BREVET DE TECHNICIEN SUPÉRIEUR
SERVICES INFORMATIQUES AUX ORGANISATIONS
Option : Solutions d'infrastructure, systèmes et réseaux

U7 – CYBERSÉCURITÉ DES SERVICES INFORMATIQUES

SESSION 2026

_____

Durée : 4 heures
Coefficient : 4

_____

Matériel autorisé :
Aucun matériel ni document n'est autorisé.

Dès que le sujet vous est remis, assurez-vous qu'il est complet.

Le sujet comporte 20 pages, numérotées de 1/20 à 20/20.

Cas NELAIT

Ce sujet comporte 20 pages dont un dossier documentaire de 14 pages.

Barème

DOSSIER A	Intégration du site distant « Le Bon Fromager »	30 points
DOSSIER B	Sûreté du réseau de stockage (baie SAN)	23 points
DOSSIER C	Analyse des vulnérabilités	27 points
	TOTAL	80 points

Dossier documentaire

Documents communs 8
Document 1 : Schéma simplifié de l'infrastructure de NELAIT intégrant « Le Bon Fromager » 8
Document 2 : Description de l'infrastructure informatique du siège de NELAIT (Cherbourg) 8

Documents associés au dossier A 9
Document A1 : Extrait de la charte informatique de la société NELAIT 9
Document A2 : L'opposabilité de la charte informatique 10
Document A3 : Résultats de l'audit PingCastle (extrait) 10

Documents associés au dossier B 12
Document B1 : Baie SAN 12
Document B2 : Technologie Auto-Tiering 13
Document B3 : Stockage de type RAID 6 13
Document B4 : Technologie iLO de Hewlett Packard Enterprise (HPE) 14

Documents associés au dossier C 15
Document C1 : Objectif d'une solution de surveillance des vulnérabilités 15
Document C2 : Présentation du produit IKare (société ITrust) 15
Document C3 : Évaluation CVSS (common vulnerability scoring system) 17
Document C4 : Dictionnaire CVE (common vulnerabilities and exposures) 19
Document C5 : Informations extraites de la dernière analyse IKare 19

Présentation du contexte

La société NELAIT, établie à Cherbourg-en-Cotentin en Normandie, joue actuellement un rôle de premier plan dans l'industrie des produits laitiers. Elle fabrique une variété de produits, notamment des fromages, du lait de consommation, du beurre et des crèmes. NELAIT s'efforce de mettre en avant les caractéristiques du terroir normand et d'autres régions de France au service des consommateurs.

À l'échelle internationale, NELAIT occupe une place significative avec des implantations dans de nombreux pays, notamment des sites stratégiques tels que Chicago aux États-Unis et Berlin en Europe. De plus, elle détient plusieurs filiales en France.

Dans le cadre de la commercialisation de ses produits, NELAIT utilise divers outils qui traitent des données essentielles pour son activité. La sécurité des données et la performance de son système d'information sont donc d'une importance cruciale pour l'entreprise. Sur un effectif total de 560 salariés, la direction des systèmes d'information (DSI) compte 25 employés.

La DSI se compose de quatre équipes :

- L'équipe « infrastructure systèmes », dirigée par le directeur des systèmes d'information (DSI), est constituée de deux administrateurs systèmes et de quatre techniciens systèmes.
- L'équipe « infrastructure réseaux » compte une administratrice réseaux et deux techniciens réseaux.
- L'équipe « support utilisateurs », supervisée par un responsable, comprend quatre ingénieurs et techniciens chargés du support de niveaux 2 et 3, ainsi que quatre techniciens d'exploitation. Sur les sites distants, des techniciens sont présents en proportion de la taille du site, assurant le support de niveau 1 en lien direct avec l'équipe de support du siège.
- L'équipe « sécurité » est dirigée par le responsable de la sécurité du système d'information (RSSI) et comprend deux ingénieurs en cybersécurité ainsi qu'une déléguée à la protection des données (DPD).

Le groupe NELAIT comprend divers établissements, tels que des fromageries, des crémeries et des glaciers. Récemment, NELAIT a acquis une petite entreprise auvergnate « Le Bon Fromager ».

En tant que membre de l'équipe DSI de NELAIT, votre responsabilité comprend la sécurisation du système d'information ainsi que l'intégration de cette nouvelle filiale.

Vous avez également en charge le maintien et le renforcement de la cybersécurité du système d'information (SI) de l'entreprise.

Vous vous appuierez sur le dossier documentaire mis à votre disposition.

Dossier A – Intégration du site distant « Le Bon Fromager »

Dans le cadre de son plan d'expansion et dans le souci de préserver les marques historiques de l'industrie fromagère, le groupe NELAIT a récemment acquis la fromagerie « Le Bon Fromager » qui, malgré un succès indéniable, n'avait trouvé aucun repreneur.

L'acquisition de l'entreprise « Le Bon Fromager » s'inscrit dans un processus plus large visant à préserver et à promouvoir le patrimoine fromager. Le groupe NELAIT souhaite conserver la tradition et la qualité qui ont fait la renommée de cette marque au fil des années.

Pour garantir une gestion optimale et uniforme de cette nouvelle acquisition, une modernisation de son système d'information s'avère indispensable. Cette modernisation implique la mise en place d'une connexion directe avec son siège social. Pour ce faire, un réseau privé virtuel (*VPN*) permettra une communication sécurisée et efficace entre la fromagerie « Le Bon Fromager » et le siège.

Mission A1 – Mise en conformité de l'infrastructure informatique « Le Bon Fromager »

Pour accompagner ces évolutions, il est essentiel d'envisager une réorganisation approfondie de l'infrastructure informatique de la fromagerie « *Le Bon Fromager* ».

L'infrastructure réseau actuelle n'étant pas segmentée, une des mesures incontournables à considérer serait la mise en place de réseaux locaux virtuels (*VLAN - virtual local area networks).*

Question A1.1
Indiquer pourquoi la mise en place de réseaux locaux virtuels est essentielle mais insuffisante pour une bonne sécurisation du réseau.

Mission A2 – Mise à jour de la solution de supervision

L'équipe informatique de NELAIT doit mettre en place une liaison entre sa solution de supervision et le nouveau site. Des éléments de performance vont devoir faire l'objet d'une surveillance.

En tant qu'administrateur(rice) systèmes et réseaux, vous êtes conscient(e) que les éléments de performance à surveiller peuvent varier en fonction des besoins spécifiques d'un réseau ou d'un système. L'objectif premier va être de se concentrer sur le routeur pare-feu dédié à la connexion internet de l'entreprise « Le Bon Fromager ».

Question A2.1
Proposer et justifier au moins trois indicateurs que l'on devrait surveiller si on se concentre uniquement sur le routeur de l'entreprise « Le Bon Fromager », pièce maîtresse du lien établi avec le siège.

Mission A3 – Application de la charte

Lors de la reprise de l'entreprise « Le Bon Fromager », les employés de cette société ont été pleinement intégrés au groupe NELAIT et ils devront par conséquent respecter les pratiques de l'entreprise en matière d'utilisation de son système d'information et plus particulièrement la charte informatique qu'elle a mise en place.

Un extrait de cette charte informatique est fourni (voir la documentation).

Question A3.1

a) Expliquer l'intérêt pour une entreprise comme NELAIT de disposer d'une charte informatique. *Vous illustrerez avec des exemples.*
b) Préciser à quelle(s) condition(s) et par quels moyens cette charte est applicable aux salariés de l'entreprise NELAIT.

Mission A4 – Audit du service d'annuaire *Active Directory*

Dans le contexte de la sécurisation du réseau, un audit de sécurité est envisagé à l'aide de plusieurs outils.

