Nom : _____ Date : _____ Note : _____

Dark web et deep web : sécurité et Différences

Indexation par les moteurs de recherche, bases de données du web profond, routage en oignon de Tor, anonymat sur le réseau et risques

PRÉSENTATION : DARK WEB ET DEEP WEB

SÉCURISÉ
CHIFFREMENT DES DONNÉES
Norme AES 256 bits

CONFORME
NORMES MONDIALES
Cadres RGPD (GDPR) et CCPA

ZERO TRUST
POLITIQUE D'ACCÈS
Authentification multifacteur

Bienvenue ! Ce dossier d'activités vous guide à travers les différences entre le Deep Web et le Dark Web. Vous étudierez les bases de données non indexées, le routage en oignon du navigateur Tor, les domaines cryptographiques .onion et les risques de sécurité liés à l'anonymat.

POINTS DE CONTRÔLE DE LA FICHE

- [ ] **Parties 1-4 : maîtrisez la cybersécurité et la prévention des menaces.**
- [ ] **Parties 5-7 : résolvez les mots croisés et les mots mêlés.**
- [ ] **Parties 8-9 : résolvez les études de cas et le défi de déchiffrement.**
- [ ] **Partie 10 : consultez les FAQ de base et avancées.**
- [ ] **Partie 11 : découvrez 10 faits concrets intéressants.**
- [ ] **Bonus : défi Réflexion rapide.**

Ouvrir le guide VPN.com de la cybersécurité

URL: https://www.vpn.com/fr/cybersecurite/dark-web-vs-web-profond/

Votre parcours d'apprentissage : stratégie face au Deep Web et au Dark Web

- Comparez le deep web (bases de données non indexées) avec le dark web (services onion).
- Comprendre comment le routage en oignon chiffre et relaie le trafic réseau.
- Évaluer les risques de sécurité liés à l'accès à des sites non vérifiés du réseau Tor.
- Déployer une passerelle sécurisée et des politiques de bac à sable (sandboxing) pour l'exploration liée au renseignement sur les menaces.
- Analysez le format d'adresse cryptographique des domaines des services onion.

GUIDE DU DEEP WEB ET DU DARK WEB : CONSIGNES

Répondez aux questions à choix multiple et vrai/faux, complétez les phrases à trous à l'aide de la banque de mots, associez les définitions et résolvez les mots croisés et les mots mêlés. Appliquez vos connaissances à la confidentialité sur le deep web et le dark web. Terminez par l'activité bonus Réflexion rapide.

BASES DE DONNÉES DU DEEP WEB ET ROUTAGE EN OIGNON DU DARK WEB (INTRODUCTION)

Le deep web se compose de pages non indexées protégées par des mots de passe et des identifiants, comme les messageries privées ou les portails bancaires d'entreprise. Le dark web est un sous-ensemble du deep web volontairement caché, qui nécessite des navigateurs spécialisés (comme Tor) et des réseaux onion pour y accéder anonymement.

LISEZ ATTENTIVEMENT CHAQUE POINT DE CONTRÔLE ET CHOISISSEZ OU ÉCRIVEZ LA BONNE RÉPONSE.

Point de contrôle 1 : Défi QCM

1. Qu'est-ce qui distingue le deep web du web de surface ?

- A. Les pages du web profond ne sont pas indexées par les moteurs de recherche publics
- B. Le trafic du deep web est illégal et surveillé par les forces de l'ordre
- C. L'accès aux sites du deep web nécessite des navigateurs spécialisés comme Tor
- D. Les pages du deep web se chargent toujours plus vite que celles du web de surface

2. Comment accède-t-on au dark web ?

- A. Grâce à des navigateurs spécialisés utilisant des réseaux de routage en oignon
- B. En configurant des paramètres DNS personnalisés sur des routeurs standard
- C. Par des consoles de recherche privées du web de surface, sur invitation uniquement
- D. En installant une extension de navigateur standard de blocage des publicités

3. Quelle structure constitue la plus grande partie du deep web ?

- A. Bases de données d'utilisateurs protégées par mot de passe et comptes privés
- B. Des forums illégaux du marché noir où s'échangent des biens illicites
- C. Protocoles de partage de fichiers pair à pair non chiffrés
- D. Bases de données du cache des moteurs de recherche publics

4. Quel effet le routage en oignon (Onion Routing) a-t-il sur le trafic réseau ?

- A. Il chiffre les paquets et les achemine par plusieurs relais
- B. Il augmente la vitesse de téléchargement en contournant les nœuds du FAI
- C. Il associe les numéros de série matériels des appareils à des enregistrements IP
- D. Il supprime les cookies du navigateur après chaque clic

