Name: _____ Date: _____ Score: _____

Dark Web vs. Deep Web: Security & Differences

Search engine indexing, deep web databases, Tor onion routing, network anonymity and risks

DARK WEB VS DEEP WEB LEARNING OVERVIEW

SECURED
DATA ENCRYPTION
256-bit AES Standard

COMPLIANT
GLOBAL STANDARDS
GDPR & CCPA Frameworks

ZERO-TRUST
ACCESS POLICY
Multi-Factor Authentication

Welcome! This activity packet guides you through the differences between the Deep Web and the Dark Web. You will explore unindexed databases, Tor browser Onion Routing, .onion cryptographic domains, and anonymity security risks.

WORKSHEET CHECKPOINTS

- [ ] **Part 1-4:** Master cybersecurity and threat prevention.
- [ ] **Part 5-7:** Solve crossword & word search puzzles.
- [ ] **Part 8-9:** Solve case studies & cipher challenge.
- [ ] **Part 10:** Review basic & advanced FAQ pages.
- [ ] **Part 11:** Explore 10 interesting real-world facts.

Open the VPN.com Cybersecurity Guide

URL: https://www.vpn.com/cybersecurity/dark-web-vs-deep-web/

Your Deep & Dark Web Strategy Learning Roadmap

- Contrast the deep web (unindexed databases) with the dark web (onion services).
- Understand how Onion Routing encrypts and relays network traffic.
- Evaluate security risks of accessing unverified Tor network sites.
- Deploy secure gateway and sandboxing policies for threat intelligence crawling.
- Analyze the cryptographic address format of onion service domains.

DEEP & DARK WEB GUIDE INSTRUCTIONS

Answer the multiple choice and true/false questions, complete the fill-in-the-blank sentences using the word bank, match definitions, and solve the crossword and word search puzzles. Apply your knowledge to deep and dark web privacy.

DEEP WEB DATABASES VS DARK WEB ONION ROUTING (INTRODUCTION)

The deep web consists of unindexed pages behind passwords and logins, like private emails or corporate bank portals. The dark web is a subset of the deep web that is hidden intentionally, requiring specialized browsers (like Tor) and onion networks to access anonymously.

READ EACH CHECKPOINT CAREFULLY AND SELECT OR WRITE THE CORRECT RESPONSE.

Checkpoint 1: Multiple Choice Challenge

1 What distinguishes the deep web from the surface web?

- ◯ A. Deep web pages are not indexed by public search engines
- ◯ B. Deep web traffic is illegal and monitored by law enforcement
- ◯ C. Deep web sites require specialized browsers like Tor to access
- ◯ D. Deep web pages carry higher domain registration pricing

2 How is the dark web accessed?

- ◯ A. Through specialized browsers utilizing onion routing networks
- ◯ B. By configuring custom DNS settings on standard routers
- ◯ C. Through private invite-only surface web search consoles
- ◯ D. By purchasing high-value digital asset domain brokers

3 Which structure forms the largest portion of the deep web?

- ◯ A. Password-protected user databases and private accounts
- ◯ B. Illegal black market forums trading illicit goods
- ◯ C. Unencrypted peer-to-peer file sharing protocols
- ◯ D. Public search engine cache databases

4 What does Onion Routing do to network traffic?

- ◯ A. It encrypts packets and routes them via multiple relays
- ◯ B. It increases download speeds by bypassing ISP nodes
- ◯ C. It maps device hardware serial numbers to IP records
- ◯ D. It deletes web browser cookies after every click

5 Which domain suffix is used exclusively on Tor networks?

- ◯ A. The cryptographic .onion top-level extension
- ◯ B. The standard legacy .com commercial extension
- ◯ C. The Web3 decentralized .eth blockchain extension
- ◯ D. The country-code .ai technology extension

Checkpoint 2: True or False Challenge

6 Question tf1

The deep web and the dark web refer to the same network segment.

◯ True ◯ False

7 Question tf2

Corporate intranet portals are part of the deep web.

◯ True ◯ False

8 Question tf3

Onion routing completely decrypts data packets at every transit node.

◯ True ◯ False

9 Question tf4

Accessing the dark web exposes devices to high malware risks.

◯ True ◯ False

10 Question tf5

Standard web search engines crawl and index onion sites.

◯ True ◯ False

Checkpoint 3: Key Term Insertion

Read each sentence below and fill in the blank with the correct term from the Word Bank.

