ESMT
École Supérieure Multinationale des Télécommunications

Formation initiale

RAPPORT D'AUDIT SI DU NETCORE-SOLUTION

TeamASR 2024-2025

09/05/2025

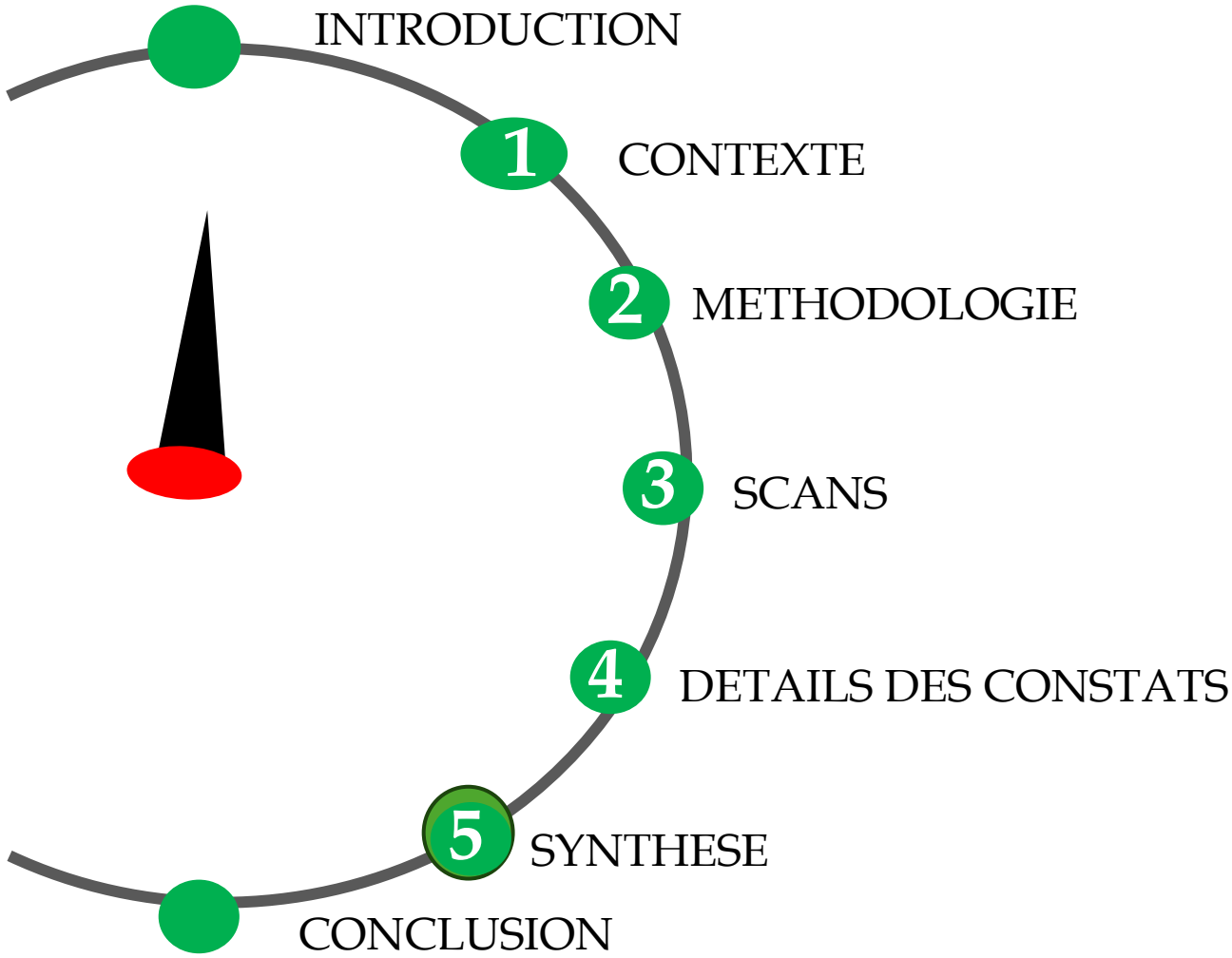
Equipe Organisationnel

- ***Madeleine Biaye (Responsible)***
- ***Sadiya Sadio Kane***
- ***Aminata Lo Fall***
- ***Mame Fama DIENG***
- ***Kabirou Oumarou Hamadou***
- ***Cheikh Sadibou Diouf***
- ***Aminata Niang***
- ***Yakeliomi Maixente KOHIO***
- ***Akhmadou Bamba DIOUF***
- ***Seydina Issa Rouhou Lahi KA***
- ***Gali Moussa Dantia***
- ***Ngonè Diop***
- ***Yaye Aby SOW***
- ***Aïcha SY***
- ***Mame Aida Kasse***
- ***Babacar Keiba KOUYATE***

Equipe Technique

- ***Sada Bousso***
- ***Pape Siriman Cissoko (Responsable)***
- ***Ndeye Aminata Diagne***
- ***Maimouna Dieng***
- ***Macode Diop***
- ***Mamadou Diop***
- ***Idy Fall***
- ***Fatou Bintou Faye***
- ***Pierre Marie Konate***
- ***Absa Ndiaye***
- ***Idy NdionE***
- ***Amadou Diarouga Sar***
- ***Ndeye Saly Sarr***
- ***Fatim Sow***
- ***Bocar Tandia***
- ***Marieme Wone***

PLAN D'ETUDE


INTRODUCTION
1
CONTEXTE
2
METHODOLOGIE
3
SCANS
4
DETAILS DES CONSTATS
5
SYNTHESE
CONCLUSION

INTRODUCTION

INTRODUCTION

Avec la généralisation du numérique et l'essor rapide des technologies de l'information, les données numériques sont devenues des ressources stratégiques. Cette transition digitale s'accompagne d'une forte augmentation des cybermenaces, rendant indispensable la sécurisation des systèmes d'information à travers des audits réguliers. L'audit de sécurité permet d'évaluer l'ensemble d'un système d'information afin d'identifier ses failles, de vérifier sa conformité aux bonnes pratiques et de proposer des mesures correctives. Il prend en compte les aspects techniques, organisationnels et humains. Dans le cadre du cours d'audit de la sécurité des réseaux, nous avons mené une mission d'audit sur le système de NETCORE-SOLUTION. Parallèlement, l'entreprise NETCORE SOLUTION nous a confié l'audit complet de son système d'information. Cette mission avait pour objectif de scanner et analyser les vulnérabilités de l'ensemble des actifs numériques, d'évaluer les configurations des systèmes, de vérifier les flux réseau ainsi que les règles de sécurité mises en place. Elle a également porté sur l'audit des applications selon les bonnes pratiques OWASP, le contrôle des flux applicatifs, l'examen des pares-feux, des accès, des règles GPO et des politiques de mot de passe. L'infrastructure réseau et les procédures IT internes ont été passées en revue, dans le but d'identifier les points d'optimisation possibles. Enfin, un plan de remédiation a été proposé afin de renforcer la sécurité globale du système et de limiter les risques liés aux menaces informatiques.

CONTEXTE

CONTEXTE

Après avoir procédé à l'implémentation et au déploiement de son infrastructure réseau, NETCORE- SOLUTION a souhaité réaliser un audit complet de son système d'information. L'objectif était de vérifier la bonne configuration du réseau, son niveau de sécurisation, ainsi que sa conformité aux normes en vigueur. Dans cette optique, l'entreprise a sollicité YAMAL -Consulting pour évaluer la conformité de ses configurations, et s'assurer de la fonctionnalité, de la sécurité et de la qualité de service de l'ensemble de son réseau..

Objectifs du projet

L'objectif principal de cette mission est de réaliser un audit exhaustif du système d'information de l'entreprise Netcore solution . Cette démarche comprend les actions suivantes :

- Le scan des vulnérabilités sur l'ensemble des actifs numériques de l'organisation;
- L'analyse approfondie des vulnérabilités identifiées et des configurations des équipements ;
- L'audit des matrices de flux réseau et l'examen des règles de sécurité en place ;
- L'évaluation des applications critiques à travers des tests d'intrusion et les standards OWASP ;
- L'analyse des flux applicatifs et la vérification de la pertinence des règles appliquées sur les pares-feux applicatifs ;
- L'audit du contrôleur d'accès, des règles GPO et des politiques de mot de passe ;
- L'évaluation de l'architecture réseau et des systèmes en vue d'optimiser leur performance et leur sécurité ;
- L'analyse des procédures IT internes ;
- Et enfin, la proposition de recommandation visant à renforcer la sécurité globale du système d'information.

METHODOLOGIE

(methodologie,approche methodolique,resume interview)

Méthodologie

1. Entretien avec les collaborateurs et définition des objectifs

Avant le démarrage des travaux, une étude préliminaire a permis de définir les objectifs et le périmètre de l'audit. Cette étape incluait :

- Des **entretiens** avec les équipes pour comprendre leurs besoins et leurs pratiques.
- L'analyse de documents clés (politiques de sécurité, configurations réseau, schémas d'architecture, etc.).

Une fois les premiers échanges réalisés, nous élaborons un cahier des charges définissant :

Les objectifs à atteindre,

Les besoins de sécurité propres à l'entreprise,

Les mesures de protection déjà existantes.

Méthodologie

2. Évaluation du système d'information et des comportements

Plusieurs tests ont été réalisés pour identifier les failles et les écarts de sécurité :

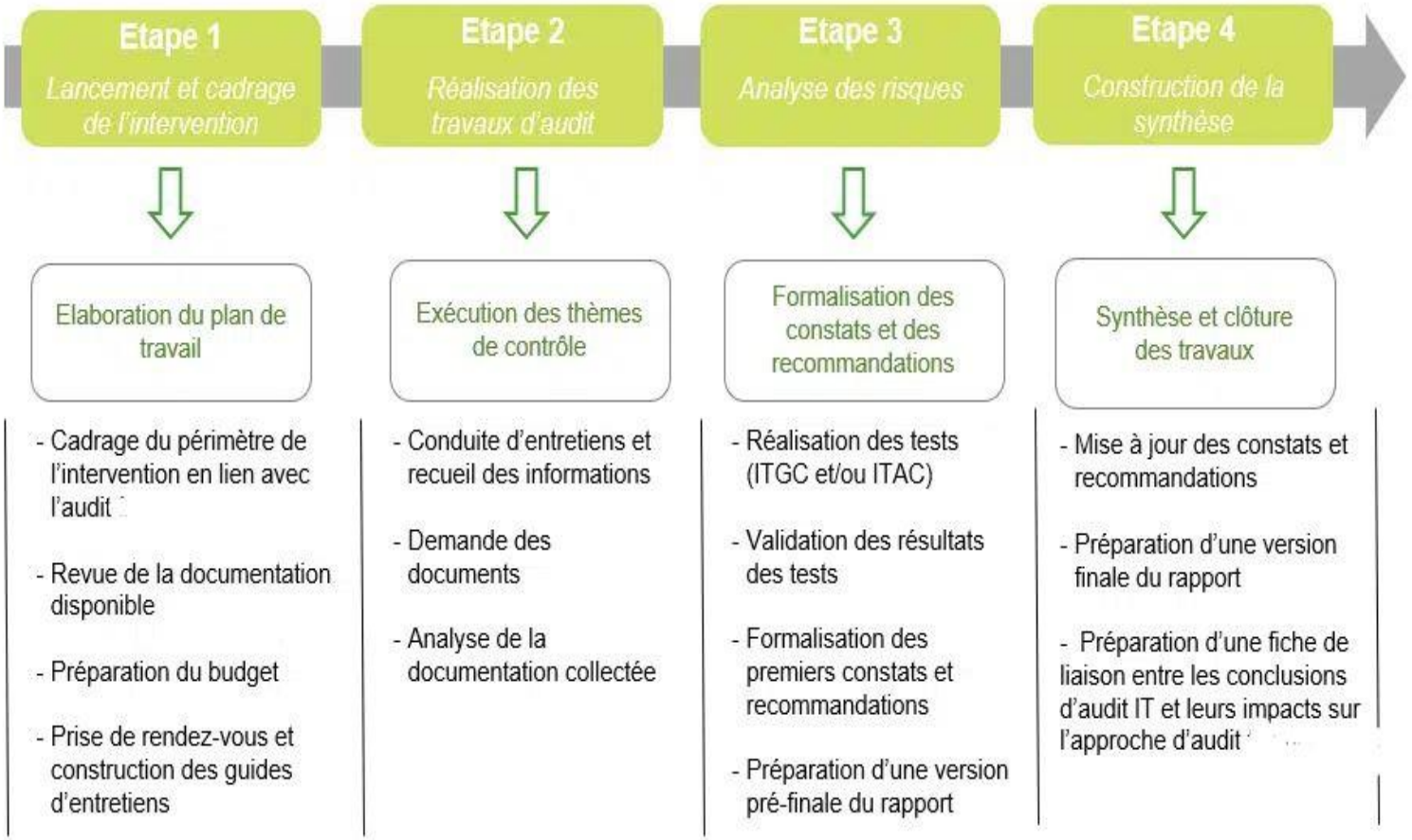
- **Analyse de l'infrastructure réseau** (topologie, segmentation, redondance).
- **Scan des vulnérabilités** (Nessus, Nmap) sur les serveurs, routeurs et postes de travail.
- **Audit des configurations** (pare-feu ASA, règles ACL, gestion des accès AD).
- **Tests d'intrusion** (pentesting manuel et automatisé).

3. Synthèse et plan d'action

- **Classement des risques** (critiques, majeurs, mineurs).
- **Recommandations prioritaires** (mises à jour matérielles, correction des règles firewall, sensibilisation des utilisateurs).

Cette méthodologie a permis d'établir un **diagnostic complet** du SI, mettant en lumière à la fois les points forts et les axes d'amélioration pour NETCORE solution.

Approche Méthodologique



SCANS

Analyse des Vulnérabilités – Rapport Synthétique

1. Vulnérabilité Moyenne - Serveurs Web (CVSS 5.3)

Sev	CVSS	VPR	EPSS	Family	Count
MEDIUM	5.3	4.0	0.8269	Web Servers	1
INFO				Web Servers	1

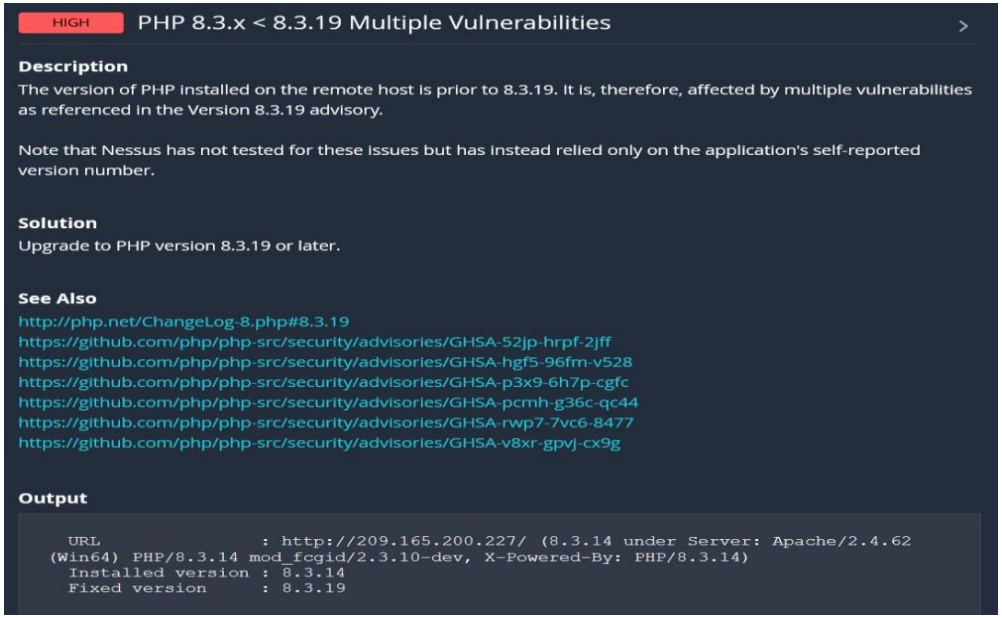
Une vulnérabilité de sévérité moyenne (CVSS 5.3, VPR 4.0, EPSS 0.8269) a été détectée dans la famille "Web Servers". Une autre entrée d'information est également répertoriée sans impact critique. .

