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 d'année

Session de Juin 2023

Examen de Fin de Formation (Epreuve de Synthèse)

Secteur :	**Digital et Intelligence Artificielle**	**Niveau :**	**Technicien Spécialisé**
Filière :	**Infrastructure Digitale Option Cybersécurité**		

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

Consignes et Conseils aux candidats :

- Toutes les réponses devront être justifiées avec le détail des calculs qui doit être indiqué sur la copie ;
- Apporter un soin particulier à la présentation de votre copie ;

Document(s) et Matériel(s) autorisés :

- Les documents ne sont pas autorisés ;
- Calculatrice simple (non programmable) autorisée.

Détail du Barème :

Théorie /40			
Dossier 1	**/17**	**Dossier 2**	**/23**
Q1	1,5	Q12	2
Q2	1	Q13	2
Q3	2	Q14	3
Q4	1	Q15	2
Q5	2	Q16	1
Q6	1	Q17	1,5
Q7	1,5	Q18	1,5
Q8	2	Q19	1
Q9	1	Q20	2
Q10	2	Q21	2
Q11	2	Q22	1
		Q23	1
		Q24	1
		Q25	2

Pratique /60			
Dossier 3	**/38**	**Dossier 4**	**/22**
Q26	2	Q40	4
Q27	2	Q41	8
Q28	2	Q42	4
Q29	2	Q43	3
Q30	2	Q44	3
Q31			
a	1		
b	1		
Q32			
c	1		
d	1		
e	2		
Q33			
f	2		
g	2		
Q34	4		
Q35	2		
Q36	4		
Q37	4		
Q38	2		
Q39	2		

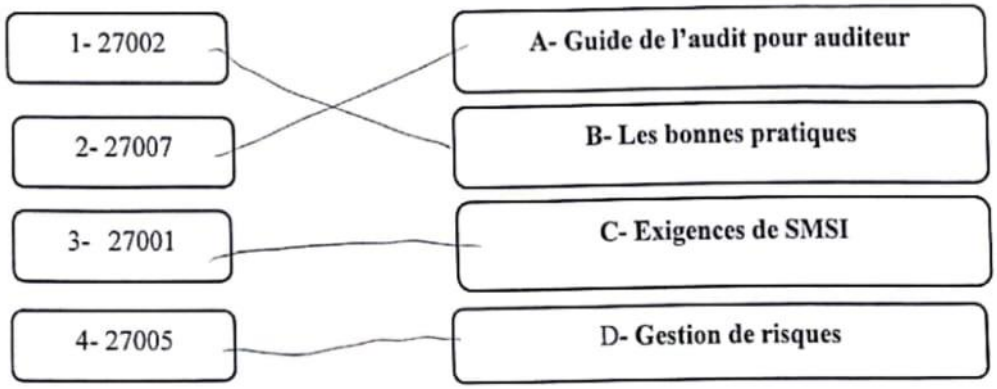
PARTIE THEORIQUE :

Dossier 1 :

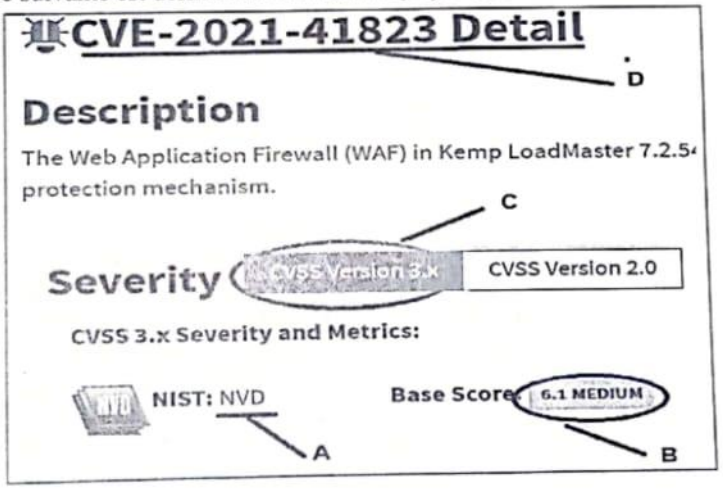
1. Choisir le besoin de sécurité (C.I.D) adéquat pour chaque mécanisme de sécurité.