5. Quel suffixe de domaine est utilisé exclusivement sur les réseaux Tor ?

- A. L'extension de premier niveau cryptographique .onion
- B. L'extension commerciale historique standard .com
- C. L'extension blockchain décentralisée .eth du Web3
- D. L'extension nationale .ai associée à la technologie

Point de contrôle 2 : Défi Vrai ou Faux

6 Question vrai/faux 6

6. Le deep web et le dark web désignent le même segment du réseau.

- ◯ Vrai
- ◯ Faux

7 Question vrai/faux 7

7. Les portails intranet d'entreprise font partie du deep web.

- ◯ Vrai
- ◯ Faux

8 Question vrai/faux 8

8. Le routage en oignon déchiffre entièrement les paquets de données à chaque nœud de transit.

- ◯ Vrai
- ◯ Faux

9 Question vrai/faux 9

9. Accéder au dark web expose les appareils à des risques élevés de logiciels malveillants.

- ◯ Vrai
- ◯ Faux

10 Question vrai/faux 10

10. Les moteurs de recherche web standard explorent et indexent les sites onion.

- ◯ Vrai
- ◯ Faux

Point de contrôle 3 : Insertion des termes clés

Lisez chaque phrase ci-dessous et complétez le blanc avec le terme correct de la banque de mots.

1. Les portails bancaires privés se trouvent dans le segment non indexé du _____ .
2. Des nœuds Tor spécialisés hébergent des services cachés du _____ .
3. Les sites Tor utilisent l'extension de premier niveau cryptographique _____ .
4. L'acheminement du trafic chiffré en plusieurs couches s'appelle le _____ .
5. Les moteurs de recherche du web de surface explorent les pages publiquement _____ .
6. Les réseaux en oignon chiffrent les IP des clients pour garantir aux utilisateurs leur _____ .

BANQUE DE MOTS DE VOCABULAIRE

ANONYMAT BASE DE DONNÉES DARK WEB DEEP WEB INDEXÉES
NŒUD DE GARDE ONION ROUTAGE EN OIGNON

Écrivez vos réponses ici :

1.
2.
3.
4.
5.
6.

Point de contrôle 4 : Association de notions sur la sécurité

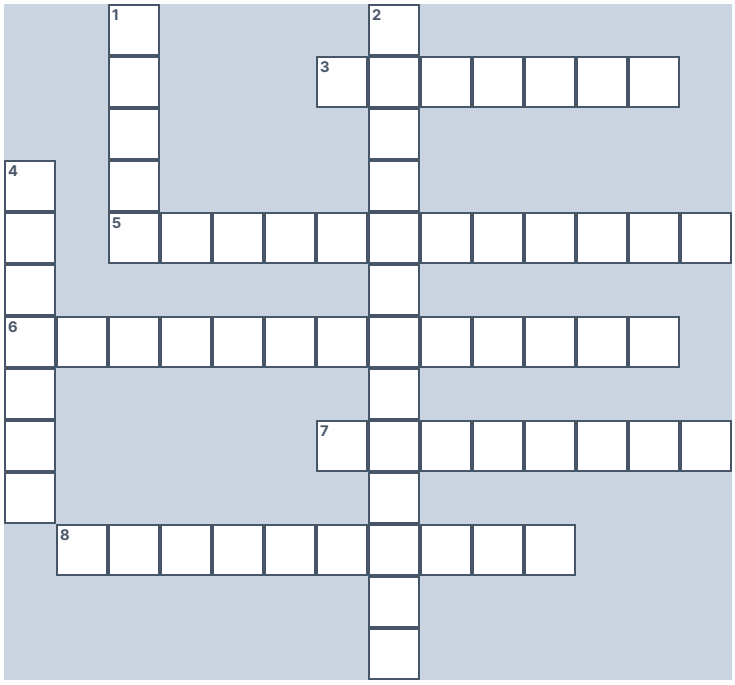
ASSOCIATION DE DÉFINITIONS

Associez chaque terme de vocabulaire à gauche à sa définition à droite en écrivant la lettre correspondante (A-H) dans la case à remplir.

☐	1. Segment du Web profond	A	Segment de réseau chiffré accessible uniquement avec des navigateurs spéciaux.
☐	2. Portail du dark web	B	Chiffrement des données en couches et relais par trois nœuds.
☐	3. Extension .onion	C	Stockage back-end sécurisé hébergeant des enregistrements système non indexés.
☐	4. Routage Tor	D	Suffixe de domaine de premier niveau cryptographique utilisé sur le réseau Tor.
☐	5. Pages indexées	E	Le nœud d'entrée utilisé pour accéder au réseau Tor.
☐	6. Anonymat de l'utilisateur	F	Contenu du web de surface compilé et consultable sur Google.
☐	7. Base de données privée	G	Dissimuler aux serveurs les adresses IP publiques des clients.
☐	8. Passerelle d'entrée	H	Contenu web non indexé, comme les connexions privées, les e-mails et les enregistrements de bases de données.