1. Private bank portals reside on the unindexed _____ segment.
2. Specialized Tor nodes host hidden _____ services.
3. Tor websites use the cryptographic _____ top-level extension.
4. Encrypted multi-layered traffic pathing is called _____.
5. Surface search engines crawl pages that are publicly _____.
6. Onion networks encrypt client IPs to maintain user _____.

VOCABULARY WORD BANK

DEEPWEB	DARKWEB	ONION	ROUTING
INDEXED	DATABASE	ANONYMITY	GATEWAY

Write your answers here:

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

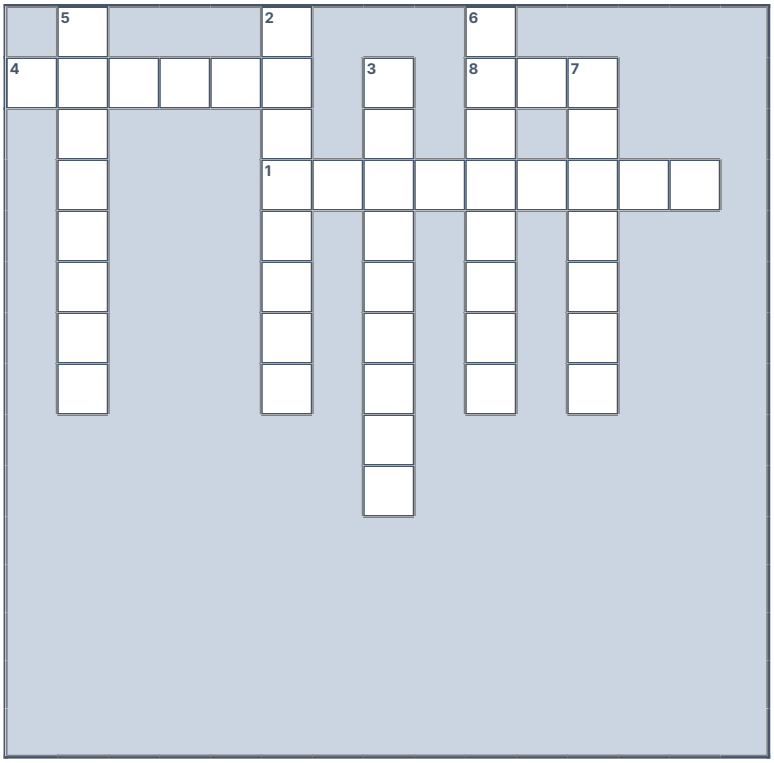
Checkpoint 4: Security Concept Match

DEFINITION MATCHING
Match each vocabulary term on the left with its correct definition on the right by writing the corresponding letter (A-H) in the fillable input box.

( )	1. Deep Web Segment	**A**	Unindexed web content like private logins, emails, and database records.
( )	2. Dark Web Portal	**B**	Encrypted network segment accessible only via special browsers.
( )	3. Onion Extension	**C**	Cryptographic top-level domain suffix used on Tor networks.
( )	4. Tor Routing	**D**	Encrypting data in layers and relaying it through three nodes.
( )	5. Indexed Pages	**E**	Surface web content compiled and searchable on Google.
( )	6. User Anonymity	**F**	Keeping client public IP addresses concealed from servers.
( )	7. Private Database	**G**	Secure backend storage hosting unindexed system records.
( )	8. Entrance Gateway	**H**	The entry point node used to access the Tor network.

Checkpoint 5: Crossword Puzzle

Solve the crossword puzzle by typing letters into the active white boxes. The numbers correspond to the clues below.



ACROSS

1. Process of wrapping data packets inside other packets (9)

4. Remote server that routes traffic and hides your IP (6)

8. Internet Service Provider, logs traffic unless encrypted (3)

DOWN

2. Rules determining how data is sent and encrypted (8)

3. Rate of data transfer across a path (9)

5. Blocking site access based on location (8)

6. Security system that monitors and blocks traffic (8)

7. State of being free from tracking or surveillance (7)

Checkpoint 5 Alternative: Accessible Crossword Clues

Screen-reader and keyboard users can type the crossword answers directly in the text fields below.