	Confidentialité	Intégrité	Disponibilité
Chiffrement des données			
Contrôle d'accès			
Hachage			
La sauvegarde et surveillance des données			

2. Quelle est la différence entre les postures défensive et offensive ?
3. Relier chaque norme ISO à son principe :

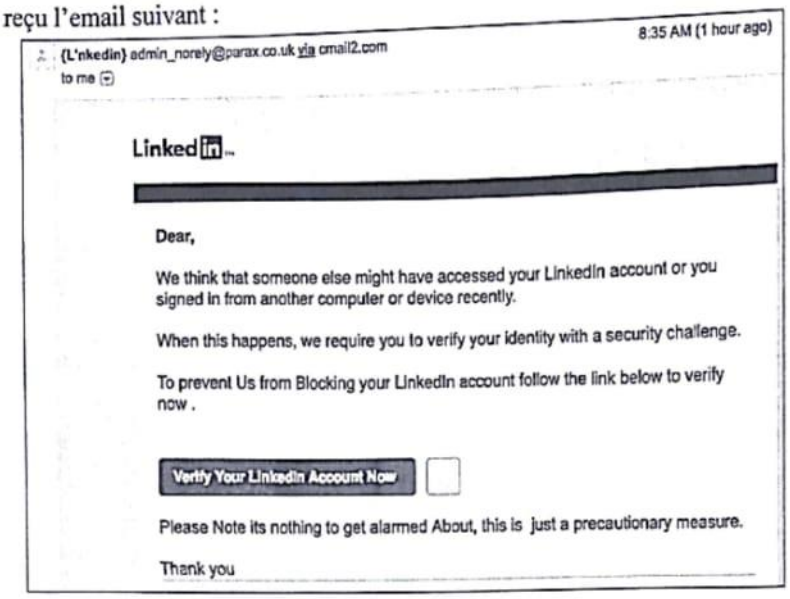


4. Présenter la politique de sécurité d'un système d'information (PSSI).
5. Utiliser la capture suivante est définir les éléments : A, B, C et D



6. C'est quoi le rôle d'un analyste SOC?
7. Donner la différence entre le rôle de **Blue Team** et **Red Team** dans le contexte de cybersécurité
8. Donner les étapes à suivre pour réussir un programme de sensibilisation à la sécurité informatique.
9. Citer les deux référentiels les plus répandus utilisés pour le durcissement de la sécurité.

10. Vous avez reçu l'email suivant :



(L'nkedin) admin_norely@parax.co.uk via email2.com 8:35 AM (1 hour ago)
to me

LinkedIn

Dear,

We think that someone else might have accessed your LinkedIn account or you signed in from another computer or device recently.

When this happens, we require you to verify your identity with a security challenge.

To prevent Us from Blocking your LinkedIn account follow the link below to verify now .

Verify Your LinkedIn Account Now

Please Note its nothing to get alarmed About, this is just a precautionary measure.

Thank you

Quel est le piège à éviter ? Quelle sont les meilleures attitudes à adopter ? Et il s'agit de quel type d'attaque et justifier votre réponse ?

11. Vous êtes technicien en cybersécurité et vous avez été chargé d'effectuer une analyse Microsoft STRIDE sur un nouvelle application web de commerce électronique. Présenter le rôle de cette méthode et les six catégories de menaces informatiques.

