

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 resources"] 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.

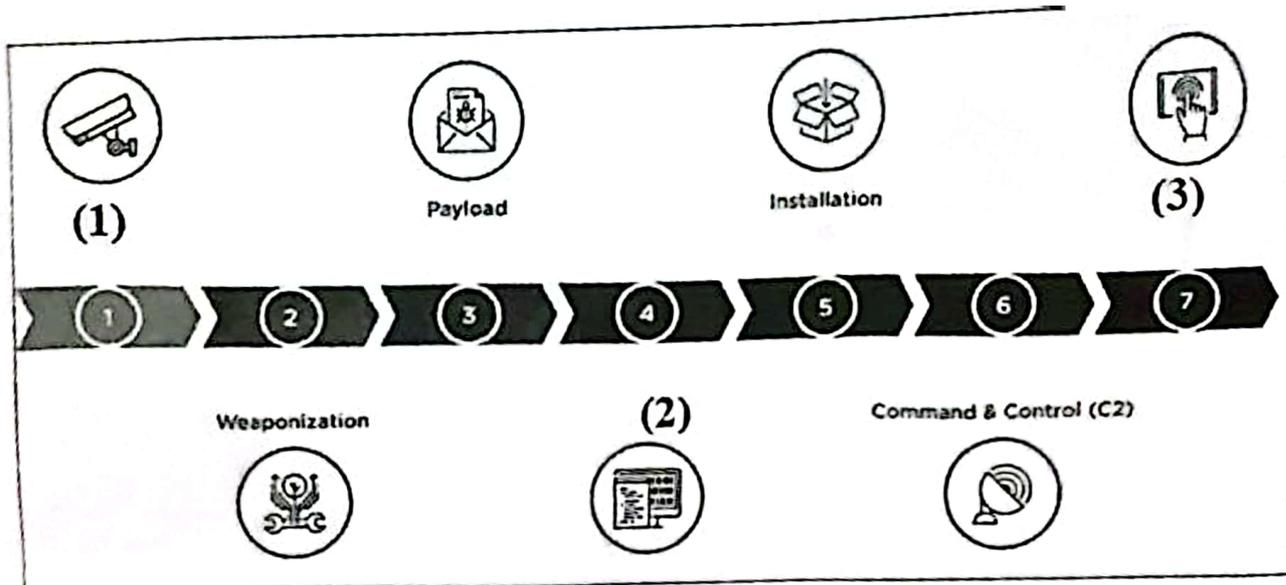
21) Expliquez le concept de Threat Hunting (chasse aux menaces).

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.

Filière	Infrastructure Digitale Option Cybersécurité	Variante	V1	Page	Page 3 sur 8
Examen	Fin de Formation	Session	Juin 2024		



24) Une équipe Soc utilise le site web MITRE 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.