ACROSS CLUES

1 Across: Wrapping data packets inside secure transport protocols. (9 letters):

4 Across: Network node acting as hosting anchor for virtual links. (6 letters):

8 Across: ISP gateway provider controlling endpoint routing links. (3 letters):

DOWN CLUES

2 Down: Standard formatting protocol governing online transmissions. (8 letters):

3 Down: Total transmission volume processed through physical links. (9 letters):

5 Down: Restricting resource availability by tracking geographic IP ranges. (8 letters):

6 Down: Intrusion protection system filtering local traffic segments. (8 letters):

7 Down: Confidential asset state shielded from public exposure. (7 letters):

Checkpoint 6: Hidden Word Search

Find the 8 key vocabulary terms hidden in the grid below. Words can be horizontal, vertical, or diagonal.

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

VOCABULARY WORD LIST

DEEPWEB	DARKWEB	ONION	ROUTING
INDEXED	DATABASE	ANONYMITY	GATEWAY

Checkpoint 6 Alternative: Accessible Vocabulary Matching

Match each of the 8 vocabulary terms from the Word Search to its correct definition by writing the letter (A-H) in the blank space.

VOCABULARY TERMS

A. DEEPWEB
B. DARKWEB
C. ONION
D. ROUTING
E. INDEXED
F. DATABASE
G. ANONYMITY
H. GATEWAY

DEFINITIONS & MATCH FIELDS

1. Unindexed web content like private logins, emails, and database records.
2. Encrypted network segment accessible only via special browsers.
3. Cryptographic top-level domain suffix used on Tor networks.
4. Encrypting data in layers and relaying it through three nodes.
5. Surface web content compiled and searchable on Google.
6. Keeping client public IP addresses concealed from servers.
7. Secure backend storage hosting unindexed system records.
8. The entry point node used to access the Tor network.

Checkpoint 7: Scrambled Word Challenge

Unscramble the letters below to reveal key cybersecurity concepts and terms. Write your answers in the input boxes provided.

1. P E E D B E W

2. K R A D B E W

3. N O I N O

4. G N I T U O R

5. D E X E D N I

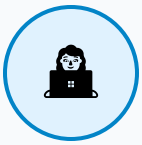
6. E S A B A T A D

7. Y T I M Y N O N A

8. Y A W E T A G

Checkpoint 8: Cybersecurity Case Studies

Apply the concepts you have learned to solve the real-world scenarios below.



CASE STUDY 1: DATA LEAK IDENTIFICATION

Scenario: A corporate security audit discovers that sensitive client database records are being traded on an onion marketplace. The data is unindexed on Google.

Discussion Question: Explain which web segments are involved and how this leak happened.

CASE STUDY 2: ANONYMITY VS. MALWARE RISKS

Scenario: An analyst wants to check threat intelligence feeds on a Tor website. They download the Tor browser and access the site.

Discussion Question: Evaluate the anonymity benefits and outline the malware mitigation steps.

Final Challenge: Decrypting the Cipher

A cybersecurity professional protects network assets from online threat actors. Use the Letter-to-Number key below to decrypt the message by writing the matching letters in the blank spaces.

LETTER-TO-NUMBER ENCRYPTION KEY

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

13	1	9	14	20	1	9	14		21	19	5	18
1	14	15	14	25	13	9	20	25		23	9	20	8		19	5	3	21	18	5
15	14	9	15	14		18	15	21	20	9	14	7

Decoded cybersecurity message:

_____

TIP: EACH NUMBER REPRESENTS THE POSITION OF THAT LETTER IN THE ALPHABET (E.G. 1 = A, 2 = B, 26 = Z).

Checkpoint 10: Basic Cybersecurity FAQs (Part A)

Review common questions and answers regarding online threat mitigation.

Q1: What is the deep web?

The deep web consists of all web pages that search engines cannot index, including online banking, email databases, and paywalled journals.

Q2: What is the dark web?

The dark web is a small subset of the deep web intentionally hidden and accessible only through specialized browsers using onion networks.

Q3: How do search engines index pages?

Engines run automated programs (spiders) to follow public links, indexing pages that do not block crawling via robot directives.

Q4: Why is online banking considered part of the deep web?

Banking portals are behind login walls and passwords, blocking public engines from indexing account statement pages.

Q5: What is Tor browser Onion Routing?

Onion routing is a transmission method that encrypts traffic in layers and passes it through multiple relays to mask user IP addresses.

