

Archiver et protéger les données et les preuves numériques

COMPÉTENCES

- Organiser la collecte et la conservation des preuves numériques
- Appliquer les procédures garantissant le respect des obligations légales

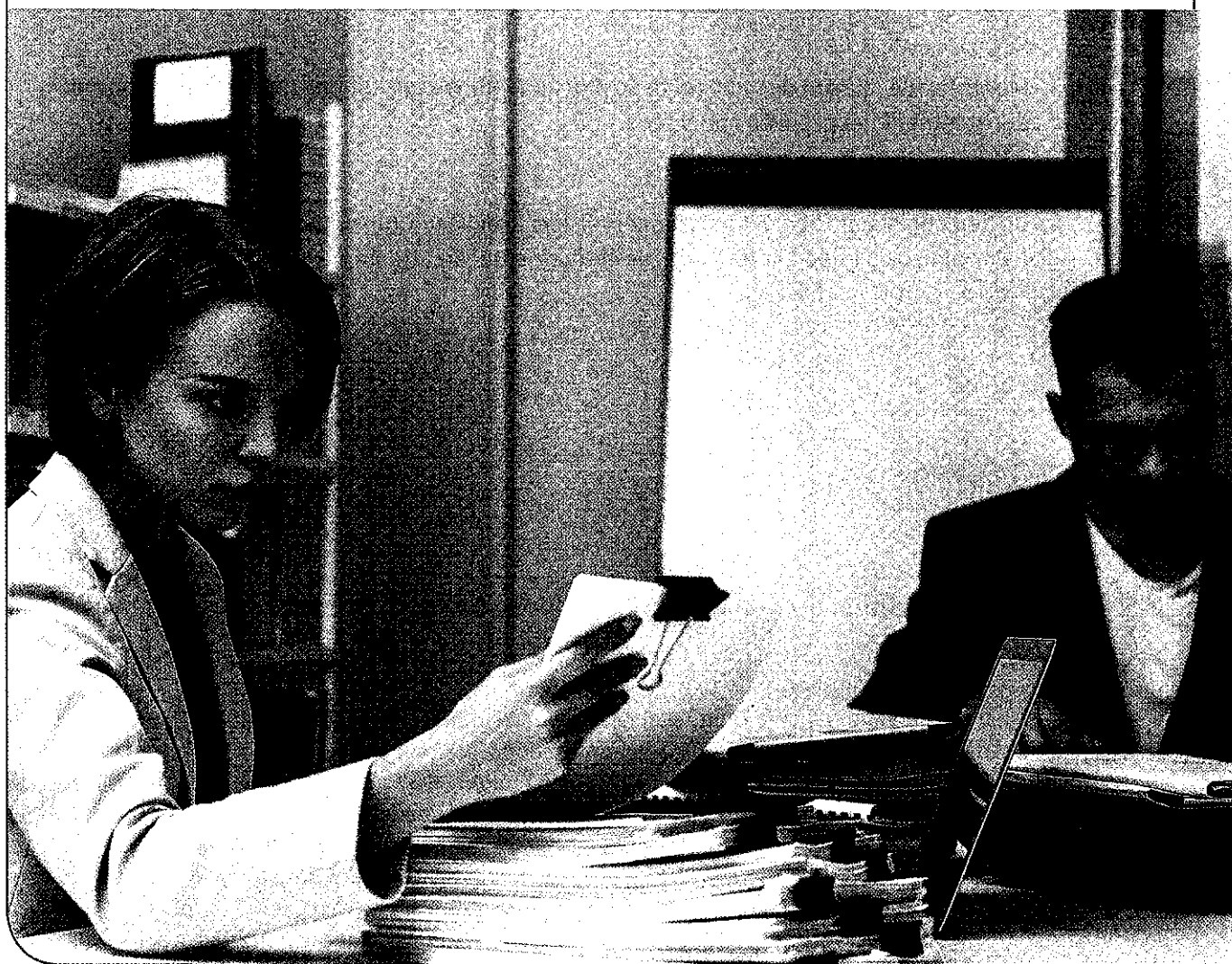
SAVOIRS ASSOCIÉS

- Outils de contrôle de la sécurité : plans de secours, traçabilité et audit technique
- Les organisations de lutte contre la cybercriminalité

Situation professionnelle

Cibeco a décidé de déposer plainte à la suite de l'attaque subie par son client Ecotri. Yaël et Sarah Darmon, les gérantes de Cibeco, ont poursuivi des investigations en vue de collecter des preuves numériques pour appuyer la plainte. Ces investigations ont permis de suspecter plusieurs menaces de sécurité qui les inquiètent.

Dans un premier temps, elles décident de procéder à la vérification de toutes les procédures de collecte et de conservation des preuves afin d'étudier leur exploitabilité. Dans un second temps, elles réalisent un audit technique pour s'assurer que les procédures prévues par Cibeco en cas de brèche de sécurité respectent bien les obligations légales.



➤ Voir présentation générale, p. 135

Missions professionnelles

Organiser la collecte et la conservation des preuves numériques

[PREUVES]



À la suite des attaques subies par Cibeco et Ecotri, Sarah Darmon souhaite savoir si des traces laissées par ces intrusions pourraient être exploitables dans le cas d'une enquête judiciaire. Elle vous charge de réaliser un audit technique sur la collecte et la conservation des preuves numériques au sein de la pépinière.

Travail à faire

- Montrez, en développant chaque argument, que Cibeco dispose des moyens techniques permettant d'appliquer les recommandations d'usage en matière de collecte des preuves numériques.
 - > Fiches savoirs technologiques 2 (p. 25) et 11
 - > Documents 1 à 4
- Relevez les événements collectés par les journaux systèmes de Cibeco et vérifiez que cette liste est bien complète.
 - > Fiches savoirs technologiques 2 (p. 25) et 11
 - > Documents 1 à 3
- Montrez que chacun des supports de stockage utilisé par Cibeco permet de conserver durablement les preuves collectées.
 - > Fiche savoirs technologiques 11
 - > Document 5
- Le lieu choisi par Cibeco pour conserver ses preuves numériques doit permettre de faire face à des sinistres importants. Citez les éléments qui en attestent.
 - > Fiche savoirs technologiques 11
 - > Document 6

Dossier documentaire

Document 1 Votre entretien avec la gérante de Cibeco au sujet de la gestion des preuves

Vous : J'ai besoin de savoir si, en cas d'attaque informatique, la pépinière est en mesure de fournir des éléments de preuve permettant d'appuyer une plainte. Comment est organisé votre système informatique pour pouvoir gérer ce type d'incident ?

S. Darmon : Nous disposons d'un serveur de centralisation des journaux systèmes qui trace toutes nos activités informatiques. Ces journaux servent de preuves en cas de besoin. Depuis l'attaque subie par notre client Ecotri, nous avons augmenté considérablement nos capacités de stockage.

