DUMAS Mathieu
MILLOT Elisa

Rapport technique SAE5.CYBER.03:

SOMMAIRE:

1. Présentation du sujet et cadre de la SAE

La SAE5.Cyber.03 s'inscrit dans la continuité de la formation du BUT Réseaux et Télécommunications, parcours cybersécurité. Elle a pour objectif principal de mettre en œuvre, dans un cadre pratique et réaliste, les notions liées à la sécurisation et à la supervision avancées d'un système d'information. Cette SAE se situe clairement dans le domaine de la lutte informatique défensive et vise à faire comprendre le rôle des équipes chargées de la détection, de l'analyse et du suivi des attaques informatiques.

Le travail demandé ne se limite pas à la mise en place d'une infrastructure fonctionnelle. Il s'agit également d'intégrer volontairement des failles de sécurité, de concevoir des scénarios d'attaque crédibles et de démontrer la capacité à détecter ces attaques à l'aide d'outils de supervision et de surveillance. L'approche retenue est progressive et réaliste, allant de la phase de reconnaissance externe jusqu'à la compromission de services internes critiques.

Cette SAE permet ainsi de se rapprocher du fonctionnement réel d'un échelon tactique de cyberdéfense, composé d'un SOC et d'un CERT. Les étudiants sont amenés à adopter une vision globale de la sécurité, en tenant compte à la fois des aspects réseaux, systèmes, applicatifs et organisationnels.

2. Objectifs pédagogiques et compétences mobilisées

L'un des objectifs majeurs de cette SAE est de comprendre qu'une attaque informatique réussie repose rarement sur une seule vulnérabilité critique, mais plutôt sur l'enchaînement de plusieurs failles techniques et humaines. À travers ce projet, il s'agissait de concevoir une infrastructure conforme à un cahier des charges précis, d'y déployer des services courants, puis d'analyser les conséquences de choix de configuration volontairement imparfaits.

Les compétences mobilisées couvrent à la fois la conception d'architectures réseaux sécurisées, l'administration de **systèmes Linux**, la mise en place de services réseaux et la supervision de l'ensemble du système d'information. Une attention particulière a également été portée à la capacité à documenter précisément les actions réalisées, les vulnérabilités exploitées et les preuves de compromission obtenues.

Cette SAE vise également à développer une posture professionnelle proche de celle attendue dans les métiers de la cybersécurité. Il ne s'agit pas uniquement de réussir une attaque, mais d'être capable de l'expliquer, de la justifier techniquement et de proposer des mesures correctives adaptées à un contexte d'entreprise.

3. Attentes techniques et contraintes imposées

Le cahier des charges de la SAE impose plusieurs contraintes fortes afin de garantir un cadre homogène pour l'ensemble des groupes. **L'infrastructure devait être conçue autour de systèmes d'exploitation Linux, l'utilisation de Windows étant interdite**. Cette contrainte vise à renforcer la maîtrise des environnements Linux, très présents dans les infrastructures professionnelles.

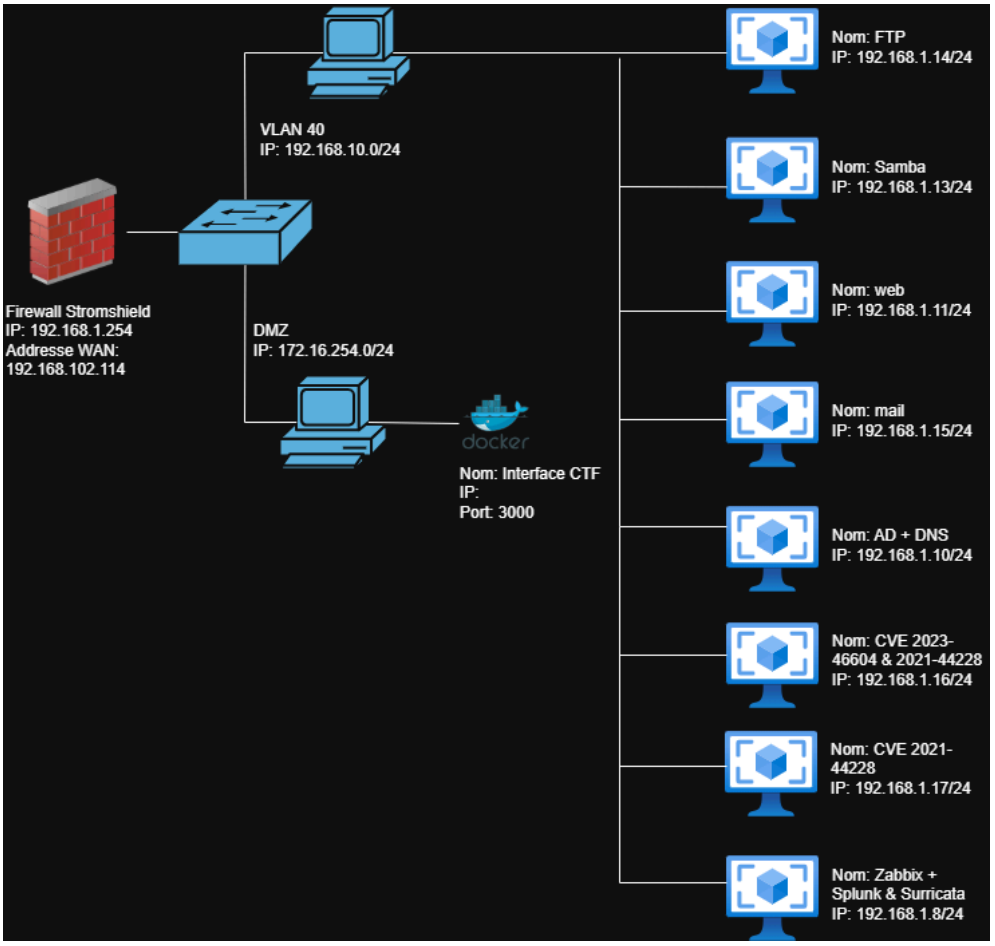
La topologie réseau devait intégrer a minima un pare-feu, une zone **DMZ**, un réseau local pour les utilisateurs, un réseau dédié à l'administration et un accès VPN permettant le télétravail. Les services obligatoires incluaient notamment un annuaire d'authentification, un serveur DNS, un serveur Web et un service de partage de fichiers. L'utilisation de solutions de virtualisation et de conteneurisation était également imposée afin de se rapprocher des pratiques actuelles.

Enfin, la SAE exigeait la mise en place d'outils de supervision et de surveillance capables de détecter les attaques en cours et de produire des alertes exploitables. Les traces et journaux collectés devaient être conservés afin de servir de base pour la SAE6.Cyber.04, orientée vers la réponse à incident et l'analyse forensic.

4. Topologie et choix d'architecture réseau

La conception de l'architecture réseau constitue une étape fondamentale de la SAE5.Cyber.03, car elle conditionne à la fois la sécurité du système d'information et la cohérence des scénarios d'attaque et de défense mis en œuvre. **L'objectif n'était pas uniquement de rendre l'infrastructure fonctionnelle, mais de concevoir une architecture réaliste**, proche de ce que l'on pourrait retrouver dans une entreprise de taille moyenne disposant de services internes et exposés.

L'ensemble de l'infrastructure repose sur des machines virtuelles utilisant Ubuntu Server 22.04.7 LTS, déployées à partir de l'ISO officiel. Les interfaces réseau des machines virtuelles sont configurées en mode bridge, ce qui permet une intégration directe dans le réseau physique de l'IUT. Ce choix facilite l'accès aux services, l'observation du trafic réel et l'interaction avec les équipements physiques, tout en restant dans un environnement de test contrôlé.



Légende: Topologie du réseau.

4.1 Segmentation réseau et **VLAN**

L'architecture retenue repose sur une segmentation logique du réseau à l'aide de **VLAN**, afin de séparer les usages et de limiter les déplacements latéraux en cas de compromission. Deux **VLAN** principaux ont été définis :

- un **VLAN** dédié aux **utilisateurs**,
- un **VLAN** réservé à **l'administration** et aux **serveurs**.

Cette séparation permet de restreindre l'accès aux ressources sensibles et d'observer l'impact d'une attaque sur un segment précis du réseau. Un troisième **VLAN** inutilisé est également présent afin d'isoler les ports non employés et de réduire la surface d'attaque au niveau de la couche 2.
Le routage inter-VLAN n'est pas assuré par le switch mais par le pare-feu, ce qui permet de centraliser le contrôle des flux et d'appliquer des règles de filtrage cohérentes entre les différentes zones du réseau.

