PARTIE THEORIQUE:/40 points

1) Quelle est la norme ISO concerne la gestion des risques de sécurité de l'information ?
2) Est-ce qu'un pare-feu peut protéger contre tous les types de cyberattaques ? justifier votre réponse
3) Définir le spoofing IP
4) Quel type d'attaques vise à accéder au système en détournant les mesures normales de sécurité ?
5) Un utilisateur consulte un site web, mais constate que le navigateur le redirige vers un autre site web et que l'URL a changé. De quel type d'attaque s'agit-il ?
6) Quelles peuvent être les approches du test d'intrusion ?
7) Quel est l'objectif principal de l'automatisation de la réponse aux incidents (Incident Response Automation) ?
8) Est-ce que VELOCIRAPTOR est un outil pour la détection proactive des menaces ? Justifier votre réponse.
9) Le directeur de la société est soucieux que n'importe quel employé puisse utiliser le système d'information de l'entreprise de manière malveillante. Quel test d'intrusion pouvez-vous faire. pour vous assurer de la sécurité de votre système d'information dans un tel scénario ?
10) Associer le numéro du terme à sa définition : *(Recopier le tableau)*

	Terme
1	Ransomware
2	VPN
3	Cryptographie

Numéro	Définition
	Chiffrement et déchiffrement des informations
	Logiciel malveillant qui exige une rançon pour débloquer l'accès aux données
	Réseau permettant une connexion sécurisée sur internet

11) Placer les phrases ci-dessous dans la colonne correspondante du tableau suivant : *(Recopier le tableau)*

A. Attaques de pirates informatiques
B. Attaques par déni de service
C. Logiciels obsolètes
D. Mots de passe faibles.

Menace	Vulnérabilité

12) Remplir le tableau suivant en les scenarios suivants : *(Recopier le tableau)*

A. Évaluez la probabilité de survenue d'une panne du système sur une échelle de 1 à 10.

B. Classez les types de menaces selon leur probabilité d'occurrence et leur impact sur les opérations de l'entreprise.

C. Donnez une estimation subjective de l'impact financier d'une cyberattaque sur l'entreprise.

D. Mesurez le nombre moyen de transactions par minute pour évaluer la charge du serveur.

Analyse quantitative	Analyse Qualitative

13) Expliquer l'importance de la norme ISO 27001.

14) Dans la sécurité du développement. Qu'est-ce que le SAST ?

15) Dans quelle phase de l'OSSTMM est-il crucial de collecter et d'analyser des informations sur la topologie réseau, y compris les adresses IP, les noms de domaine et les informations sur les réseaux sociaux ?

16) Quelle étape de la méthodologie PTES implique l'identification des vulnérabilités de sécurité qui pourraient être exploitées par des attaquants pour compromettre la sécurité du système ?

17) Selon l'OWASP, quelle phase du processus de test est essentielle pour évaluer comment les utilisateurs sont authentifiés et autorisés à accéder aux ressources de l'application ?

18) Afin que les pentesters utilisent des informations pour lancer une campagne d'ingénierie sociale. La syntaxe suivante d'opérateurs google **[intitle:internet inurl:intranet +intext:"human ressources"]** a été utilisée pour trouver des informations sensibles sur une entreprise et ses employés **:[site:linkedin.com intitle:"social security number"]**. Donner l'utilité de cette requête.

19) Citer deux normes de gestion des risques en cyber sécurité.