Vous : Pouvez-vous en dire plus sur ce serveur de centralisation ?

S. Darmon : Il s'agit d'une grappe de deux serveurs redondés, située dans la salle des serveurs, qui collecte en temps réel les journaux systèmes de tous les serveurs de la pépinière et de nos clients. Si un serveur tombe en panne, le second prend le relais automatiquement.

Vous : Et concernant l'horodatage ?

S. Darmon : Nous disposons, en plus, d'un serveur de temps qui garantit que tous nos serveurs, ainsi que ceux de nos clients, sont à l'heure exacte.

...
Vous : Que collectez-vous dans vos journaux systèmes ?

S. Darmon : Tout ce que nous trouvons utile, notamment suite aux dernières cyberattaques, c'est-à-dire les accès aux ressources et les activités de nos systèmes.

Vous : Comment organisez-vous cette collecte ?

S. Darmon : Nos journaux systèmes sont collectés sur des grappes de disques configurés en RAID 5. Le tout est dans une baie spécifique dotée d'une climatisation et d'une alimentation redondante. L'accès à cette baie nécessite une clé.

Vous : Et pour la conservation à long terme ?

S. Darmon : Chaque fin de semaine, les journaux sont compressés et conservés sur des bandes magnétiques en double. De nouveaux fichiers sont alors créés sur les disques pour accueillir les journaux de la nouvelle semaine.

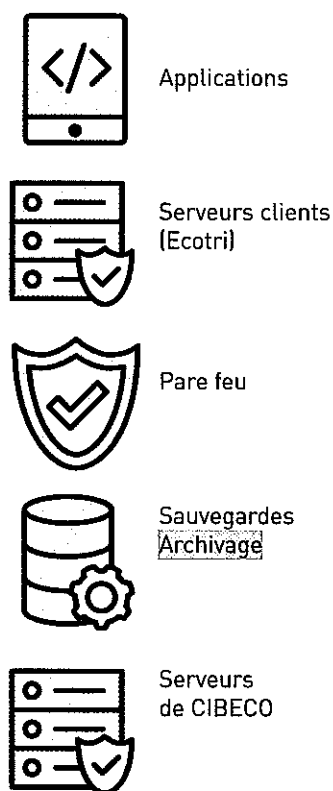
Vous : Puis-je avoir le détail des configurations dont nous venons de discuter ?

S. Darmon : Oui, je demande à Yaël de vous fournir des fiches techniques précises sur chacun de ces éléments.

Document 2 Le réseau de collecte des preuves numériques de Cibeco

La collecte des preuves s'appuie sur l'enregistrement des journaux systèmes. Un réseau dédié à cette collecte s'appuie sur trois serveurs : deux serveurs pour centraliser les journaux systèmes et un serveur de temps pour assurer un horodatage précis.

Sources des journaux systèmes



Serveur syslog de CIBECO :

- Outil utilisé : Syslog kiwi
- Gestion des logs en temps réel : oui
- Filtrage des logs : équipement, IP, date, heure
- Envoi d'alertes : oui par courriel
- Nombre de sources : illimité

Liste des événements collectés :

- Authentification sur les serveurs : connexions, déconnexions
- Accès aux ressources : fichiers, serveurs, partages...
- Activité des programmes : utilisation, incident
- Activité des systèmes : arrêt, redémarrage, utilisation, erreurs, avertissements...

• La séparation des flux

La collecte des journaux systèmes s'effectue sur le VLAN SERVEUR via un réseau dédié séparé des autres réseaux utilisés par Cibeco et ses clients.

• La bande passante





Une bande passante minimale est garantie pour les flux de collecte des journaux systèmes via un mécanisme de

priorisation des flux. Cette bande passante minimale est configurée sur le pare-feu de Cibeco. Elle est conçue de sorte qu'au moins 10 % de la bande passante totale soit garantis pour le transit des journaux vers le serveur de centralisation, quel que soit le niveau de trafic sur le réseau.

➤ Voir lexique BTS SIO, p. 221

Document 3 La configuration de la collecte des preuves par Cibeco

- Yaël Darmon vous fournit un extrait de la configuration des niveaux de traces enregistrés sur les serveurs de centralisation. Cette configuration dépend des événements collectés par les serveurs de la pépinière et de ses clients.

Événement tracé	Code de collecte configuré	
Succès d'authentification sur la page du forum du client Ecotri		INFORMATION
Plusieurs échecs d'authentification répétés pour déverrouiller l'accès aux archives de Cibeco		AVERTISSEMENT
Arrêt inopiné du serveur de base de données contenant les données des clients d'Ecotri		ERREUR
Inaccessibilité du site Web du client Ecotri		ALERTE CRITIQUE

- Suite aux attaques informatiques récentes, l'entreprise a configuré une supervision de l'espace de stockage disponible pour l'enregistrement des journaux systèmes. Yaël Darmon a programmé la notification automatique d'une alerte lorsque le taux de remplissage des disques dépasse 75 %.

Taux de remplissage des disques	Notifications	Destinataires
> 75 %	Affichage d'un avertissement sur le tableau de bord de l'outil Syslog Kiwi	Yaël et Sarah Darmon
> 90 %	Envoi automatique d'un courriel d'alerte	

Document 4 Un exemple de consultation de preuves collectées par Cibeco

Le tableau de bord de l'application Syslog Kiwi pour la gestion des journaux systèmes permet de faire des recherches sur des événements passés à l'aide de filtres : date, adresse IP, serveur, etc.

Date	Heure	Priorité	Adresse IP	Message
09-06-2019	16:44:54	System4.info	82.54.99.66	Utilisateur jdupont connecté au forum du client Ecotri
09-06-2019	19:44:51	Local5.Alert	99.23.14.67	Inaccessibilité du site Web d'Ecotri

Document 5 La conservation des preuves numériques par Cibeco

- Chaque fin de semaine, les preuves collectées dans les journaux systèmes sont extraites automatiquement des disques puis sont compressées en vue de leur transfert sur des bandes magnétiques dans une **baie de stockage** climatisée et verrouillée. La nouvelle collecte peut écraser la collecte de la semaine précédente sur les disques, et ainsi de suite. La salle des serveurs qui abrite cette baie est dotée d'un système anti-incendie, installé récemment.

COLLECTE DES PREUVES NUMÉRIQUES

Rotation de la collecte chaque semaine



Compression puis transfert

CONSERVATION DES PREUVES NUMÉRIQUES



Enregistrement sur des disques en RAID 5

Conservation sur bandes magnétiques

- Le système de conservation utilisé par Cibeco présente les caractéristiques suivantes :

Caractéristiques de conservation	Valeurs
Nombres de bandes disponibles	10
Capacité de stockage par bande	10 To
Copie en double	OUI
Politique de nommage des fichiers de journaux conservés	Nom indiquant la date de création Exemple : Logs_18112019

Document 6 Le lieu de conservation des preuves numériques

La baie utilisée par Cibeco pour collecter et conserver les éléments de preuves numériques se situe dans la salle des serveurs S02 du bâtiment A.