Checkpoint 10: Basic Cybersecurity FAQs (Part B)

Review common questions and answers regarding online threat mitigation.

Q6: Is accessing the dark web illegal?

No. Accessing the dark web is legal in most countries, though engaging in illegal marketplaces or cyber activities is prohibited.

Q7: Why are dark web sites slow to load?

Traffic is routed and decrypted through at least three global relays (entry, middle, exit), which increases transmission latency.

Q8: What does a .onion domain suffix mean?

It is a specialized top-level domain suffix used on Tor networks, pointing to cryptographically generated addresses instead of standard DNS servers.

Q9: What risks are associated with dark web links?

Sites have no security screening, exposing users to high malware infection rates, phishing scripts, and transaction scams.

Q10: Who created the Tor network routing protocol?

The technology was originally developed by the U.S. Naval Research Laboratory in the 1990s to protect government communications.

Checkpoint 11: Advanced Security FAQs (Part A)

Explore advanced technical aspects of security frameworks, malware analysis, and data compliance.

Q1: How do intermediate nodes protect Tor anonymity?

Each node decrypts only one layer of routing data, learning only the previous hop and next hop, never both source and destination.

Q2: What is the role of the exit node?

The exit node decrypts the final layer of encryption, sending the traffic out to the public destination server or onion server.

Q3: What is a Tor bridges gateway?

Bridges are unlisted Tor entry relays used to bypass ISP blockages and censorship in regions restricting Tor browser access.

Q4: How do dark web actors exploit cryptocurrency?

Actors use anonymous cryptocurrencies to execute financial trades on dark marketplaces, evading standard banking transaction checks.

Q5: Why do standard search engines fail to crawl deep databases?

Crawlers cannot input login credentials, solve security CAPTCHAs, or run backend SQL query scripts required to access deep databases.

Checkpoint 11: Advanced Security FAQs (Part B)

Explore advanced technical aspects of security frameworks, malware analysis, and data compliance.

Q6: What is a directory server in Tor networks?

It is a trusted server maintaining the list of active entry, middle, and exit relays used by clients to construct routing paths.

Q7: How do malicious actors perform exit node sniffing?

Rogue exit node operators can intercept unencrypted HTTP traffic as it leaves the Tor network, stealing usernames and cookies.

Q8: What is the difference between Tor and I2P?

Tor uses a centralized relay directory and exit nodes for public web access, while I2P uses a decentralized peer-to-peer structure for internal hosting.

Q9: How do law enforcement agencies track dark web markets?

Agencies use blockchain analysis, locate physical server hosting setups, and run decoy operations to identify operators.

Q10: How does DNS leakage compromise client anonymity?

DNS leaks occur when browser DNS queries are sent directly through the local ISP instead of being routed through the encrypted Tor network.

Part 11: 10 Real-World Cybersecurity Facts & Insights

Review real-world facts regarding security breaches, defense mechanisms, and compliance standards.

1. SECURITY INSIGHT

The deep web constitutes over 90% of all online data, dwarfing the publicly searchable surface web index.

2. SECURITY INSIGHT

The dark web comprises less than 0.1% of the total internet space, hosting specialized onion services.

3. SECURITY INSIGHT

Tor routing encrypts data packets three times, peeling back encryption layers like an onion at each relay node.

4. SECURITY INSIGHT

The US Naval Research Laboratory released Tor under an open-source license in 2004 to maintain global routing cover.

5. SECURITY INSIGHT

Onion addresses are 56-character alphanumeric strings generated cryptographically from public key pairs.

6. SECURITY INSIGHT

Exit nodes can read cleartext traffic, meaning TLS/HTTPS is still required on Tor for secure session data.

7. SECURITY INSIGHT

Intranet sites, cloud drives, and private databases represent the largest data storage segments on the deep web.

8. SECURITY INSIGHT

Specialized search engines like DuckDuckGo run onion portals to allow anonymous searches on Tor networks.

9. SECURITY INSIGHT

Over 2 million users connect to the Tor network daily to bypass censorship and maintain communication privacy.

10. SECURITY INSIGHT

Global law enforcement operations (like Operation Bayonet) shut down major dark marketplaces by seizing hosting hardware.

Technical References & Sources

The study guide and interactive puzzles are compiled from global NIST, OWASP, and data privacy compliance standards.