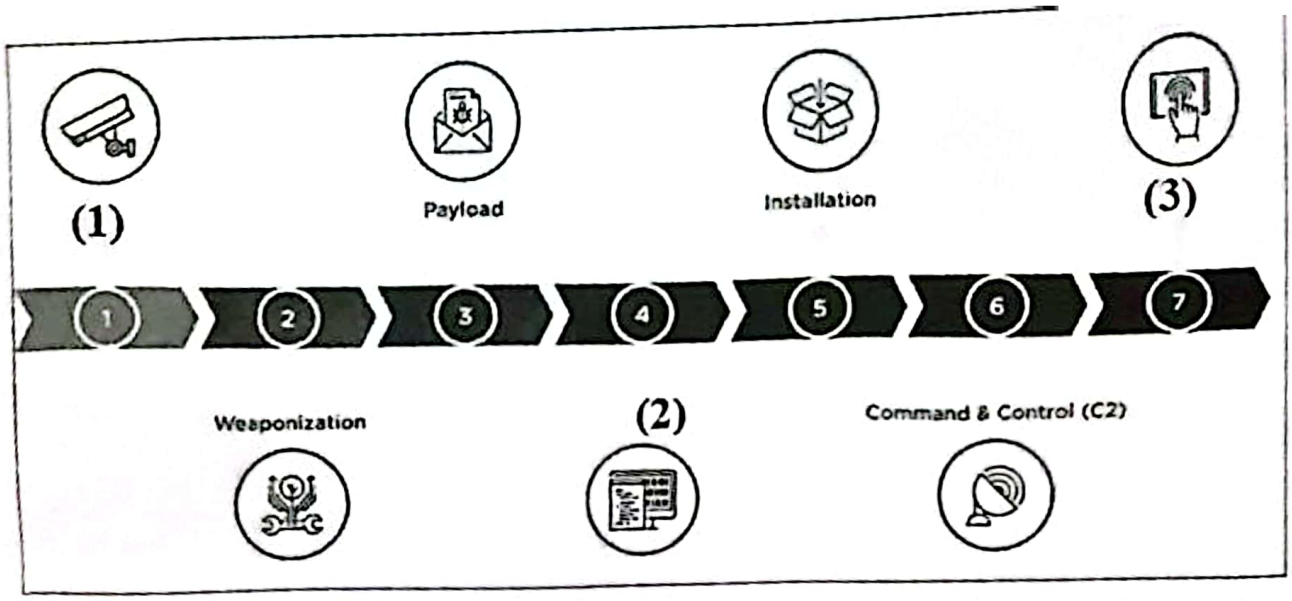
20) Donner les différentes étapes de la gestion des risques.

21) Expliquez le concept de Threat Hunting (chasse aux menaces).