2. Vulnérabilités de Sévérité Moyenne - Score CVSS 6.5

Sev	CVSS	VPR	EPSS	Family	Count
MEDIUM	6.5			General	1
MEDIUM	6.5			General	1

Deux vulnérabilités de sévérité moyenne (CVSS 6.5) ont été identifiées dans la catégorie "General", chacune ayant un compte de 1.

3Vulnérabilités Multiples dans PHP 8.3.x Avant la Version 8.3.19



HIGH PHP 8.3.x < 8.3.19 Multiple Vulnerabilities

Description

The version of PHP installed on the remote host is prior to 8.3.19. It is, therefore, affected by multiple vulnerabilities as referenced in the Version 8.3.19 advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

Solution

Upgrade to PHP version 8.3.19 or later.

See Also

http://php.net/ChangeLog-8.php#8.3.19
https://github.com/php/php-src/security/advisories/GHSA-52jp-hrpf-2jff
https://github.com/php/php-src/security/advisories/GHSA-hgf5-96fm-v528
https://github.com/php/php-src/security/advisories/GHSA-p3x9-6h7p-cgfc
https://github.com/php/php-src/security/advisories/GHSA-pcmh-g36c-qc44
https://github.com/php/php-src/security/advisories/GHSA-rwp7-7vc6-8477
https://github.com/php/php-src/security/advisories/GHSA-v8xr-gpvj-cx9g

Output

```
  URL               : http://209.165.200.227/ (8.3.14 under Server: Apache/2.4.62
(Win64) PHP/8.3.14 mod_fcgid/2.3.10-dev, X-Powered-By: PHP/8.3.14)
  Installed version : 8.3.14
  Fixed version     : 8.3.19
```

La version PHP 8.3.14 installée sur le serveur est obsolète et affectée par plusieurs vulnérabilités critiques. Nessus n'a pas testé ces failles mais s'est basé sur la version reportée par l'application.

Solution : Mettre à jour PHP vers la version 8.3.19 ou une version ultérieure.

4. Vulnérabilités Identifiées sur l'Hôte 209.165.200.227

L'hôte 209.165.200.227 présente un total de 16 vulnérabilités :

- 1 vulnérabilité critique (en rouge)
- 1 vulnérabilité moyenne (en orange)
- 14 vulnérabilités faibles (en bleu)

5- Vulnérabilité SSL : Certificat Non Fiable

MEDIUM SSL Certificate Cannot Be Trusted >

Description

The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below :

- First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.

- Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.

- Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.

If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host.

Solution

Purchase or generate a proper SSL certificate for this service.

Le certificat SSL du serveur ne peut pas être approuvé pour trois raisons possibles :

1.Certificat auto-signé ou non reconnu par une autorité de certification.

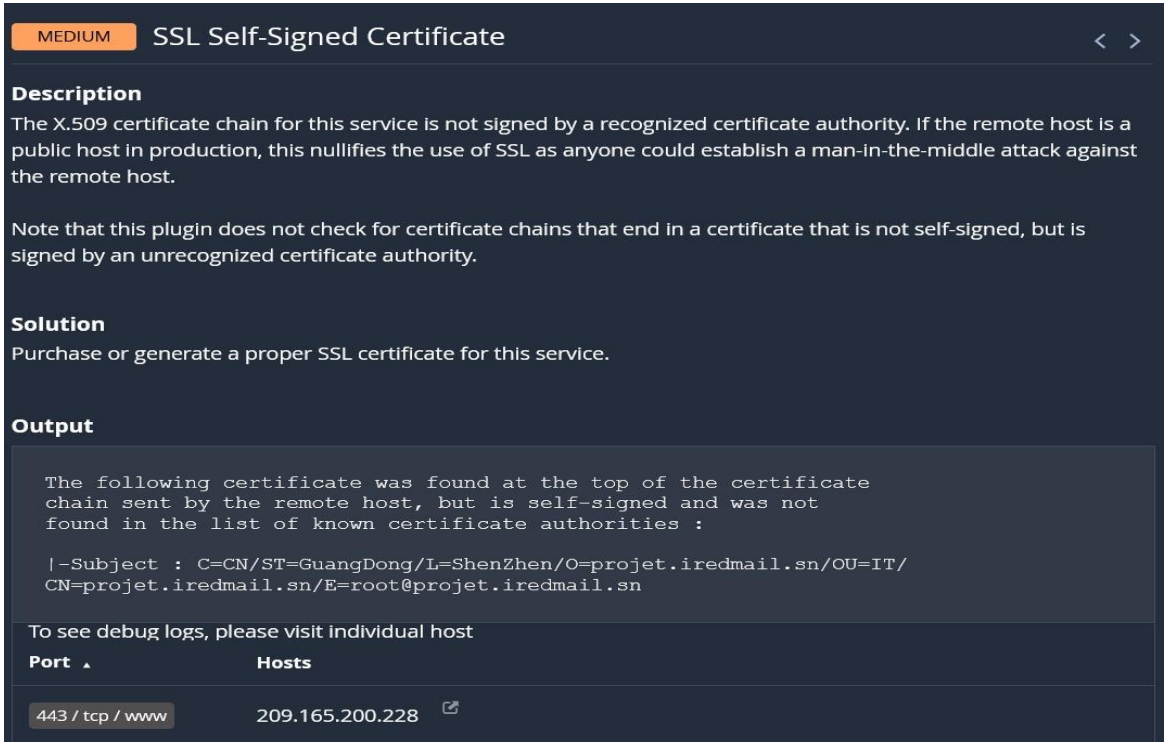
2.Certificat expiré ou non encore valide.

3.Signature non vérifiable ou incorrecte.

Solution : Remplacer le certificat par un SSL valide émis par une autorité reconnue.

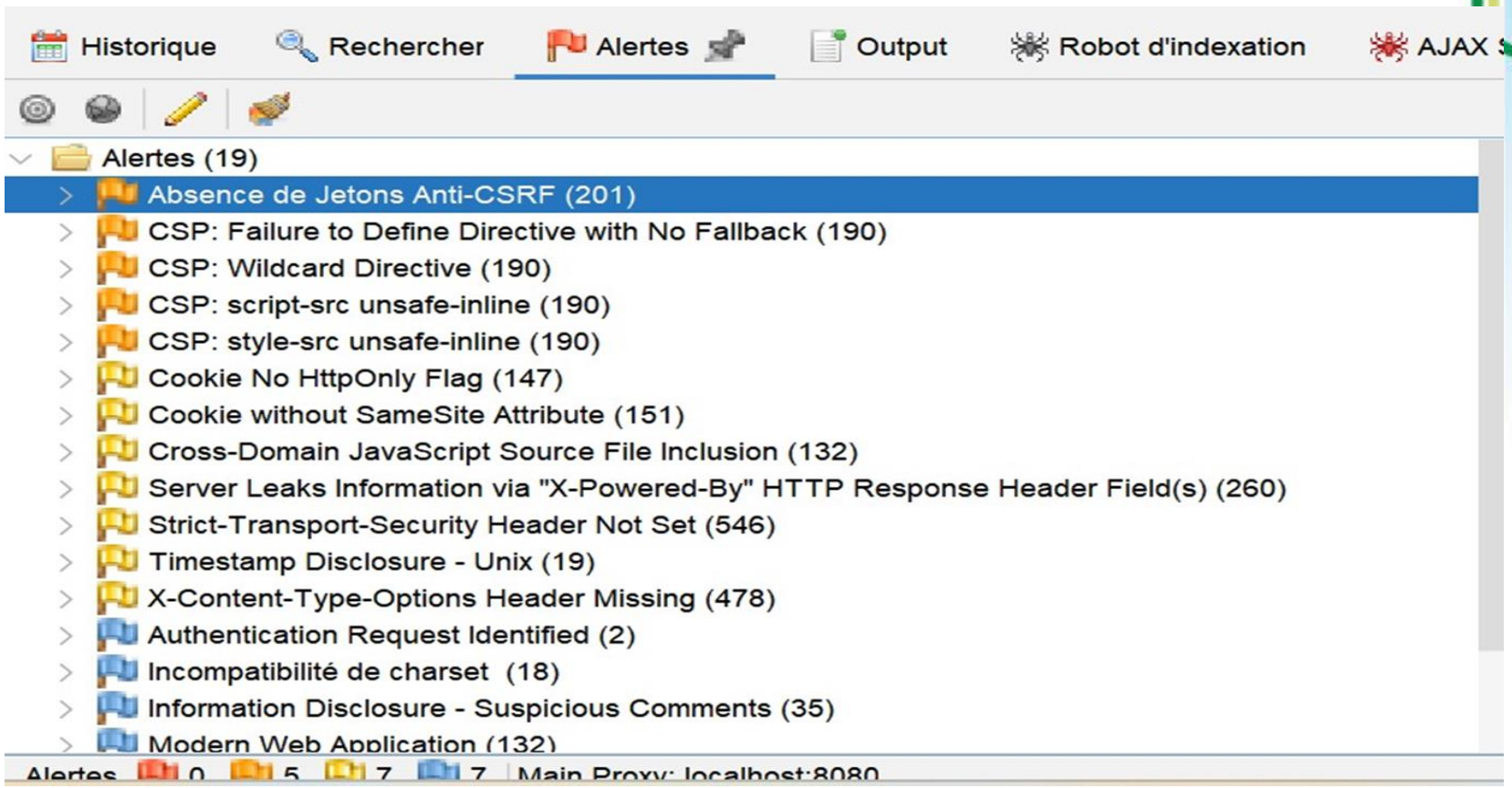
.

6. Vulnérabilité SSL : Certificat Auto-Signé Non Reconnue



Un certificat SSL auto-signé a été détecté pour le service sur le port 443 (IP : 209.165.200.228). Ce certificat n'a pas été émis par une autorité de certification reconnue, ce qui peut exposer le service à des attaques de type "man-in-the-middle".

Solution : Remplacer le certificat auto-signé par un certificat SSL valide et reconnu


Historique
Rechercher
Alertes
Output
Robot d'indexation
AJAX
Alertes (19)
Absence de Jetons Anti-CSRF (201)
CSP: Failure to Define Directive with No Fallback (190)
CSP: Wildcard Directive (190)
CSP: script-src unsafe-inline (190)
CSP: style-src unsafe-inline (190)
Cookie No HttpOnly Flag (147)
Cookie without SameSite Attribute (151)
Cross-Domain JavaScript Source File Inclusion (132)
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s) (260)
Strict-Transport-Security Header Not Set (546)
Timestamp Disclosure - Unix (19)
X-Content-Type-Options Header Missing (478)
Authentication Request Identified (2)
Incompatibilité de charset (18)
Information Disclosure - Suspicious Comments (35)
Modern Web Application (132)
Alertes
0
5
7
7
Main Proxy: localhost:8080

Analyse des Vulnérabilités du Système

La page affiche un ensemble de 19 alertes de sécurité, comprenant :

- **201 occurrences** d'absence de jetons Anti-CSRF.
- **190 occurrences** de directives CSP non définies ou avec des configurations risquées (unsafe-inline, wildcard).
- **147 occurrences** de cookies sans le flag HttpOnly.
- **546 occurrences** de l'absence de l'en-tête Strict-Transport-Security.
- **478 occurrences** de l'absence de l'en-tête X-Content-Type-Options.
- **260 occurrences** de fuites d'informations via l'en-tête X-Powered-By.
- Autres alertes : Incompatibilité de charset, inclusion de fichiers JavaScript externes, divulgation de timestamp Unix, etc.

Analyse des vulnérabilités

Tout d'abord , le site ne possède pas de protection contre les attaques CSRF (Cross-Site Request Forgery). Cela signifie qu'un attaquant pourrait inciter un utilisateur connecté à exécuter une action à son insu, comme changer son mot de passe ou effectuer un transfert, simplement en visitant une page piégée.
Ensuite , la politique de sécurité de contenu (Content Security Policy – CSP) est mal configurée. Elle autorise les scripts et styles en ligne via les directives unsafe-inline, ce qui facilite les attaques par injection de scripts (XSS). De plus, l'usage de l'astérisque (*) dans les directives CSP permet le chargement de ressources depuis n'importe quelle origine, ce qui réduit considérablement le niveau de sécurité du site. Les cookies utilisés ne sont pas correctement sécurisés.
Enfin , l'absence du drapeau HttpOnly permet à des scripts JavaScript d'y accéder, ce qui est dangereux en cas d'injection XSS. L'attribut SameSite est également absent, ce qui signifie que les cookies peuvent être envoyés avec des requêtes provenant d'autres sites, rendant le site vulnérable aux attaques CSRF.
Des scripts sont chargés depuis des domaines externes. Si l'un de ces domaines est compromis, il pourrait injecter du code malveillant dans le site. Cela accroît le risque global pour les utilisateurs.

VOLET ORGANISATIONNEL

CONSTATS & RECOMMANDATIONS - AUDIT ORGANISATIONNEL

Niveau de criticité	**Constat 01** Carence en politiques et procédures de gouvernance SI
Extrême	NETCORE SOLUTION ne dispose pas de plan de continuité d'activités (PCA), son plan de reprise d'activités (PRA) n'est pas formalisé
Majeur	
Modéré	
Mineur	

Risques
L'absence de Plan de Continuité d'Activités (PCA), malgré un Plan de Reprise d'Activités (PRA), expose NETCORE SOLUTION à des risques de désorganisation, d'interruption prolongée des services et de non-responsivité face aux crises. Le PRA pourrait être inefficace sans une stratégie claire pour maintenir les activités critiques avant son déclenchement, ce qui compromet la résilience de l'organisation.

Recommandations
Il est recommandé de formaliser un Plan de Continuité d'Activités (PCA) complémentaire au PRA, en identifiant les activités critiques, en établissant des priorités et en définissant des procédures claires pour maintenir la continuité des services avant la mise en œuvre du PRA. Des tests réguliers doivent être réalisés pour valider l'efficacité du PCA et du PRA ensemble.

