.
- **Organisation des Flux :** Les flux d'informations ont été organisés par catégories (vulnérabilités, mises à jour de sécurité, analyses techniques, etc.) pour une consultation plus efficace.



## 1.2. Surveillance Quotidienne

Chaque jour, je vérifiais les nouvelles publications sur Feedly pour détecter les vulnérabilités et les menaces récentes. Ce processus consistait en :

- **Identification des Vulnérabilités :** Lecture des articles et rapports pour repérer les nouvelles vulnérabilités signalées.
- **Vérification des CVE :** Les CVE (Common Vulnerabilities and Exposures) sont des identifiants uniques attribués aux vulnérabilités de sécurité. Je vérifiais les CVE pour obtenir des détails

techniques et des évaluations de criticité.

# Vulnérabilité dans OpenSSH (01 juillet 2024)

CERT-FR / Jul 1, 2024 at 5:23 PM // keep unread // hide



**Feedly detected 1 CVE.** Automatically tag, enrich, and export CVEs, Threat Actors, Malware Families, TTPs, and IoCs

[LEARN MORE](#)

Le 1 juillet 2024, OpenSSH a publié un avis de sécurité concernant la vulnérabilité critique CVE-2024-6387 ☒. Cette vulnérabilité permet à un attaquant non authentifié d'exécuter du code arbitraire à distance avec les privilèges `*root*`. L'éditeur précise que les versions 8.5p1 à 9.7p1 sont...

[VISIT WEBSITE](#)

## 1.3. Vérification de l'Impact sur l'Infrastructure

Une fois les vulnérabilités identifiées, il était crucial de déterminer si elles affectaient les systèmes en place chez Securitas. Pour cela, j'utilisais deux outils principaux dont j'ai installé les agents (annexes p 19) :

### 1.3.1. OCS Inventory

OCS Inventory (Open Computer and Software Inventory) est un outil de gestion d'inventaire qui permet de recenser les équipements matériels et logiciels présents sur le réseau.

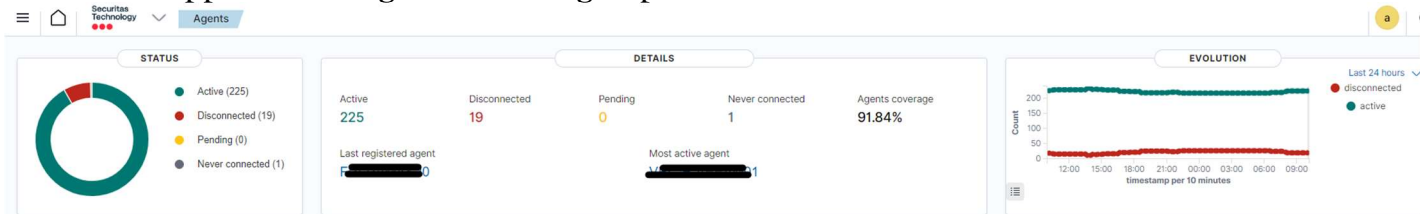
- Consultation de l'Inventaire : J'utilisais OCS Inventory pour vérifier si le hardware ou le software mentionné dans les rapports de vulnérabilités était présent dans notre infrastructure.
- Évaluation de l'Exposition : Basé sur les résultats de l'inventaire, j'évaluais l'exposition de notre infrastructure aux nouvelles vulnérabilités.

### 1.3.2. Wazuh

Wazuh est un outil SIEM (une solution de sécurité qui permet aux organisations de détecter les menaces avant qu'elles ne perturbent leurs activités).

- Installation des Agents : J'ai installé les agents Wazuh sur les machines pour collecter et analyser les données de sécurité.
- Surveillance Continue : Wazuh permettait de surveiller en continu les événements de sécurité et de détecter les comportements anormaux ou les indicateurs de compromission.

- **Alertes et Rapports : Configuration de règles pour**



- générer des alertes en cas de détection de vulnérabilités ou d'incidents de sécurité.

## 2. Processus de Veille et Réponse aux Vulnérabilités

### 2.1. Identification des Vulnérabilités

Chaque jour, après avoir parcouru les flux Feedly, je compilais une liste des nouvelles vulnérabilités découvertes. Les vulnérabilités critiques et celles potentiellement exploitables étaient notées en priorité.

### 2.2. Vérification de l'Impact

Pour chaque vulnérabilité identifiée, je procédais comme suit :

- Recherche dans OCS Inventory : Vérification de la présence des logiciels ou matériels vulnérables.
- Analyse avec Wazuh : Utilisation de Wazuh pour détecter toute activité suspecte ou indicateurs de compromission liés à la vulnérabilité.