4.2 Rôle du pare-feu **Stormshield**

Le **pare-feu Stormshield** constitue l'élément central de l'architecture. Il assure à la fois la sécurité périmétrique et le contrôle des communications internes. Plusieurs interfaces ont été configurées afin de représenter une architecture réaliste
:

- une interface WAN, disposant de l'adresse IP **192.168.102.114**, connectée au réseau de l'IUT ;
- une interface associée au LAN utilisateurs (**VLAN** 20) avec l'adresse **192.168.1.254** ;
- une interface dédiée à l'administration et aux serveurs (**VLAN** 40) avec l'adresse **192.168.10.254** ;
- une interface **DMZ**, configurée avec l'adresse **172.16.254.254**, destinée à héberger les services exposés.

Ce découpage permet d'appliquer des politiques de filtrage distinctes selon les zones, tout en conservant certaines règles volontairement permissives dans un objectif pédagogique. **Le**

filtrage principal autorise les flux LAN vers WAN, tandis que le filtrage inter-VLAN reste limité afin de démontrer les risques liés à un cloisonnement insuffisant.

4.3 **DMZ** et **NAT**

La **DMZ** a été mise en place afin d'isoler les services exposés du reste du système d'information. Les flux entre la **DMZ** et les réseaux internes sont strictement contrôlés par le pare-feu, ce qui permet d'illustrer concrètement l'importance de cette zone dans la réduction de l'impact d'une compromission.

Le **NAT** est appliqué uniquement sur la **DMZ**, afin d'exposer certains services tout en masquant l'adressage interne. Aucun **NAT** n'est appliqué directement sur les réseaux internes, ce qui correspond à une configuration classique en entreprise et permet de mieux observer les flux lors des attaques.

4.4 Switch et sécurité de niveau 2

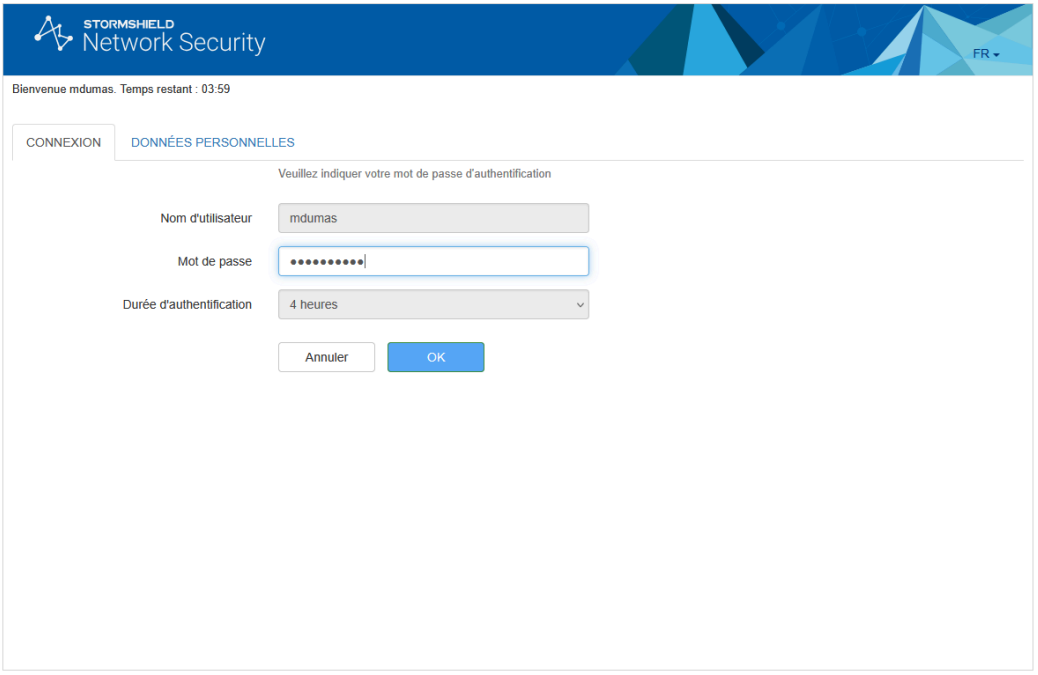
Le switch manageable constitue le point de concentration du réseau local. Il permet la mise en œuvre de la segmentation par **VLAN** et l'application de mécanismes de sécurité de niveau 2. Les ports utilisés sont configurés en mode access et associés à leur **VLAN** respectif, tandis que les ports inutilisés sont placés dans un **VLAN** dédié et administrativement désactivés.

Des mécanismes tels que le port-security, la limitation du nombre d'adresses MAC par port, l'activation du BPDU Guard et du PortFast ont été mis en place afin de limiter les risques liés aux connexions non autorisées et aux attaques de type boucle ou spoofing. L'administration du switch est restreinte à un réseau spécifique et accessible uniquement via SSH.

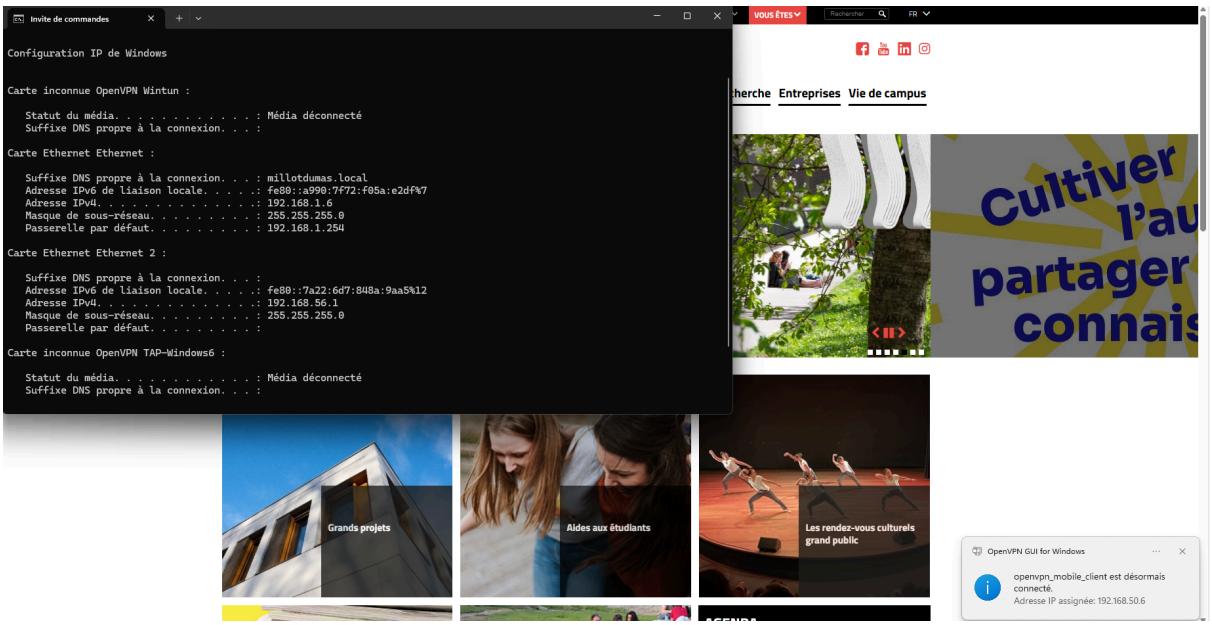
4.5 Accès VPN SSL

Un accès **VPN SSL** a été configuré sur le pare-feu afin de représenter un cas d'usage courant en entreprise, à savoir le télétravail. L'accès se fait via l'interface web du pare-feu à l'adresse https://192.168.102.114/auth, en utilisant les identifiants mdumas / Test1234./. Une fois authentifié, l'utilisateur peut récupérer la configuration **VPN** et établir un tunnel lui donnant accès au réseau interne.

La configuration du VPN reste volontairement basique, avec un seul utilisateur et des droits étendus permettant l'accès au LAN. Ce choix permet d'illustrer les risques liés à une gestion trop permissive des accès distants et met en évidence l'importance du principe du moindre privilège.



Légende: Connexion à un compte VPN de l'entreprise



Légende: Connexion réussit au VPN de l'entreprise.

4.6 Interface CTF et conteneurisation

Dans le cadre de la SAE, un conteneur **Docker** a été utilisé pour héberger l'interface CTF. Ce conteneur est exécuté sur la machine hôte et expose le service sur le port **3000**. Une règle de redirection a été configurée sur le pare-feu afin que tout flux entrant sur le port **3000** du pare-feu soit redirigé vers l'interface réseau de la machine hébergeant le conteneur **Docker**, également sur le port **3000**.

Cette mise en œuvre permet de combiner virtualisation, conteneurisation et filtrage réseau, tout en conservant une architecture simple et lisible.

4.7 Accès Internet et adresse réservée

Enfin, une adresse IP réservée a été attribuée au pare-feu (192.168.102.114/21), permettant un accès direct à Internet sans passer par le portail captif de l'IUT. Ce choix simplifie les mises à jour système, l'installation des outils de supervision et l'accès aux ressources nécessaires au projet, tout en restant conforme au périmètre autorisé.