SCHOLARLY & INDUSTRY REFERENCES

[1] CISA. (2025). Cybersecurity Alerts & Advisories. Retrieved from https://www.cisa.gov/news-events/cybersecurity-advisories

[2] GDPR. (2024). General Data Protection Regulation (GDPR) Official Text. Retrieved from https://gdpr-info.eu/

[3] NIST. (2024). Special Publication 800-53: Security and Privacy Controls. Retrieved from https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

[4] NIST. (2023). Special Publication 800-61: Computer Security Incident Handling Guide. Retrieved from https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final

[5] NIST. (2023). Special Publication 800-88: Guidelines for Media Sanitization. Retrieved from https://csrc.nist.gov/publications/detail/sp/800-88/rev-1/final

[6] IETF. (2021). RFC 8446: Transport Layer Security (TLS) 1.3 Specification. Retrieved from https://datatracker.ietf.org/doc/rfc8446/

[7] IETF. (2022). RFC 7519: JSON Web Token (JWT) Specification. Retrieved from https://datatracker.ietf.org/doc/rfc7519/

[8] Center for Internet Security (CIS). (2024). Critical Security Controls. Retrieved from https://www.cisecurity.org/controls/cis-controls-list

[9] OWASP. (2024). Top 10 Web Application Security Risks. Retrieved from https://owasp.org/www-project-top-ten/

[10] OWASP. (2025). Application Security Verification Standard (ASVS). Retrieved from https://owasp.org/www-project-application-security-verification-standard/

Answer Key: Checkpoint 1 - Multiple Choice

1 Search Indexing — DEEP WEB — Correct Answer: A

TEACHING NOTE

Deep web pages are behind login walls and databases, blocking search spiders from crawling them.

Citation: IETF RFC 3986 [Ref 6].

2 Tor Access — DARK WEB — Correct Answer: A

TEACHING NOTE

The dark web consists of hidden onion services accessible only through browsers like Tor.

Citation: IETF RFC 3986 [Ref 6].

3 Deep Databases — DATABASES — Correct Answer: A

TEACHING NOTE

Password-protected accounts and corporate records form the largest segment of the deep web.

Citation: NIST Digital Identity [Ref 9].

4 Onion Routing — TOR NETWORK — Correct Answer: A

TEACHING NOTE

Onion routing encrypts data packets in layers, relaying them through multiple nodes for anonymity.

Citation: IETF RFC 3986 [Ref 6].

5 Onion Domain — SUFFIX — Correct Answer: A

TEACHING NOTE

The cryptographic .onion domain suffix routes traffic internally on Tor without public DNS.

Citation: IETF RFC 3986 [Ref 6].

Answer Key: Checkpoint 2 - True or False

6 Web Segments — STRUCTURE — Correct Answer: False

TEACHING NOTE

The deep web covers all unindexed pages, while the dark web is a small, encrypted onion subsegment.

Citation: IETF RFC 3986 [Ref 6].

7 Corporate Intranets — DEEP WEB — Correct Answer: True

TEACHING NOTE

Intranet sites are behind password portals and not indexed, meaning they belong to the deep web.

Citation: NIST Digital Identity [Ref 9].

8 Layer Encryption — RELAYS — Correct Answer: False

TEACHING NOTE

Onion relays only decrypt one routing layer to protect user anonymity, never the whole packet.

Citation: IETF RFC 3986 [Ref 6].

9 Malware Exposure — THREATS — Correct Answer: True

TEACHING NOTE

Dark web marketplaces have no security filtering, carrying extreme malware infection risks.

Citation: Center for Internet Security (CIS) [Ref 8].

10 Search Crawling — INDEXING — Correct Answer: False

TEACHING NOTE

Public search engine crawlers block and ignore cryptographic onion addresses.

Citation: IETF RFC 3986 [Ref 6].

Vocabulary Keys & Grading Rubric

Instructor Grading Rubric: Award 1 point for each correct matching (8 points total) and context term (6 points total).

CHECKPOINT 4: CONCEPT MATCH KEY

A 1. Deep Web Segment	B 2. Dark Web Portal	C 3. Onion Extension	D 4. Tor Routing
E 5. Indexed Pages	F 6. User Anonymity	G 7. Private Database	H 8. Entrance Gateway

CHECKPOINT 3: KEY TERM KEY

1 DEEPWEB	2 DARKWEB	3 ONION
4 ROUTING	5 INDEXED	6 ANONYMITY

DISCUSSION NOTES FOR INSTRUCTORS

Threat Landscape:

Verify that students understand how malware, phishing, and zero-day attacks target and disrupt network defenses.