Point de contrôle 5 : Mots croisés

Résolvez la grille de mots croisés en tapant des lettres dans les cases blanches actives. Les numéros correspondent aux définitions ci-dessous.



HORIZONTALEMENT

3. Segment de réseau chiffré accessible uniquement avec des navigateurs spéciaux (7)

5. Point d'entrée utilisé pour accéder au réseau Tor (12)

6. Contenus du web de surface compilés et consultables sur Google (13)

7. Fait de cacher aux serveurs l'adresse IP publique du client (8)

8. Chiffrement des données en plusieurs couches et relais via trois nœuds (10)

VERTICALEMENT

1. Suffixe cryptographique de domaine de premier niveau utilisé sur les réseaux Tor (5)

2. Stockage dorsal sécurisé hébergeant des enregistrements système non indexés (13)

4. Contenus web non indexés, comme les espaces de connexion privés, les e-mails et les enregistrements de bases de données (7)

Point de contrôle 5, variante : Définitions de mots croisés accessibles

Les utilisateurs de lecteurs d'écran et de clavier peuvent saisir les réponses des mots croisés directement dans les champs de texte ci-dessous.

HORIZONTALEMENT

3 horizontal: Segment de réseau chiffré accessible uniquement avec des navigateurs spéciaux (7 lettres):

5 horizontal: Point d'entrée utilisé pour accéder au réseau Tor (12 lettres):

6 horizontal: Contenus du web de surface compilés et consultables sur Google (13 lettres):

7 horizontal: Fait de cacher aux serveurs l'adresse IP publique du client (8 lettres):

8 horizontal: Chiffrement des données en plusieurs couches et relais via trois nœuds (10 lettres):

VERTICALEMENT

1 vertical: Suffixe cryptographique de domaine de premier niveau utilisé sur les réseaux Tor (5 lettres):

2 vertical: Stockage dorsal sécurisé hébergeant des enregistrements système non indexés (13 lettres):

4 vertical: Contenus web non indexés, comme les espaces de connexion privés, les e-mails et les enregistrements de bases de données (7 lettres):

Point de contrôle 6 : Mots cachés

Trouvez les 8 termes de vocabulaire clés cachés dans la grille ci-dessous. Les mots peuvent être horizontaux, verticaux ou en diagonale.

S K T S V R Z E H E S C A L Q

E C R O T E G A T U O R Z D D

E M K V O N I O N R U A A E S

N W J M M H H N H R F R E K T

N L R W H B U F Y O K P Y W S

O H T X A P U N N W W Z O I Q

D T I P V U O U E E U K A E P

E M K A N V G B B G P Q X Y J

D K V J Y W Y P J I Z I J N A

E E I A T A M Y N O N A S A J

S P A G E S I N D E X E E S F

A W E K Z K E K Q N J A F O K

B N N O E U D D E G A R D E D

N C D H I B A P R L P W T I Y

F Y S G X W H F R T N U K R D

LISTE DE MOTS DE VOCABULAIRE

DEEPWEB DARKWEB ONION ROUTAGETOR PAGESINDEXEES ANONYMAT BASEDEDONNEES NOEUDDEGARDE

Point de contrôle 6, variante : Association de vocabulaire accessible

Associez chacun des 8 termes de vocabulaire de la grille de mots cachés à sa définition en écrivant la lettre (A-H) dans l'espace prévu.

TERMES DE VOCABULAIRE
A. DEEPWEB
B. DARKWEB
C. ONION
D. ROUTAGETOR
E. PAGESINDEXEES
F. ANONYMAT
G. BASEDEDONNEES
H. NOEUDDEGARDE

DÉFINITIONS ET CHAMPS D'ASSOCIATION	
	1. Fait de cacher aux serveurs l'adresse IP publique du client.
	2. Stockage dorsal sécurisé hébergeant des enregistrements système non indexés.
	3. Chiffrement des données en plusieurs couches et relais via trois nœuds.
	4. Contenus web non indexés, comme les espaces de connexion privés, les e-mails et les enregistrements de bases de données.
	5. Segment de réseau chiffré accessible uniquement avec des navigateurs spéciaux.
	6. Suffixe cryptographique de domaine de premier niveau utilisé sur les réseaux Tor.
	7. Point d'entrée utilisé pour accéder au réseau Tor.
	8. Contenus du web de surface compilés et consultables sur Google.