5. Présentation des services mis en place

Dans le cadre de cette SAE, l'infrastructure ne se limite pas à la mise en place de services applicatifs isolés. Une attention particulière a également été portée aux équipements réseaux et de sécurité, afin de reproduire une architecture d'entreprise cohérente, fonctionnelle et exploitable dans un contexte de cyberdéfense. L'ensemble repose sur une combinaison de services systèmes, d'équipements d'interconnexion et de dispositifs de sécurité périmétrique, tous intégrés dans une logique de segmentation et de supervision.

Le service Web constitue l'un des premiers points d'entrée du système d'information et joue un rôle central dans la phase initiale de reconnaissance et d'exploitation. Il est hébergé sur un serveur Linux disposant de l'adresse IP 192.168.1.11/24 et repose sur un serveur **Apache HTTP** configuré de manière classique, conformément aux méthodes vues en cours. Le site est accessible depuis le réseau utilisateur et simule un portail interne d'entreprise.

Les pages du site sont développées en PHP, ce qui permet l'exécution de scripts côté serveur sans recourir à des fichiers externes complexes. Ce choix facilite l'introduction volontaire de vulnérabilités applicatives telles que des injections SQL, des failles de type path traversal et l'exposition de fichiers sensibles, notamment des sauvegardes de bases de données accessibles via des répertoires mal protégés. Ces failles illustrent les risques liés à l'absence de validation des entrées utilisateur, à une mauvaise gestion des droits sur le système de fichiers et à un cloisonnement insuffisant entre les composants applicatifs.

Le service **FTP** a été déployé afin de simuler un espace d'échange de fichiers internes utilisé par les collaborateurs. Il permet le dépôt et la récupération de documents professionnels, mais repose sur une configuration volontairement permissive. En particulier, certaines commandes avancées du protocole **FTP** sont laissées actives, notamment les commandes **SITE CPFR** et **SITE CPTO**. Cette mauvaise configuration permet à un utilisateur authentifié de copier des fichiers depuis n'importe quel emplacement du serveur vers un autre, à condition de connaître le chemin exact du fichier ciblé.

Cette faille rend possible la récupération de fichiers de configuration sensibles et facilite l'accès à des données critiques. Elle permet également, de manière indirecte, de compromettre des comptes à privilèges élevés, notamment en exploitant des fichiers liés aux sessions ou aux utilisateurs critiques, tels que la session du compte patron. Le service FTP devient ainsi un pivot important dans la progression de l'attaque.

Le service de partage de fichiers **Samba** assure la mise à disposition de ressources communes au sein de l'entreprise. Il repose sur un partage basique, volontairement peu cloisonné, afin de respecter le cahier des charges tout en illustrant l'impact d'un enchaînement de mauvaises pratiques. L'utilisation d'une version vulnérable du service, combinée à des droits d'accès trop permissifs, démontre qu'un simple accès authentifié peut conduire à des conséquences graves, notamment la récupération d'informations sensibles et la compromission d'autres comptes internes.

Un service de messagerie interne a également été mis en place afin de reproduire un environnement de travail réaliste. Accessible via le protocole IMAP, il permet aux utilisateurs de consulter leurs courriels professionnels à l'aide d'un client de messagerie configuré manuellement. Ce service illustre le facteur humain comme élément central de la sécurité du système d'information. Des informations sensibles y sont volontairement présentes, telles que des identifiants Active Directory transmis par erreur ou des échanges internes révélant des détails organisationnels. L'exploitation de ce service démontre l'importance de la sensibilisation des utilisateurs et des politiques de sécurité associées aux échanges électroniques.

L'annuaire Active Directory constitue le cœur du système d'information. Il centralise la gestion des comptes utilisateurs, des groupes et des autorisations d'accès aux ressources internes. L'objectif final de la chaîne d'attaque est d'atteindre cet annuaire, ce qui permet de démontrer qu'une compromission progressive, reposant sur des failles multiples et des mauvaises pratiques, peut mener à un contrôle quasi total du système d'information. La récupération d'identifiants via les **services Web**, **FTP**, **Samba** ou **Mail** permet d'illustrer les risques liés à la réutilisation des mots de passe et à l'absence de segmentation stricte des privilèges.

En complément des services applicatifs, un switch manageable a été mis en place afin d'assurer la segmentation du réseau interne. Celui-ci repose sur l'utilisation de **VLAN** distincts pour séparer les utilisateurs, l'administration et les serveurs. Cette segmentation permet de limiter la propagation des attaques et d'améliorer la lisibilité des flux réseau. Des mécanismes de sécurité de niveau 2 ont été configurés, tels que le port-security, la limitation du nombre d'adresses MAC par port, la désactivation des ports inutilisés et la protection contre les attaques de type BPDU. L'administration du switch est restreinte au réseau d'administration et sécurisée via le protocole SSH.

Le **pare-feu Stormshield** joue enfin un rôle central dans la protection périmétrique et interne du système d'information. Il assure le filtrage des flux entre les différents **VLAN**, le contrôle des accès vers Internet et l'exposition limitée de certains services en zone **DMZ**. Plusieurs interfaces ont été configurées afin de refléter une architecture d'entreprise réaliste, incluant une interface WAN, une interface dédiée aux utilisateurs, une interface réservée à l'administration et aux serveurs, ainsi qu'une interface **DMZ**. Les règles de filtrage ont été définies de manière volontairement minimaliste et partiellement permissive, afin de permettre la progression du scénario d'attaque et de mettre en évidence les risques liés à un cloisonnement insuffisant.

Le pare-feu assure également la mise en place d'un **VPN SSL**, permettant à un utilisateur distant de se connecter au réseau interne. Dans le cadre pédagogique de la SAE, les droits associés à ce **VPN** sont volontairement étendus, offrant un accès direct au LAN. Cette configuration permet d'illustrer concrètement les dangers d'une mauvaise gestion des accès distants et souligne l'importance du principe du moindre privilège dans un contexte réel.

6. Mise en place volontaire des vulnérabilités

Dans le cadre de cette SAE, **les vulnérabilités présentes sur les différents services n'ont pas été découvertes de manière accidentelle, mais intégrées volontairement** afin de construire une chaîne d'attaque cohérente, progressive et réaliste. L'objectif pédagogique était de démontrer qu'une compromission globale d'un système d'information repose rarement sur une faille unique, mais plutôt sur l'enchaînement de mauvaises pratiques, de configurations insuffisamment sécurisées et de vulnérabilités connues ou évitables.

Chaque service a donc été installé de manière classique, conformément aux méthodes vues en cours, puis configuré de façon volontairement permissive ou obsolète afin de permettre leur exploitation dans un cadre contrôlé.

6.1 Vulnérabilités du service Web

Le service Web a été mis en place de manière classique sur un serveur **Ubuntu Server 22.04.7 LTS**, disposant de l'adresse IP **192.168.1.11/24**. Il repose sur un serveur Apache HTTP avec le module PHP activé, selon une installation standard (**apache2, php, libapache2-mod-php**). Le site Web est hébergé dans le répertoire par défaut **/var/www/html** et accessible depuis le réseau utilisateur.

Les pages du site sont développées en PHP, ce qui permet l'exécution de scripts côté serveur sans recourir à des frameworks ou bibliothèques externes. Cette simplicité facilite l'introduction volontaire de failles applicatives. Les formulaires présents sur le site (authentification, recherche interne) construisent dynamiquement des requêtes **SQL** à partir des entrées utilisateur, sans utiliser de requêtes préparées ni de mécanismes d'échappement des caractères spéciaux. Cette mauvaise pratique permet la réalisation d'injections SQL, illustrant un cas fréquent de vulnérabilité liée au développement applicatif. En complément, des vulnérabilités de type path traversal ont été introduites via des paramètres d'URL permettant de charger dynamiquement des fichiers. **L'absence de validation sur les chemins d'accès autorise un attaquant à remonter l'arborescence du serveur** et à accéder à des fichiers situés en dehors du répertoire Web. Cette faille permet notamment de récupérer des fichiers de configuration ou des sauvegardes stockées localement sur le serveur.

Enfin, des fichiers sensibles, tels que des sauvegardes de bases de données ou des archives internes, ont été volontairement laissés accessibles depuis le serveur Web. Cette

situation illustre les risques liés à une mauvaise gestion des données sensibles, à l'absence de séparation entre environnement applicatif et données critiques, et à un contrôle insuffisant des permissions sur le système de fichiers.