CONSTATS & RECOMMANDATIONS - AUDIT ORGANISATIONNEL

Niveau de criticité	Auto-certification SSL en Environnement Local
Extrême	Certains services du réseau local utilisent des certificats SSL/TLS autosignés, ce qui entraîne l'affichage d'alertes de sécurité sur les navigateurs des utilisateurs et l'absence de validation par une autorité de certification reconnue.
Majeur	
Modéré	
Mineur	

Risque

Risques accrus de man-in-the-middle (MITM)

- Sans validation par une autorité tierce, un attaquant pourrait facilement usurper un certificat et intercepter des communications.
- Les certificats autosignés ne bénéficient pas d'un processus de renouvellement automatique.

Incompatibilité avec certains services ou clients

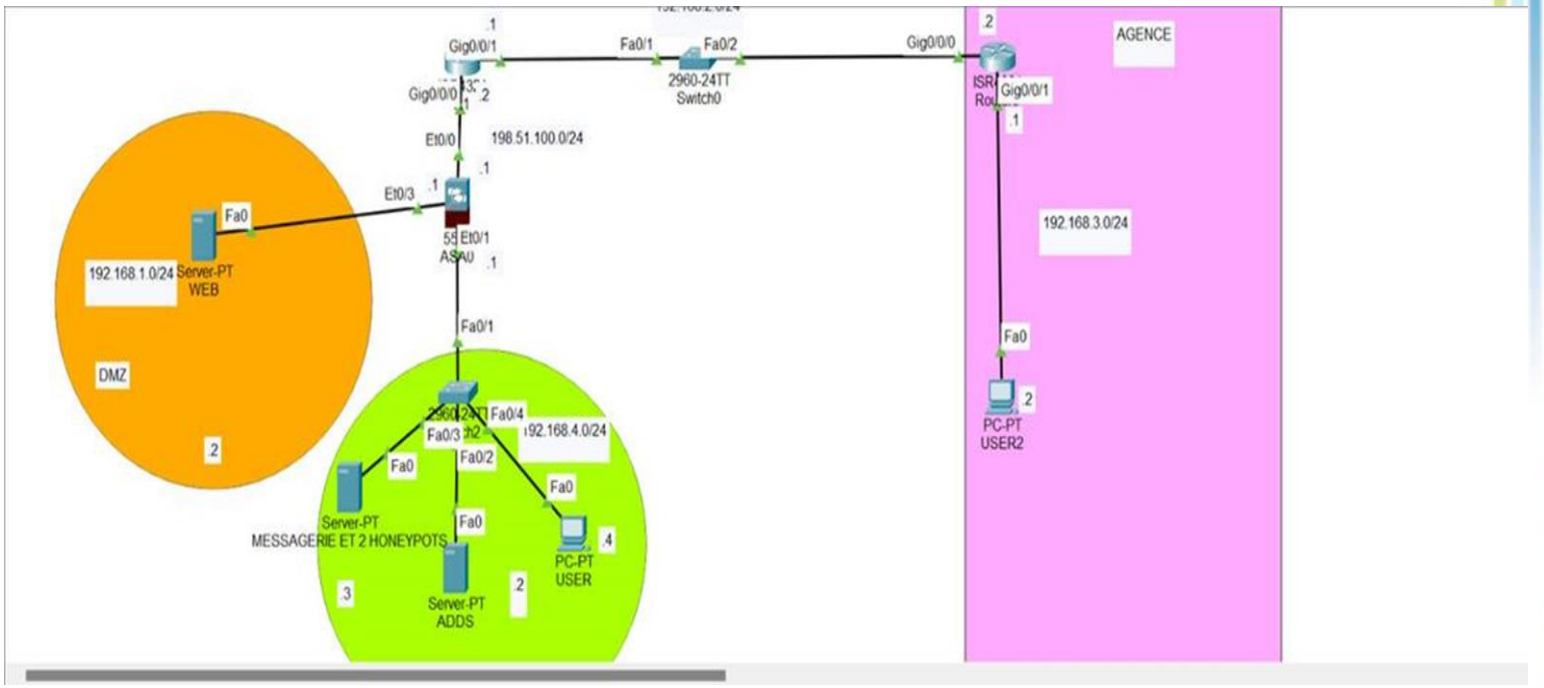
- Certaines applications ou API refusent de se connecter à des services utilisant des certificats non validés.

Recommandations

- Mettre en place une autorité de certification interne (PKI privée).
- Sécuriser les clés privées et limiter leur accès.
- Distribuer le certificat racine aux clients pour éviter les alertes.
- Passer à une autorité reconnue (ex : Let's Encrypt) si le service est accessible depuis l'extérieur.
- Renouveler les équipements obsolètes par des matériels compatibles avec le support et les mises à jour de sécurité

Volet Réseau

Description de l ’architecture



L’architecture réseau repose sur un pare-feu ASA, deux routeurs (R1 et R2), et deux switches d’accès (SWITCH-INSIDE, SWITCH-AGENCY). La segmentation réseau est organisée en trois zones : LAN interne, DMZ, et agence distante. Le firewall ASA est bien configuré avec des interfaces distinctes pour inside, outside et dmz, avec traduction d’adresses NAT. Les VLANs sont utilisés, et la sécurité des switches est renforcée (port-security, DHCP snooping, BPDU guard, etc.).

CONSTATS & RECOMMANDATIONS - AUDIT RESEAU

Niveau de criticité :

- ○ Extrême
- ● Majeur
- ○ Modéré
- ○ Mineur

Constat 00: Analyse de l'architecture réseau et des dispositifs de sécurité interzones

Ainsi , plusieurs points d'alerte sont relevés :

- Absence de routage dynamique entre les sites (tout est en statique).
- Absence de redondance des liens : tout repose sur un chemin unique.
- Le serveur web en DMZ (192.168.1.2) est exposé publiquement via une NAT statique, sans WAF ni proxy de sécurité.

RISQUES

- Risque de panne réseau majeure en cas de coupure d'un lien ou d'un équipement, faute de redondance.
- Risque d'attaque externe sur le serveur web exposé directement sans filtrage applicatif.

Recommandations

1.Mettre en place un routage dynamique sécurisé (OSPF avec authentification ou EIGRP) pour faciliter la gestion des routes entre R1, R2 et ASA.

2 .Ajouter des liens de redondance ou utiliser des protocoles de basculement (HSRP/VRRP) pour assurer la haute disponibilité.

3 .Déployer un WAF ou un reverse proxy devant le serveur web pour inspecter le trafic HTTP/HTTPS avant exposition.

VOLET APPLICATIF

CONSTATS & RECOMMANDATIONS - AUDIT APPLICATIF

Niveau de criticité

- ○ Extrême
- ● Majeur
- ○ Modéré
- ○ Mineur

Constat 00:Évaluation de l'exposition et de la sécurité des services applicatifs

L'architecture héberge plusieurs services applicatifs critiques :

•Serveur Web (SRV-WEB – 192.168.1.2) en DMZ, exposé à l'extérieur via une NAT statique (209.165.200.227)

•Serveur de messagerie (SRV-MSG – 192.168.4.3) et Contrôleur de domaine Active Directory (SRV-ADDS – 192.168.4.4) en réseau interne, eux aussi exposés via NAT statique

.•Aucune indication de pare-feu applicatif (WAF).

•Il n'est pas précisé si les services web ou mails utilisent des connexions chiffrées (HTTPS, SMTPS, LDAPS).

•Les serveurs critiques semblent hébergés sur Windows 11, un système non recommandé pour des services de production.

Risques

•Exposition directe d'applications critiques à Internet sans protection applicative (serveur web, messagerie, AD).

•Absence de chiffrement potentiel des flux applicatifs sensibles (HTTP, SMTP, LDAP), favorisant les attaques par interception.
•Hébergement non conforme (Windows 11 au lieu de Windows Server), augmentant le risque de failles ou d'instabilité.
•Risque d'exploitation des services exposés (ex : faille CVE sur IIS, failles RPC/LDAP sur AD).
•Manque de supervision : absence de détection en temps réel en cas de compromission applicative.

Recommandations

1.Déployer un WAF (Web Application Firewall) devant le serveur web (mod_security, Azure WAF, FortiWeb…).
2.Migrer les serveurs critiques vers des OS serveur (ex : Windows Server 2019/2022 pour l'ADDS et la messagerie).
3.Activer le chiffrement SSL/TLS sur tous les services exposés (HTTPS, SMTPS, LDAPS).
4. Limiter les accès applicatifs via des ACLs, des firewalls applicatifs et des listes blanches IP.
5 Mettre en place un système de supervision applicative (ex : Zabbix, Nagios, ELK stack) pour surveiller en temps réel les anomalies
6.Effectuer des tests de vulnérabilités réguliers avec des outils comme OWASP ZAP, Nessus ou OpenVAS pour identifier les failles dans les applications hébergées.

VOLET SYSTEME

CONSTATS & RECOMMANDATIONS - AUDIT SYSTÈME

Niveau de criticité	Constat 00:Audit des systèmes d'exploitation et de l'environnement serveur
Extrême	Les serveurs hébergeant les services critiques (Web, ADDS, Messagerie) sont installés sur des machines Windows 11, système orienté poste client. Le système utilise **Windows Server 2012**, une version **obsolète** et **non sécurisée** car plus supportée par Microsoft. Cette situation expose le serveur à des **failles non corrigées**. De plus, des **incohérences de configuration** sont présentes, notamment autour de PowerShell, et l'**accès à distance désactivé** complique l'administration. Une **mise à niveau** est indispensable.
Majeur	
Modéré	
Mineur	

Risques

- Système d'exploitation inadapté : Windows 11 n'est pas conçu pour héberger des services réseau critiques (pas de support serveur étendu, pas de services AD/DNS/DHCP intégrés nativement de manière sécurisée).
- Exposition aux vulnérabilités : l'usage d'un système client pour des services critiques favorise l'exploitation de failles non corrigées ou de configurations par défaut.
- Absence de durcissement : pas de contrôle d'accès renforcé, pas d'antivirus ou d'EDR professionnel.
- Risque d'instabilité ou de panne lors des mises à jour automatiques ou de sessions utilisateur non contrôlées
- Persistance et traçabilité faibles : malgres de logs système centralisés, pas de solution SIEM ou de suivi en cas d'incident

Recommandations

Procéder à une **mise à niveau vers une version récente de Windows Server** (2019 ou 2022) pour garantir le support et les mises à jour de sécurité. Corriger les **incohérences de configuration** (exécution PowerShell) et rétablir l'**accès à distance sécurisé** pour les administrateurs via un contrôle d'accès strict et l'authentification réseau (NLA).

AUDIT PHYSIQUE

SECURITE PHYSIQUE

L’audit de la sécurité Physique consiste à évaluer les conditions physiques et environnementales dans lesquelles sont exploités les équipements informatiques critiques, notamment dans les salles serveurs ou datacenters. Il examine les risques liés à la température, à l’humidité, à la poussière, aux champs électromagnétiques, aux vibrations, ainsi qu'aux sinistres tels que les incendies, inondations ou coupures électriques. L’audit vérifie également la présence et l’efficacité des dispositifs de détection et de protection (climatisation, onduleurs, systèmes anti-incendie, générateurs de secours, etc.). L’objectif est d’assurer la continuité de service et la préservation des données face aux aléas environnementaux.

LUMIERE

MAINTENANCE

HYGIENE

CONSTATS & RECOMMANDATIONS - AUDIT SECURITE PHYSIQUE

Niveau de criticité

- ○ Extrême
- ● Majeur
- ○ Modéré
- ○ Mineur

Constat 01:Conditions inadaptées à la préservation des équipements

- Un seul climatiseur placé à l'entrée, insuffisant pour les équipements situés au fond.
- Entretien insuffisant, accumulation de poussière risquant d'endommager le matériel.
- L'humidité dégrade les équipements et laisse des marques visibles sur les murs.

Évidences & captures

Impacts /Conclusion

Risque de Surchauffe des équipements
réduction de la durée de vie des équipements

Recommandations

- Netcore-solution devrait faire l'installation d'un système de climatisation approprié au moins deux climatiseurs dans la salle ,
- faire une surveillance de la température de l'humidite et une maintenance régulière.

CONSTATS & RECOMMANDATIONS - AUDIT PHYSIQUE

Niveau de criticité :

- Extrême
- Majeur
- Modéré
- Mineur

Constat 02:La salle présente des conditions inadéquates pour la sécurité et la protection des équipements

La salle serveurs présente plusieurs **défauts d'aménagement critiques** : elle ne dispose **d'aucune issue de secours**, l'**accès y est libre**, ce qui compromet la sécurité physique, et **aucune barrière anti-inondation** n'est en place. Cela augmente fortement le **risque d'infiltration d'eau** en cas d'incident, mettant en danger l'intégrité des équipements.

Évidences & captures

Impacts /Conclusion

-Menace d'infiltration d'eau.

-Non-conformité aux réglementations

-Non-respect des normes en vigueur.

Recommandations

- Mettre en place une barrière anty inondation
- l'installation d'issue de secours,
- l'installation d'une alarme d'incendie.
- Elaborer un plan d'évacuation et former son personnel.

CONSTATS & RECOMMANDATIONS - AUDIT PHYSIQUE

Niveau de criticité :	**Désorganisation du câblage réseau menaçant la fiabilité et la sécurité des infrastructures**

- Extrême
- Majeur
- Modéré
- Mineur

L'environnement technique présente un **câblage désordonné et non étiqueté**, avec des équipements exposés et des fils **emmêlés ou non protégés**, ce qui complique la maintenance, **accroît le risque de déconnexion accidentelle** et constitue un **danger pour la sécurité électrique et physique** des installations.

Évidences & captures



Impacts /Conclusion

Non-conformité aux normes de sécurité
- Court-circuit
-Détérioration des câbles
-Difficulté de maintenance et de dépannage

Recommandations

- une maintenance régulière préventive,
- utiliser des gaines de protection ,
- faire un étiquetage des cables,
- faire une inspection régulière des équipements afin de retirer ceux hors service.

CONSTATS & RECOMMANDATIONS - AUDIT PHYSIQUE

Niveau de criticité	Constat 04:Installations électriques et protections lumineuses inadéquates
○ Extrême ● Majeur ○ Modéré ○ Mineur	L'environnement électrique est **mal entretenu** : l'**éclairage est non fonctionnel**, les **prises et le boîtier de distribution** sont en **état de dégradation**, et l'absence de **rideaux** expose les équipements à une **chaleur excessive** due aux **rayons solaires**, ce qui peut nuire à leur bon fonctionnement.