Dossier 2 :

12. Classer les caractéristiques suivantes selon test d'intrusion ou Hacking ? (Copier le tableau dans votre feuille)

A. Se réalise sur une période donnée B. Recherche opportuniste des vulnérabilités C. Pas de cadre défini D. Un cadre bien défini E. Pas de méthodologie	F. N'est pas cadré dans le temps G. Objectif de compromission H. Suit des méthodologies de test I. Se base sur des standards de gouvernance

Hacking	Test d'intrusion
C - E - F - G	A B D H I

13. Donner deux qualités les plus importantes pour un pentester.

14. Remplir le tableau de comparaison entre les méthodologies de test d'intrusion (copier le tableau dans votre feuille).

	OSSTMM	PTES	OWASP
Type de test d'intrusion (*Interne ou Externe*)	interne	interne et externe	interne et externe
Domaine d'utilisation (*Industrie, Application Web ou Système d'Information*)	Industriel	Système d'information	A. W

15. Quelle est la différence entre reconnaissance active et passive?
16. A quoi sert le processus de gestion des incidents ?
17. Citer deux impacts d'un incident de sécurité sur l'entreprise.
18. Quels sont les niveaux de qualification des incidents ?
19. Quel est le principe de Kill-Chain ?
20. Quelle est la différence entre la Chasse structurée et non structurée de Threat Hunting ?
21. Donner les 6 étapes du plan de réponse aux incidents (SANS).
22. Définir une attaque APT.
23. Définir le principe de l'investigation numérique et proposer deux outils à utiliser.
24. Définir le durcissement d'un système d'information et citer ses 3 principes.
25. Donner les étapes pour mettre en place un programme DLP.

PARTIE PRATIQUE :

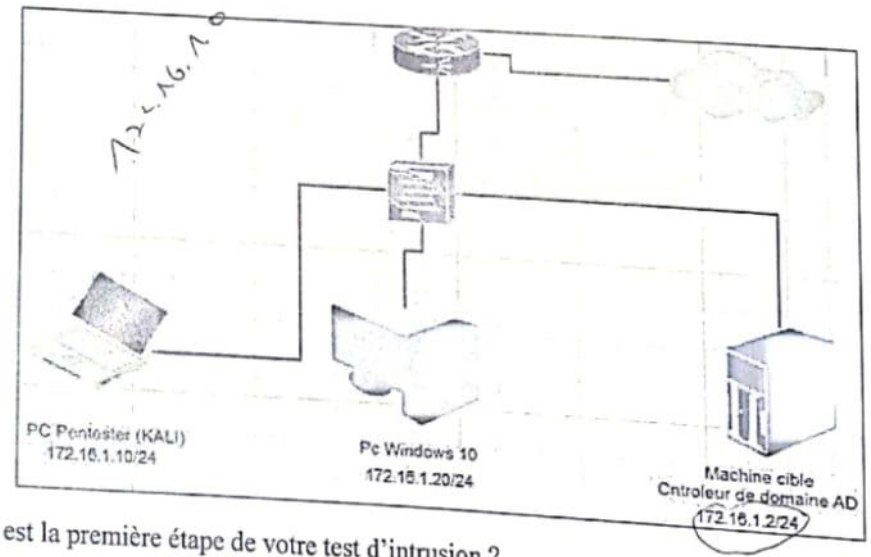
Dossier 3 :

Partie 1 :

Vous serez dans le rôle d'un pentester de sécurité informatique. Vous êtes mandaté par la société ABC pour tester la sécurité de son système d'information interne Active Directory.
Active Directory est une solution de Microsoft qui permet de gérer des parcs informatiques d'entreprises. Les entreprises utilisent cette solution pour gérer leurs utilisateurs, les postes de travail, les serveurs, etc. Dans cette démarche, vous vous mettrez à la place d'un administrateur d'entreprise qui souhaite sécuriser son environnement. Cela vous permettra d'avoir suffisamment d'informations pour être le plus exhaustif possible dans vos recherches, et d'avoir les clés nécessaires pour sécuriser et surveiller votre environnement.

Votre objectif en tant que pentester est d'identifier les serveurs et postes potentiellement vulnérables qui pourront par la suite être utilisés comme point d'entrée par un attaquant.