Question A4.1
Expliquer en quoi consiste un audit de sécurité du réseau et ses objectifs.

Pour renforcer la sécurité du service d'annuaire *Active Directory* (AD) et garantir son intégrité, l'équipe a mis en place un outil d'audit spécifique, à savoir *PingCastle*. Cet outil a été utilisé pour effectuer une évaluation approfondie du système d'information, en mettant particulièrement l'accent sur le service d'annuaire AD.

L'outil *PingCastle* a généré un certain nombre de points clés qui ont été mis en avant suite à cet audit. Ces points mettent en lumière les aspects critiques de la sécurité du service AD et serviront de base pour les efforts d'amélioration continue de la sécurité. Une partie des résultats de cet audit a été mis à votre disposition pour étude.

Question A4.2
Donner trois éléments permettant d'améliorer le score *PingCastle* et donc la sécurité de l'annuaire AD, en justifiant pour chacun en quoi cela est bénéfique pour la sécurité.

Dans un respect permanent du RGPD, la déléguée à la protection des données vous sollicite sur l'exploitation faite des données à caractère personnel gérées par le logiciel *PingCastle*.

Question A4.3
Indiquer en quoi l'outil *PingCastle* respecte les obligations en matière de collecte et de traitement de données à caractère personnel.

Dossier B – Sûreté du réseau de stockage (baie SAN)

Mission B1 – Vérification et reconfiguration de la baie SAN

Certains serveurs sont virtualisés en grappe *(cluster*) de serveurs physiques, partageant une baie SAN (*Storage Area Network*). Le responsable informatique envisage une évolution de cette baie pour deux raisons :

- les performances des accès disques sont insuffisantes, des lenteurs sont parfois observées ;
- la question de la capacité de stockage se pose à moyen terme. Il faudrait l'augmenter significativement (+50 %).

Actuellement l'entreprise dispose d'une baie de stockage HPE comme indiqué dans le dossier documentaire.

Question B1.1
Analyser la situation actuelle (en justifiant vos réponses) :

a) Calculer la capacité utile disponible actuellement.
b) Indiquer le nombre de disque(s) dur(s) que l'on peut perdre simultanément, par grappe, tout en maintenant la disponibilité des données.
c) Préciser le rôle du disque de rechange (*spare*) dans l'objectif d'une meilleure disponibilité de données.
d) Justifier le fait que le disque de rechange (*spare)* soit configuré en mode global à la baie et non dédié à une grappe donnée.

Le société NELAIT a demandé à une entreprise de services du numérique (ESN) de la conseiller pour envisager une évolution de la baie. L'entreprise consultée propose une solution d'évolution basée sur du mécanisme « Auto-Tiering ».
Une proposition d'évolution, tenant compte des conseils de cette ESN, est fournie dans la documentation.

Question B1.2
Analyser la proposition d'évolution de la baie (en justifiant vos réponses) :

a) Calculer la future capacité utile totale disponible avec la configuration proposée.
b) Indiquer le nombre de disque(s) dur(s) que l'on peut perdre simultanément, par grappe, tout en maintenant la disponibilité des données.
c) Indiquer si la nouvelle configuration permet d'atteindre les objectifs prévus : meilleures performances, meilleure disponibilité, augmentation de la capacité disque utile.

La présence de disques de rechange (*spare*) dans la baie est un atout pour permettre la mise en service rapide d'un nouveau disque en cas de panne de l'un des disques.

Question B1.3
Indiquer l'impact éventuel du temps de reconstruction sur la disponibilité des données.

Mission B2 – Utiliser l'interface d'administration iLO pour l'administration à distance

Bien que la plupart des serveurs soient de marque *Hewlett Packard Enterprise*, l'entreprise utilisait peu jusqu'à présent l'interface d'administration iLO. De ce fait certains serveurs ne disposaient même pas de la licence d'utilisation de cet outil d'administration.
Avant d'investir sur ces licences, le responsable vous demande d'identifier les plus-values de l'outil par rapport à une administration distante des serveurs classiques : utilisation de l'interface d'administration des machines virtuelles (*vSphere* en l'occurrence), utilisation du bureau à distance ou client sécurisé - SSH pour l'accès aux machines physiques ou virtuelles.

Question B2.1
Indiquer quelles peuvent être les atouts d'un outil comme iLO dans les domaines suivants :

- cybersécurité dans le cadre de la surveillance des équipements,
- maintenance des serveurs,
- intervention en cas d'incident sur un serveur physique.

Dossier C – Analyse des vulnérabilités

Dans un souci perpétuel d'amélioration de ses services (référentiel *ITIL*[1] *:* roue de Deming d'itération d'amélioration), le groupe NELAIT a souhaité tester la solution *IKare* de la société *ITrust*.

Suite à des premiers tests sur l'infrastructure d'exploitation, certaines failles ont été détectées sur des éléments réseaux essentiels. Vous êtes amené(e) à justifier l'intérêt et la complémentarité de ce produit avec les services déjà existants auprès du RSSI.

Mission C1 – Étude d'opportunité de la solution IKare

Le groupe NELAIT dispose déjà des solutions informatiques suivantes : *GLPI* (gestion des tickets et gestion d'inventaire), *Centreon* (solution de supervision) et *WSUS* (mise à jour centralisée des logiciels *Microsoft*). Le budget dédié au système informatique a été augmenté de 50 % l'année dernière de manière à répondre au nombre grandissant de cyberattaques.

Le RSSI vous demande de lui rédiger un compte-rendu succinct spécifiant la complémentarité de la solution *IKare* face aux trois services existants, cités ci-dessus, tout en garantissant le respect du RGPD.

Question C1.1
a) Expliquer l'intérêt de posséder le service *IKare* dans l'infrastructure du groupe NELAIT, en justifiant sa valeur ajoutée par rapport aux services réseaux existants (*GLPI, Centreon* et *WSUS*).
b) Indiquer au moins deux caractéristiques essentielles du produit *IKare* en ce qui concerne le respect des données à caractère personnel.

Mission C2 – Analyse des vulnérabilités critiques et moyennes remontées par l'outil *IKare*

Dans un objectif de test restreint mais néanmoins en exploitation, il a été décidé d'utiliser la solution *IKare*, en version d'évaluation, sur certaines adresses IP d'exploitation de l'infrastructure NELAIT. Trois alertes de vulnérabilités vous ont été confiées pour étude et traitement.
Une recherche approfondie vous a indiqué que la vulnérabilité 3 nommée « Vulnérabilité dans VMware Tools (VMSA-2021-0011) » n'a pas de code d'exploitation (*exploit*[2]) connu à ce jour.

Question C2.1
a) Expliquer pourquoi le fait qu'une faille ne possédant pas encore de code d'exploitation justifie une note CVSS moyenne et non très élevée. Vous préciserez la métrique qui la prend en compte.

b) Déduire de l'identifiant CVE de la vulnérabilité 2 nommée « Vulnérabilités multiples Microsoft Windows (KB4558998) » votre étonnement. Justifier votre réaction.

c) Expliquer l'intérêt de prendre contact avec le responsable du service *WSUS* de NELAIT, suite à l'étude de cette vulnérabilité 2, avant de demander la mise en œuvre d'une solution pour y remédier.