6.2 Vulnérabilités du service FTP

Le service FTP a été installé de manière classique à l'aide de **ProFTPD**, conformément aux méthodes vues en cours. Le serveur repose sur une configuration standard, avec une authentification basée sur des comptes locaux du système et des communications non chiffrées. L'absence de FTPS ou de SFTP permet la transmission des identifiants en clair sur le réseau.

Les vulnérabilités principales reposent sur une gestion trop permissive des droits et l'activation volontaire de commandes avancées du protocole FTP. En particulier, les commandes SITE CPFR et SITE CPTO (également appelées commandes quote) ont été explicitement autorisées dans la configuration du serveur. Ces commandes permettent de copier des fichiers depuis n'importe quel emplacement du système vers un autre, à condition de connaître le chemin exact du fichier source.

Cette configuration illustre une mauvaise séparation des privilèges et permet à un attaquant authentifié d'accéder à des fichiers sensibles qui n'auraient jamais dû être exposés via un service de transfert de fichiers. L'exploitation de cette faille facilite la récupération de fichiers de configuration, d'informations d'authentification et contribue à la compromission de comptes critiques, notamment ceux utilisés sur d'autres services du système d'information.

6.3 Vulnérabilités du service **Samba**

Le service de partage de fichiers **Samba** a été mis en place de manière basique afin de respecter le cahier des charges du projet. Il repose sur un partage accessible à l'aide d'une session valide, ainsi qu'un partage public dont les droits sont volontairement trop larges. **Aucune CVE spécifique n'a été exploitée sur ce service**. Les vulnérabilités reposent essentiellement sur des mauvaises pratiques de configuration, telles qu'un contrôle insuffisant des accès, une absence de cloisonnement entre les partages et la présence d'informations sensibles accessibles à des utilisateurs non autorisés. Cette situation démontre qu'un service correctement installé mais mal configuré peut représenter un risque

majeur pour la sécurité du système d'information.

6.4 Vulnérabilités du service de messagerie

Le service de messagerie interne a été installé de manière classique à l'aide de **Dovecot**, avec une gestion des boîtes mail en local, indépendamment de l'**Active Directory**. Les comptes de messagerie sont donc basés sur des utilisateurs système et non sur l'annuaire centralisé, ce qui reflète une architecture encore rencontrée dans certaines entreprises. **Les vulnérabilités introduites reposent principalement sur le facteur humain** et les mauvaises pratiques des utilisateurs. Des mots de passe faibles ou réutilisés entre plusieurs services ont été volontairement configurés. De plus, des informations sensibles ont été laissées dans les boîtes mail, telles que des identifiants **Active Directory**, des échanges internes détaillant l'organisation du système d'information ou des indications sur des événements internes à venir.

Cette mise en situation permet de montrer que la messagerie constitue une source d'information particulièrement riche pour un attaquant et qu'une simple compromission de boîte mail peut suffire à accélérer considérablement une attaque.

6.5 Vulnérabilités liées aux services internes et aux **CVE**

Deux vulnérabilités majeures ont été intégrées sous forme de bonus techniques exploitables via Metasploit, afin d'illustrer l'impact de services obsolètes et de dépendances logicielles non corrigées.

Le premier service vulnérable repose sur **Apache ActiveMQ**, installé sur un serveur disposant de l'adresse IP 192.168.1.17. Le service est lancé manuellement au démarrage à l'aide des commandes suivantes :

```
cd /opt/activemq
sudo ./bin/activemq start
ss -tulnp | grep 61616
```

La version utilisée est volontairement vulnérable à la CVE-2023-46604, permettant une exécution de code à distance. Cette vulnérabilité est exploitée depuis une machine attaquante Kali Linux à l'aide de Metasploit, via un module dédié. L'exploitation permet

l'obtention d'un shell distant et l'accès aux fichiers du système, notamment un fichier flag.txt servant de preuve de compromission. Cette vulnérabilité met en évidence les risques liés à l'exposition de services internes sans filtrage adéquat et à l'utilisation de versions logicielles obsolètes.

Le second service vulnérable concerne la faille **Log4Shell**, exploitée sur un serveur Java disposant de l'adresse IP **192.168.1.16. Le service repose sur une version vulnérable de la bibliothèque Log4j 2.14.1**, intégrée volontairement sans correctif. Le serveur est démarré manuellement à l'aide d'une commande Java incluant explicitement les options JNDI vulnérables.

L'attaque repose sur l'injection de charges malveillantes dans les en-têtes HTTP à l'aide d'un module Metasploit spécialisé. Cette exploitation permet également l'obtention d'un shell distant et la récupération d'un flag attestant de la compromission. Cette vulnérabilité illustre l'impact critique que peut avoir une dépendance logicielle mal maintenue et l'importance de la gestion des mises à jour de sécurité.

6.6 Vulnérabilités liées à l'architecture réseau

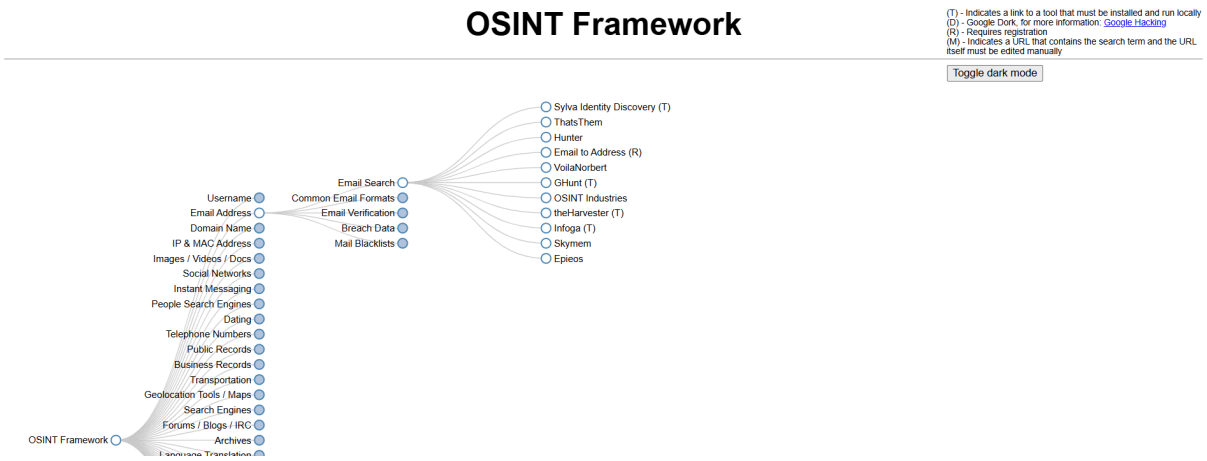
Enfin, certaines vulnérabilités ne reposent pas sur des services applicatifs, mais sur des choix d'architecture réseau. Le filtrage inter-VLAN sur le pare-feu est volontairement limité, autorisant des communications excessives entre les segments du réseau. Cette configuration facilite les déplacements latéraux après une première compromission.

L'accès **VPN** SSL est également associé à des droits trop larges, permettant un accès direct au LAN interne sans restrictions suffisantes. Ce choix illustre les risques liés à une mauvaise gestion des accès distants et démontre qu'un **VPN** mal configuré peut devenir un point d'entrée critique dans le système d'information.

7. Chaîne d'attaque et exploitation progressive du système d'information

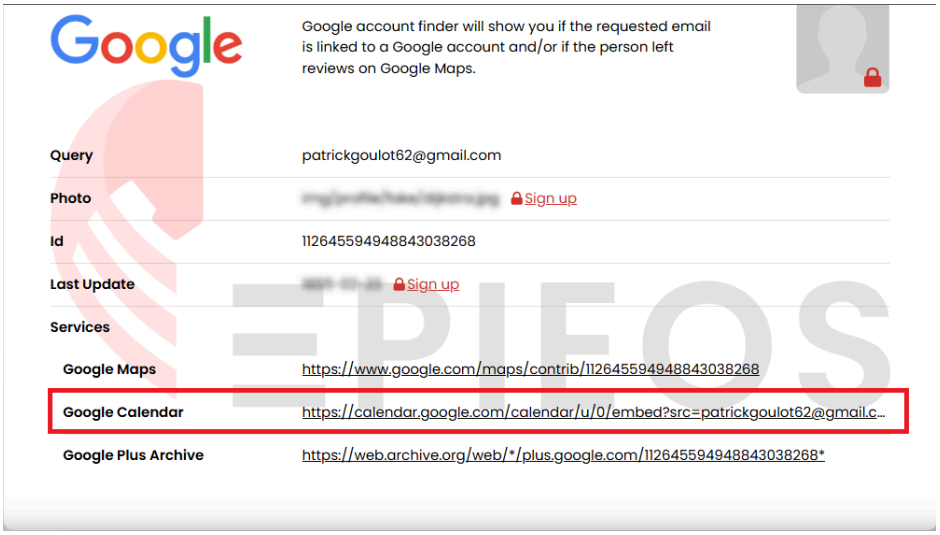
La compromission du système d'information de l'entreprise Millot Dumas repose sur une chaîne d'attaque structurée, réaliste et progressive. Chaque étape s'appuie sur les informations obtenues précédemment et illustre la manière dont un attaquant peut exploiter des failles techniques, organisationnelles et humaines pour avancer vers un objectif final : le contrôle de l'infrastructure interne.