Reconnaissance 10 techniques	Resource Development 8 techniques	Initial Access 10 techniques	Execution 14 techniques	Persistence 20 techniques	Privilege Escalation 14 techniques	Defense Evasion 43 techniques	Credential Access 17 techniques	Discovery 32 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 17 techniques	Exfiltration 9 techniques	Impact 14 techniques
Active Scanning 016	Acquire Access 016	Content Injection 016	Cloud Administration Command 016	Account Manipulation 016	Abuse Elevation Control Mechanism 016	Abuse Elevation Control Mechanism 016	Adversary-in-the-Middle 016	Account Discovery 016	Exploitation of Remote Services 016	Adversary-in-the-Middle 016	Application Layer Protocol 016	Automated Exfiltration 016	Account Access Removal 016
Gather Victim Host Information 016	Acquire Infrastructure 016	Drive-by Compromise 016	Command and Scripting Interpreter 016	BITS Jobs 016	Access Token Manipulation 016	Access Token Manipulation 016	Brute Force 016	Application Window Discovery 016	Internal Spearphishing 016	Archive Collected Data 016	Communication Through Removable Media 016	Data Transfer Size Limits 016	Data Destruction 016
Gather Victim Identity Information 016	Compromise Accounts 016	Exploit Public-Facing Application 016	Container Administration Command 016	Boot or Logon Autostart Execution 016	Account Manipulation 016	Account Manipulation 016	Credentials from Password Stores 016	Browser Information Discovery 016	Lateral Tool Transfer 016	Audio Capture 016	Content Injection 016	Exfiltration Over Alternative Protocol 016	Data Encrypted for Impact 016
Gather Victim Network Information 016	Compromise Infrastructure 016	External Remote Services 016	Deploy Container 016	Boot or Logon Initialization Scripts 016	Account Manipulation 016	Account Manipulation 016	Exploitation for Credential Access 016	Cloud Infrastructure Discovery 016	Remote Service Session Hijacking 016	Automated Collection 016	Data Encoding 016	Data Manipulation 016	Data Manipulation 016
Gather Victim Org Information 016	Develop Capabilities 016	Hardware Additions 016	Exploitation for Client Execution 016	Browser Extensions 016	Boot or Logon Autostart Execution 016	Debugger Evasion 016	Forced Authentication 016	Cloud Service Dashboard 016	Remote Services 016	Browser Session Hijacking 016	Data Obfuscation 016	Exfiltration Over C2 Channel 016	Deactivation 016
Pushing for Information 016	Establish Accounts 016	Phishing 016	Inter-Process Communication 016	Compromise Client Software Binary 016	Boot or Logon Initialization Scripts 016	Declassified/Decade Files or Information 016	Forge Web Credentials 016	Cloud Service Discovery 016	Replication Through Removable Media 016	Clipboard Data 016	Dynamic Resolution 016	Exfiltration Over Other Network Medium 016	Disk Wipe 016
Search Cloud Sources 016	Obtain Capabilities 016	Replication Through Removable Media 016	Native API 016	Create Account 016	Boot or Logon Initialization Scripts 016	Deploy Container 016	Input Capture 016	Cloud Storage Object Discovery 016	Software Deployment Tools 016	Data from Cloud Storage 016	Encrypted Channel 016	Endpoint Denial of Service 016	Endpoint Denial of Service 016
Search Open Technical Databases 016	Stage Capabilities 016	Supply Chain Compromise 016	Scheduled Task Job 016	Create or Modify System Process 016	Create or Modify System Process 016	Direct Volume Access 016	Modify Authentication Process 016	Container and Resource Discovery 016	Target Shared Content 016	Data from Configuration Repository 016	Fallback Channels 016	Financial Theft 016	Financial Theft 016
Search Open Websites/ Domains 016	Trusted Relationship 016	Trusted Relationship 016	Shared Modules 016	Event Triggered Execution 016	Domain Policy Modification 016	Domain Policy Modification 016	Multi-Factor Authentication Interception 016	Debugger Evasion 016	Use Alternate Authentication Material 016	Data from Information Repositories 016	Ingress Tool Transfer 016	Firmware Corruption 016	Firmware Corruption 016
Search Victim-Owned Websites 016	Valid Accounts 016	Valid Accounts 016	Software Deployment Tools 016	External Remote Services 016	Escape to Host 016	Exploitation for Defense Evasion 016	Multi-Factor Authentication Request Generation 016	Device Driver Discovery 016	Domain Trust Discovery 016	Data from Local System 016	Multi-Stage Channels 016	Exfiltration Over Web Service 016	Exfiltration Over Web Service 016
	System Services 016	System Services 016	System Services 016	Hijack Execution Flow 016	Event Triggered Execution 016	File and Directory Discovery 016	Network Sniffing 016	File and Directory Discovery 016	File and Directory Discovery 016	Data from Network Shared Drive 016	Non-Application Layer Protocol 016	Scheduled Transfer 016	Network Denial of Service 016

- Qu'est-ce que MITRE ATT&CK ?
- Combien de catégories de tactiques compose-t-il le cadre ATT&CK ?
- 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 magasins 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.