### 2.3. Actions Correctives

Si une vulnérabilité affectait l'infrastructure de Securitas, des actions correctives étaient planifiées :

- Mises à Jour et Correctifs : Application des correctifs de sécurité fournis par les éditeurs de logiciels ou les fabricants de matériel.
- Configurations de Sécurité : Modification des configurations de sécurité pour atténuer les risques.
- Alertes et Notifications : Communication avec les équipes concernées pour les informer des vulnérabilités et des mesures prises.

## Conclusion

Le travail de veille technologique a été une composante essentielle de mon stage, permettant d'assurer la sécurité continue des infrastructures de Securitas. Grâce à l'utilisation de Feedly, OCS Inventory et Wazuh, j'ai pu identifier rapidement les vulnérabilités, évaluer leur impact et prendre les mesures nécessaires pour les corriger. Cette expérience m'a permis de développer des compétences précieuses en matière de surveillance de la sécurité et de réponse aux incidents.

# Conclusion

Mon stage chez Securitas Technology a été une expérience enrichissante qui m'a permis d'approfondir mes connaissances en gestion de réseaux et en cybersécurité. J'ai eu l'opportunité de travailler sur des projets variés et concrets, notamment la mise en place d'un système de gestion des adresses IP (IPAM), la réalisation d'un test d'intrusion (pentest), et la mise en place d'une veille technologique efficace.

Le projet IPAM m'a permis de comprendre l'importance d'une gestion centralisée et automatisée des adresses IP pour éviter les conflits, optimiser les ressources réseau, et améliorer la sécurité. J'ai contribué à la configuration des sous-réseaux, à l'importation des plages IP, et à la documentation du processus, facilitant ainsi une transition en douceur pour les employés.

La réalisation du pentest a été une expérience particulièrement formatrice, me donnant l'occasion de mettre en pratique des techniques de sécurité avancées. J'ai appris à utiliser des outils comme Nessus et Kali Linux, et à effectuer des recherches ciblées pour identifier des vulnérabilités. Les résultats obtenus ont mis en lumière des points forts et des faiblesses de l'infrastructure réseau de Securitas, offrant ainsi des pistes d'amélioration pour renforcer la sécurité.

Enfin, la mise en place de la veille technologique m'a permis de développer une méthodologie rigoureuse pour suivre et répondre aux nouvelles menaces de sécurité. En utilisant des outils comme Feedly, OCS Inventory, et Wazuh, j'ai pu identifier rapidement les vulnérabilités, évaluer leur impact sur notre infrastructure, et prendre les mesures correctives nécessaires.

Je remercie sincèrement toute l'équipe de Securitas Technology, et particulièrement mon maître de stage, Anis Djerrah, pour leur encadrement et leur soutien tout au long de ce stage. Cette expérience m'a non seulement permis d'acquérir des compétences techniques précieuses mais aussi de me familiariser avec le milieu professionnel, préparant ainsi au mieux mon avenir dans le domaine de l'informatique et de la cybersécurité.