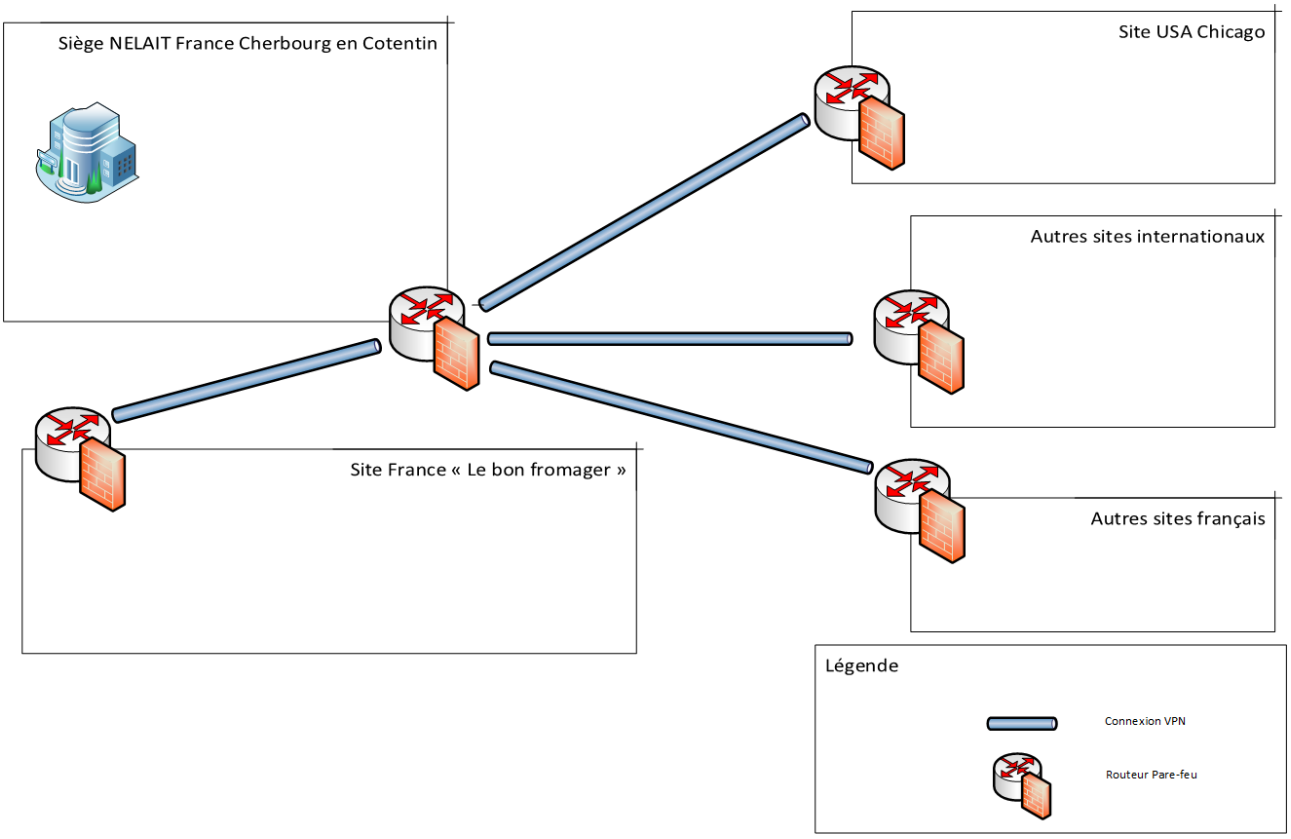
Le RSSI vous demande d'intervenir en priorité sur la vulnérabilité 1 (critique) liée au serveur *web* www.nelait.fr (192.168.30.1) ».

Question C2.2
a) Expliquer en quoi la résolution de cette faille est prioritaire pour votre RSSI. *Vous donnerez moins deux raisons.*
b) Indiquer votre préconisation, en précisant les différentes phases à prévoir, pour répondre à cette faille.

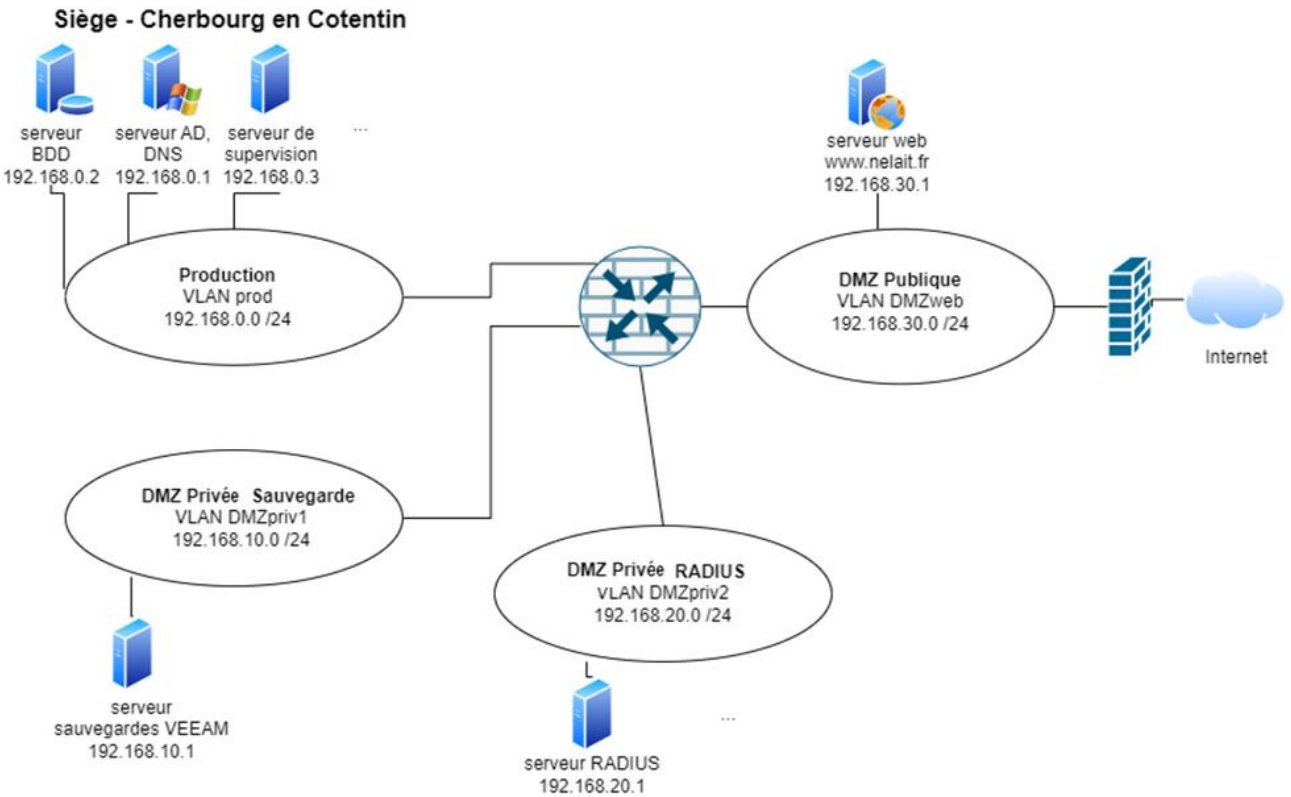
[1] ITIL : *Information Technology Infrastructure Library*
[2] Un code d'exploitation (*exploit*) est, dans le domaine de la sécurité informatique, un élément de programme permettant à un individu ou à un logiciel malveillant d'exploiter une faille de sécurité dans un système informatique (*Source Wikipedia*).

Documents communs

Document 1 : Schéma simplifié de l'infrastructure de NELAIT intégrant « Le Bon Fromager »



Document 2 : Description de l'infrastructure informatique du siège de NELAIT (Cherbourg)



La virtualisation de certains serveurs n'est pas indiquée de manière à garder une approche logique et non physique de l'infrastructure.