La topologie du réseau :



26. Quelle est la première étape de votre test d'intrusion ?
27. Quelle est la commande pour découvrir l'adresse IP de votre cible ?

28. Quel est outil à utiliser pour scanner la cible afin d'avoir les ports ouverts, les services actifs, le système d'exploitation ? Nmap Nmap -sS -sV -A 192.168.1.2

29. Donner la commande permettant d'afficher les protocoles (services) trouvés dans la machine cible.

30. Donner deux outils pour scanner les vulnérabilités de la cible Nessus Nmap

31. Votre collègue, un stagiaire, au sein de votre service, vous a envoyé la capture suivante :

```
┌──(kali㉿kali)-[ ]
└─$ searchsploit apache 2.4
------------------------------------------------ ---------------------------------
 Exploit Title                                  |  Path
------------------------------------------------ ---------------------------------
Apache + PHP < 5.3.12 / < 5.4.2 - cgi-bin Remote Co | php/remote/29290.c
Apache + PHP < 5.3.12 / < 5.4.2 - Remote Code Execu | php/remote/29316.py
Apache 2.2.4 - 413 Error HTTP Request Method Cross- | unix/remote/30835.sh
Apache 2.4.17 - Denial of Service                   | windows/dos/39037.php
Apache 2.4.17 < 2.4.38 - 'apache2ctl graceful' 'log | linux/local/46676.php
Apache 2.4.23 mod_http2 - Denial of Service         | linux/dos/40909.py
Apache 2.4.7 + PHP 7.0.2 - 'openssl_seal()' Uniniti | php/remote/40142.php
Apache 2.4.7 mod_status - Scoreboard Handling Race  | linux/dos/34133.txt
Apache < 2.2.34 / < 2.4.27 - OPTIONS Memory Leak    | linux/webapps/42745.py
Apache CXF < 2.5.10/2.6.7/2.7.4 - Denial of Service | multiple/dos/26710.txt
Apache HTTP Server 2.4.49 - Path Traversal & Remote | multiple/webapps/50383.sh
Apache HTTP Server 2.4.50 - Path Traversal & Remote | multiple/webapps/50406.sh
Apache HTTP Server 2.4.50 - Remote Code Execution ( | multiple/webapps/50446.sh
Apache HTTP Server 2.4.50 - Remote Code Execution ( | multiple/webapps/50512.py
```

a) Quel est le rôle de la commande suivante **searchsploit apache 2.4**?

b) Comment vous définissez les éléments de la colonne « **Title** » ?

32. Une autre capture envoyée par ce stagiaire :

```
       =[ [redacted] v6.2.23-dev                          ]
+ -- --=[ 2259 exploits - 1188 auxiliary - 402 post       ]
+ -- --=[ 951 payloads - 45 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

[redacted] tip: Use the edit command to open the
currently active module in your editor
[redacted] Documentation: https://docs.[redacted].com/

msf6 > [redacted]
```

a) Donner la commande exécutée pour démarrer cet outil.

b) Quel est le nom de cet outil et quel est son utilité ?

c) Quelle est la différence entre exploits et payloads

33. Il a exécuté la commande : **search ms06-312**

```
msf6 > search ms17-010

Matching Modules
================

   #  Name                                      Disclosure Date  Rank     Check  Descr
iption
   -  ----                                      ---------------  ----     -----  -----
------
   0  exploit/windows/smb/ms17_010_eternalblue  2017-03-14       average  Yes
[redacted] EternalBlue SMB Remote Windows Kernel Pool Corruption
   1  exploit/windows/smb/ms17_010_psexec       2017-03-14       normal   Yes
[redacted] EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
   2  auxiliary/admin/smb/ms17_010_command      2017-03-14       normal   No
[redacted] EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
   3  auxiliary/scanner/smb/smb_ms17_010                         normal   No
[redacted] SMB RCE Detection
   4  exploit/windows/smb/smb_doublepulsar_rce  2017-04-14       great    Yes    SMB D
OUBLEPULSAR Remote Code Execution
```