# Annexes





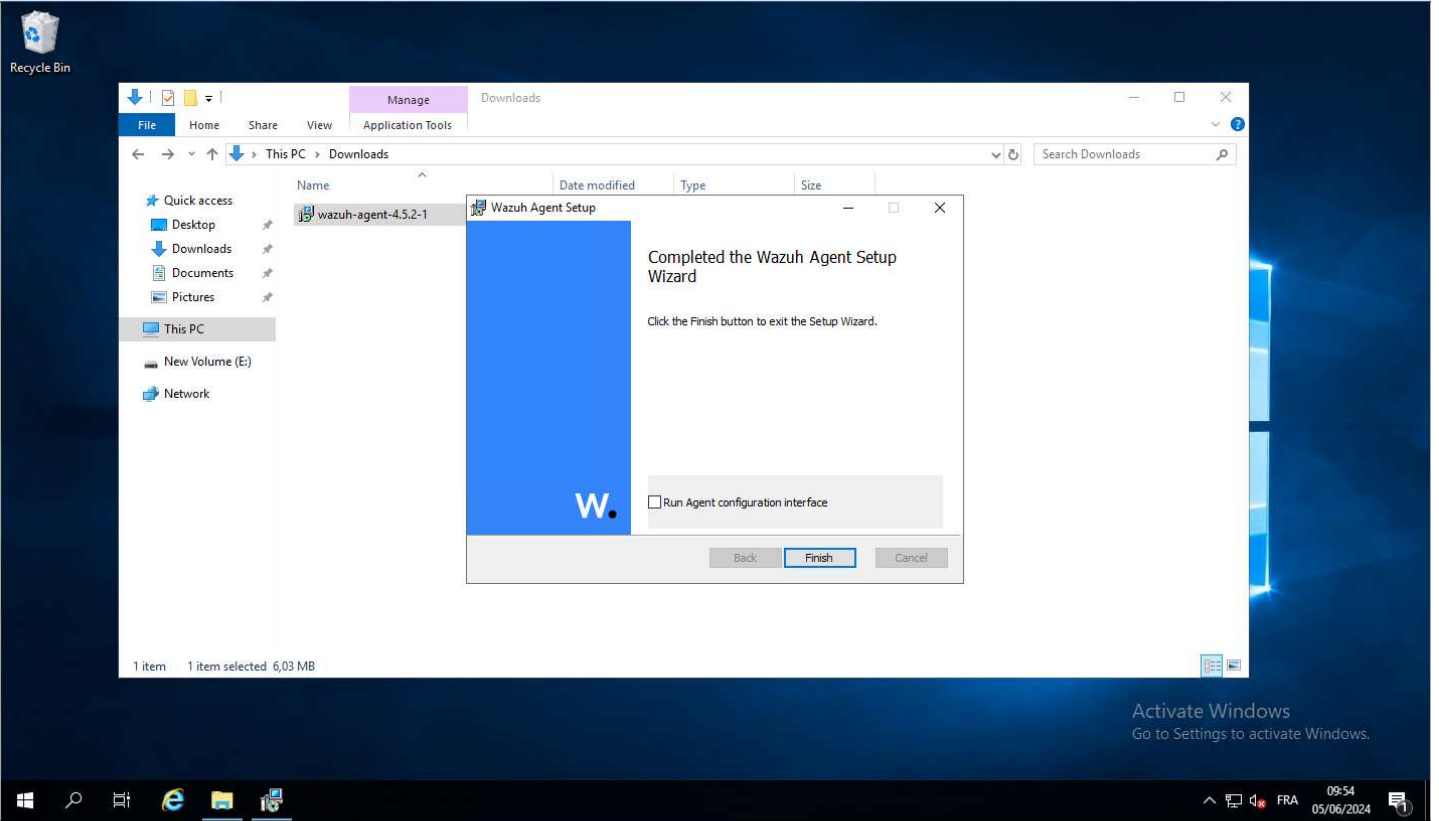
# IT-Monitoring-IPAM

## Recherche d'IP libre, Paramétrage IP, S-R, Vlan

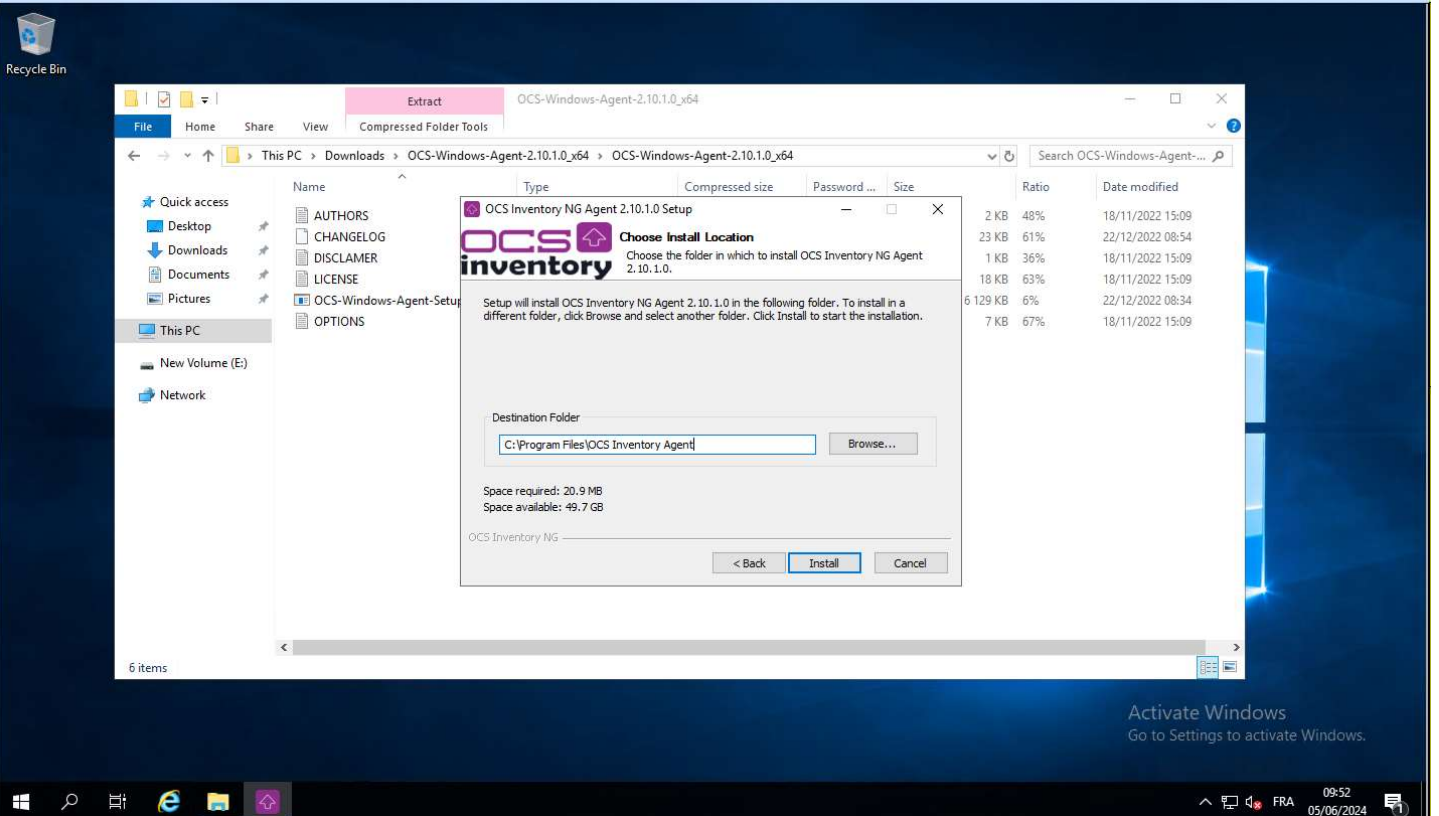
### Procédure

Etapes	Nom & Fonction	Date	Visa
Préparation	Benoît DOUBLE	11/06/2024	✓
Vérification			
Validation			

Référence	XXXX
Version	1.0
Etat	Non validé
Confidentialité	Confidentiel
Date de la dernière mise à jour	11/06/2024
Nombre de pages	10



Activate Windows  
Go to Settings to activate Windows.



Activate Windows  
Go to Settings to activate Windows.

Kali-Pentest - VMware Workstation 17 Player (Non-commercial use only)

Player | 1 2 3 4 | 10:96.0.48 | 9:37

https://myhackkali:8834/#scans/folders/my-scans

Kali Linux | Kali Tools | Kali Docs | Kali Forums | Kali NetHunter | Exploit-DB | Google Hacking DB | OffSec

tenable Nessus Expert Scans Settings myhack

FOLDERS: My Scans, All Scans, Trash

RESOURCES: Policies, Plugin Rules, Customized Reports, Terrascan, Web App Scanning

My Scans

Plugins are done compiling.

This folder is empty. Create a new scan.

**Welcome to Nessus Expert**

To get started, launch a host discovery scan to identify what hosts on your network are available to scan. Hosts that are discovered through a discovery scan do not count towards the 32 host limit on your license.