Évidences & captures

Impacts /Conclusion

- Inexistence d'un groupe électrogène pour assurer la reprise après coupure
- Pas d'onduleurs pour assurer la continuité de la fourniture d'électricité jusqu'aux appareils si la panne de courant persiste
- Non isolation du boitier de distribution électrique

Recommandations

- Installez des onduleurs pour assurer une alimentation ininterrompue en cas de coupure de courant. Les onduleurs doivent être dimensionnés pour prendre en charge tous les équipements critiques pendant une période raisonnable.
- Mise en place d'un groupe électrogène de secours
- Isoler le boitier de distribution électrique
- Remplacer les lampes non fonctionnelles
- Mise en conformité du boitier de distribution électrique avec un couvercle sécurisé

Architecture Réseau

CONSTATS & RECOMMANDATIONS - ARCHITECTURE RESEAU

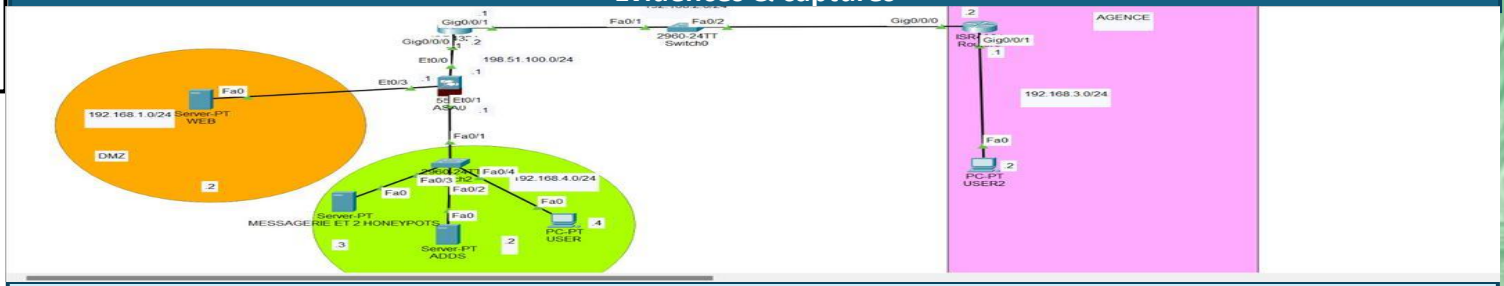
Niveau de criticité

- Extrême
- Majeur
- Modéré
- Mineur

Constat 01:ARCHITECTURE RESEAU NON HIERARCHISEE ET SEGMENTATION INSUFFISANTE

L'architecture réseau observée ne respecte pas le modèle hiérarchique en trois couches (accès, distribution, cœur) recommandé pour les infrastructures professionnelles. Le switch principal remplit plusieurs rôles (accès et interconnexion), aucune couche de distribution n'est identifiée, et le cœur de réseau est inexistant. Par ailleurs, la segmentation entre les différentes zones fonctionnelles (DMZ, LAN interne, agence, honeypots, serveurs critiques) est insuffisante ou mal isolée. Certains éléments sensibles, comme les honeypots et le contrôleur de domaine (ADDS), partagent le même réseau local, augmentant le risque d'exposition interne. La centralisation excessive du routage et de la sécurité sur l'ASA et le routeur sans redondance limite la résilience du réseau

Évidences & captures



RISQUES

Manque de scalabilité et de performance à moyen/long terme.

- Faible tolérance aux pannes (point de défaillance unique).
- Risque d'attaques latérales entre segments insuffisamment isolés.
- Exposition de ressources critiques (ex. : serveur AD) à des zones à haut risque (ex. : honeypots)..

Recommandations

2

Implémenter une architecture hiérarchisée avec des couches distinctes (accès, distribution, cœur).
Introduire un switch de distribution pour gérer le routage inter-VLAN, les ACLs, et les politiques de sécurité. Créer une couche cœur redondante pour améliorer la performance et la disponibilité. Renforcer la segmentation réseau via des VLANs bien définis, des ACLs adaptées, et une DMZ isolée pour les services exposés. Séparer les honeypots des serveurs critiques pour éviter tout impact interne en cas d'attaque.

EQUIPEMENTS

CONSTATS & RECOMMANDATIONS - AUDIT EQUIPEMENT

Niveau de criticité :

- ○ Extrême
- ● Majeur
- ○ Modéré
- ○ Mineur

Constat 01:switches obsoletes sans support cisco (Cisco 2960)

L'organisation a utilisé 2 switch niveau 2 modèle 2960 **.** Les commutateurs Cisco 2960 ont tous atteint la fin de commercialisation et de prise en charge de Cisco . Cela signifie qu'ils ne sont plus disponibles à la vente et que Cisco ne fournit plus de support technique pour ces produits .

Évidences & captures

Last Date of Support: HW	The last date to receive applicable service and support for the product as entitled by active service contracts or by warranty terms and conditions. After this date, all support services for the product are unavailable, and the product becomes obsolete.	October 31, 2019

Impacts /Conclusion

Les commutateurs Cisco 2960 présentent des risques de sécurité car ils ne sont plus pris en charge par Cisco, ne recevant ainsi plus de mises à jour de sécurité, avec des vulnérabilités connues non corrigées, exposant à des risques d'attaques par déni de service, intrusion et vol de données.

Recommandations

Mettre à niveau les commutateurs vers des modèles plus récents pris en charge par Cisco.

CONSTATS & RECOMMANDATIONS - AUDIT EQUIPEMENT

Niveau de criticité

- Extrême
- Majeur
- Modéré
- Mineur

Constat 02:Etude d'obsolescence du ASA 5505

L'organisation utilise un pare-feu Cisco ASA 5505, un modèle de la série Adaptive Security Appliance (ASA). Cet équipement est physiquement en service, comme l'indiquent les voyants lumineux actifs (Power, Status, Active, VPN). Cependant, il est important de noter que ce modèle est obsolète. Cisco a officiellement annoncé l'arrêt de commercialisation et de support du modèle ASA 5505 le 25 août 2017 (réf. EOL11376). De plus, les dernières mises à jour logicielles ne sont plus disponibles pour cette plateforme, ce qui signifie que les failles de sécurité découvertes après cette date ne sont pas corrigées .

Évidences & captures

Étapes de fin de vie

Tableau 1. Étapes et dates de fin de vie du dispositif de sécurité adaptatif Cisco ASA 5505

Jalon	Définition	Date
Date d'annonce de fin de vie	Date à laquelle le document annonçant la fin de commercialisation et la fin de vie d'un produit est distribué au grand public.	24 février 2017

Impacts /Conclusion

Le maintien en production d'un équipement de sécurité réseau obsolète expose l'organisation à des risques accrus :

- Absence de correctifs de sécurité en cas de vulnérabilités critiques
- Failles exploitables pouvant entraîner des attaques par (Dos), des intrusions ou des fuites de donnée.

Recommandations

Remplacer le pare-feu Cisco ASA 5505 par un modèle plus récent encore supporté par Cisco (par exemple ASA 5506-X ou Firepower) ou migrer vers une solution UTM (Unified Threat Management) adaptée aux besoins actuels de sécurité de l'organisation.

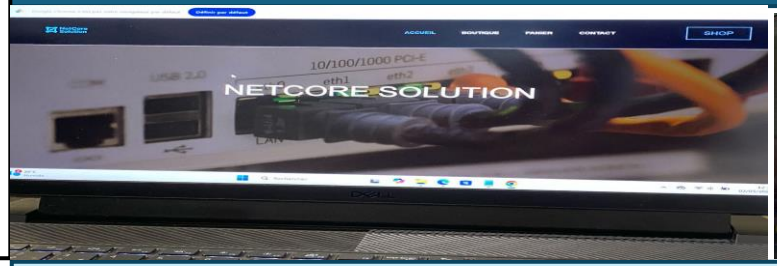
CONSTATS & RECOMMANDATIONS - AUDIT EQUIPEMENT

Niveau de criticité:	**Constat 03:Serveur web hébergé sur une machine inadaptée à un environnement de production.**

- Extrême
- Majeur
- Modéré
- Mineur

Le serveur Web (ex. IIS, Apache, XAMPP) est hébergé sur un poste de travail Windows 11, système conçu principalement pour un usage client. La machine semble exposée à Internet ou accessible via le réseau local. Aucune mention explicite de durcissement du système ou d'environnement virtualisé dédié n'a été faite.

Évidences & captures



RISQUES

Surface d'attaque élargie : Windows 11 exécute par défaut de nombreux services non essentiels au rôle de serveur.

- Manque de durcissement : absence probable de configuration de sécurité serveur (GPO, firewall renforcé, désactivation des ports/services inutiles).
- Exposition à des failles client : vulnérabilités Windows 11 (ex. SmartScreen, Shell, pilotes) peuvent compromettre l'ensemble de la machine.
- Confusion des rôles : risque d'avoir un mélange d'usage personnel/utilisateur et d'hébergement (navigation, e-mail, stockage)

Recommandations

- Migrer vers un OS serveur dédié (ex. Windows Server ou Linux) dans un environnement sécurisé OU alors:
- Désactiver tous les services inutiles via services.msc.
- Configurer le pare-feu Windows avec des règles strictes (seulement les ports Web ouverts).

CONSTATS & RECOMMANDATIONS - AUDIT EQUIPEMENT

Niveau de criticité

- Extrême
- Majeur
- Modéré
- Mineur

Constat 03:Routeurs désorganisés, non protégés et obsolètes, compromettant la fiabilité du réseau

Etat: Les routeurs sont dans un mauvais état. Ils sont couverts de poussière, les câbles sont emmêlés et certains sont maintenus avec du ruban adhésif, sans support ni étiquettes, ce qui complique toute intervention et peut provoquer des erreurs de branchement, Certains câbles sont abimés et bricolés, ce qui risque de couper le signal ou de créer des interférences. Enfin, ces équipements sont posés sur un bureau non ventilé et ne sont pas protégés dans un rack, les exposant aux chocs et aux pannes, de plus, leur modèle Cisco 2901 est en fin de vie, sans mises à jour ni pièces de rechange.

Évidences & captures

Étape	Définition	Date
Date d'annonce de fin de vie	Date à laquelle le document annonçant la fin de commercialisation et la fin de vie d'un produit est diffusé au grand public.	9 septembre 2016

Impacts /Conclusion

- Risque de panne et d'interruption de service
- Dégradation de la qualité de connexion supérieures
- Allongement des délais d'intervention
- Vulnérabilités accrues
- Coûts de support et de renouvellement

Recommandations

- Nettoyer régulièrement les routeurs et leurs grilles d'aération pour éviter la surchauffe.
- Organiser les câbles avec des goulottes, des attaches Velcro et des étiquettes pour faciliter les interventions.
- Remplacer les câbles abimés par des modèles aux normes.
- Installer chaque routeur dans un rack ventilé et fermé pour le protéger.
- Prévoir le renouvellement des Cisco 2901 en fin de vie et suivre la température et la disponibilité du réseau.

CONSTATS & RECOMMANDATIONS - AUDIT EQUIPEMENT

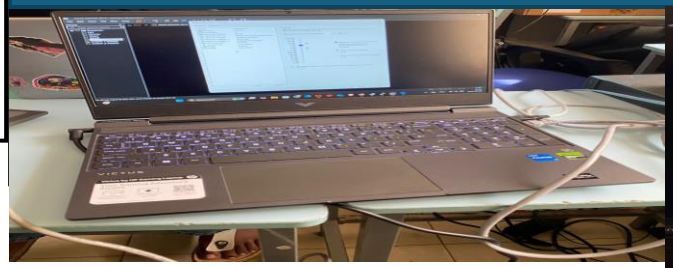
Niveau de criticité

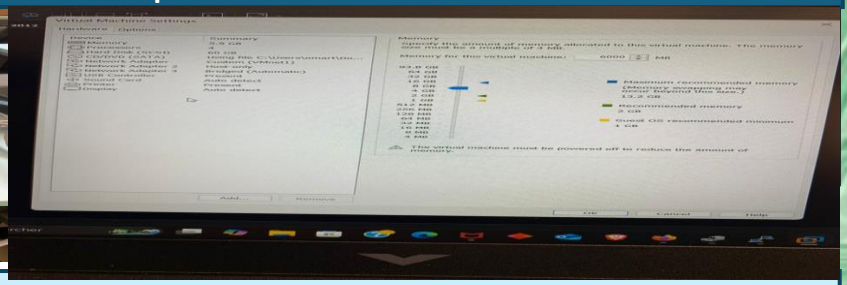
- ○ Extrême
- ○ Majeur
- ● Modéré
- ○ Mineur

AUDIT 06:Serveur AD DS obsolète et insuffisamment sécurisé.

L'entreprise utilise un serveur virtuel sous Windows Server 2012, hébergé sur un ordinateur portable HP Victus via VMware. Ce serveur assure des services essentiels comme AD DS, DNS, DHCP et un serveur web. Bien que certaines mesures de sécurité soient présentes, comme le pare-feu et des sauvegardes régulières, l'absence d'antivirus et la fin de support du système d'exploitation posent un risque. De plus, aucune redondance ni supervision n'est en place, et aucun projet de migration n'a encore été lancé.

Évidences & captures





Impacts /Conclusion

Malgré son fonctionnement apparent ,L'environnement obsolète et insuffisamment protégé exposant l'entreprise à des risques élevés de sécurité, de non-conformité et d'interruption des services.

Recommandations

Il est recommandé de migrer vers une version récente de Windows Server, d'installer un antivirus, de moderniser le matériel ou passer à une solution cloud, et de mettre en œuvre des outils de supervision, de redondance et un plan de continuité. Un effort de mise en conformité réglementaire doit également être engagé.

CONFIGURATIONS

CONSTATS & RECOMMANDATIONS - AUDIT configuration

Niveau de criticité :

- ○ Extrême
- ● Majeur
- ○ Modéré
- ○ Mineur

Constat 03: Analyse des failles de Sécurité Techniques et organisationnelles dans l'architecture Réseau de l'Agence

Aucune mesure de sécurité technique (pas de VLAN /present seulement au niveau de l'asa ,) . Aucun dispositif de détection ou réaction aux incidents n'est prévu (IDS, supervision, alertes) . Le système d'exploitation adds utilise une version anterieur . Absence de redondance réseau .

Risque

L'architecture actuelle de l'agence ne répond pas aux exigences minimales de sécurité pour garantir la protection des données personnelles , telles que prévues par les textes en vigueur (notamment la loi numéro 2008-12 du Sénégal et les principes du RGPD) . L'absence de VLAN expose le réseau à des attaques internes et à un accès non contrôlé aux segments critiques. L'absence de dispositifs de détection et de réponse aux incidents empêche la surveillance en temps réel des menaces, augmentant ainsi le risque de compromission. De plus, l'utilisation d'un système d'exploitation obsolète expose le réseau aux vulnérabilités non corrigées, tandis que l'absence de redondance réseau crée un point de défaillance unique qui pourrait gravement affecter la disponibilité des services en cas de panne.

Recommandations

Mettre en place des VLANs pour isoler les segments critiques du réseau et limiter la propagation des menaces. Cela permettra de restreindre les mouvements latéraux des attaquants et de protéger les données sensibles conformément à la loi n° 2008-12 du Sénégal et au RGPD

CONSTATS & RECOMMANDATIONS - AUDIT configuration

Niveau de criticité

- Extrême
- Majeur
- Modéré
- Mineur

Constat 01: Règles de filtrage trop permissives sur le pare-feu ASA

Les règles de filtrage ASA autorisent :
- Le trafic TCP sortant sur les portsutilises .

Impacts /Conclusion

Les ports utilisés peuvent être exploités par des attaquants pour lancer des attaques ciblées sur des services spécifiques, exfiltrer des données en utilisant des protocoles légitimes, ou contourner les contrôles de sécurité en utilisant des ports autorisés pour des communications malveillantes. Ils peuvent également être scannés pour détecter des services vulnérables et servir de points d'entrée pour des attaques de commande et de contrôle.

Recommandations

-mettre en place des systèmes de détection pour identifier les comportements anormaux sur ces ports.