Bâtiment A	Salle des serveurs avec baie de conservation des preuves numériques
Bâtiment B	Uniquement des bureaux. Liaison fibre avec le bâtiment A

➤ Voir lexique BTS SIO, p. 221

Missions professionnelles

Appliquer les procédures garantissant le respect des obligations légales

Suite à l'audit technique réalisé après l'attaque du site Web du client Ecotri, plusieurs brèches de sécurité sont suspectées et signalées dans des feuilles de révélation et d'analyse des problèmes (FRAP). Ces fiches vous sont remises afin que vous puissiez vérifier si les procédures prévues pour faire face aux brèches de sécurité suspectées respectent bien les obligations légales.



Travail à faire

Le premier point qui ressort de l'audit concerne la **confidentialité** des accès aux ressources informatiques de Cibeco.

1. Indiquez, en argumentant, si la procédure prévue par Cibeco pour faire face à la brèche de sécurité mentionnée dans la FRAP n° 1 garantit le respect des obligations légales.

- > Fiches savoirs technologiques 2, 9 (pp. 25 et 151) et 11
- > Documents 1 et 2

Le deuxième point relevé par l'audit concerne la procédure de transfert des journaux systèmes des disques vers les bandes magnétiques.

2. Expliquez en quoi la procédure prévue par Cibeco pour faire face à la brèche de sécurité mentionnée dans la FRAP n° 2 ne garantit pas la confidentialité et l'**intégrité** des journaux systèmes exigées par la loi.

- > Fiches savoirs technologiques 2, 9 (pp. 25 et 151) et 11
- > Documents 1 et 3

La troisième FRAP concerne le **risque** lié à l'indisponibilité des applications des clients de la pépinière.

3. Montrez que la procédure technique prévue par Cibeco pour faire face à la brèche de sécurité mentionnée dans la FRAP n° 3 ne suffit pas à garantir l'intégrité des applications Web des clients prévue dans l'accord de niveau de service.

- > Fiches savoirs technologiques 2 (p. 25) et 11
- > Documents 1 et 4

4. Expliquez pourquoi les organismes de lutte contre la cybercriminalité exigent que ces procédures garantissent le respect des obligations légales.

- > Fiche savoirs CEJMA 9
- > Document 1

Document 1 Entretien sur les procédures de gestion des incidents chez Cibeco

Y. Darmon : Nous venons de terminer l'audit technique sur nos procédures en cas de brèche de sécurité.

S. Darmon : Qu'en est-il exactement ?

Y. Darmon : J'ai relevé plusieurs problèmes potentiels qui pourraient impacter la confidentialité, l'intégrité et la **disponibilité** de nos systèmes. J'ai notifié sur des FRAP tous ces problèmes potentiels en indiquant les procédures prévues actuellement pour y faire face s'ils venaient à se concrétiser.

S. Darmon : Nous avons donc encore des problèmes potentiels... Je ne m'y attendais pas, nous avons tellement investi après l'intrusion dans nos archives. Notre système de **traçabilité** Syslog Kiwi a coûté cher, sans compter tous nos efforts pour augmenter nos capacités de stockage.

Y. Darmon : C'est vrai, notre analyse montre que nous disposons de bons outils pour conserver les preuves en cas d'intrusion. Mais posséder ces outils ne suffit pas. Il faut appliquer correctement les procédures qui vont avec. Il y a des lois à respecter et il faut absolument vérifier que les procédures prévues dans nos

FRAP répondent aux obligations légales qui s'imposent.

S. Darmon : Nos procédures en cas d'incidents ne sont donc pas valables ?

Y. Darmon : C'est ce qu'il faut vérifier. J'ai relevé trois FRAP représentatives. Par exemple, je m'interroge sur la procédure de transfert de nos journaux systèmes sur bandes... Car si l'analyse montre que la collecte est conforme aux recommandations d'usage, il y a peut-être un risque pour l'intégrité au moment du transfert. Or, la loi impose une garantie de cette intégrité.

S. Darmon : Et les deux autres ?

Y. Darmon : Si la confidentialité de nos clés d'administration des serveurs est compromise, notre procédure de secours est sans doute insuffisante. De plus, certains de nos serveurs ne sont pas redondés. Nous avons bien des serveurs de secours, mais leur configuration ne garantit peut-être pas une reprise de la disponibilité totale pour nos clients.

S. Darmon : Il y a urgence. Notre technicien doit faire un bilan de tout cela immédiatement.

Document 2 Extrait de la FRAP n° 1 sur la procédure de secours pour l'accès aux serveurs

FRAP n° 1 Procédure de secours pour l'accès à distance aux serveurs	
Problème	L'accès à distance aux principaux serveurs de Cibeco nécessite une authentification par clé. Seules les personnes habilitées ont connaissance des clés. Celles-ci sont présentes uniquement sur les ordinateurs portables de Yaël et Sarah. Dans ce scénario, on envisage la perte de ces ordinateurs portables.
Procédure prévue (faits, constats)	Dans le scénario envisagé, la procédure suivante est prévue : <ol style="list-style-type: none"> 1. génération de nouvelles clés par Sarah directement depuis les serveurs. Une seule et même clé permet l'accès à tous les serveurs en mode administrateur ; 2. copie du fichier contenant la nouvelle clé sur une clé USB déposée sur le bureau de Yaël, avec un post-it indicatif ; 3. confirmation de la réception de la nouvelle clé par Yaël.
Détail de la procédure	<ul style="list-style-type: none"> – Suppression des anciennes clés : non. – Chiffrement du disque de l'ordinateur portable et de la clé USB : non. – Effacement sécurisé de la clé USB : non.

Missions professionnelles

Document 3 Extrait de la FRAP n° 2 sur l'exploitation des journaux systèmes suite à une fraude


FRAP n° 2 Procédure d'exploitation des journaux systèmes suite à une fraude	
Problème	Cibeco soupçonne des tentatives d'accès frauduleuses à ses serveurs et compte mettre à profit les journaux systèmes pour compromettre la personne malveillante.
Procédure prévue (faits, constats)	Dans le scénario envisagé, la procédure de conservation et de consultation des journaux systèmes utilisés est la suivante : <ol style="list-style-type: none"> 1. collecte des journaux systèmes sur des disques ; 2. transfert des journaux sur des bandes magnétiques ; 3. extraction des journaux avec un filtre en vue d'une suite judiciaire.
Détail de la procédure	La phase de transfert des journaux systèmes des disques vers les bandes magnétiques présente les caractéristiques suivantes : <ul style="list-style-type: none"> – transit par le réseau de Cibeco : oui ; – compression : oui ; – chiffrement : non ; – vérification des sommes de contrôles : non.