Point de contrôle 7 : Défi des mots mélangés

Remettez les lettres ci-dessous dans l'ordre pour découvrir des notions et termes clés de la cybersécurité. Écrivez vos réponses dans les champs prévus.

1. PEDWBEE
2. ONOIN
3. APDXEESGNSIEE
4. EENSODSDENBAE
5. WBKRDEA
6. OATETROGRU
7. ATYMANNO
8. GEDREENDODAU

Activité bonus : Réflexion rapide

3 RÉPONSES PAR CATÉGORIE. LE PREMIER À REMPLIR SA LISTE GAGNE.

1	Raisons de rester à l'écart du dark web			
2	Choses qu'un moteur de recherche ne peut pas trouver			
3	Appareils qui peuvent être piratés			
4	Raisons légales d'utiliser Tor			
5	Raisons de mettre à jour les logiciels			
6	Signaux d'alerte dans un e-mail			
7	Choses vendues illégalement sur le dark web			
8	Personnes à qui demander de l'aide informatique			
9	Bonnes habitudes de sécurité à adopter dès aujourd'hui			
10	Choses à faire après une fuite de données			
11	Choses qui font partie du deep web			
12	Sites que vous utilisez avec un identifiant			
13	Mots liés à l'anonymat			
14	Informations que vous ne devriez jamais partager			
15	Choses qui se trouvent 'sous la surface'			

Point de contrôle 8 : Études de cas sur la cybersécurité

Appliquez les notions apprises pour résoudre les scénarios réels ci-dessous.

ÉTUDE DE CAS 1 : IDENTIFICATION D'UNE FUITE DE DONNÉES



Scénario : Un audit de sécurité d'entreprise découvre que des enregistrements sensibles de la base de données clients s'échangent sur une place de marché en .onion. Les données ne sont pas indexées par Google.

Question de discussion : Expliquez quels segments du Web sont concernés et comment cette fuite s'est produite.

ÉTUDE DE CAS 2 : ANONYMAT OU RISQUES DE LOGICIELS MALVEILLANTS



Scénario : Un analyste veut consulter des flux de renseignement sur les menaces sur un site Tor. Il télécharge le navigateur Tor et accède au site.

Question de discussion : Évaluez les avantages en matière d'anonymat et décrivez les mesures de protection contre les logiciels malveillants.

Point de contrôle 9 : Déchiffrer le code

Un professionnel de la cybersécurité protège les ressources réseau contre les acteurs malveillants en ligne. Utilisez la clé de correspondance lettres-chiffres ci-dessous pour déchiffrer le message en écrivant les lettres correspondantes dans les cases vides.

CLÉ DE CHIFFREMENT LETTRE-CHIFFRE

A=1 B=2 C=3 D=4 E=5 F=6 G=7 H=8 I=9 J=10

K=11 L=12 M=13 N=14 O=15 P=16 Q=17 R=18 S=19 T=20

U=21 V=22 W=23 X=24 Y=25 Z=26

1	14	15	14	25	13	1	20		16	18	5	19	5	18	22	5		16	1	18

12	5		18	15	21	20	1	7	5		5	14		15	9	7	14	15	14

Message déchiffré :

ASTUCE : CHAQUE NOMBRE REPRÉSENTE LA POSITION DE LA LETTRE DANS L'ALPHABET (P. EX. 1 = A, 2 = B, 26 = Z).

Point de contrôle 10 : Questions fréquentes de base sur la cybersécurité (Partie A)

Passez en revue les questions et réponses courantes sur la réduction des menaces en ligne.

Q1: Qu'est-ce que le deep web ?

Le deep web comprend toutes les pages web que les moteurs de recherche ne peuvent pas indexer, notamment les services bancaires en ligne, les bases de données de messagerie et les revues payantes.

Q2: Qu'est-ce que le dark web ?

Le dark web est un petit sous-ensemble du deep web, volontairement caché et accessible uniquement avec des navigateurs spécialisés utilisant des réseaux onion.

Q3: Comment les moteurs de recherche indexent-ils les pages ?

Les moteurs exécutent des programmes automatisés (robots d'exploration) qui suivent les liens publics et indexent les pages qui ne bloquent pas l'exploration au moyen de directives pour robots.

Q4: Pourquoi la banque en ligne est-elle considérée comme faisant partie du deep web ?

Les portails bancaires sont protégés par des identifiants et des mots de passe, ce qui empêche les moteurs de recherche publics d'indexer les pages de relevés de compte.