CONSTATS & RECOMMANDATIONS - AUDIT configuration

Niveau de criticité	Constat 05:LE SERVEUR WEB DANS LA DMZ EST EXPOSE VIA LE NAT STATIQUE
○ Extrême ● Majeur ○ Modéré ○ Mineur	Le serveur web (192.168.1.2) est accessible depuis l'extérieur via l'IP publique 209.165.200.227 avec une translation statique nat .
	Impacts /Conclusion
	Exposition directe aux attaques web (SQLi, XSS, etc.). - Risque d'exploitation en cas de faille non corrigée sur l'application ou le serveur
	Recommandations
	○ Protéger avec un WAF (Web Application Firewall). - Appliquer les dernières mises à jour de sécurité. - Surveiller les logs en temps réel.

CONSTATS & RECOMMANDATIONS – AUDIT configuration

Niveau de criticité	Constat 05: HONEYPOTS EXPOSES SANS SEGMENTATION NI JOURNALISATION RENFORCEE
○ Extrême ○ Majeur ● Modéré ○ Mineur	Les honeypots sont présents sur le réseau, mais il n'est pas mentionné de segmentation dédiée.
	Impacts /Conclusion
	Un attaquant peut compromettre le honeypot et pivoter vers d'autres équipements. - Données d'observation insuffisantes pour analyse post-attaque.
	Recommandations
	○ - Isoler les honeypots sur un VLAN dédié. . - Ajouter des alertes sur activités suspectes.

CONSTATS & RECOMMANDATIONS - AUDIT configuration

Niveau de criticité :	Constat 05: SERVEUR DE MESSAGERIE ACCESSIBLE DEPUIS INTERNET SANS FILTRAGE
○ Extrême ● Majeur ○ Modéré ○ Mineur	Le serveur de messagerie (192.168.4.3) est publié via NAT statique et accessible en HTTPS depuis Internet
	Impacts /Conclusion
	Surface d'attaque large : accès non chiffré, bruteforce, spam relay. - Risque de compromission des identifiants ou de l'intégrité du serveur.
	Recommandations
	○ Imposer TLS/SSL. - Filtrer par IP d'origine connue. - Activer la protection anti-relay et l'analyse antivirus/antispam.

CONSTATS & RECOMMANDATIONS - AUDIT configuration

Niveau de criticité :	Constat 05: Absence de protection contre le spoofing sur R1ET R2
○ Extrême ● Majeur ○ Modéré ○ Mineur	Les routeurs R1 et R2 n'utilisent pas de mécanismes comme Unicast Reverse Path Forwarding (uRPF) pour vérifier l'authenticité des adresses sources (utilisation ACL)
	Impacts /Conclusion
	L'absence de uRPF expose le réseau à des attaques par usurpation d'adresse IP, des amplifications DDoS, des interceptions de trafic et une faible traçabilité des incidents
	Recommandations
	Mettre en place le mécanisme **Unicast Reverse Path Forwarding (uRPF)** sur les routeurs R1 et R2 pour valider les adresses sources des paquets entrants et filtrer ceux dont les adresses sources ne correspondent pas aux routes connues, réduisant ainsi le risque d'attaques par usurpation d'adresse IP.

SYNTHESE

L’audit révèle que l’organisation dispose d’une politique de sécurité non conforme aux normes et d’un PRA, mais pas de PCA. Les incidents sont gérés via des GPO, sans programme clair de sensibilisation. La sécurité physique est basique, sans surveillance vidéo. Le réseau est segmenté et protégé par firewall et IDS, mais sans Wi-Fi ni redondance sur les switches. Les systèmes sont à jour partiellement, avec des règles GPO et Wordfence côté messagerie. Aucun service critique n’est hébergé en interne et les certificats sont autosignés. Les sauvegardes existent, mais aucune procédure de restauration n’est maîtrisée. Il n’y a ni SIEM ni conformité aux normes. Les mots de passe sont bien gérés, mais les équipements sont partiellement obsolètes. Enfin, les tests d’intrusion sont peu détaillés et la détection des attaques reste limitée.

RAPPORT EBIOS

Synthèse Atelier 1

Nom Societe: NETCORE SOLUTION

Mission: Vente d'équipements réseaux

Nature Valeur Metier: INFORMATION

Denomination Valeur Metier: Données commerciales (commandes, devis, factures)

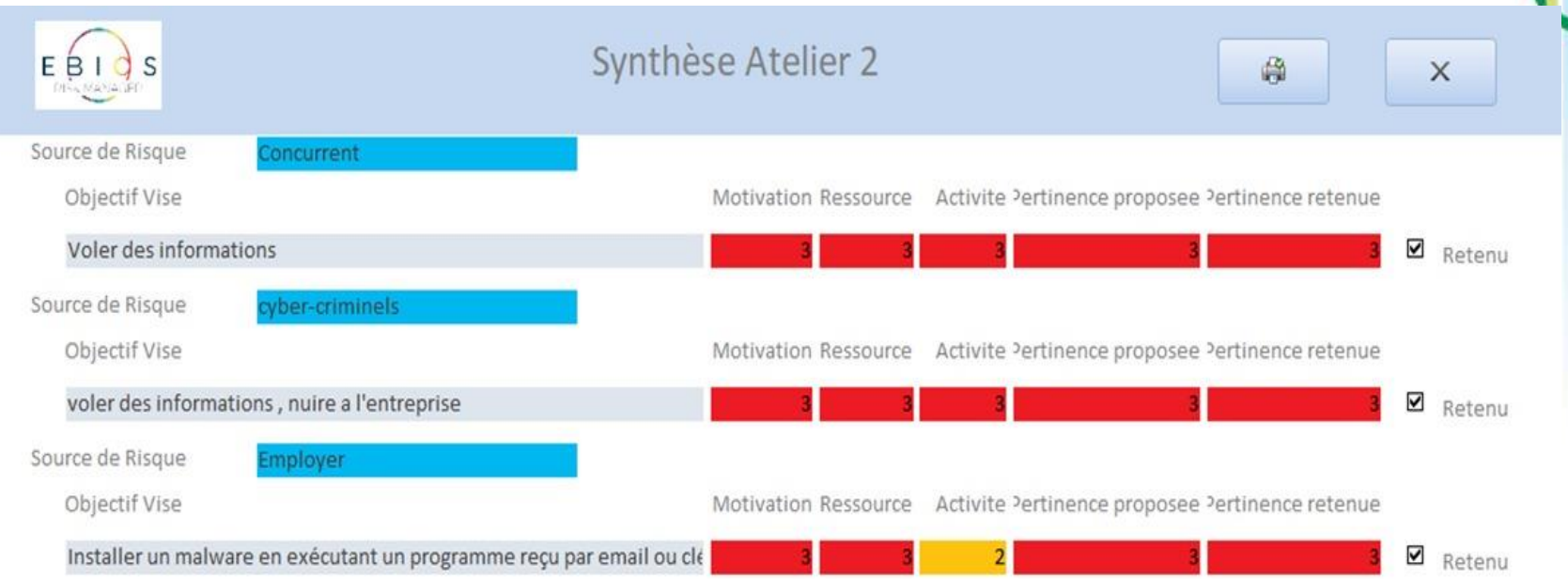
Denomination Bien Support Associe	Entite Personne Responsable	Evenement Redoute	Gravite
Base de données commerciale	RSSI	Fuite d'informations stratégiques (prix, contracts...)	4
Base de données commerciale	RSSI	Perte ou altération des données commerciales	3
Base de données commerciale	RSSI	Altération ou perte des documents	3
Serveur de fichiers	Responsable commercial	Fuite d'informations stratégiques (prix, contracts...)	4
Serveur de fichiers	Responsable commercial	Perte ou altération des données commerciales	3
Serveur de fichiers	Responsable commercial	Altération ou perte des documents	3

Denomination Valeur Metier: Données des clients

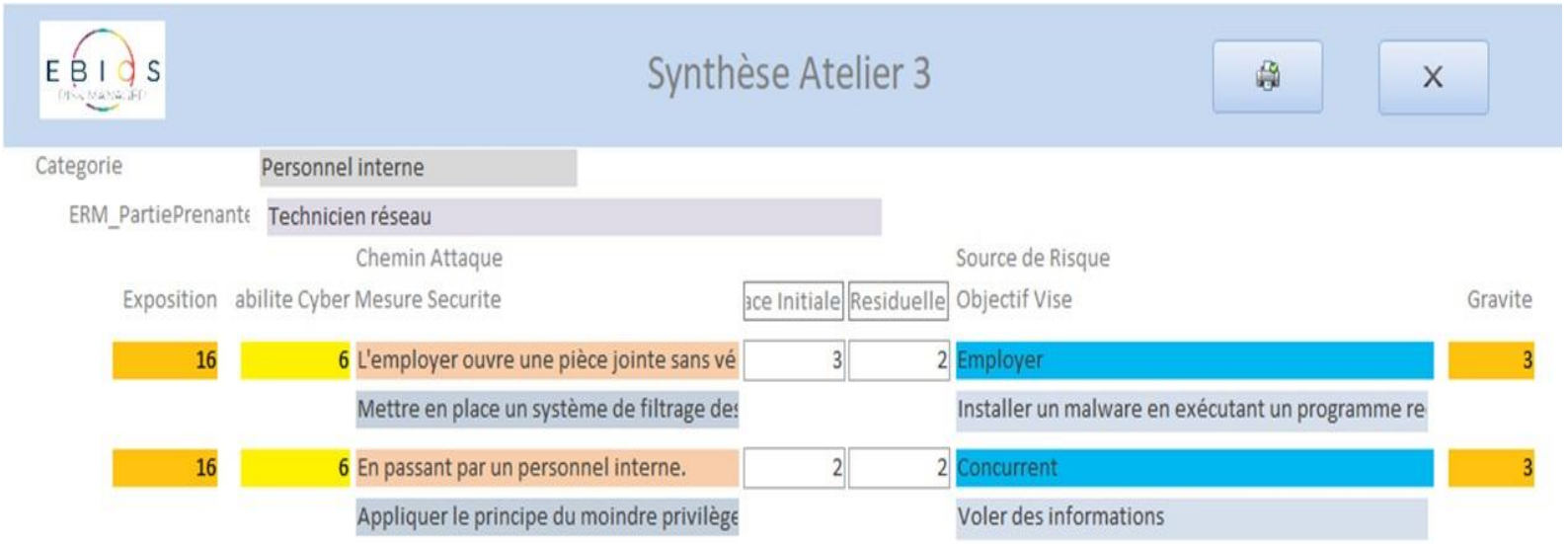
Denomination Bien Support Associe	Entite Personne Responsable	Evenement Redoute	Gravite
Serveur web	Responsable du serveur wet	Altération ou suppression des données	3
Serveur web	Responsable du serveur wet	Divulgation ou vol des données personnelles des clients	4
Base de données clients	RSSI	Altération ou suppression des données	3
Base de données clients	RSSI	Divulgation ou vol des données personnelles des clients	4

Nature Valeur Metier	PROCESSUS		
Denomination Valeur Metier	Disponibilité du site de vente en ligne		
Denomination Bien Support Associe	Entite Personne Responsable	Evenement Redoute	Gravite
Serveur web	Responsable du serveur wet	Piratage du site	4
Serveur web	Responsable du serveur wet	Indisponibilité du site (panne, attaque DDoS)	3

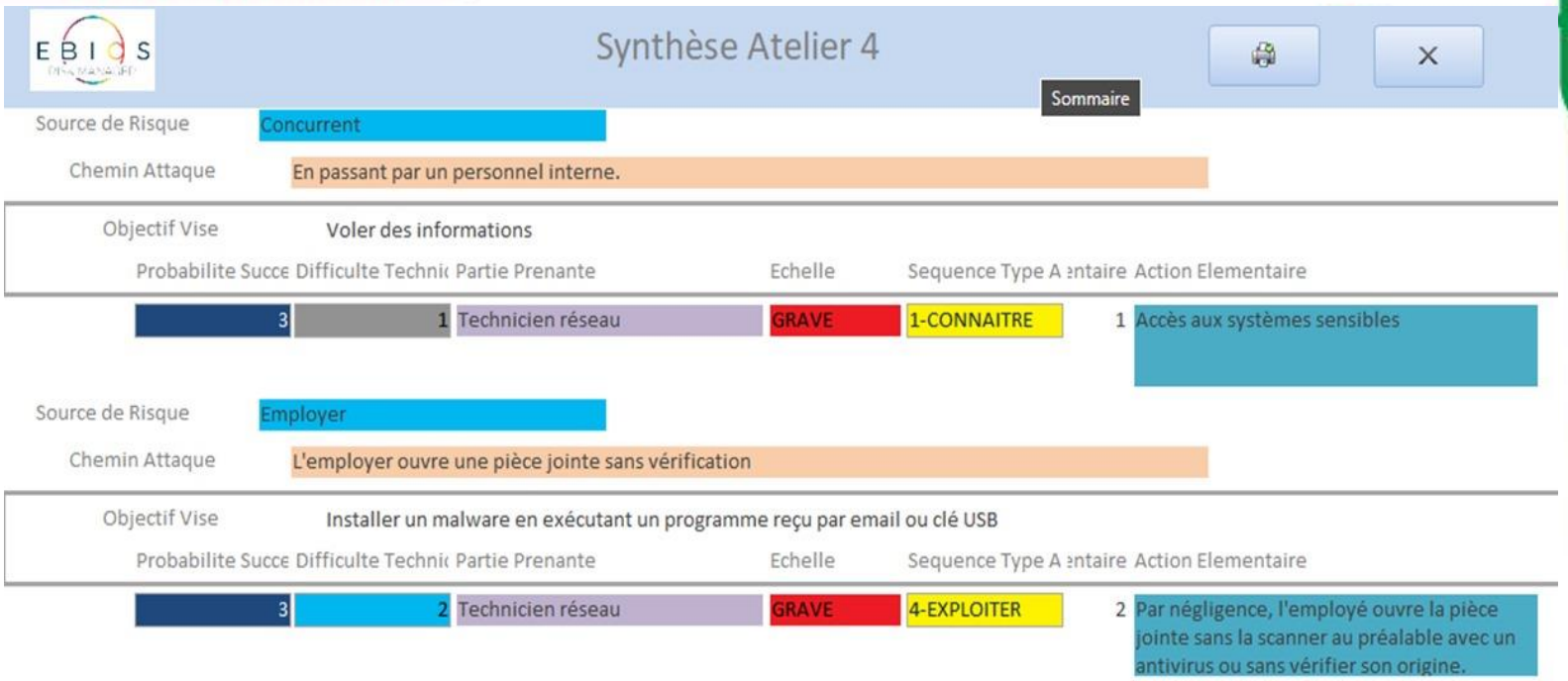
Atelier 1 – Cadrage et socle de sécurité:L'atelier 1 d'EBIOS RM, appelé "Cadrage et socle de sécurité", permet de poser les bases de l'analyse de risque. Il sert à définir le périmètre de l'étude, les valeurs métier à protéger (informations ou processus essentiels), ainsi que les événements redoutés pouvant les affecter. Cet atelier permet également d'évaluer le socle de sécurité existant, c'est-à-dire les protections déjà en place. C'est une étape stratégique qui oriente les ateliers suivants en ciblant les véritables enjeux de sécurité pour l'organisation.



Atelier 2 – Sources de risques et objectifs visés :Cet atelier permet à l'organisation :de se concentrer sur les scénarios les plus crédibles et dangereux ;d'éviter de se perdre dans des centaines de menaces improbables ;et surtout, de préparer les scénarios d'attaque concrets dans les prochains ateliers.