Documents associés au dossier A

Document A1 : Extrait de la charte informatique de la société NELAIT

Ce texte a pour objet de préciser la responsabilité des utilisateurs en accord avec la législation, afin d'instaurer un usage conforme des ressources informatiques et des services internet relevant de la société NELAIT. […]

1. Définitions

On désignera de façon générale sous le terme « *ressources informatiques* » : les réseaux, les moyens informatiques locaux, ainsi que ceux auxquels il est possible d'accéder à distance, les logiciels, les applications, les bases de données… […]
On désignera sous le terme « *utilisateur* » : la personne ayant accès ou utilisant les ressources informatiques et services internet quel que soit son statut. […]

2. Accès aux ressources informatiques et services internet

L'utilisation des ressources informatiques et l'usage des services internet ainsi que du réseau pour y accéder sont destinés à l'activité professionnelle des utilisateurs conformément à la législation en vigueur. […]
L'utilisation des ressources informatiques partagées et la connexion d'un équipement privé et extérieur (tels qu'un ordinateur, commutateur, borne d'accès sans-fil, etc.) sur le réseau sont soumises à autorisation du directeur des systèmes d'infromation et aux règles de sécurité. […]

3. Règles d'utilisation et de sécurité

Tout utilisateur est responsable de l'usage des ressources informatiques auxquelles il a accès.
L'utilisation de ces ressources doit être rationnelle et loyale afin d'en éviter la saturation ou leur détournement à des fins personnelles. […]
Il doit notamment appliquer les recommandations de sécurité et se conformer aux dispositifs mis en place pour lutter contre les virus et les attaques par programmes informatiques […]

4. Les services internet (*web*, messagerie, forum, téléphonie IP, etc.)

Internet est un outil de travail ouvert à des usages professionnels dont l'utilisation doit respecter des principes généraux et des règles propres aux divers sites qui les proposent, ainsi que dans le respect de la législation en vigueur.
L'utilisateur ne doit pas se connecter ou essayer de se connecter sur un serveur autrement que par les dispositions prévues par ce serveur ou sans y être autorisé par les responsables habilités. […]

La messagerie électronique est un outil de travail ouvert à des usages professionnels.
Tout message sera réputé professionnel sauf s'il comporte une mention particulière et explicitée dans son objet indiquant son caractère privé ou s'il est stocké dans un espace privé de données. […]

5. Analyse et contrôle de l'utilisation des ressources

Pour des nécessités de maintenance et de gestion technique, de contrôle à des fins statistiques, de traçabilité, d'optimisation, de sécurité ou de détection des abus, l'utilisation des ressources informatiques et des services internet, ainsi que les échanges via le réseau peuvent être analysés et contrôlés dans le respect du RGPD et de la loi « Informatique et Libertés ». […]

6. Sanctions

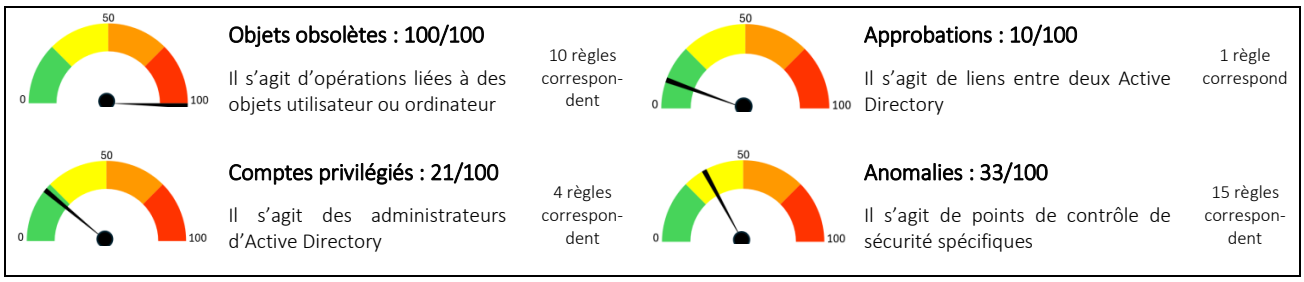
Le manquement aux règles et mesures de sécurité de la présente charte est susceptible d'engager la responsabilité de l'utilisateur et d'entraîner à son encontre des avertissements, des limitations ou suspensions d'utilisation de tout ou partie du système d'information et de communication, voire des sanctions disciplinaires, proportionnées la gravité des faits concernés. […]

Document A2 : L'opposabilité de la charte informatique

L'opposabilité de la charte nécessite […] son acceptation par les utilisateurs (signature de la charte ou annexe au contrat de travail).
Toutefois, afin d'éviter tout refus de l'utilisateur ou renégociation du contrat de travail, la charte peut être annexée au règlement intérieur de l'entité. Dans ce cas, outre la consultation des instances représentatives du personnel (comité d'entreprise, comité technique paritaire ou instance équivalente) lorsqu'elles existent et la communication à l'inspection du travail, la charte devra être portée à la connaissance des utilisateurs. Cette information peut avoir lieu au travers d'une notification individuelle de la charte (remise en mains propres, message électronique, etc.) ou être affichée ou diffusée sur l'intranet de l'entité par exemple, avec le règlement intérieur.
[…]
En cas de contentieux, des sanctions prises à l'encontre d'utilisateurs n'ayant pas connaissance de la charte pourraient être annulées par les juges.
Source : https://www.ssi.gouv.fr/uploads/2017/06/guide-charte-utilisation-moyens-informatiques-outils-numeriques_anssi.pdf

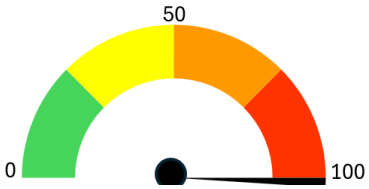
Document A3 : Résultats de l'audit PingCastle (extrait)

Le service *Active Directory* devient rapidement un point de défaillance critique dans toute grande entreprise, car il est à la fois complexe et coûteux à sécuriser.
L'outil *Pingcastle* ne fournit pas de solutions pour protéger une infrastructure. C'est un outil qui permet de découvrir ce qui doit être protégé, évaluer son niveau de sécurité et fournir des informations.



Il est important de noter que le score obtenu par l'outil *PingCastle* est un indicateur de la sécurité du service AD. Plus ce score se rapproche de 0, plus votre service AD est considéré comme sécurisé.

Objets obsolètes



Objets obsolètes : 100/100

Il s'agit d'opérations liées à des objets utilisateur ou ordinateur

Détails de la règle sur les objets obsolètes [10 règles correspondent sur un total de 34]

Présence de Windows 2003 = 3	*+ 20 Point(s)*
Nombre de comptes pouvant avoir un mot de passe vide (peut être remplacé par GPO) : 6	*+ 15 Point(s)*
Présence de comptes avec DES (Data Encryption Standard – Standard de chiffrement de données) activé = 11	*+ 15 Point(s)*
Nombre d'ordinateurs sans changement de mot de passe depuis au moins 3 mois : 7	*+ 15 Point(s)*
Présence de Windows 2008 = 18	*+ 15 Point(s)*
Nombre relativement élevé de comptes d'utilisateurs inactifs : 40 % (plus de 25 % de tous les utilisateurs)	*+ 10 Point(s)*
Nombre relativement élevé de comptes ordinateurs inactifs : 24 % (plus de 20 % de tous les ordinateurs)	*+ 10 Point(s)*
Présence de Windows 7 = 490	*+ 5 Point(s)*

…/…

Questions fréquemment posées
Voici les réponses aux questions les plus fréquemment posées.

Quelle est la configuration requise pour exécuter l'outil *PingCastle* ?
L'outil *PingCastle* nécessite une connectivité réseau au domaine tel que LDAP (*Lightweight Directory Access Protocol* - Protocole léger d'accès aux annuaires) (tcp/389), ADWS (*Active Directory Web Services* - Services Web pour Active Directory) (tcp/9389), SMB (*Server Message Block* - Bloc de messages serveur) (tcp/445) et l'autorisation de se connecter sur le domaine qui est accordée par défaut aux comptes du domaine local ou aux comptes de confiance domaines.