Enter targets as hostnames, IPv4 addresses, or IPv6 addresses. For IP addresses, you can use CIDR notation (e.g., 192.168.0.0/24), a range (e.g., 192.168.0.1-192.168.0.255), or a comma-separated list (e.g., 192.168.0.0, 192.168.0.1).

**Targets**

Example: 192.168.1.1-192.168.1.5, 192.168.2.0/24, test.com

Close Submit

09:37 03/07/2024

Kali-Pentest - VMware Workstation 17 Player (Non-commercial use only)

Player | 1 2 3 4 | 10:07 | 10:07

https://myhackkali:8834/#scans/reports/19/history

Kali Linux | Kali Tools | Kali Docs | Kali Forums | Kali NetHunter | Exploit-DB | Google Hacking DB | OffSec

tenable Nessus Expert Scans Settings myhack

FOLDERS: My Scans, All Scans, Trash

RESOURCES: Policies, Plugin Rules, Customized Reports, Terrascan, Web App Scanning

espaceCLI

Back to My Scans

Hosts 3 | Vulnerabilities 1 | History 1

Search History 1 History

Start Time	Last Scanned	Status
Current Today at 10:04 AM	N/A	Running

Scan Details

Policy: Basic Network Scan  
 Status: Running  
 Severity Base: CVSS v3.0  
 Scanner: Local Scanner  
 Start: Today at 10:04 AM

Vulnerabilities

- Critical
- High
- Medium
- Low
- Info

10:07 03/07/2024