Atelier 3 – Scénarios stratégiques:L’objectif de cet atelier est de :Raconter comment l’attaque se déroulerait concrètement.Identifier les acteurs vulnérables de l’écosystème (ici, un technicien réseau interne).Évaluer la gravité si l’attaque aboutissait.Et surtout, proposer des premières mesures de sécurité pour briser la chaîne d’attaque.



Atelier 4 – Scénarios opérationnels:L'atelier 4 a pour objectif de décrire techniquement comment un attaquant pourrait réaliser les scénarios stratégiques définis précédemment. On y détaille les moyens concrets qu'il utiliserait (malware, phishing, exploitation de faille, etc.) pour compromettre un bien support et atteindre une valeur métier. Chaque scénario est évalué en termes de vraisemblance, ce qui permet de compléter l'analyse du risque en combinant gravité et probabilité.

Formation initiale

Type Mesure	DEFENSE									
Mesure Securite	Surveillance renforcée des flux entrants et sortants . Analyse des journaux d'évènements à l'aide d'un outil.									
omplexite	mois	Status	Responsat	Scenario	Source Risque	Objectif Vise	Valeur Metier	Gravite Residuel	raisemblance esiduel	
2	3	Terminé	equipe M	R1	Concurrent	Voler des informations	Données commerciales	3	2	
								3	2	
Type Mesure	PROTECTION									
Mesure Securite	Renforcement du contrôle d'accès physique au niveau du serveur de messagerie									
omplexite	mois	Status	Responsat	Scenario	Source Risque	Objectif Vise	Valeur Metier	Gravite Residuel	raisemblance esiduel	
2	3	Terminé	equipe M	R2	Employer	Installer un malware en exécutant	Disponibilité du site de	4	2	
								4	2	
Type Mesure	RESILIENCE									
Mesure Securite	Renforcement du plan de continuité d'activité									
omplexite	mois	Status	Responsat	Scenario	Source Risque	Objectif Vise	Valeur Metier	Gravite Residuel	raisemblance esiduel	
2	6	A lancer	RSSI	R2	Employer	Installer un malware en exécutant	Disponibilité du site de	4	2	
								4	2	

Atelier 5 – Traitement du risque: L'atelier 5 permet de prendre des décisions face aux scénarios de risque identifiés. On y établit une stratégie de traitement : réduire, éviter, transférer ou accepter le risque. Pour chaque scénario, on construit un plan d'action, avec des mesures de sécurité adaptées, des responsables désignés et un calendrier. Cet atelier aboutit à une vision claire et priorisée des actions de sécurité à mener, selon les enjeux et les ressources de l'organisation.

AUDIT TECHNIQUE

1- AUDIT SYSTEME ET RESEAU

CONSTATS & RECOMMANDATIONS - AUDIT ATTAQUE

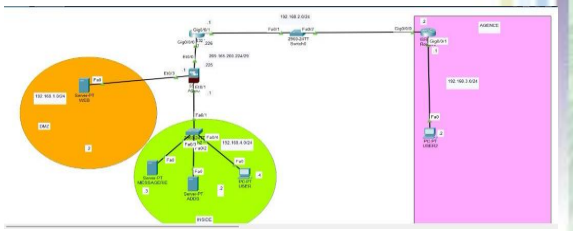
Niveau de criticité :

- ○ Extrême
- ● Majeur
- ○ Modéré
- ○ Mineur

Pare-feu basique : il est en place mais les règles sont trop générales.

La configuration actuelle du pare-feu est trop permissive, ne filtrant pas efficacement les flux réseau. Cela expose l'organisation à des risques d'intrusion et rend difficile la détection des activités suspectes.

Évidences & captures



Impacts /Conclusion

Impact : Risque d'intrusion externe, accès non autorisé entre les zones réseau, absence de détection des activités anormales.
Conclusion : La configuration actuelle ne permet pas de filtrer efficacement les flux ni de détecter des attaques, exposant le système à des compromissions.

Recommandations

Renforcer les règles avec des politiques plus strictes (filtrage par service, logs, détection d'intrusion…).

CONSTATS & RECOMMANDATIONS - AUDIT ATTAQUE

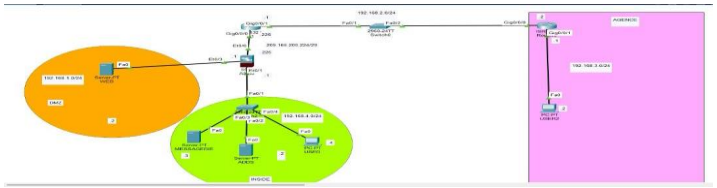
Niveau de criticité :

- ○ Extrême
- ● Majeur
- ○ Modéré
- ○ Mineur

Absence de solution IDS/IPS (système de détection/prévention d'intrusion)

Le réseau ne dispose d'aucun mécanisme pour détecter ou bloquer en temps réel les intrusions, laissant passer des attaques comme les scans ou les exploitations de vulnérabilités.

Évidences & captures



Impacts /Conclusion

Impact : Les attaques réseau passent inaperçues (scans, exploitation de failles).
Conclusion : Aucun système ne permet d'identifier ou bloquer les intrusions en temps réel.

Recommandations

Déployer une solution IDS/IPS (comme Snort, Suricata ou Zeek).

CONSTATS & RECOMMANDATIONS – AUDIT ATTAQUE

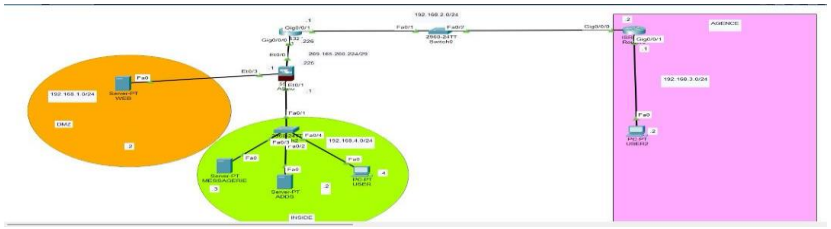
Niveau de criticité :

- ○ Extrême
- ○ Majeur
- ● Modéré
- ○ Mineur

Point de défaillance unique dans l'infrastructure utilisateur

Tous les utilisateurs sont connectés à un seul switch. En cas de panne matérielle, cela entraîne une coupure totale du réseau pour les utilisateurs.

Évidences & captures



Impacts /Conclusion

Impact : Coupure totale du réseau utilisateur en cas de panne matérielle.
Conclusion : Un point de défaillance unique existe, ce qui nuit à la disponibilité du service.

Recommandations

Ajouter un switch de secours pour assurer une redondance physique.

CONSTATS & RECOMMANDATIONS – AUDIT ATTAQUE

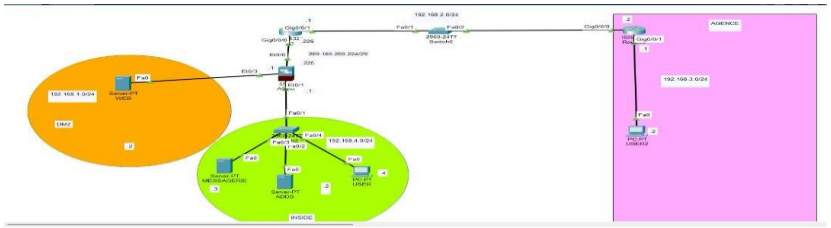
Niveau de criticité :

- ○ Extrême
- ○ Majeur
- ● Modéré
- ○ Mineur

Absence de commutateur dedie en DMZ

Il n'y a aucun commutateur pour isoler la zone DMZ. Cela augmente le risque de propagation d'attaques vers le réseau interne si un serveur exposé est compromis.

Évidences & captures



Impacts /Conclusion

Impact : Absence de segmentation expose l'infrastructure interne en cas de compromission du serveur web. Un attaquant pourrait potentiellement se deplacer lateralement vers d'autres parties de reseau interne.

Recommandations

Mettre en place un commutateur dans la DMZ pour permettre la segmentation en VLANs et un controle interne du traffic

CONSTATS & RECOMMANDATIONS – AUDIT ATTAQUE

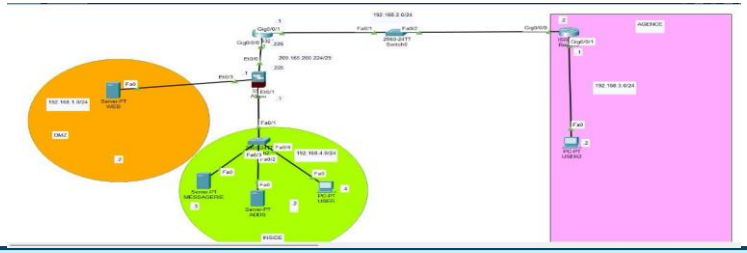
Niveau de criticité :

- ○ Extrême
- ○ Majeur
- ● Modéré
- ○ Mineur

Pas de gestion hors bande des équipements

En cas de panne réseau, il est impossible de gérer les équipements à distance car aucun accès alternatif (hors bande) n'est disponible.

Évidences & captures



Impacts /Conclusion

Impact : Impossible de gérer les équipements en cas de panne réseau.
Conclusion : Aucun accès alternatif n'est prévu pour l'administration en cas de coupure.

Recommandations

Ajouter une interface de gestion hors bande (ex: console out-of-band).

CONSTATS & RECOMMANDATIONS – AUDIT ATTAQUE

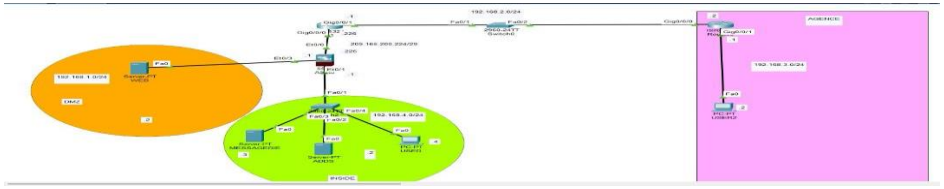
Niveau de criticité :

- ○ Extrême
- ● Majeur
- ○ Modéré
- ○ Mineur

FAI non documenté et absence de redondance WAN

Aucun détail sur le fournisseur d'accès Internet (nom, contrat, liaison, IP publique) n'est documenté. En cas de panne du fournisseur principal, aucun lien secondaire n'est prévu pour garantir la continuité de service.

Évidences & captures



Impacts /Conclusion

Impact : Coupure Internet/WAN prolongée en cas de panne du fournisseur.
Conclusion : Aucune documentation sur le FAI ni solution de secours n'est prévue.

Recommandations

Ajouter les détails du FAI (liaison, IP publique, contrat, points de coupure...).

CONSTATS & RECOMMANDATIONS – AUDIT ATTAQUE

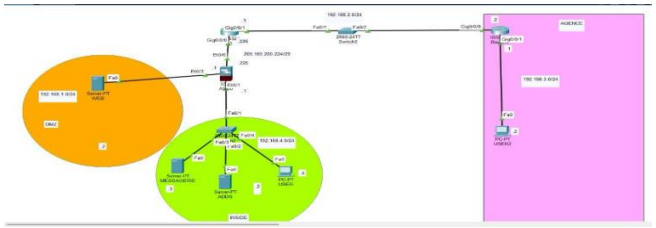
Niveau de criticité .

- ○ Extrême
- ○ Majeur
- ● Modéré
- ○ Mineur

Privilèges techniques identiques pour tous

Tous les membres techniques disposent des mêmes droits d'accès, ce qui empêche toute séparation des rôles ou contrôle des responsabilités. Cela augmente considérablement les risques d'abus, d'erreurs humaines et de compromission interne.

Évidences & captures



Impacts /Conclusion

Impact : Risque d'abus, erreurs humaines, compromission interne.
Conclusion : Aucun contrôle différencié des droits d'accès n'est appliqué.

Recommandations

Appliquer une stratégie RBAC (role-based access control).

CONSTATS & RECOMMANDATIONS – AUDIT ATTAQUE

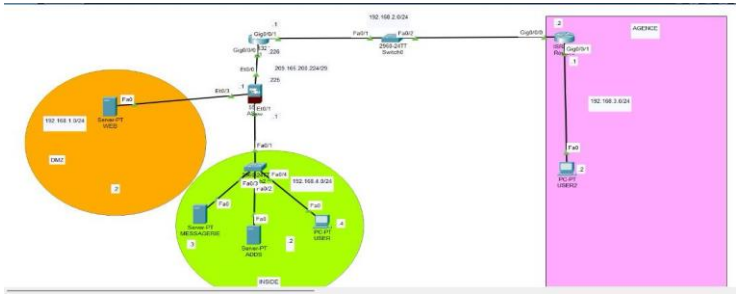
Niveau de criticité :

- ○ Extrême
- ● Majeur
- ○ Modéré
- ○ Mineur

Services critiques sans redondance (DHCP/DNS/AD)

Les services essentiels comme DHCP, DNS et Active Directory sont centralisés sur une seule machine, sans plan de secours. Une défaillance de ce serveur entraînerait une interruption complète des services réseau.

Évidences & captures



Impacts /Conclusion

Impact : Panne critique des services en cas de défaillance du serveur.
Conclusion : Aucune redondance des services essentiels.

Recommandations

Installer un serveur secondaire pour assurer la haute disponibilite.

CONSTATS & RECOMMANDATIONS – AUDIT ATTAQUE

Niveau de criticité :

- ○ Extrême
- ● Majeur
- ○ Modéré
- ○ Mineur

Aucun plan de reprise d'activité (PRA)

L'organisation ne dispose pas d'un plan formel pour restaurer les services après un incident majeur (sinistre, attaque, panne). En l'absence de PRA, la perte de données et l'indisponibilité des services peuvent durer indéfiniment.

Évidences & captures

Impacts /Conclusion

Impact : Perte de données ou interruption prolongée des services après incident.
Conclusion : L'entreprise n'est pas préparée à un sinistre majeur.

Recommandations

Créer un PRA + PCA avec des tests réguliers.

CONSTATS & RECOMMANDATIONS – AUDIT ATTAQUE

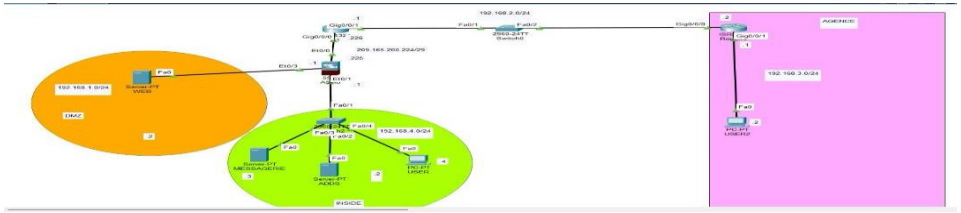
Niveau de criticité :

- ○ Extrême
- ○ Majeur
- ● Modéré
- ○ Mineur

Pas d'outil de supervision réseau

Aucun logiciel de monitoring réseau (comme Zabbix ou PRTG) n'est en place pour suivre les performances ou détecter des anomalies. Cela entraîne un manque de visibilité sur l'état du réseau et retarde la réponse en cas d'incident.

Évidences & captures



Impacts /Conclusion

Impact : Détection tardive des pannes ou incidents réseau.
Conclusion : Aucun outil ne permet de suivre l'état du réseau en temps réel.