L'outil *PingCastle* est-il conforme au RGPD ?
L'outil *PingCastle* respecte les principes définis par l'Union européenne et essaie de minimiser la quantité de données collectées. Être décentralisé vous permet d'être le contrôleur et le sous-traitant des données pour répondre à une politique plus stricte.

Où puis-je trouver la liste des règles utilisées lors d'une évaluation ?
Le service *PingCastleReporting* peut produire un fichier *Excel* contenant toutes les règles. *PingCastle* peut produire un rapport HTML contenant les mêmes données.

Collectez-vous des informations ?
L'outil *PingCastle* ne collecte aucune autre information que celle écrite dans le rapport. Aucune connexion internet n'est requise, sauf si vous souhaitez vérifier la signature.

L'outil *PingCastle* fonctionne-t-il sur un réseau non connecté ?

Oui, PingCastle ne nécessite pas de connexion internet. De plus, le rapport lisible par machine peut être chiffré à l'aide d'une clé RSA (Rivest, Shamir et Adleman) adaptée au transfert par courrier électronique.

Comment gérez-vous la confidentialité des données ?

Les seules données collectées liées au règlement RGPD sont le nom du compte administrateur, l'heure de création du compte et l'heure de la dernière connexion. Ces données sont contenues dans le rapport lisible par l'homme et l'auditeur est responsable de leur utilisation.

Comment puis-je protéger les données contenues dans le rapport ?

Le rapport peut contenir des données qui sont, sur la base de notre politique de sécurité, restreintes. Cela peut être un problème lorsque vous devez transférer ces données sur le réseau. Pour limiter ce risque, l'outil PingCastle peut travailler sur un rapport chiffré avec une clé RSA : le rapport peut être stocké, chiffré ou transmis en toute sécurité tandis que seule l'instance ayant accès à la clé privée peut le traiter.

Source : https://www.pingcastle.com/

Documents associés au dossier B

Document B1 : Baie SAN



Baie HPE MSA2060 dotée de 24 emplacements pour disques 2,5".

Situation actuelle : 11 disques durs HDD SAS[3] seulement sont réellement présents dans la baie. Chaque disque a une capacité de 2 To. Pour utiliser les 2 contrôleurs présents, 2 grappes de 5 disques sont configurées selon la technique RAID 5. Le 11ème disque sert de disque de rechange *(spare)* autrement dit de disque en attente pour la reconstruction d'un ensemble RAID en cas de défaillance d'un disque sur l'une ou l'autre grappe. Il n'est donc pas dédié à une grappe.
À l'occasion d'un changement de disque défaillant, on s'est rendu compte que la reconstruction des données sur le disque nouvellement mis en service prenait environ 12 h.

Projet d'évolution : Le responsable souhaite une évolution permettant une augmentation de la capacité disque utile globale, tout en respectant les propositions de la société de services qui a préconisé les éléments suivants :

- utilisation du mécanisme *Auto-Tiering* (hiérarchisation automatique) en misant sur 10 à 20% de capacité en disques SSD SAS,
- utilisation du système RAID 6 pour une meilleure tolérance aux pannes,
- utilisation des deux contrôleurs actifs en parallèle pour obtenir de meilleures performances : pour utiliser les 2 contrôleurs, il faudra créer 2 systèmes hybrides (utilisant à la fois des disques HDD SAS et des disques SSD) et donc 4 grappes RAID (2 avec des disques HDD SAS et 2 avec des disques SSD SAS),
- maintien de disques de secours (*spare)*, mais il en faut un dans chaque technologie (HDD SAS et SSD SAS).

La proposition suivante est faite pour atteindre les objectifs, en utilisant les 24 emplacements de la baie :

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
HDD SAS 2 To	HDD SAS 2 To	HDD SAS 2 To	HDD SAS 2 To	HDD SAS 2 To	HDD SAS 2 To	HDD SAS 2 To	HDD SAS 2 To	HDD SAS 2 To	HDD SAS 2 To	HDD SAS 2 To	HDD SAS 2 To	HDD SAS 2 To	HDD SAS 2 To	HDD Spare 2 To	SSD SAS 1 To	SSD SAS 1 To	SSD SAS 1 To	SSD SAS 1 To	SSD SAS 1 To	SSD SAS 1 To	SSD SAS 1 To	SSD SAS 1 To	SSD Spare 1 To
Grappe HDD (RAID6)							Grappe HDD (RAID6)								Grappe SSD (RAID6)				Grappe SSD (RAID6)				

[3] SAS : *Serial Attached SCSI,* interface de connexion pour disque dur plus performants que SATA (*Serial Advanced Technology Attachment*). La technologie SSD correspond à un stockage flash plus performant qu'un disque mécanique (HDD)

Document B2 : Technologie Auto-Tiering

La technologie *Auto-Tiering* sur une baie de stockage SAN (*storage area network*) est une technologie qui automatise le déplacement des données entre différents niveaux de stockage (généralement des disques SSD rapides et des disques durs plus lents type SAS) en fonction de leur utilisation. Voici comment cela fonctionne et ses avantages :

1. **Détection de l'utilisation des données** : La technologie *Auto-Tiering* surveille en permanence l'utilisation des données (blocs) stockées sur la baie de stockage. Elle analyse quelles données sont fréquemment utilisées et quelles données sont moins sollicitées.

2. **Classification des données** : En fonction de l'utilisation, les données sont classées en différents niveaux de stockage. Les données très actives, telles que les bases de données en cours d'accès, sont placées sur des disques SSD rapides, tandis que les données moins actives, telles que les archives ou les fichiers inactifs, sont stockées sur des disques durs plus lents.

3. **Déplacement automatisé** : La technologie *Auto-Tiering* déplace automatiquement les données entre ces niveaux de stockage en temps réel. Ainsi, si une donnée qui était initialement stockée sur des disques SSD devient moins active, elle sera déplacée vers des disques durs plus lents pour libérer de l'espace sur les disques SSD pour les données plus actives.

Les avantages de la technologie *Auto-Tiering* sur une baie de stockage SAN sont nombreux :

- **Optimisation des performances** : Les données critiques bénéficient d'un accès plus rapide en étant stockées sur des disques SSD, ce qui améliore les performances des applications.

- **Économie d'espace** : Les données moins actives sont déplacées vers des disques durs type SAS, ce qui libère de l'espace précieux sur les disques SSD pour les données actives.

- **Automatisation** : Cette technologie réduit la gestion manuelle du placement des données, ce qui économise du temps et des ressources.

- **Économies de coûts** : En utilisant des disques SSD de manière plus efficace et en tirant parti des disques durs moins chers, vous pouvez réduire les coûts de stockage.

En résumé, la technologie *Auto-Tiering* sur une baie de stockage SAN permet d'optimiser les performances, de gérer l'espace de stockage de manière plus efficace et de simplifier la gestion des données dans un environnement SAN complexe.

Source : compilation issue de ChatGPT

Document B3 : Stockage de type RAID 6

Depuis des dizaines d'années, il est courant de combiner plusieurs disques durs en un seul lecteur logique. Au fil du temps, plusieurs configurations **se sont avérées particulièrement efficaces**. Elles ont donc été standardisées en niveaux RAID (*redundant arrays of independent disks*).
L'approche RAID 6 est rarement utilisée, bien qu'elle soit tout à fait pertinente du fait de sa **grande résilience**, grâce à la double parité.
Le RAID 6 a bien évidemment un impact sur la capacité utile, puisque 2 disques de la grappe (ou matrice) sont dédiés à la parité. Ainsi, pour un ensemble de 4 disques, la mise en place d'un système RAID 6 occasionne une perte de 50 % de la capacité réelle.