Document 4 Extrait de la FRAP n° 3 sur la panne d'un serveur Web d'un client

FRAP n° 3 Panne d'un serveur Web d'un client	
Problème	Le serveur Web d'un client tombe en panne.
Procédure prévue (faits, constats)	Dans le scénario envisagé, la procédure de dépannage est la suivante : <ol style="list-style-type: none"> 1. chaque serveur Web d'un client fait l'objet d'une sauvegarde tous les trois mois ; 2. après une panne, cette sauvegarde est injectée dans un serveur de secours via une copie en temps différé ; 3. le serveur de secours est mis en production afin de restaurer l'accès des clients.
Détail de la procédure	La sauvegarde des serveurs Web des clients présente les caractéristiques suivantes : <ul style="list-style-type: none"> – copie des pages Web : oui, une fois par trimestre ; – copie de la base de données associée au site Web : oui, une fois par trimestre.

Organiser la collecte des preuves numériques



>  Fiche savoirs technologiques 11

Afin de réduire ses coûts, Cibeco souhaite s'orienter vers un nouveau pare-feu *open source*. La solution pfSense semble intéressante, mais il faut la tester avant de la valider.




À partir des machines virtuelles utilisées pour le travail en laboratoire du chapitre 6, vous effectuerez des configurations permettant de valider les moyens de preuves numériques offerts par cette solution. Deux types de tests sont à réaliser :

- d'abord, la configuration d'un serveur de temps : vous configurez un serveur de temps afin de garantir que toutes les preuves collectées par le pare-feu pfSense indiquent une heure exacte ;
- ensuite, la configuration de la collecte des traces : vous configurez sur pfSense l'enregistrement des traces des clients qui se connectent au serveur Web Mutillidae.



ÉTAPE 1 La préparation de l'environnement de travail

1. Préparez votre environnement de travail en suivant les étapes décrites dans le document 1, puis démarrez toutes les machines.
2. Connectez-vous au pare-feu en suivant les étapes décrites dans le document 2.

ÉTAPE 2 La configuration du serveur de temps sous pfSense

3. Mettez votre pare-feu pfSense à l'heure.
>  Document 3
4. Configurez votre pare-feu pfSense pour qu'il soit un serveur de temps.
>  Document 4
5. Mettez le serveur Web Mutillidae à l'heure en vous appuyant sur le serveur de temps pfSense.
>  Document 5

ÉTAPE 3 La configuration de l'enregistrement des traces

6. Configurez votre pare-feu pfSense pour qu'il enregistre les traces des connexions du hacker sur le serveur Web Mutillidae.
>  Document 6
7. Connectez-vous au serveur Web Mutillidae depuis la machine du hacker, puis vérifiez que le pare-feu trace votre connexion dans les journaux systèmes.
>  Document 7

Document 1 La préparation de l'environnement de travail

Pour préparer l'environnement de travail :

- si vous avez effectué le travail en laboratoire du chapitre 6, vous pouvez passer directement à la question n° 2 du travail à faire ;
- si vous n'avez pas effectué le travail en laboratoire du chapitre 6, vous devez configurer l'environnement de travail initial en suivant les procédures décrites dans l'étape 1 du travail en laboratoire du chapitre 6, p. 145.

Document 2 La procédure de connexion au pare-feu

Afin de disposer d'un horodatage correct lors de la collecte des journaux systèmes servant de preuves, il est nécessaire que le serveur Web Mutillidae soit à l'heure (voir Fiche savoirs technologiques 11). Dans la maquette utilisée, c'est le pare-feu pfSense qui joue le rôle de serveur de temps. Les autres serveurs se mettent à l'heure en interrogeant le serveur de temps sous pfSense. Pour se connecter au pare-feu pfSense, il faut suivre la procédure suivante :

Depuis la machine **DELAGRAVE-CLIENT-LEGITIME-UBUNTU** :

Ouvrir le navigateur et utiliser l'URL ci-dessous afin de se connecter au pare-feu :

<https://192.168.50.254>

L'adresse IP indiquée correspond à celle du pare-feu sur l'interface servant de passerelle pour les machines clientes du réseau **LAN-IN** (voir le schéma du réseau, p. 145). Par défaut, l'authentification sur le pare-feu pfSense se fait avec l'identifiant **admin** et le mot de passe **pfsense**.



Document 3 La mise à l'heure du pare-feu

Il convient de s'assurer que le pare-feu est configuré sur le bon fuseau horaire. Pour cela, il faut :

- d'abord, aller dans le menu **System**, puis cliquer sur **General Setup**.
- ensuite, dans la rubrique de localisation, sélectionner la zone géographique **Europe/Paris** ;
- enfin, valider en cliquant sur **Save** en bas de l'écran.

Document 4 La configuration du serveur de temps sous pfSense

Lorsque le pare-feu pfSense est sur le bon fuseau horaire, il faut suivre une procédure pour le configurer comme un serveur de temps :

- d'abord, aller dans le menu Services, puis cliquer sur **NTP** ;
- ensuite, indiquer l'interface sur laquelle le **serveur de temps** écoute les requêtes de mise à l'heure ainsi que le **pool de serveurs sur Internet** (groupe de serveurs) permettant une mise à l'heure correcte.

• En ce qui concerne l'interface d'écoute du serveur NTP : il faut sélectionner l'interface SRV-IN. C'est sur cette interface que se situe la zone serveur du contexte. Ce réseau ne comporte qu'un seul serveur Web, qui héberge l'application Web Mutillidae.

• En ce qui concerne le **pool de serveurs sur Internet**, il s'agit d'un fonctionnement par strates. Le serveur Web qui héberge Mutillidae se met à l'heure via le serveur de temps du pare-feu pfSense, qui, lui-même, se met à l'heure exacte en consultant d'autres serveurs de temps présents sur Internet dans le pool sélectionné. C'est pourquoi votre pare-feu pfSense doit avoir accès à Internet. Dans votre laboratoire, il suffit de laisser la valeur proposée par défaut à **0.pfsense.pool.ntp.org**. Enfin, cliquer sur **Save** en bas de l'écran. Votre pare-feu fait désormais office de serveur de temps.

Document 5 La mise à l'heure du serveur Web Mutillidae

Lorsque le serveur de temps pfSense est à l'heure, vous pouvez l'utiliser pour mettre à l'heure votre serveur Web Mutillidae. La procédure à suivre est la suivante :

Depuis la machine **DELAGRAVE-SERVEUR-UBUNTU** :

- ouvrir le fichier **ntp.conf** localisé dans le **répertoire /etc** avec la commande **sudo nano /etc/ntp.conf** ;
- dans ce fichier, supprimer toutes les lignes commençant par **pool** et les remplacer par la seule ligne suivante : **server 172.16.10.254** ;

- enregistrer le fichier, puis quitter l'éditeur de texte nano. L'adresse IP indiquée est celle du pare-feu, donc du serveur de temps ;
- redémarrer le service avec la commande **sudo service ntp restart** ;
- utiliser la commande **ntpq -pn** afin de vérifier que l'adresse IP de votre serveur de temps s'affiche.