Recommandations

Déployer un outil de monitoring(Zabbix, PRTG, ou Nagios)pour suivre la bande passante, les pannes, etc.

CONSTATS & RECOMMANDATIONS - AUDIT ATTAQUE

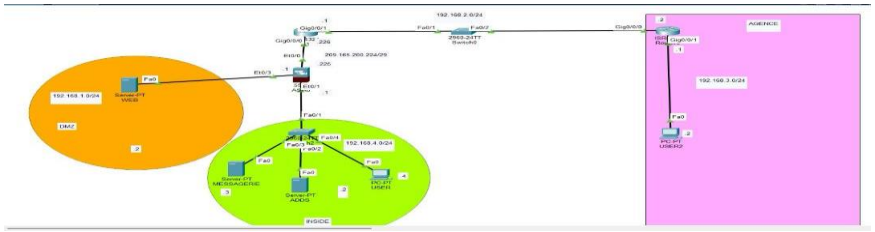
Niveau de criticité

- Extrême
- Majeur
- Modéré
- Mineur

Absence de VLAN VoIP et de QoS

Le trafic VoIP n'est pas isolé ni priorisé sur le réseau. En cas de congestion, la qualité des appels se détériore fortement, avec latence

Évidences & captures



Impacts /Conclusion

Impact : Mauvaise qualité des appels VoIP, latence élevée.
Conclusion : Aucun mécanisme ne priorise le trafic voix.

Recommandations

Créer un VLAN VoIP et prioriser le trafic audio.

CONSTATS & RECOMMANDATIONS - AUDIT ATTAQUE

Niveau de criticité :

- ○ Extrême
- ● Majeur
- ○ Modéré
- ○ Mineur

Version obsolète de SSH utilisée (SSH v1.5)

Le port 22/TCP (SSH) est ouvert sur le système audité, et la version détectée est SSH-1.25, correspondant au protocole SSH v1.5. Cette version obsolète présente de nombreuses failles cryptographiques et ne prend pas en charge les algorithmes modernes, ce qui la rend vulnérable aux attaques de type "Man-In-The-Middle" (MITM).

Évidences & captures

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV --script vuln 192.168.3.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-06 12:01 CEST
Nmap scan report for 192.168.3.1
Host is up (0.0027s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     Cisco SSH 1.25 (protocol 1.5)
23/tcp open  telnet  Cisco IOS telnetd
MAC Address: DC:7B:94:94:93:4B (Cisco Systems)
Service Info: OS: IOS; Device: switch; CPE: cpe:/o:cisco:ios

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 36.80 seconds

┌──(root㉿kali)-[/home/kali]
```

Impacts /Conclusion

Impact : SSH v1.5 utilise un chiffrement faible et est vulnérable aux attaques de type MITM, exposant les connexions à des interceptions.

Conclusion : Ce protocole obsolète compromet la sécurité des accès distants et doit être remplacé par SSH v2.

Recommandations

Mettre à jour le service SSH pour utiliser uniquement SSH version 2

Mettre en place une authentification forte (par clés SSH) et désactiver l'authentification par mot de passe si possible. Activer la journalisation des connexions SSH

CONSTATS & RECOMMANDATIONS - AUDIT ATTAQUE

Niveau de criticité :

- Extrême
- Majeur
- Modéré
- Mineur

Telnet activé (port 23)

Le protocole Telnet transmet les informations en clair, sans aucun chiffrement. Cela expose les identifiants et données sensibles à toute interception sur le réseau.

Évidences & captures

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV --script vuln 192.168.3.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-06 12:01 CEST
Nmap scan report for 192.168.3.1
Host is up (0.0027s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     Cisco SSH 1.25 (protocol 1.5)
23/tcp open  telnet  Cisco IOS telnetd
MAC Address: DC:7B:94:94:93:4B (Cisco Systems)
Service Info: OS: IOS; Device: switch; CPE: cpe:/o:cisco:ios

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 36.80 seconds

┌──(root㉿kali)-[/home/kali]
```

Impacts /Conclusion

Telnet fonctionne sans chiffrement, exposant les identifiants et données sensibles à toute interception sur le réseau.

Recommandations

Désactiver et désinstaller Telnet et le remplacer par SSH v2

Mettre en place des contrôles d'accès réseau pour s'assurer que seuls les hôtes autorisés peuvent accéder aux services distants (via un pare-feu ou des listes de contrôle d'accès).

2- AUDIT AD -DS

CONSTATS & RECOMMANDATIONS - AUDIT ATTAQUE

Niveau de criticité .

- ○ Extrême
- ○ Majeur
- ● Modéré
- ○ Mineur

Patch MS17-010 présent – mais sans preuve de gestion centralisée des mises à jour

Bien que la faille MS17-010 semble corrigée, aucun système centralisé de gestion des mises à jour n'est en place. Cela laisse penser que d'autres vulnérabilités critiques peuvent ne pas être traitées.

Impacts /Conclusion

Lors des tests de pénétration, l'exploitation via MS17-010 (EternalBlue) n'a pas réussi. Cela suggère que les systèmes sont à jour sur ce point. Cependant, rien ne garantit qu'un processus de gestion de patchs est en place, ni que d'autres correctifs critiques ont été appliqués.
Conclusion : L'environnement semble protégé contre MS17-010, mais l'absence de preuve de gestion active des correctifs laisse penser que ce n'est peut-être qu'un cas isolé.

Recommandations

Mettre en place une solution de gestion centralisée des mises à jour (WSUS, SCCM).
Réaliser un audit global des correctifs sur l'ensemble du parc serveur.
Documenter les versions installées et la politique de patch management.

CONSTATS & RECOMMANDATIONS - AUDIT ATTAQUE

Niveau de criticité :

- ○ Extrême
- ● Majeur
- ○ Modéré
- ○ Mineur

Port SMB (445) exposé

Le port 445 reste accessible sur le contrôleur de domaine, ce qui est un vecteur connu d'attaques comme WannaCry. Même corrigé, son exposition sans contrôle est un risque important.

Impacts /Conclusion

Le port TCP 445 (SMB) était ouvert sur le contrôleur de domaine, ce qui est une condition nécessaire à l'exploitation de MS17-010. Même si le correctif est appliqué, le port reste une surface d'attaque majeure : vecteur de ransomware (WannaCry, NotPetya) ou d'attaques SMB relay.

Conclusion : L'équipe défense a laissé un port critique exposé, ce qui est risqué même sans faille connue exploitable aujourd'hui.

Recommandations

Restreindre l'accès au port 445 uniquement aux machines autorisées (VLAN, firewall).
Désactiver SMBv1 complètement.
Utiliser un IPS/IDS pour surveiller les flux SMB suspects.

CONSTATS & RECOMMANDATIONS – AUDIT ATTAQUE

Niveau de criticité :

- ○ Extrême
- ● Majeur
- ○ Modéré
- ○ Mineur

Aucune alerte lors des scans ou attaques

Les scans réseau et tentatives d'exploit n'ont généré aucune alerte, ce qui indique l'absence de détection. Cela rend impossible toute réaction rapide face à une attaque en cours.

Impacts /Conclusion

Les scans Nmap, les tentatives de connexion sur SMB et l'exploitation via EternalBlue n'ont déclenché aucune alerte ni blocage. Cela montre une absence de système de détection ou une mauvaise configuration des alertes de sécurité.

Conclusion : L'équipe défense n'est pas en mesure de détecter ou réagir à des comportements anormaux sur son réseau.

Recommandations

Mettre en place un IDS (Snort, Zeek) ou un SIEM (Wazuh, Graylog).

Surveiller les scans de ports, les connexions SMB suspectes et les exploits connus.

CONSTATS & RECOMMANDATIONS - AUDIT ATTAQUE

Niveau de criticité :

- ○ Extrême
- ● Majeur
- ○ Modéré
- ○ Mineur

Pas de segmentation réseau vers les services critiques

Les services comme Active Directory ou SMB sont accessibles à toutes les machines, sans filtrage IP ni cloisonnement. Une machine compromise peut facilement attaquer les serveurs sensibles.

Impacts /Conclusion

Les contrôleurs de domaine sont accessibles sans restriction par n'importe quel hôte du réseau (pas de filtrage IP ou segmentation). Cela facilite la propagation latérale ou l'exploitation de failles comme MS17-010 depuis n'importe quel poste compromis.
Conclusion : Cette architecture expose inutilement les services critiques à toute machine, y compris compromise.

Recommandations

- **Mettre en place des ACL sur les switches et firewalls internes.**
- **Isoler les serveurs AD dans un VLAN spécifique.**
- **Restreindre les flux uniquement aux ports strictement nécessaires.**

CONSTATS & RECOMMANDATIONS – AUDIT ATTAQUE

Niveau de criticité :

- ○ Extrême
- ● Majeur
- ○ Modéré
- ○ Mineur

Sécurité SMB négligée

Aucun durcissement n'a été observé sur le protocole SMB (signature, désactivation de SMBv1, etc.). Cela facilite les attaques relay ou NTLM relay, encore très répandues.

Impacts /Conclusion

Aucune preuve de configuration renforcée sur SMB (désactivation de SMBv1, signature SMB activée, etc.) n'a été observée. Ces mesures sont pourtant essentielles pour bloquer les attaques connues comme SMB relay ou NTLM relay.

<u>Conclusion :</u> L'équipe défense semble négliger la sécurisation de services historiques mais toujours critiques.

Recommandations

- **Désactiver SMBv1.**
- **Forcer la signature SMB.**
- **Désactiver l'authentification NTLM là où Kerberos est disponible.**

3- AUDIT SERVICE MESSAGERIE

CONSTATS & RECOMMANDATIONS - AUDIT ATTAQUE

Niveau de criticité .

- ○ Extrême
- ● Majeur
- ○ Modéré
- ○ Mineur

Noyau Linux vulnérable

Utilisation d'un noyau Linux vulnérable: L'exécution d'un noyau Linux obsolète ou non patché expose le système à des failles de sécurité connues

Évidences & captures

Impacts /Conclusion

Des attaquants peuvent exploiter les vulnérabilités pour obtenir un accès non autorisé, exécuter du code malveillant, ou prendre le contrôle complet du système.

Conclusion : L'équipe défense devrait maintenir leur noyau à jour, surtout si des vulnérabilités spécifiques ont été signalées dans ta version. La sécurité et la stabilité du système en dépendent.

Recommandations

Mettre à jour à la version 5.10.227, 5.15.168, 6.1.113, 6.6.54, 6.10.13 ou 6.11.2 élimine cette vulnérabilité.

CONSTATS & RECOMMANDATIONS – AUDIT ATTAQUE

Niveau de criticité :

- ○ Extrême
- ● Majeur
- ○ Modéré
- ○ Mineur

Pas d'authentification multifacteur (MFA) pour les admins

Absence d'authenfication multifacteurs pour les administrateurs: Ne pas appliquer une authentification multifacteurs (MFA) pour les comptes administrateurs augmente considérablement le risque d'accès non autorisé en cas de compromise des identifiants

Impacts /Conclusion

Si des comptes administrateurs ou utilisateur sont protégés uniquement par un mot de passe, un attaquant ayant volé ou deviné ce mot de passe peut accéder à tous les paramètres du serveur, aux boîtes mail, et aux données sensibles.

Conclusion: l'absence de MFA dans iRedMail augmente drastiquement le risque de sécurité, et peut entraîner une vulnérabilité critique si une attaque réussie se produit.

Recommandations

- S'assurer que tu utilises la dernière version d'iRedMail pour bénéficier des correctifs de sécurité
- Si iRedMail ne supporte pas nativement MFA, configure MFA via ton fournisseur d'identité, par exemple en intégrant un SSO (Single Sign-On) sécurisé.

CONSTATS & RECOMMANDATIONS - AUDIT ATTAQUE

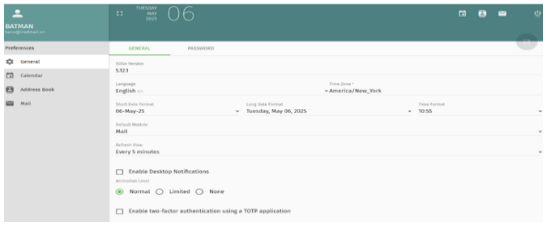
Niveau de criticité .

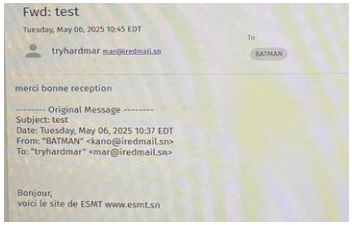
- ○ Extrême
- ○ Majeur
- ● Modéré
- ○ Mineur

Pas de synchronisation NTP

L'absence de synchronisation régulière avec un serveur NTP fiable peut entraîner des décalages temporels, affectant la cohérence des logs, la validité des certificats, ou la synchronisation des politiques de sécurité

Évidences & captures





Impacts /Conclusion

Problèmes de cohérence dans les certificats ou journaux, Problèmes avec les certificats TLS/SSL, Difficultés pour la journalisation et l'audit, Risque de vulnérabilités exploitant des écarts temporels.

<u>Conclusion :</u> L'absence de synchronisation NTP (Network Time Protocol) a un impact sur la cohérence des horloges système, ce qui peut avoir plusieurs conséquences en terme de sécurité

Recommandations

- **Mettre en place la synchronisation NTP sur tous les systèmes**
- **Utiliser des serveurs NTP fiables et sécurisés,**
- **Vérifier régulièrement la synchronisation**

CONSTATS & RECOMMANDATIONS - AUDIT ATTAQUE

Niveau de criticité :

- ○ Extrême
- ● Majeur
- ○ Modéré
- ○ Mineur

Utilisation d'un hyperviseur de type 1

Bien que robuste, un hyperviseur de type 1 mal configuré ou ancien peut constituer une cible privilégiée pour des attaques qui cherchent à compromettre l'intégrité ou la disponibilité de l'ensemble de l'environnement virtualisé

Impacts /Conclusion

- **Vulnérabilité à la fuite ou à la propagation d'attaques**
- **Gaspillage des ressources**
- **Perte de disponibilité**

Conclusion : L'utilisation d'un hyperviseur de type 1 a un impact significatif sur la sécurité, la gestion et la performance de ton environnement.

Recommandations

- **Maintenir l'hyperviseur à jour**
- **Restreindre l'accès à l'hyperviseur**
- **Configurer l'authentification forte**

CONSTATS & RECOMMANDATIONS – AUDIT ATTAQUE

Niveau de criticité :

- ○ Extrême
- ● Majeur
- ○ Modéré
- ○ Mineur

Absence de relais de messagerie

Ne pas mettre en place de relais SMTP sécurisé expose le serveur à un risque accru de spam, d'usurpation d'identité, ou d'injection de pièces jointes malveillantes, tout en compliquant la gestion centralisée des flux mail.