La première phase de l'attaque repose sur une démarche de reconnaissance passive, sans interaction directe avec le système d'information. À partir des informations initiales connues, telles que le nom, le prénom et la date de naissance d'un cadre de l'entreprise, une phase d'OSINT est menée. Cette recherche permet de découvrir des informations indirectes sur l'organisation interne, notamment via des services publics.

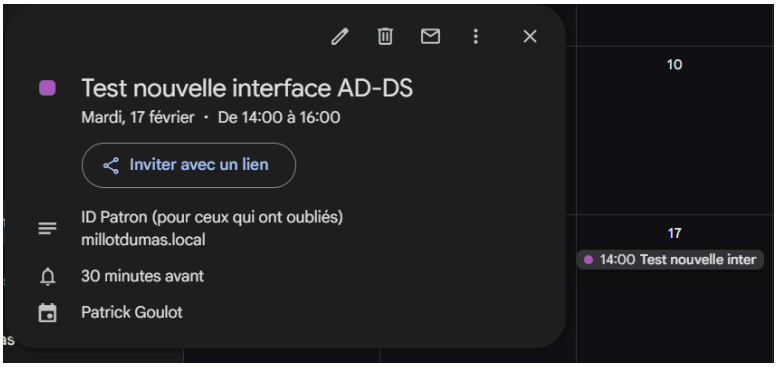


Légende: https://osintframework.com/ qui permet de trouver le calendrier.

La mise en place volontaire d'un calendrier Google accessible publiquement permet d'illustrer à quel point des données apparemment anodines peuvent révéler des éléments sensibles. L'analyse de ce calendrier permet d'identifier le nom de domaine interne de l'entreprise ainsi que des indices liés à des projets en cours, constituant ainsi le premier flag et validant la réussite de cette phase.



Légende: Comment avoir accès au calendrier de Patrick GOULOT

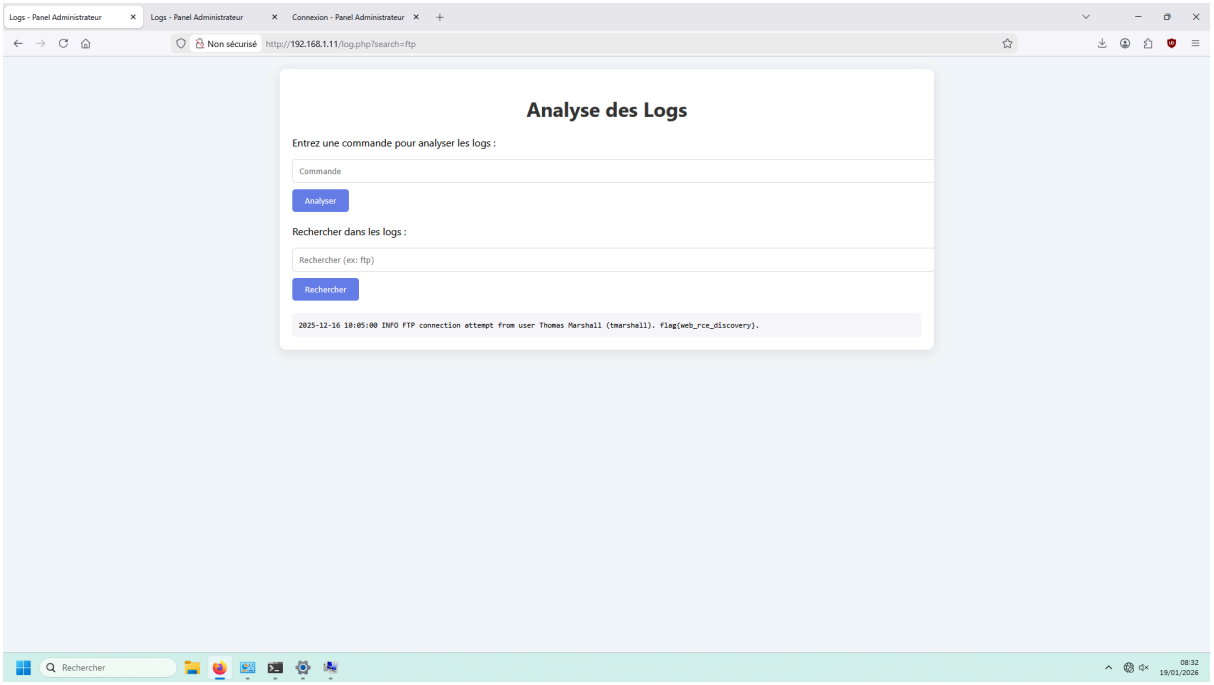


Légende: Information trouvée sur le calendrier de GOULOT Patrick

Une fois le domaine interne identifié, l'attaquant peut affiner sa reconnaissance en s'intéressant à l'infrastructure réseau et aux services exposés. Cette phase de découverte permet d'identifier l'existence d'un site Web interne, accessible depuis le réseau utilisateur. L'analyse du site révèle rapidement plusieurs failles applicatives. Une injection SQL sur la page d'authentification permet de contourner les mécanismes de sécurité et d'accéder à une interface d'administration. L'exploitation de cette faille constitue une étape clé, car elle donne accès à des journaux, des fichiers de sauvegarde et des informations sur les services internes utilisés par l'entreprise.

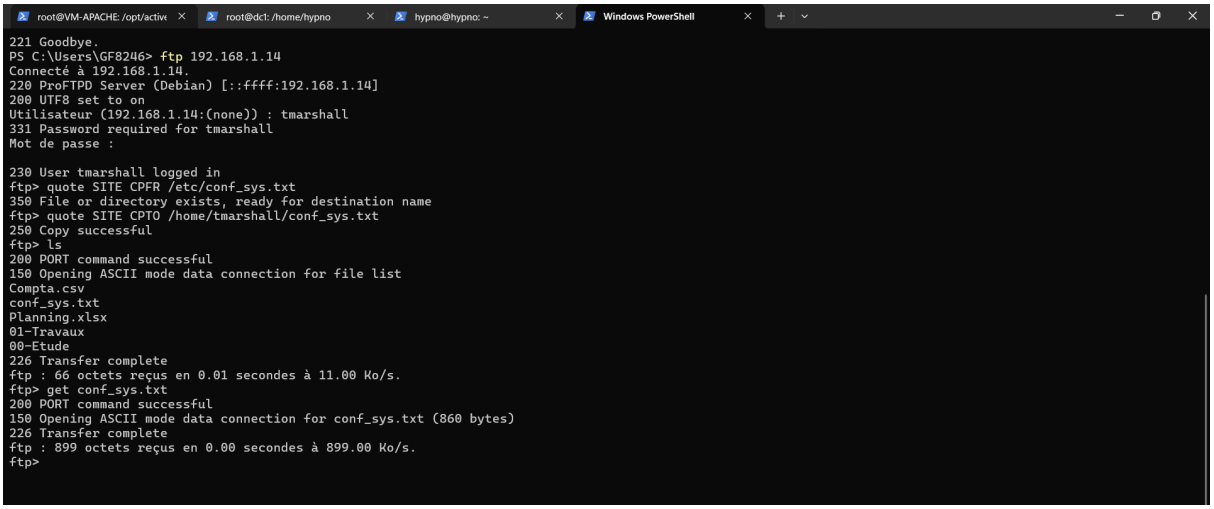
*

Légende: Injection SQL pour se connecter au site web de l'entreprise



Légende: Information pour le FTP ainsi que le flag

L'exploitation des **vulnérabilités Web** permet également de récupérer des identifiants menant vers d'autres services, notamment le service **FTP**. L'accès au serveur **FTP** met en évidence des mauvaises pratiques de configuration, telles que des droits excessifs et la possibilité d'utiliser des commandes avancées. Ces failles facilitent la récupération de fichiers de configuration internes et permettent d'obtenir des identifiants réutilisés sur d'autres services, notamment **Samba**.