Le niveau RAID 6 est une approche de stockage consistant à combiner au moins quatre disques durs pour former un seul lecteur logique. Par rapport aux supports de données individuels, les matrices de ce niveau offrent une plus grande résilience et améliorent également la vitesse de lecture.
Un système RAID 6 peut gérer la panne simultanée de deux disques durs sans que cela ne compromette son fonctionnement.
Il améliore les performances en lecture (grâce à la répartition des données par bande), mais diminue les performances en écriture (du fait de la parité).

Source : d'après https://www.ionos.fr

Document B4 : Technologie iLO de Hewlett Packard Enterprise (HPE)



iLO, qui signifie *Integrated Lights-Out*, est une fonctionnalité développée par *Hewlett Packard Enterprise* (HPE) et utilisée sur certains de leurs serveurs. Il s'agit d'une interface de gestion à distance intégrée qui offre plusieurs avantages pour la gestion, la surveillance et la maintenance des serveurs. Voici quelques-uns des principaux avantages de l'interface iLO sur les serveurs HPE :

1. **Gestion à distance** : l'interface iLO permet aux administrateurs informatiques de gérer les serveurs à distance, même en dehors du réseau local. Cela est particulièrement utile pour effectuer des opérations de maintenance, des mises à jour du micrologiciel (*firmware*) ou des interventions sur le système sans avoir besoin d'un accès physique au serveur.

2. **Surveillance système** : l'interface iLO offre des fonctionnalités de surveillance en temps réel pour divers paramètres du système, tels que la température, la tension, l'utilisation du processeur, la mémoire, etc. Les administrateurs peuvent recevoir des alertes en cas de conditions anormales, ce qui permet une gestion proactive des problèmes potentiels.

3. **Redémarrage et réinitialisation à distance** : en cas de problème logiciel ou système, les administrateurs peuvent redémarrer ou réinitialiser les serveurs à distance via l'interface iLO, contribuant ainsi à la résolution des problèmes sans intervention physique.

4. **Installation de système d'exploitation à distance** : l'interface iLO permet l'installation d'un système d'exploitation à distance. Cela peut être particulièrement utile dans les centres de données où l'accès physique aux serveurs peut être limité ou difficile.

5. **Gestion des licences** : certaines fonctionnalités de l'interface iLO nécessitent des licences, pour l'enregistrement vidéo, la redirection graphique à distance, etc. L'interface iLO facilite la gestion de ces licences à partir d'une interface centralisée.

6. **Sécurité** : l'interface iLO intègre des fonctionnalités de sécurité avancées, telles que l'authentification à deux facteurs, le chiffrement SSL/TLS, et la possibilité de définir des autorisations d'accès basées sur les rôles. Cela renforce la sécurité lors de l'accès à distance aux serveurs.

7. **Enregistrement vidéo** : L'interface iLO peut enregistrer des sessions vidéo de la console à distance, ce qui peut être utile pour l'audit, le dépannage ou la formation.

8. **Gestion de l'énergie** : l'interface iLO permet la surveillance et la gestion de la consommation d'énergie des serveurs, offrant ainsi des possibilités d'optimisation énergétique.

En résumé, l'interface iLO sur les serveurs HPE fournit une puissante solution de gestion à distance qui permet aux administrateurs de surveiller, gérer, et maintenir les serveurs de manière efficace, même sans accès physique au matériel. Cela améliore la disponibilité, la fiabilité et la sécurité des infrastructures informatiques.

Source : adaptée de différentes sources HPE

Documents associés au dossier C

Document C1 : Objectif d'une solution de surveillance des vulnérabilités

Une solution de surveillance des vulnérabilités est un ensemble d'outils, de processus et de technologies conçus pour identifier, évaluer et atténuer les faiblesses potentielles dans un système informatique, un réseau ou une application. Ces vulnérabilités peuvent inclure des erreurs de configuration, des failles de sécurité, des défauts de codage ou d'autres faiblesses susceptibles d'être exploitées par des attaquants pour compromettre la sécurité d'un système.

Les solutions de surveillance des vulnérabilités effectuent généralement les actions suivantes :

1. Découverte des vulnérabilités : elles analysent les systèmes à la recherche de faiblesses connues ou potentielles. Cela peut inclure des scans automatisés des réseaux, des applications et des configurations.
2. Évaluation des risques : elles évaluent la gravité des vulnérabilités identifiées en fonction de leur impact potentiel sur la sécurité et la confidentialité des données.
3. Rapports et alertes : elles génèrent des rapports détaillés sur les vulnérabilités détectées et fournissent des alertes en temps réel pour permettre aux équipes de sécurité de réagir rapidement.
4. Corrections et atténuation : elles peuvent recommander des mesures correctives ou des solutions d'atténuation pour remédier aux vulnérabilités identifiées.
5. Suivi et tableau de bord (*reporting*) : elles permettent généralement un suivi continu des vulnérabilités au fil du temps, fournissant des informations essentielles pour une gestion proactive de la sécurité.

L'objectif principal de ces solutions est d'aider les organisations à maintenir un niveau élevé de sécurité en identifiant et en corrigeant rapidement les vulnérabilités avant qu'elles ne puissent être exploitées par des cybercriminels.

Extrait du résultat obtenu à partir d'une recherche ChatGPT

Document C2 : Présentation du produit IKare (société ITrust)

L'analyseur de vulnérabilités « Made in France » labellisé et souverain

Maîtrisez les vulnérabilités informatiques avec IKare

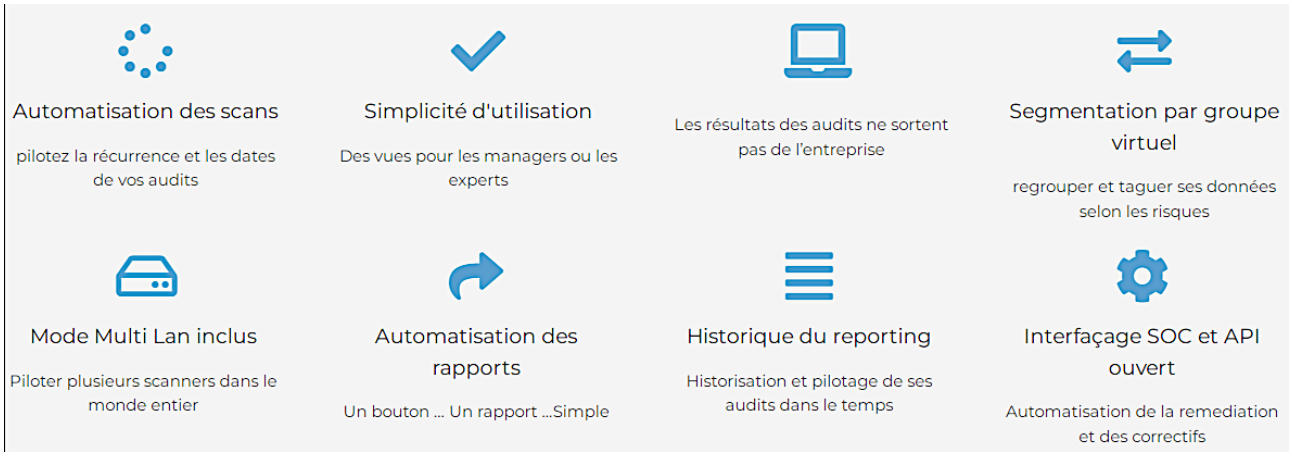
IKare est un outil qui automatise la mise en place des meilleures pratiques de sécurité et du management des vulnérabilités. Vous obtenez une solution simple de monitoring réseau, ainsi qu'une gestion rapide et un contrôle facile des principaux facteurs de sécurité.