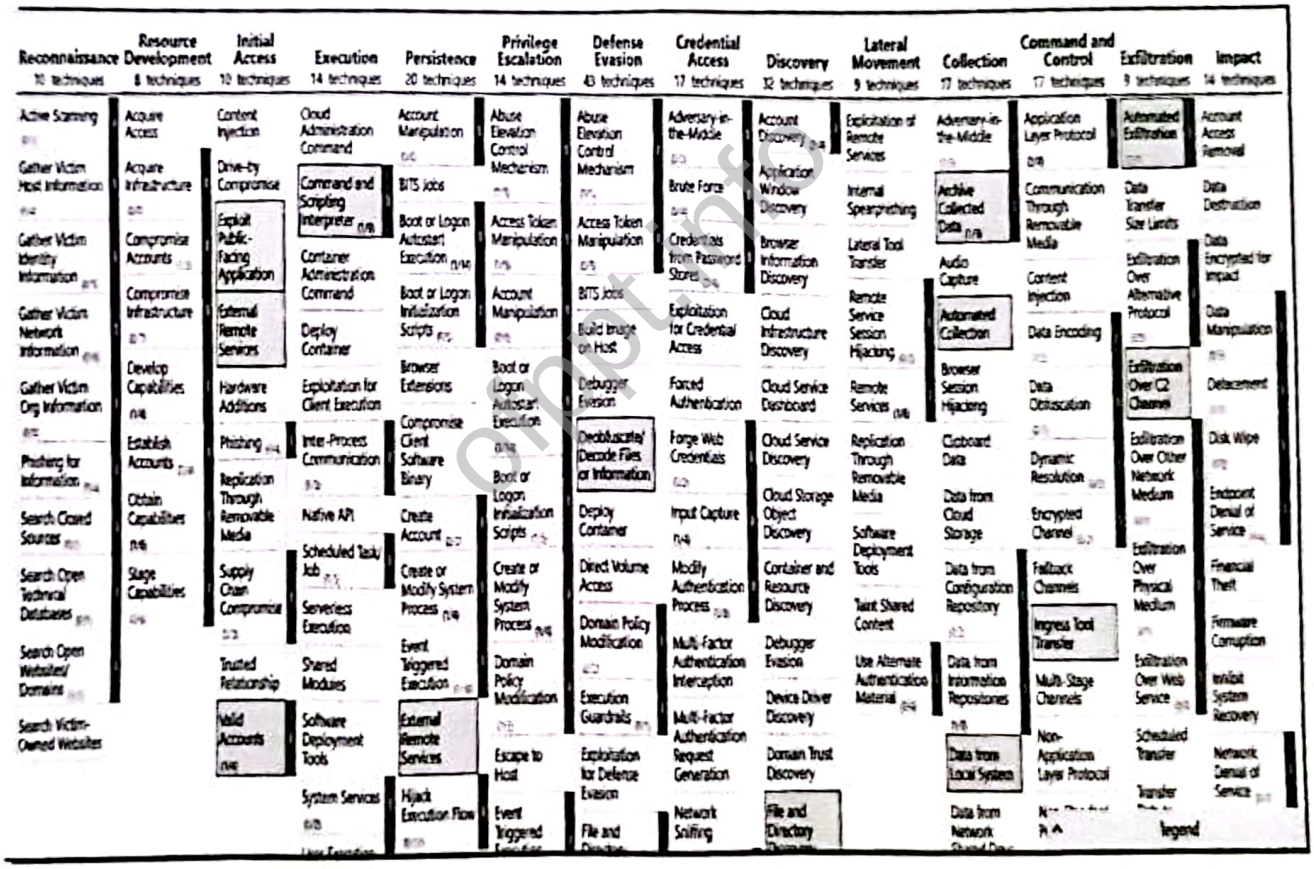
22) Quels sont les caractéristiques les plus importantes de menaces persistantes avancées ?

Citer trois

23) Compléter les étapes manquantes **(1 ,2 et 3)** dans la figure.



24) Une équipe Soc utilise le site web MITTRE ATT&CK pour identifier les techniques et les tactiques utilisées par un groupe de menace. En se base sur les résultats trouvés dans la figure ci-dessous.



a) Qu'est-ce que MITTRE ATT&CK ?

b) Combien de catégories de tactiques compose-t-il le cadre ATT&CK ?

c) Citer trois techniques utilisées par ce groupe de menace d'après les résultats trouvés

PARTIE PRATIQUE : /60 points

Contexte

La société « *VETMA* » de vente et de distribution de vêtements dans des points de vente physiques de la région Rabat-Salé-Kénitra. VETMA se compose du siège et une dizaine de magasin dans la région. L'ensemble des magasins est connecté au siège par VPN.

En vue de développer ses opérations à des régions en dehors de ses points de vente physiques, VETMA possède son site Web de commerce électronique afin d'agir comme vitrine pour sa marque de vêtements.

Récemment, VETMA a été victime d'une attaque qui a modifié le contenu sans autorisation de son site web.

En tant que membre de l'équipe de sécurité, vous devez mener une enquête approfondie pour comprendre les détails de l'attaque, identifier les failles exploitées et prendre des mesures pour empêcher de futures intrusions.

Le schéma réseau de la société VETMA sur la figure 1.