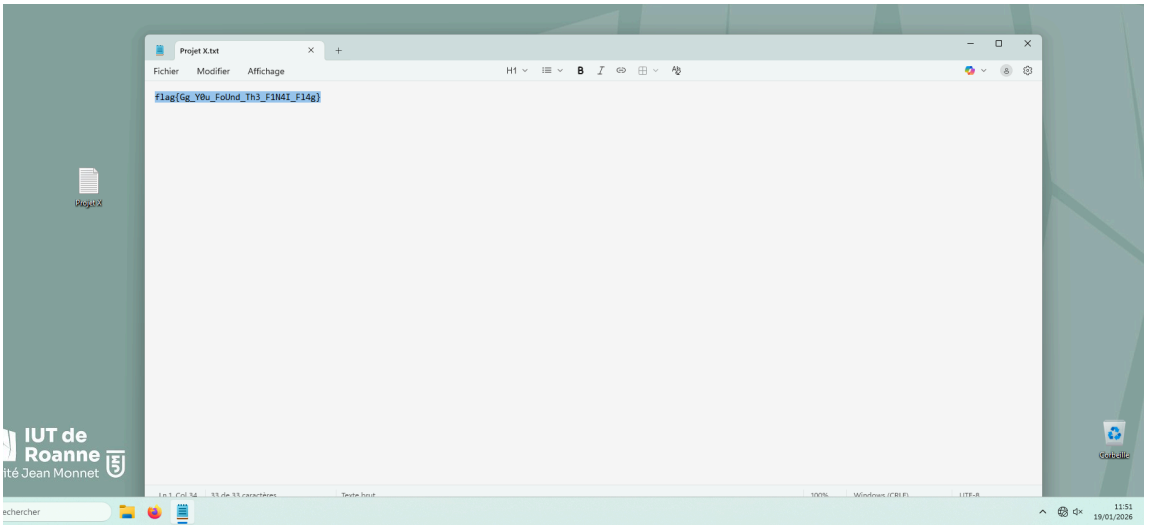
Légende: Mauvaise pratique sur le FTP

Grâce aux informations récupérées via le **FTP**, l'attaquant peut accéder aux **partages Samba** internes. L'exploitation d'une version vulnérable du service, combinée à des permissions trop larges, permet d'accéder à des répertoires sensibles. Cette étape marque une escalade importante dans la compromission, car elle permet de récupérer des documents internes et des informations liées à l'organisation du système d'information. L'obtention de nouveaux flags à ce stade confirme la progression de l'attaque.

La compromission du service de messagerie interne constitue une étape charnière. En exploitant des identifiants faibles ou réutilisés, l'attaquant accède aux boîtes mail de certains utilisateurs. L'analyse des courriels révèle des échanges internes contenant des informations critiques, notamment des identifiants **Active Directory** transmis de manière non sécurisée. Cette étape illustre parfaitement l'impact du facteur humain dans une attaque et démontre que la sécurité technique seule ne suffit pas à protéger un système d'information.

Parallèlement à ces attaques « classiques », des vulnérabilités critiques de type **CVE** sont exploitées sur des services internes. L'exploitation d'**Apache ActiveMQ** permet d'obtenir une exécution de code à distance sur un serveur interne, offrant à l'attaquant un accès direct au système. De la même manière, l'exploitation de la vulnérabilité **Log4Shell** sur un service Java permet de démontrer l'impact majeur des bibliothèques non mises à jour. Ces attaques, bien que techniques, s'intègrent naturellement dans la chaîne d'attaque globale et permettent de valider des flags bonus.

L'ensemble de ces compromissions converge vers l'objectif final : l'accès à l'annuaire **Active Directory**. Grâce aux identifiants récupérés via les services précédents, l'attaquant obtient un accès étendu aux ressources internes. La consultation des partages réseau et des profils utilisateurs permet de valider la compromission complète du système d'information et d'obtenir les derniers flags. À ce stade, l'attaquant dispose de preuves suffisantes pour démontrer que la sécurité globale de l'entreprise est défaillante.



Légende: Flag finales qui se trouve sur la session “Patron”

Cette chaîne d’attaque met en évidence une réalité essentielle en cybersécurité : ce ne sont pas toujours des vulnérabilités extrêmement complexes qui causent les plus grands dégâts, mais l’accumulation de failles simples, de mauvaises pratiques et d’un manque de cloisonnement. Chaque étape, prise isolément, pourrait sembler bénigne, mais leur enchaînement conduit à une compromission totale du système d’information.

8. Supervision, détection et analyse des incidents

La mise en place d'un système d'information sécurisé ne se limite pas à la prévention des attaques. Il est tout aussi essentiel de disposer de mécanismes permettant de détecter, analyser et comprendre les actions malveillantes. Dans le cadre de cette SAE, une architecture de supervision et de détection a été déployée afin d'assurer une visibilité globale sur l'état du système et sur les événements de sécurité.

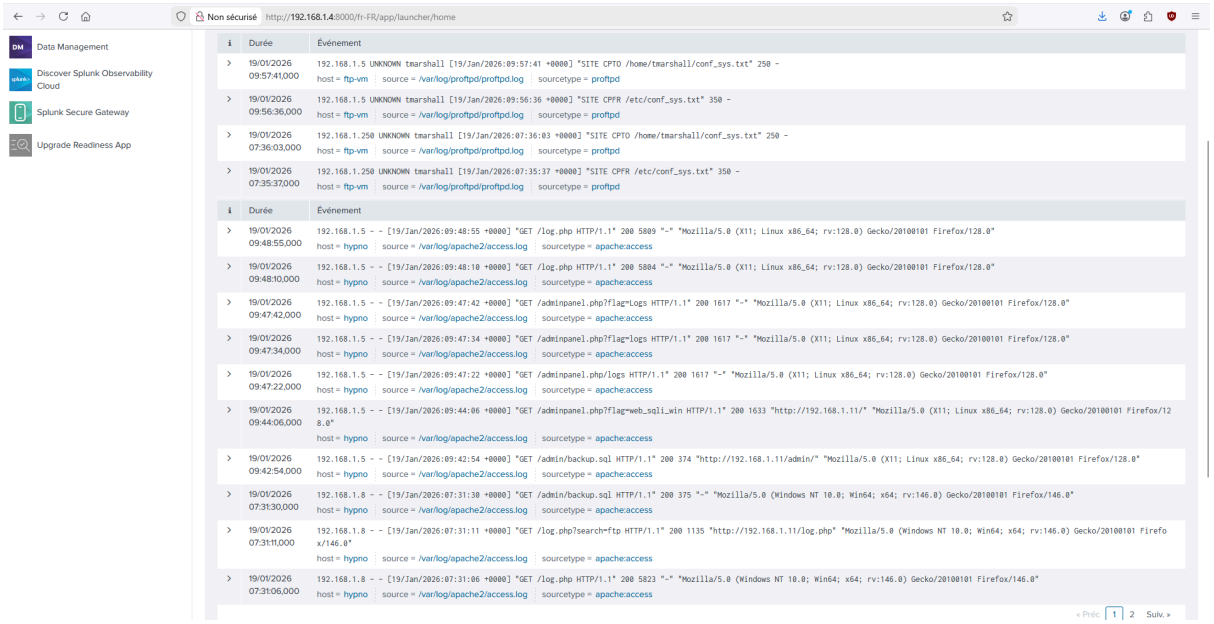
La supervision de l'infrastructure repose principalement sur l'outil **Zabbix**. Celui-ci permet de surveiller en temps réel la disponibilité des serveurs, l'état des services critiques et certaines métriques système, telles que la charge processeur, l'utilisation de la mémoire ou l'espace disque. Les **services Web**, **FTP**, **Samba**, le service de messagerie et l'annuaire **Active Directory** sont tous intégrés dans la supervision. Lors des phases d'attaque, **Zabbix** permet de constater des comportements anormaux, comme des indisponibilités de service, des pics de charge ou des redémarrages inattendus, fournissant ainsi de premiers indicateurs d'un incident en cours.

Légende: Les remontées d'alertes sur Zabbix

La détection des attaques réseau est assurée par Suricata, déployé comme système de détection d'intrusion. Suricata analyse le trafic réseau et compare les paquets observés à des signatures connues d'attaques. Lors des tentatives d'exploitation des services Web ou des vulnérabilités critiques comme **Log4Shell** ou **Apache ActiveMQ**, **Suricata** génère des alertes indiquant des comportements suspects, tels que des requêtes anormales, des tentatives d'exploitation ou des communications vers des ports inhabituels. Ces alertes permettent d'identifier rapidement les phases actives de l'attaque.

L'ensemble des journaux et des alertes générés par les différents composants de l'infrastructure est centralisé dans **Splunk**, utilisé comme solution de type **SIEM**. Splunk permet de collecter les logs issus des serveurs, du pare-feu, de **Suricata** et des services applicatifs. Grâce à la corrélation des événements, il devient possible de reconstituer

précisément la chronologie des attaques, depuis les premières tentatives de reconnaissance jusqu'à la compromission des services internes. Cette centralisation facilite également l'analyse post-incident et la conservation de preuves exploitables.