Q5: Qu'est-ce que le routage en oignon (Onion Routing) du navigateur Tor ?

Le routage en oignon est une méthode de transmission qui chiffre le trafic en couches et le fait passer par plusieurs relais pour masquer les adresses IP des utilisateurs.

Point de contrôle 10 : Questions fréquentes de base sur la cybersécurité (Partie B)

Passez en revue les questions et réponses courantes sur la réduction des menaces en ligne.

Q6: Accéder au dark web est-il illégal ?

Non. Accéder au dark web est légal dans la plupart des pays, mais participer à des marchés illégaux ou à des cyberactivités illégales est interdit.

Q7: Pourquoi les sites du dark web sont-ils lents à charger ?

Le trafic est acheminé et déchiffré via au moins trois relais dans le monde (entrée, intermédiaire, sortie), ce qui augmente la latence de transmission.

Q8: Que signifie le suffixe de domaine .onion ?

Il s'agit d'un suffixe de domaine de premier niveau spécial utilisé sur le réseau Tor, qui pointe vers des adresses générées cryptographiquement au lieu de serveurs DNS standard.

Q9: Quels risques sont associés aux liens du dark web ?

Les sites n'ont aucun contrôle de sécurité, ce qui expose les utilisateurs à des taux élevés d'infection par des logiciels malveillants, à des scripts d'hameçonnage et à des escroqueries lors des transactions.

Q10: Qui a créé le protocole de routage du réseau Tor ?

Cette technologie a été développée à l'origine par le U.S. Naval Research Laboratory dans les années 1990 pour protéger les communications gouvernementales.

Point de contrôle 10 : Questions fréquentes avancées sur la sécurité (Partie C)

Découvrez les aspects techniques avancés des cadres de sécurité, de l'analyse des logiciels malveillants et de la conformité des données.

Q1: Comment les nœuds intermédiaires protègent-ils l'anonymat sur Tor ?

Chaque nœud ne déchiffre qu'une seule couche de données de routage et ne connaît que le saut précédent et le saut suivant, jamais à la fois la source et la destination.

Q2: Quel est le rôle du nœud de sortie ?

Le nœud de sortie déchiffre la dernière couche de chiffrement et envoie le trafic vers le serveur de destination public ou le serveur onion.

Q3: Qu'est-ce qu'une passerelle de ponts Tor ?

Les ponts (bridges) sont des relais d'entrée Tor non répertoriés, utilisés pour contourner les blocages des FAI et la censure dans les régions qui restreignent l'accès au navigateur Tor.

Q4: Comment les acteurs du dark web exploitent-ils les cryptomonnaies ?

Des acteurs malveillants utilisent des cryptomonnaies anonymes pour effectuer des transactions financières sur des marchés clandestins, en échappant aux contrôles bancaires habituels.

Q5: Pourquoi les moteurs de recherche classiques n'arrivent-ils pas à explorer les bases de données profondes ?

Les robots d'indexation ne peuvent pas saisir d'identifiants de connexion, résoudre des CAPTCHA de sécurité ni exécuter les scripts de requêtes SQL côté serveur nécessaires pour accéder aux bases de données profondes.

Point de contrôle 10 : Questions fréquentes avancées sur la sécurité (Partie D)

Découvrez les aspects techniques avancés des cadres de sécurité, de l'analyse des logiciels malveillants et de la conformité des données.

Q6: Qu'est-ce qu'un serveur d'annuaire dans les réseaux Tor ?

Il s'agit d'un serveur de confiance qui tient à jour la liste des relais d'entrée, intermédiaires et de sortie actifs utilisés par les clients pour construire leurs chemins de routage.

Q7: Comment les acteurs malveillants interceptent-ils le trafic sur les nœuds de sortie ?

Les opérateurs malveillants de nœuds de sortie peuvent intercepter le trafic HTTP non chiffré lorsqu'il quitte le réseau Tor, et voler des noms d'utilisateur et des cookies.

Q8: Quelle est la différence entre Tor et I2P ?

Tor utilise un annuaire de relais centralisé et des nœuds de sortie pour accéder au web public, tandis qu'I2P utilise une structure décentralisée de pair à pair pour l'hébergement interne.

Q9: Comment les forces de l'ordre traquent-elles les marchés du dark web ?

Les autorités utilisent l'analyse de la blockchain, localisent l'hébergement physique des serveurs et mènent des opérations d'infiltration pour identifier les opérateurs.

Q10: Comment une fuite DNS compromet-elle l'anonymat du client ?