Document 6 La configuration de la collecte des traces

Pour que le pare-feu pfSense enregistre les traces des connexions des clients au serveur Web Mutillidae, il faut éditer une règle de filtrage. La procédure à suivre est la suivante :

Depuis la machine **DELAGRAVE-CLIENT-LEGITIME-UBUNTU** :

- d'abord, se connecter au pare-feu via le navigateur Web et cliquer sur le menu **Firewall**, puis sur **Rules** ;
- ensuite, cliquer sur l'interface **LAN_IN**, puis cliquer sur l'icône permettant de modifier la deuxième règle qui autorise l'accès au serveur Web Mutillidae (voir ci-contre). Une page permettant d'éditer la règle de filtrage s'ouvre. Aller en bas de la page et cocher la case permettant de tracer les événements associés à cette règle de filtrage :

Journal ☒ **Journaliser les paquets gérés par cette règle**

- enfin, valider en cliquant sur les boutons **Save** et **Apply Changes**. Tout accès au serveur Web Mutillidae depuis le réseau LAN-IN est maintenant tracé.

➤ Voir lexique BTS SIO, p. XXX

Document 7 Le test de collecte des journaux systèmes

Pour vérifier si une connexion au serveur Web Mutillidae est bien tracée à l'heure exacte, il faut effectuer les manipulations suivantes.

Depuis la machine **DELAGRAVE-CLIENT-HACKER-UBUNTU** :

- ouvrir le navigateur et se connecter à l'application Web Mutillidae en utilisant l'URL suivante : **http://172.16.10.5/mutillidae**. Il est inutile de s'authentifier. Il suffit de naviguer sur n'importe quelle page de l'application pour générer des traces ;
- ensuite, se rendre sur le pare-feu pour vérifier les traces collectées en réalisant le travail qui suit.

Depuis la machine **DELAGRAVE-CLIENT-LEGITIME-UBUNTU** :



- se connecter au pare-feu et cliquer sur le menu **Firewall**, puis sur l'interface **LAN_IN**. Ensuite, cliquer sur l'icône des journaux systèmes situé en haut, à droite de la page ;



- ensuite, utiliser un **filtre** permettant de tracer toutes les connexions à distance du serveur Web Mutillidae. L'icône de filtrage est située en haut, à droite de l'écran.

Les plans de secours, la traçabilité et l'audit technique

Le contrôle de la sécurité nécessite des outils permettant de prévoir un plan de secours, la traçabilité des événements ainsi qu'un audit technique des procédures prévues par l'organisation en cas de brèche de confidentialité, d'intégrité ou de disponibilité.

I Les plans de secours

Le plan de continuité d'activité (PCA) et le plan de reprise d'activité (PRA) permettent aux organisations de poursuivre leur activité en cas d'incident ou de sinistre.

Plan de continuité d'activité	L'objectif est d'assurer la continuité des activités en cas d'incident. Un PCA peut, par exemple, prévoir des sauvegardes, qui permettent des restaurations en cas de pertes de données.
Plan de reprise d'activité	L'objectif est d'assurer la reprise des activités en cas de sinistre important (incendie, inondations, etc.). Par exemple, une entreprise peut prévoir un site de secours.

II La traçabilité

La traçabilité permet de suivre les actions réalisées au sein d'un système informatique. Elles sont enregistrées dans des *logs* qui peuvent servir de preuves numériques. L'ANSSI recommande d'enregistrer les événements suivants :

Événements	Exemples
Authentification	Réussites et échecs d'authentification, utilisation des différents mécanismes d'authentification, élévation de <u>privileges</u> .
Gestion des comptes et des droits	Ajouts, suppressions de comptes ou de groupes, affectations ou suppressions de droits aux comptes ou aux groupes, modifications des données d'authentification.
Accès ou modification des ressources et des configurations	Accès ou tentatives d'accès en lecture, écriture ou exécution aux ressources et aux applications. Réinitialisation de configurations.
Activité des processus (programmes) et des systèmes (matériels et systèmes d'exploitation)	Démarrages ou arrêts, dysfonctionnements, surcharges du système, chargement ou déchargement de modules, activité matérielle (défaillance, connexions, déconnexions).

Afin que l'exploitation juridique des preuves numériques soit garantie, l'ANSSI recommande également d'appliquer les procédures ci-dessous.

1. La conservation des traces

Les journaux systèmes doivent être collectés dans un format lisible et facilement consultable. Ils doivent faire l'objet d'un chiffrement et d'une compression. Il faut également prévoir un espace disque suffisant, redondé et supervisé afin de garantir la continuité de la collecte.

2. La centralisation et la rotation des traces

Les journaux systèmes doivent être centralisés afin d'éviter l'utilisation de plusieurs sources incohérentes. Il est nécessaire de prévoir un processus qui automatise la permutation, la suppression et l'envoi des journaux selon des intervalles de temps permettant une conservation pendant une certaine durée : trois mois pour les réseaux d'entreprise, et une année pour les fournisseurs d'accès à Internet.

3. L'horodatage

La collecte doit être effectuée avec des serveurs parfaitement à l'heure afin d'obtenir des informations exactes sur la date et l'heure. Le serveur de temps peut être utilisé pour synchroniser les horloges de l'ensemble des serveurs. Il s'appuie sur le protocole NTP (*Network Time Protocol*).

4. Le transfert en temps réel

L'enregistrement des événements doit être réalisé immédiatement, et non en temps différé, pour garantir qu'il correspond à la photographie exacte des faits enregistrés au moment de la consultation des traces.

5. Le réseau dédié

Afin de séparer les flux, il convient de faire transiter les journaux par un réseau dédié avec une bande passante minimale garantie.

III L'audit technique

L'audit technique vise à évaluer les procédures prévues par une organisation en cas de brèche de sécurité. Cet audit s'appuie sur l'élaboration de FRAP (feuilles de révélation et d'analyse des problèmes). Ces documents sont complétés lorsque des dysfonctionnements ou des risques sont détectés : constat du problème, causes, conséquences, recommandations.

IV Les outils de contrôle de la sécurité des critères DIC

Disponibilité	Utilisation de solutions de hautes disponibilités (<i>High Availability</i> , HA) permettant de garantir une continuité de service en cas de défaillance d'un serveur ou d'une application. Exemple : redondance d'un serveur pour l'accès à un service.
Intégrité	Utilisation d'algorithmes de sommes de contrôles, qui calculent un condensé unique à partir d'une information donnée. La moindre modification de contenu entraîne un changement du résultat de la somme de contrôle. Exemple : l'algorithme MD5 (<i>Message Digest 5</i>) ou le SHA-256 (<i>Secure Hash Algorithm</i>).
Confidentialité	Utilisation d'algorithmes de chiffrement récents et robustes. Exemple : l'algorithme AES (<i>Advanced Encryption Standard</i>), qui est approuvé par la NSA (<i>National Security Agency</i>) aux États-Unis.