d) Expliquer le rôle de la commande **search ms17-010**

e) Quel est le meilleur exploit à essayer, pourquoi ?

```
msf6 > use (A)
[*] Using configured payload windows/x64/meterpreter/reverse_tcp
msf6 exploit(          (B)                    ) > options

Module options (exploit/windows/smb/smb_doublepulsar_rce):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS         (C)        yes       The target host(s), see https://github.com/rap
                                       id7/metasploit-framework/wiki/Using-Metasploit
   RPORT    445              yes       The SMB service port (TCP)


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, p
                                        rocess, none)
   LHOST                      yes       The listen address (an interface may be spec
                                        ified)
   LPORT     4444             yes       The listen port
```

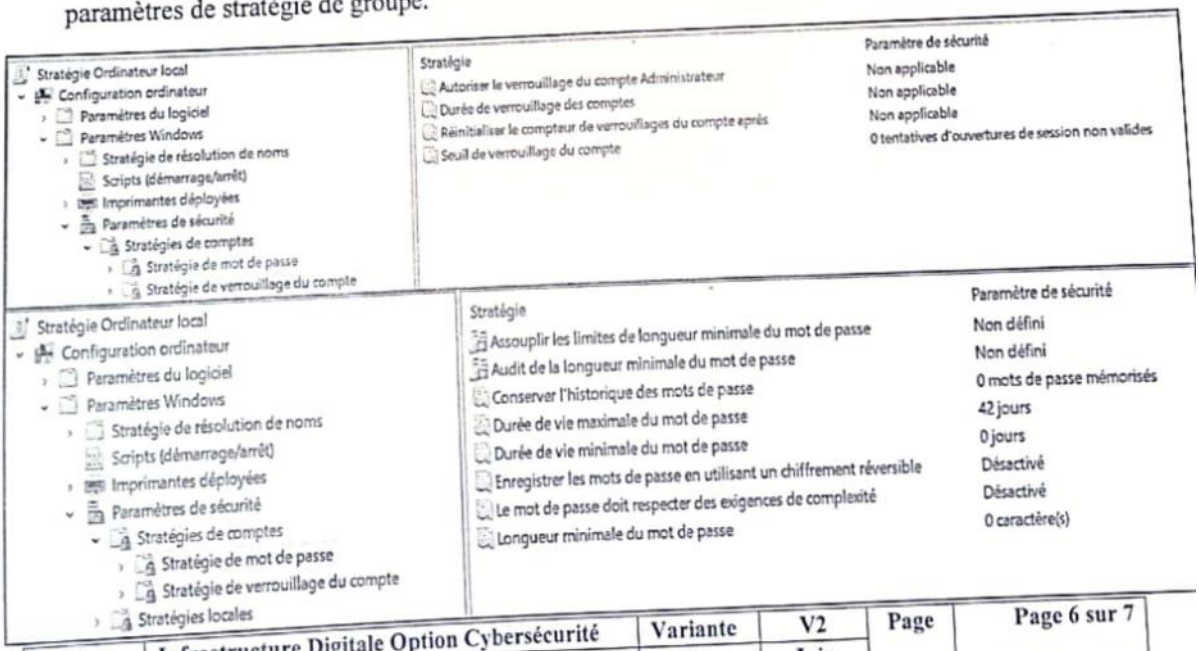
34. Vous voulez tester une intrusion sur le pc Windows 10. En utilisant la capture précédente, remplir le vide par les équivalents de **A, B, C**, donner la commande pour paramétrer le (C) et quel est le payload utilisé par défaut ?
35. Quels sont les éléments que vous devez inclure au rapport de test d'intrusion ?