Impacts /Conclusion

- **Risque d'interception ou de falsification**
- **Augmentation de la charge pouvant entraîner une surcharge ou une configuration incohérente, surtout dans un environnement multi-serveurs.**

<u>Conclusion:</u> L'absence d'un relais de messagerie dédié et sécurisé peut compromettre la délivrabilité, la sécurité et la gestion centralisée de l'échange d'emails

Recommandations

- **Mettre en place un relais SMTP sécurisé**
- **Configurer un relais centralisé**
- **Surveiller et auditer**

CONSTATS & RECOMMANDATIONS – AUDIT ATTAQUE

Niveau de criticité :

- ○ Extrême
- ● Majeur
- ○ Modéré
- ○ Mineur

Serveur non relié au contrôleur de domaine Active Directory

L'absence de liaison avec le contrôleur de domaine AD empêche une gestion centralisée, une authentification unifiée et une cohérence dans la gestion des utilisateurs et des politiques de sécurité, augmentant le risque d'erreurs ou d'incohérences.

Impacts /Conclusion

Obligation de création manuelle de compte pour chaque utilisateur, Perte d'authentification centralisée, Incohérence des données d'authentification, administration inefficace, difficultés pour appliquer des politiques ou des correctifs.

Conclusion: Cette situation compromet la stabilité, la conformité et la sécurité globale de l'environnement informatique.

Recommandations

- Restaurer la liaison avec le contrôleur de domaine

- La mise en place d'un SSO (Single Sign-On) via AD est fortement recommandée pour centraliser l'authentification, renforcer la sécurité et réduire les erreurs administratives.

CONSTATS & RECOMMANDATIONS - AUDIT ATTAQUE

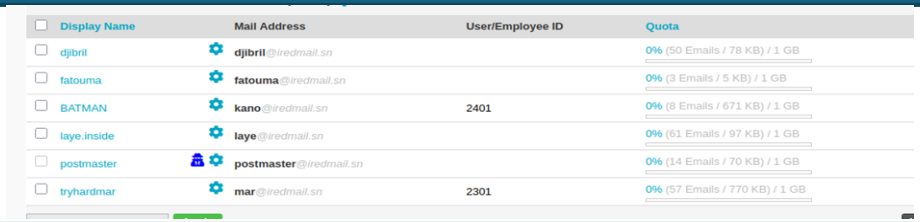
Niveau de criticité .

- ○ Extrême
- ○ Majeur
- ● Modéré
- ○ Mineur

Quota limité à 1 Go

Un quota de stockage restreint peut rapidement devenir un obstacle, provoquant la saturation des boîtes mail, la perte de messages ou l'interruption du service, tout en engendrant une gestion administrative accrue.

Évidences & captures



Display Name	Mail Address	User/Employee ID	Quota
djibril	djibril@iredmail.sn		0% (50 Emails / 78 KB) / 1 GB
fatouma	fatouma@iredmail.sn		0% (3 Emails / 5 KB) / 1 GB
BATMAN	kano@iredmail.sn	2401	0% (8 Emails / 671 KB) / 1 GB
laye.inside	laye@iredmail.sn		0% (61 Emails / 97 KB) / 1 GB
postmaster	postmaster@iredmail.sn		0% (14 Emails / 70 KB) / 1 GB
tryhardmar	mar@iredmail.sn	2301	0% (57 Emails / 770 KB) / 1 GB

Impacts /Conclusion

Chaque utilisateur dispose d'un quota de 1 Go, ce qui est défini, mais il n'existe aucun contrôle actif empêchant de dépasser ce quota ou générant une alerte en cas de dépassement. La taille maximale des pièces jointes que les utilisateurs peuvent envoyer ou recevoir n'est pas limitée.
Conclusion : Au risque d'impacter la productivité il est néceéssaire de garantir une gestion efficace de l'espace de stockage.

Recommandations

- **Revoir et augmenter le quota**
- **Encourager ou automatiser l'archivage**
- **Surveiller l'utilisation du stockage**

CONSTATS & RECOMMANDATIONS – AUDIT ATTAQUE

Niveau de criticité :

- ○ Extrême
- ● Majeur
- ○ Modéré
- ○ Mineur

Stockage des données utilisateurs en clair

Le stockage en clair de données sensibles ou personnelles expose ces informations à un risque majeur en cas de fuite ou de compromission, compromettant la confidentialité et violant souvent les réglementations en vigueur.

Impacts /Conclusion

Risque élevé de compromission des données , Violation de la confidentialité, Augmentation du risque d'attaques internes.

Conclusion : Le stockage en clair des données utilisateurs représente une vulnérabilité critique susceptible d'entraîner des fuites massives d'informations.

Recommandations

- **Mettre en œuvre un chiffrement fort**
- **Utiliser des mécanismes d'accès contrôlés**
- **Former le personnel à la gestion sécurisée des données sensibles.**

CONSTATS & RECOMMANDATIONS – AUDIT ATTAQUE

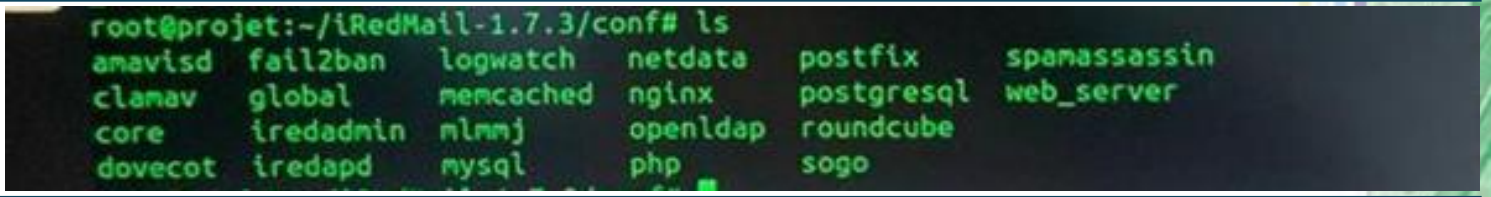
Niveau de criticité :

- ○ Extrême
- ● Majeur
- ○ Modéré
- ○ Mineur

Activation d'installations inutiles ou non fonctionnelles

Activer ou laisser actives des services ou modules inutilisés ou non fonctionnels augmente la surface d'attaque, consomme inutilement des ressources et complique la maintenance, facilitant d'éventuelles exploitations malveillantes.

Évidences & captures



Impacts /Conclusion

Augmentation de la surface d'attaque, Risques de failles de sécurité , Détérioration des performances, complique la détection d'incidents ou d'anomalies, rendant le respect des normes de sécurité plus difficile.

<u>Conclusion :</u> Il est crucial de désactiver ou supprimer tout composant non essentiel, en veillant à maintenir une configuration minimale et sécurisée, adaptée à l'usage réel.

Recommandations

- **Désactiver ou désinstaller toutes les fonctionnalités inutilisés dans IRedMail.**
- **Effectuer un audit régulier des composants activés**
- **Surveiller les journaux et alertes**

4- AUDIT SERVICE WEB

CONSTATS & RECOMMANDATIONS - AUDIT ATTAQUE

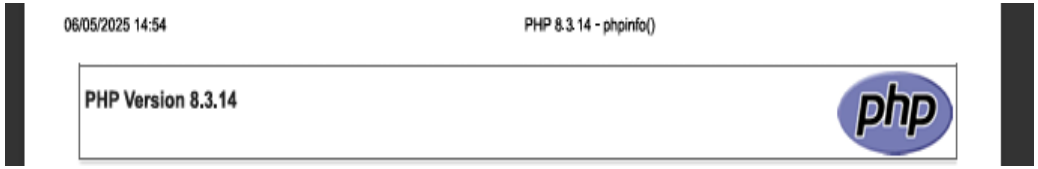
Niveau de criticité

- ○ Extrême
- ○ Majeur
- ● Modéré
- ○ Mineur

Utilisation d'une version récente de PHP (PHP 8.3.14)

Même si PHP 8.3.14 est récent, certaines applications ou extensions ne sont pas encore compatibles. Cela peut causer des erreurs de fonctionnement imprévues.

Évidences & captures



Impacts /Conclusion

Impact : L'utilisation d'une version récente de PHP est en général positive pour la sécurité et les performances. Toutefois, certaines bibliothèques ou CMS ne sont pas encore totalement compatibles avec PHP 8.3, ce qui peut causer des erreurs de compatibilité.

Recommandations

S'assurer que toutes les extensions utilisées et l'application web ont été entièrement testées avec PHP 8.3.

CONSTATS & RECOMMANDATIONS - AUDIT ATTAQUE

Niveau de criticité

- ○ Extrême
- ○ Majeur
- ● Modéré
- ○ Mineur

Affichage du chemin complet du serveur

Des informations comme le chemin absolu sont visibles dans les erreurs ou les logs. Ces données facilitent les attaques de type LFI (Local File Inclusion) ou path disclosure.

Évidences & captures

DOCUMENT_ROOT	C:/wamp64/www
SCRIPT_FILENAME	C:/wamp64/www/index.php

Impacts /Conclusion

Impact : Donne des informations sur la structure interne du serveur. Utile pour les attaques de type LFI/RFI ou path disclosure..

Recommandations

Eviter d'exposer ces chemins dans des environnement accessible publiquement.

CONSTATS & RECOMMANDATIONS – AUDIT ATTAQUE

Niveau de criticité

- ○ Extrême
- ● Majeur
- ○ Modéré
- ○ Mineur

Câble réseau du serveur web défectueux

Le câble réseau connecté au serveur web est emmêlé ,mal fixé entraînant des déconnexions fréquentes. Cela affecte la stabilité du service web.

Impacts /Conclusion

Impact : **Risque accru d'interruptions du service, de dégradation matérielle et d'indisponibilité réseau.**

Recommandations

Remplacer et sécuriser le câblage réseau.

CONSTATS & RECOMMANDATIONS - AUDIT ATTAQUE

Niveau de criticité

- Extrême
- Majeur
- Modéré
- Mineur

Injection SQL détectée

Le site web est vulnérable à l'injection SQL, permettant à un attaquant de manipuler ou lire la base de données. Cette faille est critique et souvent exploitée.

Évidences & captures

Impacts /Conclusion

Impact : Cette vulnérabilité permettrait à un attaquant d'injecter des requêtes malveillantes, compromettant la base de données du site.

Recommandations

Valider et échapper les entrées utilisateurs, utiliser des requêtes paramétrées, mettre à jour les frameworks.

CONSTATS & RECOMMANDATIONS - AUDIT ATTAQUE

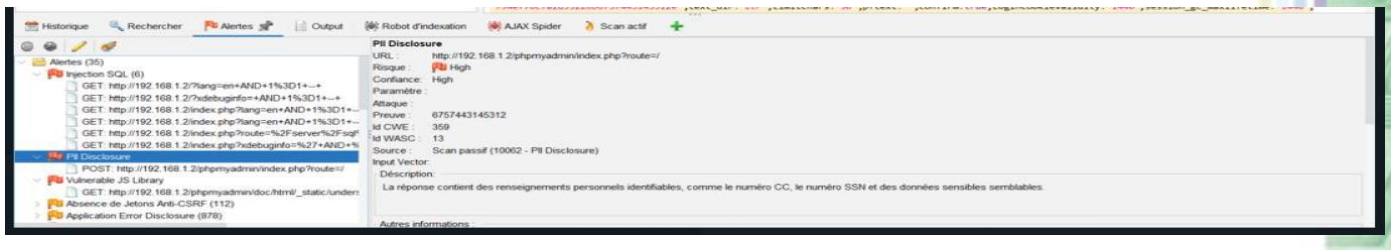
Niveau de criticité

- ○ Extrême
- ● Majeur
- ○ Modéré
- ○ Mineur

Fuite d'informations personnelles (PII)

Une vulnérabilité de type PII Disclosure a été détectée sur le site, exposant des informations personnelles identifiables dans des réponses HTTP, des paramètres d'URL ou d'autres canaux non sécurisés.

Évidences & captures



Impacts /Conclusion

Impact : Cette faille expose les données personnelles des utilisateurs, violant les obligations de confidentialité et les réglementations sur la protection des données. Elle peut mener à des fuites de données, du vol d'identité ou d'autres abus.

Recommandations

Supprimer toute donnée personnelle des messages d'erreur, logs et réponses HTTP, Chiffrer ou masquer les identifiants sensibles dans les URLs et les pages, Réaliser un audit complet de la gestion des données personnelles sur le site.

CONSTATS & RECOMMANDATIONS - AUDIT ATTAQUE

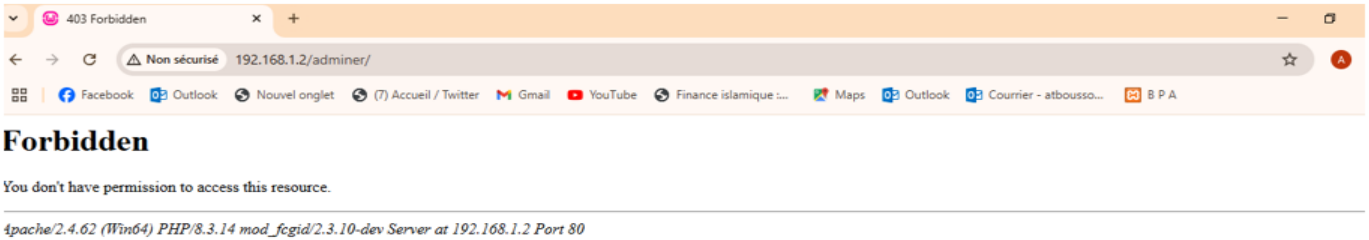
Niveau de criticité

- ○ Extrême
- ● Majeur
- ○ Modéré
- ○ Mineur

Pages web en erreur (ex : admin)

Constat sur le site: **Certaines pages du site présentent des erreurs comme la page admin**

Évidences & captures



Impacts /Conclusion

Impact : Impact négatif sur l'expérience utilisateur et la confiance.

Recommandations

Corriger les erreurs identifiées , valider les liens et les formulaires.

CONSTATS & RECOMMANDATIONS - AUDIT ATTAQUE

Niveau de criticité

- ○ Extrême
- ○ Majeur
- ● Modéré
- ○ Mineur

Divulgation de la version d'Apache

Constat : La configuration expose la version d'Apache. Le serveur web affiche sa version exacte, ce qui aide un attaquant à cibler des vulnérabilités connues. Il est important de masquer ces informations dans les entêtes HTTP.

Évidences & captures

Impacts /Conclusion

Impact: Risque de divulgation d'informations sur l'environnement serveur.

Recommandations

Configurer ServerTokens Prod et ServerSignatureOff , désactiver les modules inutiles

CONCLUSION

Au terme de cet audit, il ressort que Netcore Solution dispose d'une infrastructure technologique globalement bien structurée et conforme aux standards courants du secteur. L'entreprise montre une volonté claire de moderniser ses outils et d'optimiser ses processus métiers grâce à des solutions logicielles innovantes. Toutefois, plusieurs axes d'amélioration ont été identifiés, notamment en matière de **sécurité des systèmes d'information**, de **gestion des identités et des accès**, ainsi que de **documentation des procédures internes**.

L'adoption de bonnes pratiques en cybersécurité, la mise en œuvre de contrôles d'accès plus rigoureux, ainsi que la formalisation d'une politique de gestion des vulnérabilités sont fortement recommandées. De plus, pour renforcer la résilience de son infrastructure, Netcore Solution gagnerait à planifier des audits réguliers, des tests d'intrusion et une veille continue sur les menaces émergentes.

En conclusion, Netcore Solution possède un socle technique prometteur, mais doit consolider sa posture de sécurité et sa gouvernance informatique pour accompagner durablement sa croissance et gagner la confiance de ses parties prenantes.