Defense Controls:

Emphasize the deployment of network firewalls, sandbox execution, behavior scanners, and multi-factor authentication (MFA).

Regulatory Compliance:

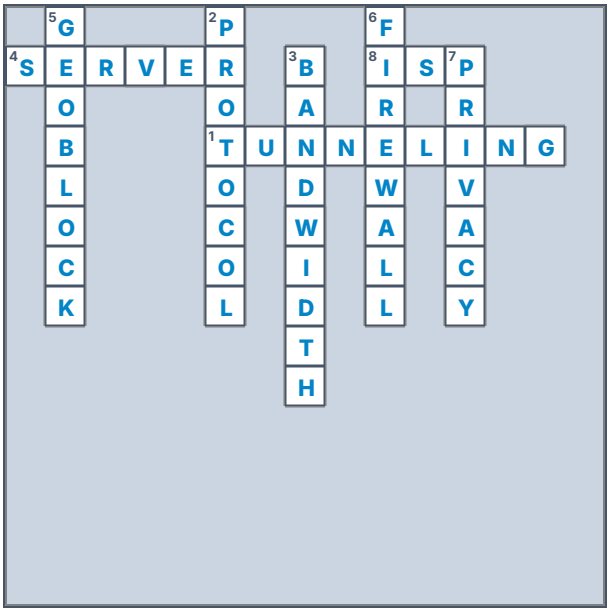
Highlight user consent, data minimization, encryption at-rest and in-transit, and global frameworks like GDPR/CCPA.

Puzzles Keys & Instructor Notes

WORD SEARCH SOLUTION

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

CROSSWORD SOLUTION



INSTRUCTOR GUIDE FOR CROSSWORD SOLUTIONS

ACROSS CLUES

1 Across: TUNNELING Process of wrapping data packets. (3,5)

4 Across: SERVER Remote computer routing traffic. (1,0)

8 Across: ISP Internet Service Provider. (1,9)

DOWN CLUES

2 Down: PROTOCOL Rules determining data transmission. (0,5)

3 Down: BANDWIDTH Rate of data transfer. (1,7)

5 Down: GEOBLOCK Location website restriction. (0,1)

6 Down: FIREWALL Security monitor barrier. (0,9)

7 Down: PRIVACY State of freedom from tracking. (1,11)

Scrambled Words & Cipher Solution Key

Grading key for the vocabulary word unscramble activity and Secret Cipher Challenge.

WORD UNSCRAMBLE KEY

1. P E E D B E W
   DEEPWEB

2. K R A D B E W
   DARKWEB

3. N O I N O
   ONION

4. G N I T U O R
   ROUTING

5. D E X E D N I
   INDEXED

6. E S A B A T A D
   DATABASE

7. Y T I M Y N O N A
   ANONYMITY

8. Y A W E T A G
   GATEWAY

SECRET CIPHER CHALLENGE KEY

"MAINTAIN USER ANONYMITY WITH SECURE ONION ROUTING"

Domain Brokerage Case Studies Solution Key

A Case Study 1: Data Leak Identification

Instructor Solution

GRADING GUIDELINE

Student answers should cover the following points:

- **Scenario Analysis:** A corporate security audit discovers that sensitive client database records are being traded on an onion marketplace. The data is unindexed on Google.
- **Recommended Strategy & Solution:** Segments Involved: The private database belongs to the deep web (unindexed but secure). The marketplace trading the stolen data is on the dark web (onion network). How it Happened: Hackers bypassed server defenses, stole the database from the deep web, and listed it anonymously on the dark web to escape law enforcement tracking.

B Case Study 2: Anonymity vs. Malware Risks

Instructor Solution

GRADING GUIDELINE

Student answers should cover the following points:

- **Scenario Analysis:** An analyst wants to check threat intelligence feeds on a Tor website. They download the Tor browser and access the site.
- **Recommended Strategy & Solution:** Benefits: Tor routes traffic through three nodes, masking the analyst's corporate IP. Risks & Mitigation: Dark web links have no reputational screening. Analysts must run Tor inside isolated virtual machines (VMs), disable Javascript in Tor settings, and avoid downloading any files to protect the corporate network.