Légende: Les remontées d'alertes de Suricata sur Splunk

La complémentarité entre Zabbix, Suricata et Splunk illustre l'importance d'une approche globale de la sécurité. Zabbix fournit une vision de la disponibilité et de la santé du système, Suricata détecte les comportements réseau suspects, et Splunk permet une analyse approfondie et transversale des événements. Ensemble, ces outils constituent une base solide pour un centre opérationnel de sécurité, même dans un contexte pédagogique.

9. Mesures correctives et recommandations de sécurité

L'analyse de la chaîne d'attaque met en évidence de nombreuses failles, tant techniques que organisationnelles. Afin de renforcer la sécurité du système d'information de Millot Dumas, plusieurs mesures correctives peuvent être envisagées.

Concernant la phase de reconnaissance et l'OSINT, il est essentiel de limiter la diffusion d'informations sensibles sur des plateformes publiques. Les données liées à l'organisation interne, aux projets ou aux infrastructures ne devraient jamais être accessibles sans contrôle. Une politique de communication stricte et une sensibilisation des employés aux risques liés aux informations publiques permettraient de réduire considérablement la surface d'attaque initiale.

Sur le plan applicatif, le service Web devrait être durci en appliquant les bonnes pratiques de développement sécurisé. L'utilisation de requêtes préparées permettrait d'éliminer les injections SQL, tandis qu'une validation stricte des entrées utilisateur empêcherait les attaques de type path traversal. Les fichiers sensibles, tels que les sauvegardes de bases de données, ne devraient jamais être accessibles depuis le serveur Web et doivent être stockés dans des emplacements protégés.

Le service FTP devrait être remplacé ou renforcé par une solution plus sécurisée, telle que SFTP ou FTPS, afin de garantir le chiffrement des communications. Les droits d'accès doivent être strictement limités aux fichiers nécessaires, et les commandes dangereuses doivent être désactivées. Une séparation claire entre les espaces utilisateurs et les fichiers système est indispensable.

Concernant **Samba**, l'application régulière des mises à jour de sécurité est une priorité. Les partages doivent être configurés selon le principe du moindre privilège, en limitant l'accès aux seuls utilisateurs ou groupes nécessaires. Une surveillance renforcée des accès aux partages sensibles permettrait également de détecter plus rapidement les comportements anormaux.

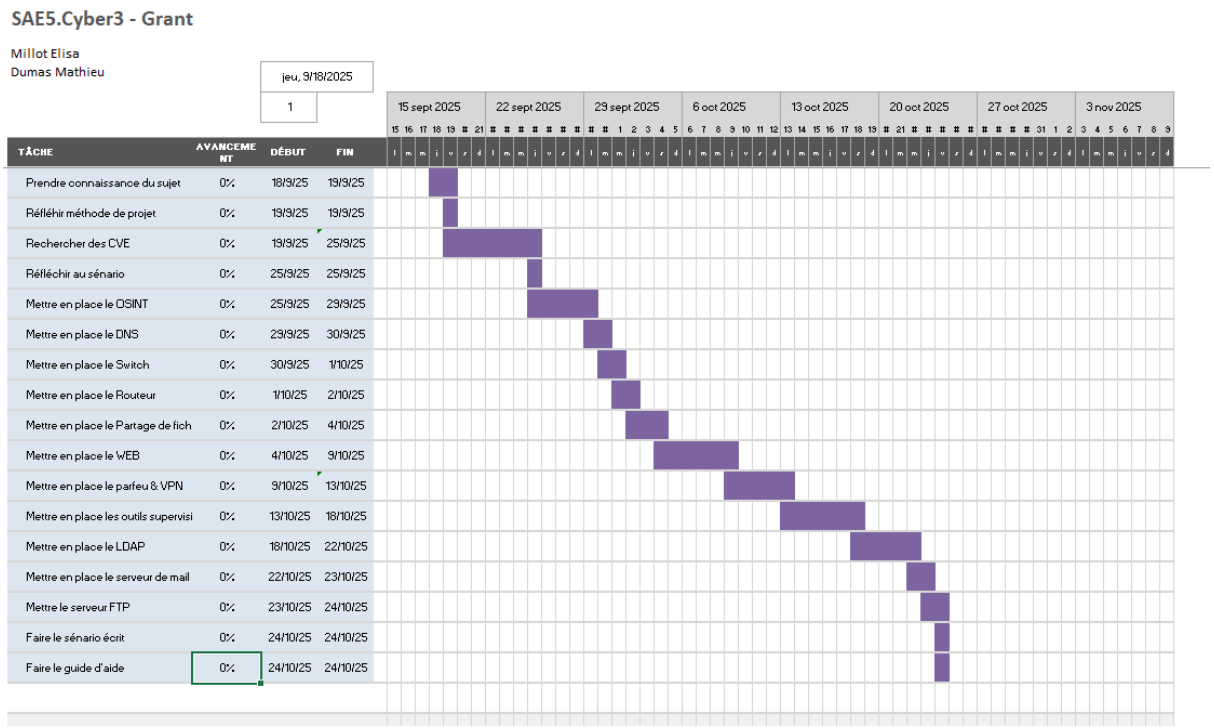
Le service de messagerie doit être protégé par des politiques de mots de passe robustes et, idéalement, par l'authentification multifacteur. Les utilisateurs doivent être sensibilisés aux risques liés à l'envoi d'informations sensibles par courrier électronique. Une classification des données et des règles claires concernant les échanges internes permettraient de limiter les fuites d'informations critiques.

Au niveau de **l'Active Directory**, une segmentation stricte des privilèges est indispensable. Les comptes à privilèges élevés doivent être utilisés uniquement lorsque nécessaire et protégés par des mots de passe forts et uniques. La journalisation des accès et des actions sensibles doit être activée et régulièrement analysée.

Enfin, l'architecture réseau et le pare-feu doivent faire l'objet de revues régulières. Le filtrage inter-VLAN doit être renforcé afin de limiter les communications inutiles entre les segments du réseau. Les accès **VPN** doivent être restreints à des utilisateurs et à des ressources précisément définis, en appliquant le principe du moindre privilège. Une surveillance continue des flux réseau et une analyse régulière des règles de filtrage permettraient de maintenir un niveau de sécurité adapté face aux évolutions des menaces.

10. Gantt

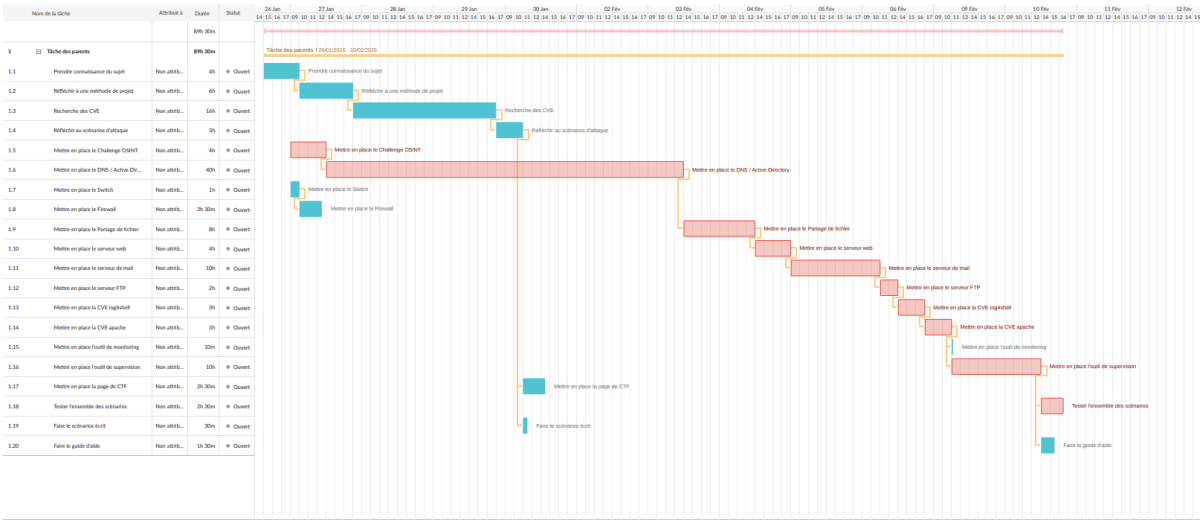
La comparaison entre le Gantt prévisionnel et le Gantt réellement effectué qui met en évidence l'évolution du projet au fil de sa réalisation. Le premier document, représenté par l'image du Gantt initial, correspond à une planification théorique établie avant le début du travail. On y voit toutes les tâches sont affichées à 0 % d'avancement, ce qui confirme qu'il s'agit d'un planning strictement prévisionnel.