Partie 2 :

Selon le Rapport d'évaluation de la configuration de la sécurité du **PC WINDOWS 10** réalisé par l'outil **CIS-CAT**, voilà un extrait de rapport :

Description	Tests					Scoring		
	Pass		Error	Unkn.	Man.	Score	Max	Percent
1 Account Policies	4	6	0	0	0	4.0	10.0	40%
1.1 Password Policy	2	5	0	0	0	2.0	7.0	29%
1.2 Account Lockout Policy	2	1	0	0	0	2.0	3.0	67%

36. Quelles sont les menaces de cette découverte ?
37. Proposer une politique stricte de mot de passe et de verrouillage du compte en se basant sur les paramètres de stratégie de groupe.



Partie 3 :

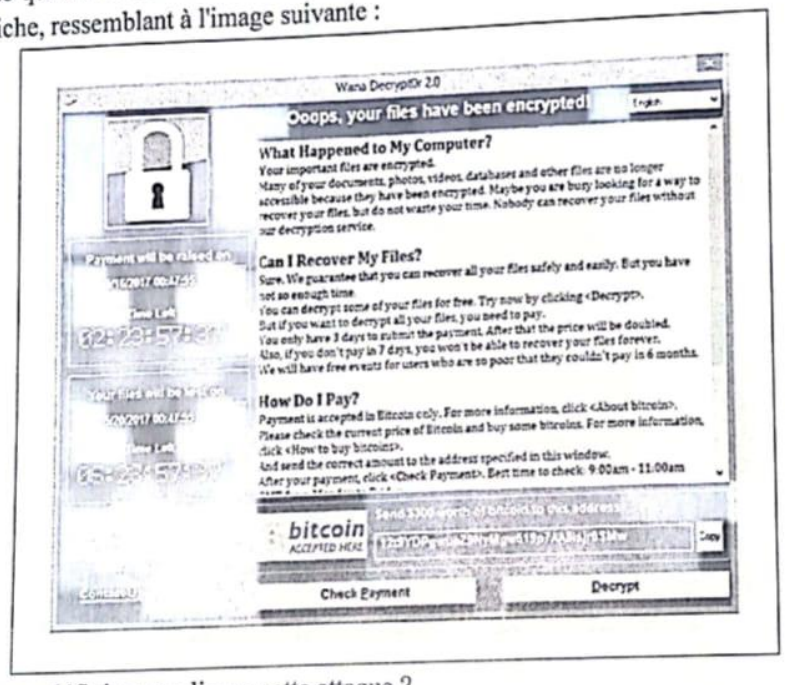
Avec les connaissances de techniques d'attaque requises pendant le test d'intrusion, vous aurez tous pour améliorer le niveau de sécurité de votre Active Directory et le surveiller. Votre client vous demande de réaliser un guide de durcissement afin de fournir des recommandations et des procédures permettant la sécurisation d'un annuaire Active Directory.

38. Le durcissement de l'Active Directory consiste principalement à réduire à l'indispensable les objets installés sur le système et la surface d'attaque disponible. Citer trois recommandations pour renforcer la sécurité de l'Active Directory.

39. En plus d'améliorer le niveau de sécurité global du système d'information, il est crucial de savoir surveiller le système pour maintenir le niveau de sécurité le plus élevé possible. Citer deux outils ou méthodes pour surveiller les événements de votre environnement Active Directory.

Dossier 4 :

Après le téléchargement d'une pièce jointe à partir d'un email personnel, un collaborateur de l'entreprise ABC remarque que ses fichiers sont inaccessibles, ont une extension étrange telle que **.WCRY** et un message s'affiche, ressemblant à l'image suivante :



40. D'après ce cas, définir et expliquer cette attaque ?

41. En se basant sur le processus de gestion des incidents contre les attaques, vous allez appliquer les phases de la procédure **ISO/IEC 27035** pour protéger votre système contre l'attaque découverte.

42. Donner trois bonnes pratiques pour éviter cette cyberattaque ?

43. Comment vous pouvez sensibiliser vos employés aux risques de sécurité de cette cyberattaque ?

44. Qu'est-ce qu'une réponse automatisée aux incidents et quels sont ses avantages ?