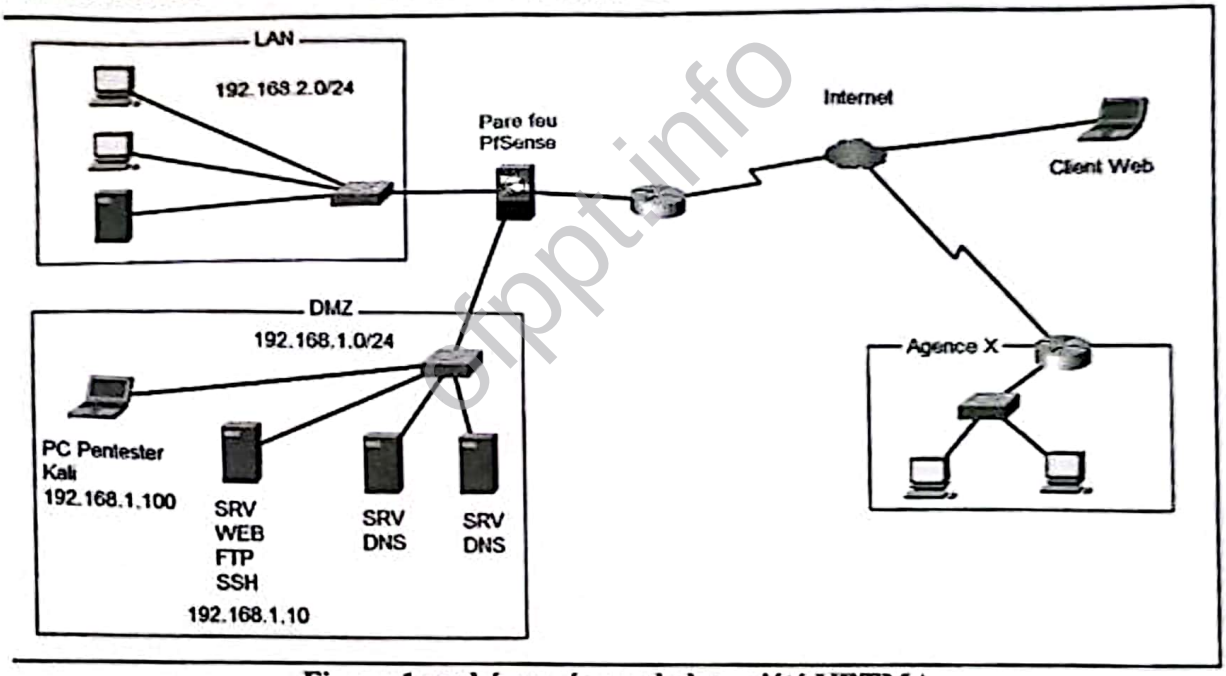


Figure 1 : schéma réseau de la société VETMA

25) Qu'est-ce que le défacement d'un site web et quelles sont les conséquences potentielles pour la société VETMA ?

26) Quelles sont les mesures de mitigation immédiates à prendre après la découverte d'un défacement ?

27) Donner les étapes du processus de gestion des incidents de sécurité selon la norme ISO 27035.

28) Donner deux outils de réponse aux incidents

La direction de la société VETMA lance une **investigation numérique** approfondie concernant l'incident de défacement du site web, l'objectif est de rechercher les **artefacts numériques.**

29) Expliquer qu'est-ce qu'une investigation numérique dans le cadre de cet incident ?

30) Donner trois (3) artefacts numériques qui permettent à un investigateur de construire la chronologie de défacement de site web.

31) Dans la phase d'acquisition, donner deux types de **données volatiles** à récupérer dans cette phase de l'enquête ? et la condition pour récupérer ce type de données.

32) La phase d'examen et d'analyse ne doivent être effectués que sur la copie d'acquisition d'image/fichier pour préserver l'intégrité de la source de données d'origine.

Le hach (empreinte numérique) du contenu de la source de données est réalisé en utilisant l'algorithme SHA-1.
Donner la commande pour calculer le hash du fichier d'acquisition suivant :

/home/kali/Desktop/hash-files/file1.raw

33) Dans le cadre de cet investigation, l'enquêteur a récupéré les formats d'acquisition d'image/fichier suivants : **PCap , RAW, Img, Evtx.**

Remplir le tableau par le format associé.