Points forts

Lorsque les vulnérabilités informatiques sont identifiées par une personne malveillante, elles peuvent être exploitées, permettant ainsi d'accéder sans autorisation à un réseau informatique ou à des informations confidentielles, de voler des secrets industriels, d'utiliser à des fins frauduleuses des données personnelles, de paralyser l'activité de l'entreprise et bien d'autres…

Tous les jours, de nouvelles vulnérabilités apparaissent dues à des failles dans les systèmes et applications et à de mauvaises configurations d'équipement. Il est donc indispensable d'agir pour la sécurisation de son système d'information.

…/…



- Sans agent et évolutif pour des réseaux larges – déploiement rapide et immédiatement opérationnel
- Monitoring en continu pour prévenir les nouvelles vulnérabilités et réduire les risques d'expositions
- Prévention et remédiation des risques plus rapide avec une interface d'utilisation intuitive et une hiérarchisation des alertes
- Contrôle complet de la politique de scans incluant les scans authentifiés pour des résultats plus précis
- Mise à jour automatique de la base de données des vulnérabilités et des nouvelles versions

Scan en mode SaaS depuis le cloud

- Complète et intégrée – solution de management des vulnérabilités, délivrée comme un service
- Haute fléxibilité – réduction ou augmentation du périmètre d'audit selon les besoins immédiats
- à la demande – aucun investissement important à prévoir
- Entièrement hébergé en France – pour respecter les conditions de souveraineté de données,
- Accord de niveau de service garanti par des partenaires sélectionnés ou par ITrust
- Opérationnel rapidement en quelques heures

Avantages de la solution

Audit de vulnérabilité automatisé & continu
IKare fournit aux organisations une console unique permettant de lancer et gérer la récurrence des analyses (*scans*) de vulnérabilité. Le réseau est automatiquement découvert et les vulnérabilités sont remontées en quasi-temps réel puis classées par ordre de criticité selon les standards CVSS. IKare permet une récurrence d'analyse très élevée, garantissant ainsi l'intégrité et l'imperméabilité de votre réseau au jour le jour.

Réduction des risques d'intrusion
Fruit de l'expérience de nos consultants en tests d'intrusion, un scanner unique développé par ITrust détecte les actifs de votre réseau, les services associés, les ports ouverts, et remonte les failles de sécurité liées au non-respect des bonnes pratiques de sécurité. IKare détecte les mots de passe par défaut ou encore les clés de chiffrements faibles et garanti ainsi un haut niveau de sécurité en préservant votre système d'information des menaces les plus fréquentes.

Une console d'administration intuitive
IKare facilite pour les RSSI la gestion de la sécurité et la collaboration avec les équipes techniques. Les tableaux de bords et rapports s'adaptent aux différentes strates de l'entreprise, du management aux techniciens, permettant ainsi à chacun d'accéder au niveau de détail qui lui correspond.

Gestion simplifiée de groupes virtuels
IKare permet aux organisations de créer et organiser simplement des groupes virtuels, par exemple avec des serveurs qui répondent à la même fonction (DMZ, Messagerie, Marketing, Compta, etc.) ou aux mêmes contraintes de conformité (RGPD, ISO, etc.), et facilite ainsi la gestion de réseaux complexes.

Mise en conformité réglementaire
Le déploiement d'IKare permet de suivre la mise en conformité avec différentes règlementations. Par exemple, le RGPD exige, entre autres, d'assurer une surveillance (*monitoring*) des vulnérabilités. IKare garantit le respect des meilleures pratiques de sécurité sur votre réseau grâce à sa recherche proactive des failles de sécurité.

Extrait du site web https://www.itrust.fr/

Document C3 : Évaluation CVSS (common vulnerability scoring system)

Dans le domaine de la sécurité informatique, le système d'évaluation standardisé de la criticité des vulnérabilités *CVSS* est établi selon des critères objectifs et mesurables. Cette évaluation est constituée de 3 mesures appelées métriques : **la métrique de base, la métrique temporelle et la métrique environnementale**. Le score final est compris entre 0 et 10, 10 correspondant aux vulnérabilités les plus critiques. La version actuelle de l'évaluation *CVSS (CVSSv4.0)* a été publiée en novembre 2023.

Métriques

L'évaluation *CVSS* est construite à partir de la métrique de base qui nous donne un score *CVSS* de base qui sera ensuite pondérée avec la métrique temporelle puis avec la métrique environnementale. Ces trois métriques se définissent comme suit :

1. La métrique de base est unique et immuable, elle se base sur les qualités intrinsèques de la vulnérabilité.
2. La métrique temporelle est unique mais peut évoluer au cours du temps.
3. La métrique environnementale est multiple et évolue en fonction de l'environnement informatique. Elle dépend du système informatique dans lequel elle est présente.

Métrique de base (métrique 1)

Vecteur d'accès

Le vecteur d'accès définit comment une vulnérabilité peut être exploitée.

Valeur	Description	Score
Local	L'attaquant doit avoir soit un accès physique au système vulnérable (exemple : attaques via le port Firewire) soit avoir un compte local (exemple : attaque d'escalade de privilèges).	0.395
Réseau local	L'attaquant doit avoir accès au domaine de diffusion ou de collision du système vulnérable (exemple : *ARP spoofing*, attaques *Bluetooth*).	0.646
Réseau	L'interface vulnérable utilise le niveau 3 ou plus de la pile OSI. Ce type de vulnérabilité est communément décrit comme exploitable à distance (exemple : un dépassement de tampon distant dans un composant réseau).	1.0

Complexité d'accès

La complexité d'accès définit le niveau de difficulté d'exploitation de la vulnérabilité découverte.

Valeur	Description	Score
Haut	Des conditions spécifiques sont nécessaires, comme une fenêtre d'exécution étroite ou un besoin d'utilisation de méthode d'ingénierie sociale qui pourraient être aisément détectée par des personnes compétentes.	0.35
Moyen	Il existe des conditions supplémentaires d'accès comme une limitation sur l'origine de l'accès ou le besoin que le système utilise une configuration non commune ou différente de celle par défaut.	0.61
Bas	Il n'y a pas de condition particulière d'accès, comme un système disponible pour un grand nombre d'utilisateurs ou que la configuration est largement répandue.	0.71

…/…

Authentification

La métrique d'authentification définit le nombre de fois qu'un attaquant doit s'authentifier sur la cible dans le but d'exploiter la vulnérabilité. Ceci fait référence spécifiquement au nombre de fois qu'une authentification est nécessaire une fois que l'accès au système a été obtenu. Ça n'inclut pas, par exemple, l'authentification au réseau utilisé pour accéder au système vulnérable. Pour des vulnérabilités exploitables localement, cette valeur ne devrait seulement être fixée à unique ou multiple si une authentification est nécessaire après avoir accédé au système.

Valeur	Description	Score
Multiple	L'exploitation de la vulnérabilité nécessite que l'attaquant s'authentifie deux fois ou plus, même si les authentifiants utilisés sont les mêmes à chaque fois.	0.45
Simple	L'attaquant doit s'authentifier une seule fois pour exploiter cette vulnérabilité.	0.56
Inexistant	Il n'y a pas besoin que l'attaquant s'authentifie.	0.704

Métrique d'impact

[…]

Confidentialité

La métrique de confidentialité définit l'impact sur la confidentialité des données stockées ou traitées par le système.

[…]

Intégrité

La métrique d'intégrité définit l'impact sur l'intégrité des données du système.

[…]

Disponibilité

La métrique de disponibilité définit l'impact de la disponibilité du système ciblé. Les attaques consommant de la bande passante, des cycles processeurs, de la mémoire, ou tout autre ressource affectent la disponibilité d'un système.