Les fuites DNS se produisent lorsque les requêtes DNS du navigateur sont envoyées directement via le FAI local au lieu de passer par le réseau chiffré Tor.

Partie 11 : 10 faits et enseignements concrets sur la cybersécurité

Découvrez des faits concrets sur les failles de sécurité, les mécanismes de défense et les normes de conformité.

1. APERÇU SÉCURITÉ

Le deep web est bien plus vaste que le web de surface consultable, car la plupart des contenus se trouvent derrière des identifiants et des bases de données.

2. APERÇU SÉCURITÉ

Le dark web est une petite partie du deep web, volontairement cachée, à laquelle on accède avec des outils comme Tor.

3. APERÇU SÉCURITÉ

Le routage Tor chiffre les paquets de données trois fois, et chaque nœud relais retire une couche de chiffrement, comme on épluche un oignon.

4. APERÇU SÉCURITÉ

Tor est issu du projet de routage en oignon mené par le U.S. Naval Research Lab, et son code a été publié en tant que logiciel libre. [1]

5. APERÇU SÉCURITÉ

Les adresses onion sont des chaînes alphanumériques de 56 caractères générées cryptographiquement à partir de paires de clés publiques.

6. APERÇU SÉCURITÉ

Les nœuds de sortie peuvent lire le trafic en clair : TLS/HTTPS reste donc nécessaire sur Tor pour sécuriser les données de session.

7. ZOOM SUR LA SÉCURITÉ

Les sites intranet, les espaces de stockage cloud et les bases de données privées représentent les plus grands segments de stockage de données du web profond.

8. ZOOM SUR LA SÉCURITÉ

Des moteurs de recherche spécialisés comme DuckDuckGo proposent des portails onion pour permettre des recherches anonymes sur les réseaux Tor.

9. ZOOM SUR LA SÉCURITÉ

Plus de 2 millions d'utilisateurs se connectent chaque jour au réseau Tor pour contourner la censure et préserver la confidentialité de leurs communications.

10. APERÇU SÉCURITÉ

Des opérations internationales des forces de l'ordre (comme l'opération Bayonet) ont fermé de grandes places de marché du dark web en saisissant le matériel d'hébergement.

Références techniques et sources

Le guide d'étude et les énigmes interactives sont tirés des normes internationales du NIST, de l'OWASP et de conformité en matière de protection des données.

RÉFÉRENCES ACADÉMIQUES ET PROFESSIONNELLES

[1] Tor Project. (n.d.). Why is it called Tor?
https://support.torproject.org/about/why-is-it-called-tor/

[2] Tor Project. (n.d.). How do Onion Services work?
https://community.torproject.org/onion-services/overview/

[3] Tor Project. (n.d.). Users – Tor Metrics.
https://metrics.torproject.org/userstats-relay-country.html

[4] CISA. (n.d.). Malware, Phishing, and Ransomware.
https://www.cisa.gov/topics/cyber-threats-and-advisories/malware-phishing-and-ransomware

[5] CISA. (2023). Phishing Guidance: Stopping the Attack Cycle at Phase One.
https://www.cisa.gov/resources-tools/resources/phishing-guidance-stopping-attack-cycle-phase-one

Corrigé : Point de contrôle 1 – Choix multiple

1 **Indexation par les moteurs de recherche** WEB PROFOND — **Bonne réponse : A**

NOTE PÉDAGOGIQUE

Les pages du deep web se trouvent derrière des pages de connexion et dans des bases de données, ce qui empêche les robots des moteurs de recherche de les explorer. Source : IETF RFC 3986.

2 **Accès à Tor** DARK WEB — **Bonne réponse : A**

NOTE PÉDAGOGIQUE

Le dark web se compose de services onion cachés, accessibles uniquement avec des navigateurs comme Tor. Citation : IETF RFC 3986.

3 **Bases de données profondes** BASES DE DONNÉES — **Bonne réponse : A**

NOTE PÉDAGOGIQUE

Les comptes protégés par mot de passe et les dossiers d'entreprise forment la plus grande partie du deep web. Source : NIST Digital Identity.

4 **Routage en oignon** RÉSEAU TOR — **Bonne réponse : A**

NOTE PÉDAGOGIQUE

Le routage en oignon chiffre les paquets de données en couches et les relaie à travers plusieurs nœuds pour assurer l'anonymat. Source : IETF RFC 3986.

5 **Domaine onion** EXTENSION — **Bonne réponse : A**

NOTE PÉDAGOGIQUE

Le suffixe de domaine cryptographique.onion achemine le trafic en interne sur Tor, sans DNS public. Citation : IETF RFC 3986.