Disque Dur	RAM	Réseau	Journal Logs

Le rapport investigation numérique a révélé la faille de sécurité qui a provoquée de défacement du site web. Le CVE-ID relative à cette vulnérabilité est : **CVE-2022-24500**

Une recherche de la **CVE-2022-24500** sur site web **CVE.MITTRE.ORG**, la zone référence renvoie sur le site « **Microsoft Security Response Center : MSRC** ».
Le MSRC liste les recommandations atténuants cette vulnérabilité :

Les pares-feux placés sur le périmètre du réseau doivent bloquer les communications non sollicitées (à partir d'Internet) et le trafic sortant (vers Internet) vers les ports suivants :

Numéro	Protocole d'application	Protocole	Port
1	SMB	TCP	445
2	Résolution du nom Net APPEL.NETS	UDP	137
3	NetS DATAgram Service	UDP	138
4	Service de session Net DOSSIERS	TCP	139

Tableau 1 : liste des protocoles/ports à bloquer

34) Dans le cadre du durcissement du pare-feu PfSense IPv4, **bloquer** le trafic **entrant** à partir d'Internet vers DMZ relatif aux numéros 1 et 3 du tableau 1.

Tout en gardant l'accès vers les serveurs WEB et DNS.

Créer les règles pour les flux correspondants. Reproduire sur la feuille de réponse la forme du tableau suivant : (au tant de règle que de ligne)

Interface	Action	Source	Protocole(s) et Port(s) source	Destination	Protocole(s) et Port(s) destination

Exemple (*= tout ou any)

Interface	Action	Source	Protocole(s) & Port(s) source	Destination	Protocole(s) & Port(s) destination
Lan	Autoriser	Lan subnet	*	Wan	TCP -22
Lan	Autoriser	Lan subnet	*	Wan	TCP -1443

Après investigation, l'équipe SOC a procédé à la restauration du serveur Web à partir des sauvegardes pour rétablir l'intégrité du serveur compromis.

Un pentester est mandaté pour réaliser un test d'intrusion afin d'identifier et de corriger les vulnérabilités potentielles sur le serveur Web avant sa mise en production.

35) Dans un premier temps, un scan de réseau avec l'outil nmap.

Donnez la commande qui permet d'afficher les ports TCP ouverts dans la machine cible (entre 20 et 200), les services associés et leurs versions.

Apres exécution de la commande précédente, le résultat affiché est le suivant :

PORT	STATE	SERVICE	VERSION
21/tcp	open	ftp	vsftpd 3.0.3
22/tcp	open	ssh	OpenSSH 7.9p1
25/tcp	open	smtp	Postfix smtpd
80/tcp	open	http	Apache httpd 2.4.38
135/tcp RPC	open	msrpc	Microsoft Windows
443/tcp	open	https	Apache httpd 2.4.38
445/tcp	open	smb	Samba smbd
1433/tcp	open	ms-sql-s	Microsoft SQL Server

Figure 2 : Capture via l'outil Metasploit

Une suite de commandes a été exécutée via l'outil Metasploit sur la machine Kali de votre réseau.

Le résultat est sur la capture suivante :

```
Msf6> .....
Matching Modules
================

#  Name                                  Disclosure Date  Rank       Check  Description
0  exploit/unix/ftp/vsftpd_234_backdoor  2024-06-08       excellent  No     VSFTPD v2.3.4 Backdoor Command Execution
Msf6>
```

Figure 3 : Capture via l'outil Metasploit

36) Quelle est la commande utilisée donnant le résultat de la figure 3 ?

37) Expliquer le résultat de la figure 3

38) Donner la commande à exécuter dans Metasploit pour connaitre les informations sur comment exploiter ce service.

39) Donner la commande pour charger le module de la figure 3

40) Expliquer le résultat de la commande suivante :

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options
```

41) Quelle commande permet de définir l'adresse IP de la cible ?

42) Quel sera le résultat de la commande suivante :

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >exploit
```

43) Quel est le but de créer un shell meterpreter ?

44) Suite à l'exploitation de cette vulnérabilité, le RSSI de VETMA vous demande de proposer des recommandations et un score à cette vulnérabilité.