Les organisations de lutte contre la cybercriminalité

La recrudescence des actes de cybercriminalité a amené de nombreux États à mettre en place des organismes spécifiques afin de lutter contre ce phénomène. Par exemple, l'Union européenne dispose d'un centre destiné à coopérer avec l'ensemble des États membres. Les services de police et de gendarmerie des États possèdent des unités spécialisées selon le type de criminalité concerné.

I L'Union européenne contre la cybercriminalité



EUROPOL

Europol (European Police Office) est une agence européenne de police criminelle qui facilite l'échange de renseignements entre les polices nationales des États membres en matière de stupéfiants, de terrorisme, de criminalité internationale, de pédophilie et de cybercriminalité au sein de l'Union européenne.

Début des missions
1^{er} juillet 1999

Siège
La Haye (Pays-Bas)



Le Centre européen de lutte contre la cybercriminalité (*European Cybercrime Centre* ou EC3) est une structure luttant contre la cybercriminalité en Europe. Elle est située dans les locaux d'Europol. La création de ce centre fait partie des mesures prises par l'UE pour protéger les citoyens contre la criminalité en ligne : fraude, maltraitance infantile, activités illicites exercées par des organisations criminelles. Europol est à l'initiative, avec la police néerlandaise et les sociétés Kaspersky Lab et McAfee, de la plateforme No More Ransom, dont le but est d'aider les victimes des rançongiciels à retrouver leurs données chiffrées sans avoir à payer les criminels.

Début des missions
1^{er} janvier 2013

Siège
La Haye (Pays-Bas)



Eurojust (Unité de coopération judiciaire de l'Union européenne) est l'agence européenne chargée de renforcer la coopération judiciaire entre les États membres, par l'adoption de mesures destinées à promouvoir une coordination optimale des actions d'enquêtes et de poursuites.

Début des missions
28 février 2002

Siège
La Haye (Pays-Bas)

II

La lutte contre la cybercriminalité en France

En France, des services spécialisés sont chargés de la lutte contre la cybercriminalité.

La police nationale



La Sous-direction de lutte contre la cybercriminalité (SDLC) est un organisme de la police française voué à la lutte contre la cybercriminalité. C'est une branche de la Direction centrale de la police judiciaire.

La gendarmerie nationale



Le Centre de lutte contre les criminalités numériques (C3N) regroupe l'ensemble des unités du pôle judiciaire de la gendarmerie nationale qui traitent directement de la criminalité et des analyses numériques. Le C3N assure également l'animation et la coordination, au niveau national, de l'ensemble des enquêtes menées par le réseau des enquêteurs numériques de la gendarmerie.

La préfecture de police



La Brigade d'enquêtes sur les fraudes aux technologies de l'information (BEFTI) est un service de la Direction régionale de la police judiciaire de Paris créé en février 1994. Sa mission essentielle est de lutter contre les atteintes aux systèmes de traitement automatisé de données (STAD), qu'il s'agisse des réseaux informatiques ou télématiques, ou des systèmes de télécommunications (GSM, autocommutateurs d'entreprises, etc.).

III

La lutte internationale contre la cybercriminalité

Dans le reste du monde, d'autres organismes luttent contre la cybercriminalité. Aux États-Unis, le FBI (*Federal Bureau of Investigation*) est la principale agence fédérale chargée d'enquêter sur les cyberattaques.

Europol a créé le J-CAT (*Joint Cybercrime Action Taskforce*), une structure de coordination spécialement dédiée à la lutte contre la cybercriminalité dans l'Union européenne et au-delà.



Retrouvez ce QCM
en version interactive
www.lienmini.fr/6988-701

1

1 Quelles sont les informations exactes concernant le PRA et le PCA ?

- ☐ Le PRA permet d'assurer la reprise des activités en cas de sinistre important.
- ☐ Le PCA permet d'assurer l'intégrité d'une preuve numérique.
- ☐ Le PCA permet d'assurer une continuité des activités de l'entreprise en cas d'incident.

2 La rotation des journaux systèmes :

- ☐ nécessite le recours à plusieurs salariés de l'entreprise.
- ☐ automatise la permutation et la suppression de journaux systèmes selon des intervalles de temps définis.
- ☐ est un processus qui augmente la capacité de stockage des disques.

3 Quels sont les organismes de lutte contre la cybercriminalité ?

- ☐ BEFTI
- ☐ OCLCTIC
- ☐ BGP

4 Un serveur de temps :

- ☐ synchronise les horloges des machines du réseau informatique.
- ☐ assure l'intégrité des échanges.
- ☐ distribue des adresses IP aux machines du réseau.

5 Les sommes de contrôle (hash) garantissent :

- ☐ l'intégrité.
- ☐ la confidentialité.
- ☐ la disponibilité.

6 Les FRAP sont :

- ☐ des feuilles d'analyse associées à un audit technique.
- ☐ des documents remplis lors de la détection d'un dysfonctionnement ou d'un risque.
- ☐ des feuilles d'analyse contenant tous les journaux du système.

7 Quels sont les algorithmes de calcul de sommes de contrôles (hash) ?

- ☐ SHA256
- ☐ MD5
- ☐ SNMP
- ☐ CBQ

8 L'algorithme de chiffrement AES :

- ☐ est un algorithme récent et robuste.
- ☐ assure la disponibilité d'une ressource.
- ☐ permet d'accéder à un seul et unique service.

9 Le protocole NTP :

- ☐ signifie *Network Transfert Protocol*.
- ☐ permet de chiffrer les échanges.
- ☐ permet de disposer d'un serveur de temps.

10 Concernant la collecte des preuves numériques, l'ANSSI recommande :

- ☐ de disposer d'un espace disque suffisant, redondé et supervisé.
- ☐ de collecter les traces en temps réel.
- ☐ d'autoriser tous les utilisateurs de l'entreprise à consulter tous les journaux systèmes.
- ☐ d'interdire le chiffrement des journaux systèmes.



- > Fiche savoirs technologiques 11
- > Fiche CEJMA 9

Situation

L'annexe ci-dessous présente deux cas concrets rencontrés dans le contexte d'un établissement scolaire. Répondez aux questions suivantes en vous reportant à cette annexe.

Cas n° 1

- 1 Indiquez si ce cas relève d'un acte malveillant. Justifiez votre réponse.
- 2 Expliquez en quoi la consultation des journaux systèmes a permis d'améliorer le fonctionnement du réseau informatique de l'établissement.

Cas n° 2

- 3 Indiquez si ce cas constitue une brèche de confidentialité sur les données à caractère personnel. Justifiez votre réponse.
- 4 Donnez le nom de l'organisme chargé d'enquêter. Indiquez qui est le responsable juridique du système d'information.
- 5 Justifiez la nécessité de consulter les journaux systèmes pour aider à la résolution de ce cas.