Corrigé : Point de contrôle 2 – Vrai ou faux

6 **Segments web** STRUCTURE

Bonne réponse : Faux

NOTE PÉDAGOGIQUE

Le deep web couvre toutes les pages non indexées, tandis que le dark web en est un petit sous-segment onion chiffré. Citation : IETF RFC 3986.

7 **Intranets d'entreprise** WEB PROFOND

Bonne réponse : Vrai

NOTE PÉDAGOGIQUE

Les sites intranet se trouvent derrière des portails protégés par mot de passe et ne sont pas indexés : ils font donc partie du web profond. Source : NIST Digital Identity.

8 **Chiffrement en couches** RELAIS

Bonne réponse : Faux

NOTE PÉDAGOGIQUE

Les relais onion ne déchiffrent qu'une seule couche de routage pour protéger l'anonymat de l'utilisateur, jamais le paquet entier. Source : IETF RFC 3986.

9 **Exposition aux logiciels malveillants** MENACES

Bonne réponse : Vrai

NOTE PÉDAGOGIQUE

Les marchés du dark web ne disposent d'aucun filtrage de sécurité et présentent des risques extrêmes d'infection par des logiciels malveillants. Source : Center for Internet Security (CIS).

10 **Question 10**

Bonne réponse : Faux

NOTE PÉDAGOGIQUE

Les robots d'indexation des moteurs de recherche ordinaires n'utilisent pas Tor : ils ne peuvent donc ni atteindre ni indexer les sites .onion.

Corrigés du vocabulaire et grille d'évaluation

Grille de notation de l'enseignant : attribuez 1 point par association correcte (8 points au total) et par terme en contexte (6 points au total).

POINT DE CONTRÔLE 4 : CORRIGÉ DE L'ASSOCIATION DE NOTIONS

H 1. Segment du Web profond	A 2. Portail du dark web	D 3. Extension .onion	B 4. Routage Tor
F 5. Pages indexées	G 6. Anonymat de l'utilisateur	C 7. Base de données privée	E 8. Passerelle d'entrée

POINT DE CONTRÔLE 3 : CORRIGÉ DES TERMES CLÉS

1 DEEP WEB	2 DARK WEB	3 ONION	4 ROUTAGE EN OIGNON
5 INDEXÉES	6 ANONYMAT		

POINT DE CONTRÔLE 6, VARIANTE : CORRIGÉ DE L'ASSOCIATION DE MOTS

1 F – ANONYMAT	2 G – BASEDEDONNEES	3 D – ROUTAGETOR	4 A – DEEPWEB
5 B – DARKWEB	6 C – ONION	7 H – NOEUDDEGARDE	8 E – PAGESINDEXEES

NOTES DE DISCUSSION POUR LES ENSEIGNANTS

Termes clés :
Vérifiez que les élèves savent expliquer Segment du Web profond, Portail du dark web et Extension .onion avec leurs propres mots et donner un exemple pour chacun.

Études de cas :
Demandez aux élèves de justifier leurs recommandations par des faits tirés de la fiche plutôt que par des suppositions.

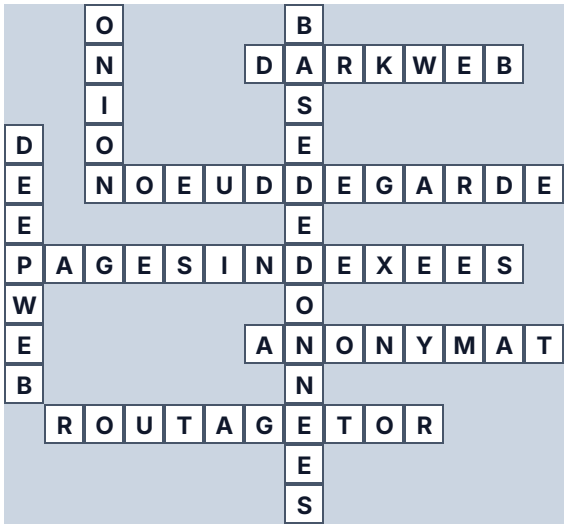
Évaluation des sources :
Faites vérifier au moins une affirmation à l'aide des sources de la fiche et discutez des raisons pour lesquelles les chiffres, les prix et les règles peuvent évoluer avec le temps.