[…]

Métrique temporelle (métrique 2)

La valeur des métriques temporelles varie au cours de la durée de vie de la vulnérabilité à mesure que :

- les codes d'exploitation (*exploit*s) sont développés, divulgués et automatisés,
- les mesures d'atténuation et les correctifs sont rendus disponibles.

Métrique environnementale (métrique 3)

Les métriques environnementales utilisent le score temporel de base et actuel pour évaluer la gravité d'une vulnérabilité dans le contexte du déploiement du produit ou du logiciel vulnérable. Cette mesure est calculée subjectivement, généralement par les parties concernées.

Extraits de fr.wikipedia.org/wiki/Common_Vulnerability_Scoring_System

Document C4 : Dictionnaire CVE (common vulnerabilities and exposures)

Le dictionnaire *common vulnerabilities and exposures* (vulnérabilités et expositions communes) ou *CVE* recense des informations publiques relatives aux vulnérabilités de sécurité. Le dictionnaire est maintenu par l'organisme MITRE, soutenu par le département de la sécurité intérieure des États-Unis.

Identifiants *CVE*

Les identifiants *CVE* sont des références de la forme CVE-AAAA-NNNN (AAAA est l'année de publication et NNNN un numéro d'identifiant). Par exemple, la faille FREAK a pour identifiant CVE-2015-0204.

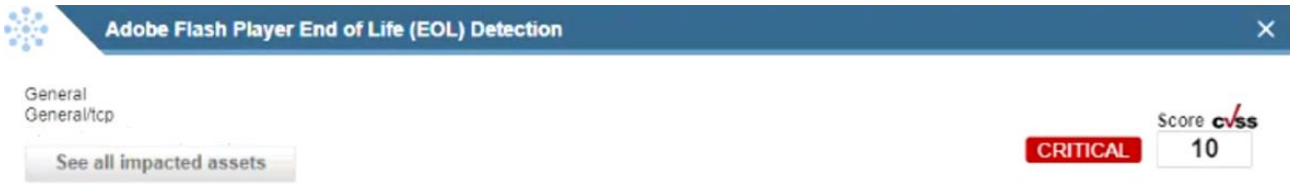
Depuis 2014, le numéro d'identifiant d'une vulnérabilité *CVE* est composé de 4 chiffres minimum et peut être augmenté sans limite si la quantité de vulnérabilités sur une année le nécessite (NNNN...N)

Le contenu du dictionnaire *CVE* peut être téléchargé. Cette liste contient une description succincte de la vulnérabilité concernée, ainsi qu'un ensemble de liens que les utilisateurs peuvent consulter pour plus d'informations.

Extraits de : fr.wikipedia.org/wiki/Common_Vulnerabilities_and_Exposures

Document C5 : Informations extraites de la dernière analyse IKare

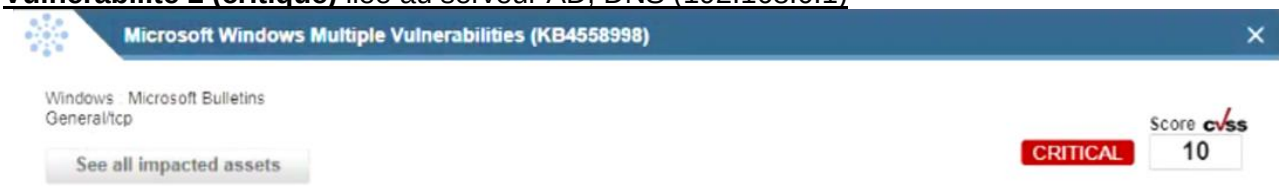
Vulnérabilité 1 (critique) liée au serveur web www.nelait.fr (192.168.30.1)



Nom : Détection fin de vie Adobe Flash Player
Résumé : Le lecteur Adobe Flash Player sur l'hôte distant a atteint la fin de vie (*EOL End OF Life*) / est abandonné et ne doit plus être utilisé.
Impact : Un produit *EOL* / abandonné ne reçoit aucune mise à jour de sécurité de la part du fournisseur. Des failles de sécurité non corrigées pourraient être exploitées par un attaquant pour compromettre la sécurité de cet hôte.
Les références :
URL : https://www.adobe.com/products/flashplayer/end-of-life.html
URL : https://theblog.adobe.com/adobe-flash-update/
Solution : WillNotFix
Aucune solution n'a été proposée par le fournisseur. Les options de solution générales consistent à mettre à niveau vers une version plus récente, désactivez les fonctionnalités respectives, supprimez le produit ou remplacez le produit par un autre.
Remarque : Le produit a atteint sa fin de vie.
Autres informations retournées :
Le produit « Adobe Flash Player » sur l'hôte distant a atteint la fin de sa durée de vie.
CPE : cpe:/a:adobe:flash_player_internet_explorer
Emplacement/URL : C:\Windows\SysWOW64
Date de fin de vie : 2020-12-31
Informations EOL : https://www.adobe.com/products/flashplayer/end-of-life.html

…/…

Vulnérabilité 2 (critique) liée au serveur AD, DNS (192.168.0.1)



Nom : Vulnérabilités multiples Microsoft Windows (KB4558998)
Résumé : Il manque à cet hôte une sécurité critique mise à jour selon Microsoft KB4558998
Aperçu : Plusieurs défauts existent en raison de :

- Les serveurs Windows Domain Name System ne parviennent pas à gérer correctement les requêtes (SIGRed, CVE-2020-1350).
- Windows System Events Broker ne parvient pas à bien gérer les opérations sur les fichiers.
- Les diagnostics de gestion des appareils Windows Mobile (MDM) ne parviennent pas à gérer correctement les objets en mémoire.
- Le service de connexions réseau Windows ne parvient pas à gérer correctement les objets en mémoire.
- SharedStream Library ne parvient pas à gérer les objets en mémoire.

Veuillez consulter les références pour plus d'informations sur les vulnérabilités.
Impact : Une exploitation réussie permettra à un attaquant d'exécuter du code arbitraire, d'élever des privilèges, de divulguer des informations sensibles et d'effectuer des attaques par déni de service.
Les références :
URL : https://www.cisa.gov/known-exploited-vulnerabilities-catalog
URL : https://support.microsoft.com/en-us/help/4558998
CVE : CVE-2020-1085, […], CVE-2020-1463, CVE-2020-1468
Solution : FournisseurFix
Le fournisseur a publié des mises à jour. Regardez les références pour plus d'informations.
Autres informations retournées :
Plage vulnérable : 10.0.17763.0 - 10.0.17763.1338
Fichier vérifié : C:\Windows\system32\Gdiplus.dll
Version du fichier : 10.0.17763.973

Vulnérabilité 3 (Moyenne) liée au serveur AD, DNS (192.168.0.1)



Résumé : VMware Tools est sujet à un déni de service vulnérabilité (VMSA-2021-0011)
Aperçu : La faille est due à une vulnérabilité dans le pilote VM3DMP.
Impact : Une exploitation réussie permettra aux attaquants avec des privilèges d'utilisateur local dans le système d'exploitation invité Windows, où VMware Tools est installé, peut déclencher une PANIQUE dans le pilote VM3DMP conduisant à une condition de déni de service dans le système d'exploitation invité Windows.
Les références :
URL : https://www.vmware.com/security/advisories/VMSA-2021-0011.html
CVE : CVE-2021-21997
Solution : FournisseurFix
Mise à niveau vers VMware Tool version 11.3.0 ou plus tard. Veuillez consulter les références pour plus d'informations.
Autres informations retournées :
Version installée : 11.0.1.14773994 / Version corrigée : 11.3.0
Installation : chemin/port : C:\Program Files\VMware\VMware Tools\