Annexe

Deux cas concrets



Cas n° 1

Les utilisateurs de l'établissement se plaignent du ralentissement de l'accès à Internet à une certaine heure de la journée. À la demande du chef d'établissement, la responsable informatique effectue une analyse volumétrique, à partir des journaux de consultation du Web et elle ne constate aucun transfert particulièrement volumineux à l'heure concernée. Elle poursuit ses investigations sur d'autres journaux des systèmes de l'établissement et finit par découvrir qu'il s'agit du processus de remontée de données du logiciel de gestion



de parc informatique. Suite à ce constat, elle reconfigure le processus de remontée afin que ce dernier opère la nuit et tout rentre dans l'ordre.

Cas n° 2

Un élève a usurpé le compte d'un de ses camarades dans l'application Gibii (Gestion informatisée du brevet informatique et Internet). L'usurpateur a déposé, dans l'application, des insultes envers un professeur, qui a porté plainte. Pour les besoins de l'enquête, la gendarmerie demande au responsable juridique du système d'information (le chef d'établissement) les journaux informatiques, qui vont permettre d'innocenter le propriétaire du compte usurpé et de remonter à l'auteur du délit.

<https://eduscol.education.fr>

3

- >  Fiche savoirs technologiques 11
- >  Fiche CEJMA 9



Situation




Vous travaillez au sein du support technique de l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC) et vous êtes chargé(e) d'enquêter sur la mise en ligne et la circulation de la photographie. Vous devez, notamment, effectuer des tests avec un outil d'investigation disponible sur Internet.

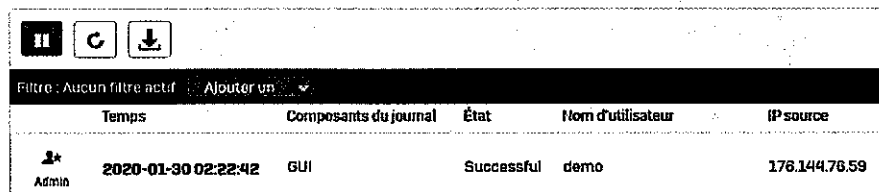
SA-Conseil fournit des prestations de conseil à de jeunes startups. L'entreprise propose, notamment, des activités de coaching et des sessions de formations dans le domaine de la gestion.

Récemment, SA-Conseil a été victime d'une attaque qui a remis en cause sa réputation. En effet, une photographie truquée avec le logo de l'entreprise et montrant le gérant en train de vomir a été publiée sur les réseaux sociaux. Très vite, le partage de cette photographie est devenu viral. Le gérant de SA-Conseil a déposé plainte.

- 1 Rappelez quel est le rôle de l'OCLCTIC dans le cadre de cette affaire.
- 2 À l'aide de recherches sur Internet, définissez les termes suivants : métadonnées, données EXIF, géolocalisation.
- 3 Rendez-vous sur le site GitHub, qui contient des exemples d'images permettant de réaliser des tests pour retrouver des métadonnées :
>  Site GitHub : www.lienmini.fr/6988-702
- 4 Ouvrez un autre onglet sur le navigateur et rendez-vous sur le site metapicz.com.
>  Site metapicz : www.lienmini.fr/6988-703
- 5 Téléchargez une image depuis le site GitHub et importez-la dans la zone d'analyse du site metapicz.com.
- 6 Relevez les métadonnées disponibles et testez à nouveau avec une autre image. Pour chaque image, vérifiez si les informations suivantes sont disponibles : auteur de l'image, géolocalisation, appareil photo utilisé.
- 7 Expliquez l'intérêt de l'outil testé dans le cadre de l'enquête en cours.

>  Fiche savoirs technologiques 11

- 1 Rendez-vous sur le site <https://www.sophos.com>, puis cliquez sur le lien permettant d'accéder aux démonstrations en ligne (<https://secure2.sophos.com/en-us/products/demos.aspx>).
- 2 Cliquez sur le bouton permettant d'accéder au pare-feu en ligne XG. Ensuite, créez un compte afin d'accéder à la démonstration en ligne. Une fois le compte validé, connectez-vous en utilisant *demo* pour le login et pour le mot de passe.
- 3 Une fois connecté(e) au pare-feu, cliquez sur le bouton *log viewer* situé en haut, à droite. Une nouvelle fenêtre s'ouvre et affiche les traces des connexions qui transitent par le pare-feu.
- 4 Relevez les noms des colonnes du tableau de synthèse des journaux systèmes. Expliquez le rôle de chaque colonne.



	Temps	Composants du journal	État	Nom d'utilisateur	IP source
Admin	2020-01-30 02:22:42	GUI	Successful	demo	176.144.76.59

- 5 Cliquez sur la liste déroulante située en haut, à droite, puis relevez les catégories d'événements tracés par le pare-feu. Cette liste de catégories d'événements tracés est-elle en conformité avec ce que recommande l'ANSSI ?

Admin

- 6 Dans la liste déroulante, sélectionnez la rubrique *Admin*, puis saisissez la chaîne de caractère *Failed* dans la zone de recherche située à droite de la liste déroulante. Validez la saisie, puis expliquez à quoi correspond le résultat affiché et quel peut être son intérêt dans le cadre de la traçabilité des événements.

Search...



Évaluation 4

L'organisation cliente

Fermabio est une entreprise familiale fondée en 2002 qui distribue des produits issus de l'agriculture biologique. Située à Nangis, dans le département de Seine-et-Marne, Fermabio s'appuie sur un solide réseau de producteurs locaux qui lui assurent un approvisionnement régulier en produits frais.

Ses clients sont des magasins bio qui passent leurs commandes sur un site extranet comportant l'ensemble des produits proposés (fruits et légumes, boissons, épicerie, hygiène et beauté). L'accès à ce site nécessite une authentification via un identifiant et un mot de passe.

Fermabio possède un entrepôt de 4 000 m² situé près d'un bâtiment comportant les services de gestion suivants : administration des ventes (ADV), logistique et achat.