Corrigés des jeux et notes pour l'enseignant

SOLUTION DES MOTS CACHÉS

S	K	T	S	V	R	Z	E	H	E	S	C	A	L	Q
E	C	R	O	T	E	G	A	T	U	O	R	Z	D	D
E	M	K	V	O	N	I	O	N	R	U	A	A	E	S
N	W	J	M	M	H	H	N	H	R	F	R	E	K	T
N	L	R	W	H	B	U	F	Y	O	K	P	Y	W	S
O	H	T	X	A	P	U	N	N	W	W	Z	O	I	Q
D	T	I	P	V	U	O	U	E	E	U	K	A	E	P
E	M	K	A	N	V	G	B	B	G	P	Q	X	Y	J
D	K	V	J	Y	W	Y	P	J	I	Z	I	J	N	A
E	E	I	A	T	A	M	Y	N	O	N	A	S	A	J
S	P	A	G	E	S	I	N	D	E	X	E	E	S	F
A	W	E	K	Z	K	E	K	Q	N	J	A	F	O	K
B	N	N	O	E	U	D	D	E	G	A	R	D	E	D
N	C	D	H	I	B	A	P	R	L	P	W	T	I	Y
F	Y	S	G	X	W	H	F	R	T	N	U	K	R	D

SOLUTION DES MOTS CROISÉS



GUIDE DE L'ENSEIGNANT : SOLUTIONS DES MOTS CROISÉS

HORIZONTALEMENT

3 horizontal: DARKWEB Segment de réseau chiffré accessible uniquement avec des navigateurs spéciaux (7 lettres)

5 horizontal: NOEUDDEGARDE Point d'entrée utilisé pour accéder au réseau Tor (12 lettres)

6 horizontal: PAGESINDEXEES Contenus du web de surface compilés et consultables sur Google (13 lettres)

7 horizontal: ANONYMAT Fait de cacher aux serveurs l'adresse IP publique du client (8 lettres)

8 horizontal: ROUTAGETOR Chiffrement des données en plusieurs couches et relais via trois nœuds (10 lettres)

VERTICALEMENT

1 vertical: ONION Suffixe cryptographique de domaine de premier niveau utilisé sur les réseaux Tor (5 lettres)

2 vertical: BASEDEDONNEES Stockage dorsal sécurisé hébergeant des enregistrements système non indexés (13 lettres)

4 vertical: DEEPWEB Contenus web non indexés, comme les espaces de connexion privés, les e-mails et les enregistrements de bases de données (7 lettres)

Corrigé des mots mélangés et du code

Corrigé de l'activité de remise en ordre des lettres du vocabulaire et du défi du code secret.

CORRIGÉ DES MOTS MÉLANGÉS

1. PEDWBEE — **DEEPWEB**
2. ONOIN — **ONION**
3. APDXEESGNSIEE — **PAGESINDEXEES**
4. EENSODSDENBAE — **BASEDEDONNEES**
5. WBKRDEA — **DARKWEB**
6. OATETROGRU — **ROUTAGETOR**
7. ATYMANNO — **ANONYMAT**
8. GEDREENDODAU — **NOEUDDEGARDE**

CORRIGÉ DU DÉFI DU CODE SECRET

"ANONYMAT PRESERVE PAR LE ROUTAGE EN OIGNON"

Corrigé des études de cas

A Étude de cas 1 : Identification d'une fuite de données

Corrigé de l'enseignant

CONSIGNE DE NOTATION

Les réponses des élèves doivent couvrir les points suivants :

- Analyse de scénario : un audit de sécurité d'entreprise découvre que des enregistrements sensibles de la base de données clients sont échangés sur une place de marché onion. Les données ne sont pas indexées sur Google.
- Stratégie et solution recommandées : Segments concernés : la base de données privée appartient au deep web (non indexée mais sécurisée). La place de marché où s'échangent les données volées se trouve sur le dark web (réseau onion). Comment c'est arrivé : des pirates ont contourné les défenses du serveur, volé la base de données du deep web et l'ont mise en vente anonymement sur le dark web pour échapper à la traque des forces de l'ordre.

B Étude de cas 2 : Anonymat ou risques de logiciels malveillants

Corrigé de l'enseignant

CONSIGNE DE NOTATION

Les réponses des élèves doivent couvrir les points suivants :

- Analyse de scénario : un analyste veut consulter des flux de renseignement sur les menaces sur un site Tor. Il télécharge le navigateur Tor et accède au site.
- Stratégie et solution recommandées : Avantages : Tor fait transiter le trafic par trois nœuds, ce qui masque l'IP professionnelle de l'analyste. Risques et atténuation : les liens du dark web ne font l'objet d'aucun filtrage de réputation. Les analystes doivent utiliser Tor dans des machines virtuelles (VM) isolées, désactiver JavaScript dans les paramètres de Tor et éviter de télécharger le moindre fichier afin de protéger le réseau de l'entreprise.