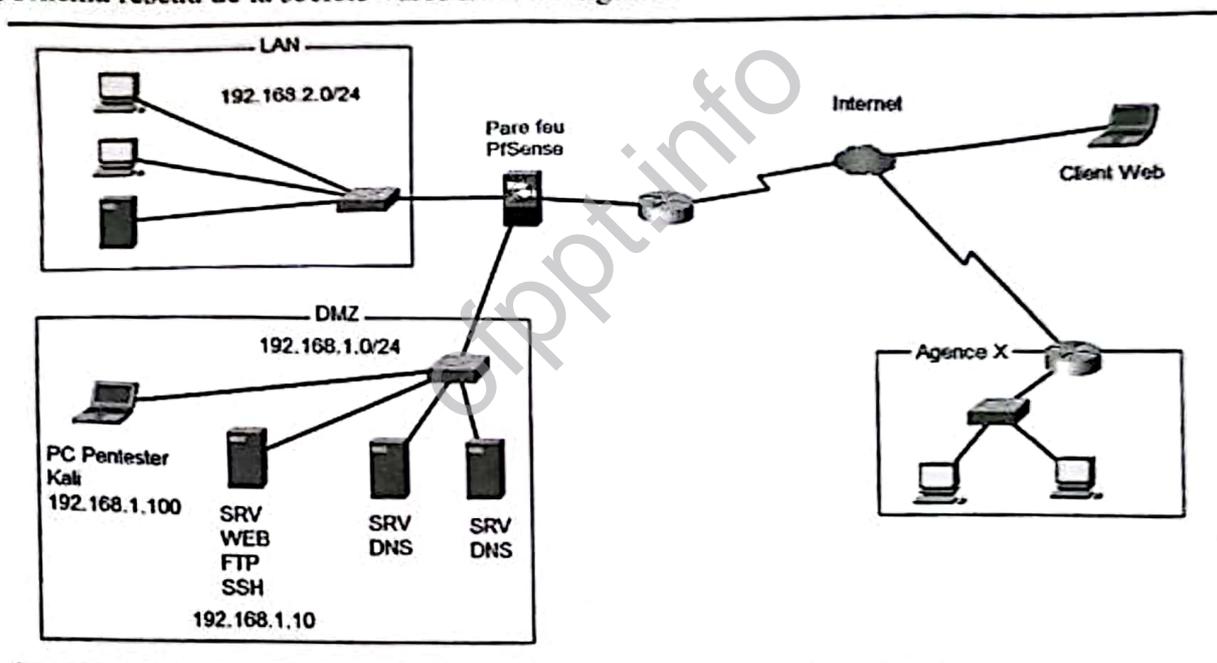


Figure 1 : schéma réseau de la société VETMA

- 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

Filière	Infrastructure Digitale Option Cybersécurité	Variante	V1	Page	Page 5 sur 8
Examen	Fin de Formation	Session	Juin 2024		

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.MITRE.ORG, la zone référence renvoie sur le site « Microsoft Security Response Center : MSRC ».

Le MSRC liste les recommandations atténuants cette vulnérabilité :

Les pare-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

Filière	Infrastructure Digitale Option Cybersécurité	Variante	V1	Page	Page 6 sur 8
Examen	Fin de Formation	Session	Juin 2024		

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.

Après 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	open	msrpc	Microsoft Windows RPC
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

Filière	Infrastructure Digitale Option Cybersécurité	Variante	V1	Page	Page 7 sur 8
Examen	Fin de Formation	Session	Juin 2024		

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 connaître 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.

Filière	Infrastructure Digitale Option Cybersécurité	Variante	V1	Page	Page 8 sur 8
Examen	Fin de Formation	Session	Juin 2024		