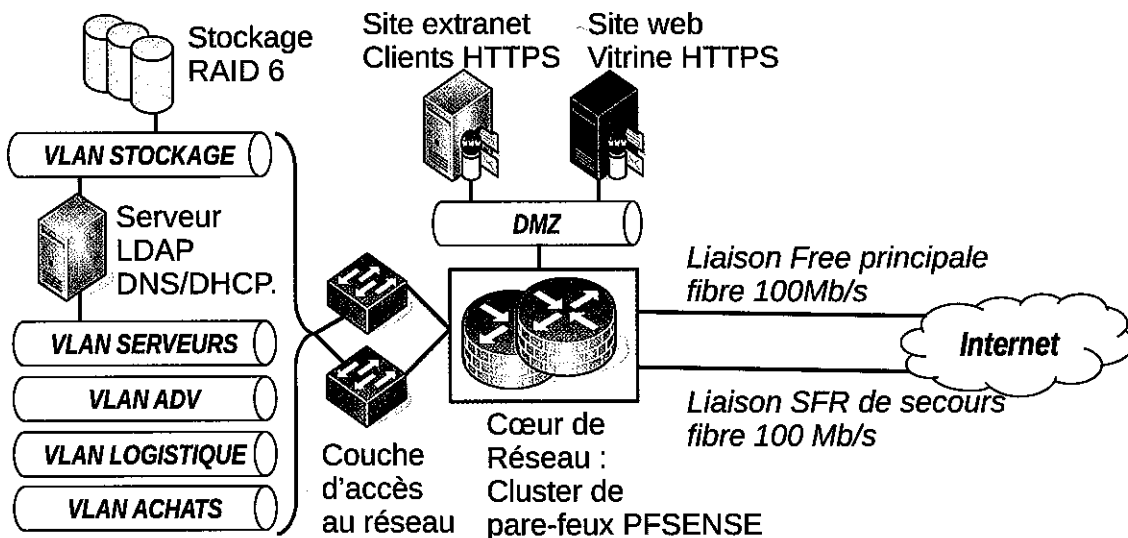
Récemment, Fermabio a été victime d'une cyberattaque. Les comptes de plusieurs clients ont été piratés. L'attaque a été détectée tardivement suite aux plaintes des victimes. Après cette attaque, Fermabio a fait appel à la société Securenet, spécialisée en conseil sur la sécurité du numérique.



Le prestataire informatique

Securenet est une entreprise spécialisée en prestations d'audit sur la cybersécurité. Elle analyse les systèmes informatiques de ses clients et produit des rapports comportant des recommandations à suivre.

Architecture réseau de Fermabio



Votre mission

Vous êtes technicien(ne) informatique chez Securenet chargé(e) d'analyser la sécurité informatique du client Fermabio. Dans un premier temps, vous analysez la sécurité du site extranet de FERMABIO. Dans un second temps, vous menez une étude de la traçabilité des événements informatiques de Fermabio afin d'améliorer la réactivité en cas de cyberattaque.

Missions

1 Analyser la sécurité du site extranet de Fermabio

Afin d'auditer la sécurité du site extranet, vous effectuez deux tests qui analysent le code source du site et le fichier de configuration du serveur Web.

- 1.1. Expliquez pourquoi le test n°1 montre que la confidentialité et l'intégrité ne sont pas garantis.
- 1.2. Proposez une modification de ce code source afin de corriger la vulnérabilité détectée.
- 1.3. En vous appuyant sur le schéma du réseau de Fermabio, expliquez quelles sont les configurations qui garantissent une disponibilité du site extranet.
- 1.4. Indiquez, en justifiant, si le résultat du test n° 2 révèle un problème de sécurité.

2 Améliorer la traçabilité des événements informatiques de Fermabio

La fraude subie n'a laissé aucune trace exploitable sur les serveurs et a été détectée tardivement par la comptabilité. Vous cherchez à comprendre cette anomalie en vérifiant les configurations d'enregistrement des journaux systèmes.

- 2.1. Expliquez le problème posé par la configuration d'enregistrement des journaux systèmes de Fermabio.
- 2.2. Listez les modifications à apporter pour disposer d'un système de traçabilité conforme aux recommandations d'usage.

Dossier documentaire

Document 1

Résultat du test n° 1

Test n° 1 : Analyse du code source à l'aide d'un scanner de vulnérabilité

Vulnérabilité XSS trouvée : niveau de risque élevé

Description	Le <i>cross-site-scripting</i> (XSS) est un type de faille de sécurité des sites Web permettant d'injecter du contenu dans une page, provoquant ainsi l'exécution de code malveillant du type Javascript lors de chaque visite de la page infectée. Une attaque XSS peut modifier le contenu de la base de données et permettre à un attaquant de capturer des cookies d'identifiants de sessions et ainsi s'identifier sur les comptes des victimes sans connaître le mot de passe.
Détail de la vulnérabilité	URL Get input <code>commentaire_commande</code> was set to <code>1'')%<cx><script>vf8s(9896)</script></code> in page <code>panier.php</code>
Conseil pour la correction de la vulnérabilité	<ol style="list-style-type: none"> 1. Vérification des données saisies dans le champ <code>commentaire_commande</code> afin de repérer qu'il n'y a pas de caractères suspects associés à du code malveillant via une liste noire de caractères interdits. 2. Encodage des données saisies afin de rendre impossible l'exécution de code malveillant via la fonction <code>htmlspecialchars</code> : <code>string htmlspecialchars (string)</code>. La fonction <code>htmlspecialchars</code> convertit des caractères spéciaux en entités HTML rendant impossible l'exécution de code malveillant (SQLi, XSS). La fonction reçoit en paramètre la chaîne à convertir et renvoie comme résultat une chaîne encodée. Par exemple, la chaîne <code><script></code> devient <code>&lt;script&gt;</code>.

Document 2

Extrait du code source contenant la vulnérabilité

```

1- <?php
2- //1-Récupération du commentaire saisi par l'utilisateur.
3- $commentaire = $_POST['commentaire_commande'];
4- //2-Exécution de la requête.
5- $requete ="UPDATE Commande set commentaire_commande = '$commentaire'
6-           where id_commande =$_SESSION[IdCommande];
7- mysqli_query($requete);

```

Document 3

Résultat du test n° 2

Test n° 2 : Calcul de la somme de contrôle (hash) du fichier de configuration apache2.conf. Ce fichier permet de piloter toute la configuration du serveur Web qui héberge le site extranet (activation du chiffrement, modules chargés...).

- Somme de contrôle du fichier apache2.conf de configuration du serveur Web calculée avant l'attaque et conservée par Fermabio

Algorithme utilisé	SHA256
Fichier de configuration testé	/etc/apache2/apache2.conf
Somme de contrôle	bc6682a799eaf7056e9ba0ffe6d6fb5f5d57f9422f07cfb69f634b2dddcab767

- Somme de contrôle du fichier apache2.conf de configuration du serveur Web calculée lors de l'intervention de Securenet

Algorithme utilisé	SHA256
Fichier de configuration testé	/etc/apache2/apache2.conf
Somme de contrôle	bc6682a561eaf7056e9ba0ffe6d6fb5f5d57f9422f07cfb69f634b2dddpm767

Document 4

Configuration de la collecte des journaux systèmes de Fermabio

Le *cluster* de pare-feu PfSense est configuré pour enregistrer les journaux systèmes et présente les caractéristiques suivantes :

Date et heure affichée	Vendredi 29 novembre 2019, 08h05
Fuseau horaire	America/Denver
Méthode d'enregistrement	Temps différé : transfert des journaux sur les disques de conservation chaque fin de semaine
Centralisation des logs	Non
Méthode de transfert vers les disques	HTTP