TÂCHE	AVANCEMENT	DÉBUT	FIN
Prendre connaissance du sujet	0%	18/9/25	19/9/25
Réfléhir méthode de projet	0%	19/9/25	19/9/25
Rechercher des CVE	0%	19/9/25	25/9/25
Réfléchir au sénario	0%	25/9/25	25/9/25
Mettre en place le OSINT	0%	25/9/25	29/9/25
Mettre en place le DNS	0%	29/9/25	30/9/25
Mettre en place le Switch	0%	30/9/25	1/10/25
Mettre en place le Routeur	0%	1/10/25	2/10/25
Mettre en place le Partage de fich	0%	2/10/25	4/10/25
Mettre en place le WEB	0%	4/10/25	9/10/25
Mettre en place le parfeu & VPN	0%	9/10/25	13/10/25
Mettre en place les outils supervisi	0%	13/10/25	18/10/25
Mettre en place le LDAP	0%	18/10/25	22/10/25
Mettre en place le serveur de mail	0%	22/10/25	23/10/25
Mettre le serveur FTP	0%	23/10/25	24/10/25
Faire le sénario écrit	0%	24/10/25	24/10/25
Faire le guide d'aide	0%	24/10/25	24/10/25

Légende: Gantt au début du projet

En revanche, le Gantt issu de la deuxième image reflète la réalité du projet. On y observe un découpage beaucoup plus précis, avec des durées exprimées en heures et minutes, ainsi que des tâches supplémentaires qui n'étaient pas prévues initialement. Ce suivi réel montre que certaines étapes ont nécessité bien plus de temps que ce qui avait été anticipé. L'exemple le plus marquant est la mise en place du DNS et de l'Active Directory, prévue sur deux jours dans le Gantt initial mais qui a finalement demandé près de quarante heures de travail. Cette différence illustre la complexité technique de cette partie du projet et la nécessité d'adapter le planning en fonction des difficultés rencontrées.



Légende: Gantt en fin de projet

On remarque également que plusieurs tâches importantes n'apparaissent pas dans le planning prévisionnel, comme l'intégration des vulnérabilités Log4Shell et ActiveMQ ou encore la phase de test des scénarios. Ces ajouts montrent que le projet s'est enrichi au fur et à mesure, notamment pour répondre aux exigences du cahier des charges et pour renforcer la cohérence globale de l'infrastructure.

Dans le fond, la différence essentielle entre les deux Gantt réside dans la profondeur du travail réalisé. Le planning initial imaginait un enchaînement simple d'installations techniques, alors que le Gantt final révèle un projet beaucoup plus complet, intégrant des vulnérabilités réelles, des tests, de la supervision et une montée en complexité progressive. Le projet est ainsi passé d'une vision théorique à une réalisation concrète, plus riche, plus réaliste et plus exigeante.

En conclusion, cette comparaison montre que le projet a évolué de manière dynamique. Le Gantt prévisionnel donnait une direction générale, mais le Gantt final témoigne d'une adaptation continue, d'une gestion du temps plus précise et d'une véritable compréhension des enjeux techniques. Cette évolution est le signe d'un travail sérieux, réfléchi et mené avec une bonne capacité d'ajustement face aux imprévus.

11. Analyse Réflexive

La SAE5.Cyber.03 nous a permis de mobiliser de manière concrète et cohérente l'ensemble des apprentissages critiques. Ce projet nous a placés dans une situation proche du monde réel, en nous confrontant à la conception, au déploiement, à l'exploitation et à la supervision d'un système d'information réaliste et fait nous même.

Les compétences liées au bloc **AC31** ont été particulièrement sollicitées lors de la conception de l'architecture réseau. La segmentation par VLAN, l'utilisation d'une DMZ, l'intégration d'un pare-feu Stormshield et la mise en place d'un accès VPN SSL ont nécessité une réflexion sur la sécurité, le cloisonnement et la gestion des flux. La rédaction du rapport technique nous a permis de structurer et de justifier nos choix, tandis que la maquette fonctionnelle déployée a servi de support à la démonstration et à l'argumentation du projet.

Les apprentissages **AC32** et **AC33** ont été mobilisés à travers le déploiement des services essentiels de l'entreprise (Web, FTP, Samba, messagerie et annuaire), leur mise en condition opérationnelle et leur exploitation. Le projet nous a permis de comprendre l'importance des accès sécurisés, notamment via le VPN, ainsi que les risques liés à des configurations trop permissives, à la réutilisation des mots de passe et à l'absence de mises à jour. L'exploitation de vulnérabilités connues (Log4Shell, Apache ActiveMQ) a également renforcé notre compréhension de la veille technologique et des enjeux liés au maintien en condition de sécurité.

Les blocs **AC34** et **AC35** constituent le cœur de cette SAE. L'analyse des risques, la mise en place volontaire de vulnérabilités et la construction d'une chaîne d'attaque progressive nous ont permis de comprendre comment une compromission globale peut résulter de l'enchaînement de failles simples. La supervision et la détection des incidents à l'aide de Zabbix, Suricata et Splunk ont apporté une vision défensive essentielle, en montrant l'importance de la surveillance, de la corrélation des événements et de la réaction face aux incidents.

En conclusion, cette SAE a renforcé notre vision globale de la cybersécurité en montrant que la protection d'un système d'information repose autant sur les choix techniques que sur les pratiques organisationnelles et humaines. Les compétences acquises constituent une base solide pour la suite de la formation et pour une future insertion professionnelle dans les métiers de la cybersécurité.

12. Conclusion

La SAE5.Cyber.03 a permis de mettre en pratique de manière complète et réaliste les compétences acquises au cours du BUT Réseaux et Télécommunications, parcours cybersécurité, en intégrant les phases de sécurisation, de supervision et de détection dans un contexte de Lutte Informatique Défensive. Le projet a reproduit un échelon tactique de cyberdéfense, combinant à la fois un SOC et un CERT, et a confronté les étudiants à des scénarios d'attaque réalistes inspirés de situations observées dans le monde professionnel.

Dans le cadre de cette SAE, nous avons conçu une infrastructure réseau segmentée avec des **VLAN** pour les utilisateurs, l'administration et les serveurs, isolant les ports inutilisés et mettant en place des mécanismes de sécurité tels que le **port-security** sur le **switch** et un pare-feu **Stormshield** assurant le filtrage **inter-VLAN**, l'accès Internet, la gestion d'un **VPN** SSL et l'exposition contrôlée des services en **DMZ**. Les services essentiels — Web, **FTP**, **Samba**, **messagerie** et **Active Directory** — ont été déployés sur des machines Linux, conformément aux exigences du projet, et des vulnérabilités pédagogiques ont été volontairement intégrées pour illustrer les risques liés à des configurations faibles, à la réutilisation de mots de passe, à des droits excessifs et à des logiciels non mis à jour.

La chaîne d'attaque a débuté par une phase **OSINT** permettant de collecter des informations publiques et indirectes, puis s'est étendue à l'exploitation de vulnérabilités applicatives et systèmes sur les différents services internes. Chaque étape a été documentée et a permis de valider des flags, illustrant la progression logique d'un attaquant et les impacts de chaque faille sur le système. L'exploitation de failles critiques comme **Apache ActiveMQ** ou **Log4Shell** a démontré l'importance du suivi des mises à jour et de la gestion des dépendances, tandis que la compromission des **services FTP**, **Samba** et de la messagerie a mis en évidence l'impact des mauvaises pratiques et du facteur humain.

La supervision et la détection ont été assurées par **Zabbix** pour la **surveillance des services** et de l'état des serveurs, **Suricata** pour l'analyse du trafic et la détection d'anomalies, et **Splunk** pour la centralisation et la corrélation des logs. Cette configuration a permis de suivre l'ensemble de la chaîne d'attaque et de générer des preuves exploitables, conformément aux objectifs de la SAE et aux exigences du SOC.

Si le projet a permis de démontrer l'efficacité d'une architecture pédagogique permettant la simulation d'attaques et l'analyse de leur impact, il a également mis en évidence ce qui n'a pas été fait ou pourrait être amélioré. Certaines configurations réseau ont été volontairement

permissives pour illustrer les risques liés à un cloisonnement insuffisant, et certains services ont été laissés volontairement vulnérables pour servir de terrain pédagogique. Ces choix ont permis de mettre en évidence la nécessité de politiques de sécurité robustes, de mises à jour régulières et de sensibilisation des utilisateurs dans le monde réel.

En conclusion, cette SAE illustre parfaitement l'importance d'une approche globale de la cybersécurité, combinant prévention, détection et réaction. Elle montre que la sécurité repose non seulement sur des outils techniques, mais également sur des pratiques organisationnelles solides et une culture de la sécurité intégrée à l'ensemble du système d'information. Les enseignements tirés de cette SAE serviront de base solide pour la phase suivante, axée sur la réponse aux incidents et la remédiation