Name: _____ Date: _____ Score: _____

Password Leaks & Credential Security

Credential stuffing, data breaches, hash algorithms, multi-factor authentication, and password security.

PASSWORD LEAKS 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 password leaks and credential security. You will explore credential stuffing, data breaches, hashing algorithms, multi-factor authentication, and password managers.

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/passwords-leak/

Your Password Security Learning Roadmap

- Understand credentials exposure risks on dark web forums.
- Implement multi-factor authentication (MFA) and credit freeze alerts.
- Design corporate security defenses against targeted social engineering scams.

PASSWORD LEAKS 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 credential protection.

PASSWORD LEAKS & CREDENTIAL SECURITY (INTRODUCTION)

Password leaks expose critical user credentials on public and dark web repositories. Implementing secure password managers, complex salting standards, bcrypt hashing algorithms, and multi-factor authentication (MFA) controls prevents automated credential stuffing compromises.

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

Checkpoint 1: Multiple Choice Challenge

1 What is credential stuffing?

- ◯ A. Using automation to test leaked username/password combinations across multiple sites
- ◯ B. Encrypting local database storage files
- ◯ C. Overwhelming web servers with network traffic requests
- ◯ D. Monitoring keyboard inputs secretly

2 Which hashing algorithm is considered cryptographically secure for storing passwords today?

- ◯ A. bcrypt
- ◯ B. MD5
- ◯ C. SHA-1
- ◯ D. ROT13

3 How does multi-factor authentication (MFA) mitigate the risk of password leaks?

- ◯ A. It requires an additional, time-sensitive verification code even if the password is stolen
- ◯ B. It automatically changes the password every hour
- ◯ C. It encrypts the username during transmission
- ◯ D. It alerts the credit bureau of fraudulent requests

4 What is a data breach dump?

- ◯ A. A collection of leaked user credentials published online or sold on hacker forums
- ◯ B. A backup copy of database files stored offsite
- ◯ C. A temporary cache of web server logs
- ◯ D. An administrative tool used to reset user passwords

5 What is the role of a password manager?

- ◯ A. Generating and storing unique, strong passwords for every account
- ◯ B. Monitoring network traffic for password leaks
- ◯ C. Blocking automated brute-force attacks at the gateway
- ◯ D. Scanning database storage blocks for unencrypted passwords

Checkpoint 2: True or False Challenge

6 Question 6

Reusing passwords across multiple accounts increases the risk of credential stuffing.

◯ True ◯ False

7 Question 7

SHA-1 is a recommended hashing function for modern password storage.

◯ True ◯ False

8 Question 8

Enforcing password complexity alone (without MFA) completely stops credential stuffing.

◯ True ◯ False

9 Question 9

Dark web monitoring tools scan the internet for compromised corporate credentials.

◯ True ◯ False

10 Question 10

Salted hashes add unique random data to passwords before hashing to defeat rainbow table attacks.

◯ 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. Testing leaked credentials across many web applications is credential _____.
2. Securely storing passwords on servers requires hashing with _____.
3. Exposure of confidential database files on the internet is a data _____.
4. Adding random values to passwords before hashing is called _____.
5. A secure local database for user credentials is a password _____.
6. Adding a second login verification step uses _____.

VOCABULARY WORD BANK

STUFFING	BCRYPT	BREACH	SALTING
MANAGER	MFA		

Write your answers here:

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

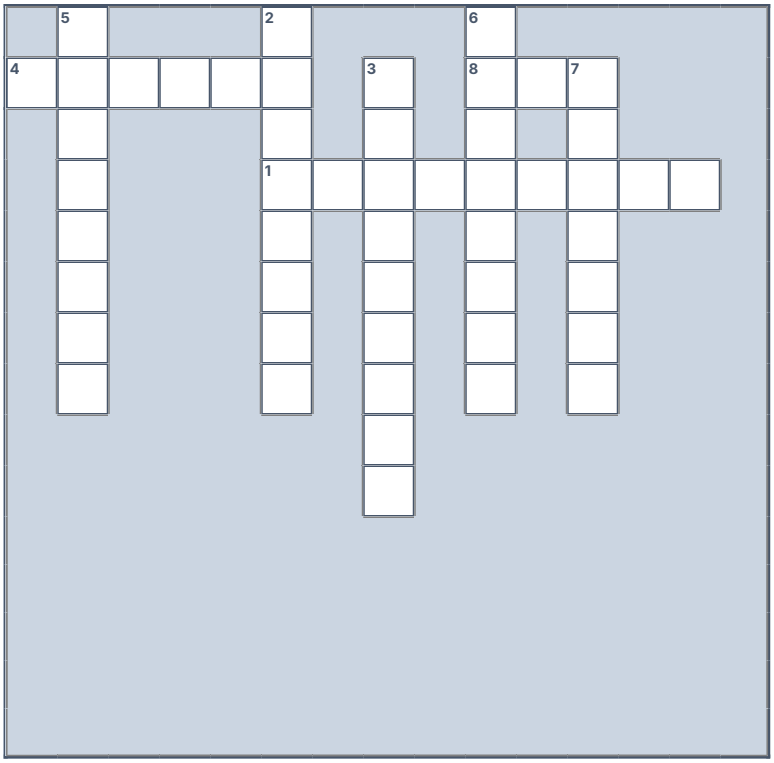
Checkpoint 4: Security Concept Match

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.

STUFFING	**A** Testing leaked credentials. (A)
BCRYPT	**B** Slow password hashing algorithm. (B)
BREACH	**C** Unauthorized database exposure. (C)
SALTING	**D** Adding random salt to password hash. (D)
MANAGER	**E** Credential storage tool. (E)
MFA	**F** Multi-factor login check. (F)
RAINBOW	**G** Precomputed table of password hashes. (G)
PHISHING	**H** Social engineering to steal logins. (H)

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: Automated testing of leaked credentials across multiple websites. (8 letters):

4 Across: Adaptive memory-hard hashing function for securing user passwords. (6 letters):

8 Across: Unauthorized database exposure revealing sensitive user records. (6 letters):

DOWN CLUES

2 Down: Adding random data to password inputs before computing hashes. (7 letters):

3 Down: Tool used to generate and securely store unique credentials. (7 letters):

5 Down: Adding an additional verification factor to password logins. (3 letters):

6 Down: Precomputed table of password hashes used for cracking. (7 letters):

7 Down: Social engineering emails designed to harvest credentials. (8 letters):

Checkpoint 6: Hidden Word Search

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

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

VOCABULARY WORD LIST

STUFFING	BCRYPT	BREACH	SALTING
MANAGER	MFA	RAINBOW	PHISHING

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. STUFFING
B. BCRYPT
C. BREACH
D. SALTING
E. MANAGER
F. MFA
G. RAINBOW
H. PHISHING

DEFINITIONS & MATCH FIELDS

1. Testing leaked credentials.
2. Slow password hashing algorithm.
3. Unauthorized database exposure.
4. Adding random salt to password hash.
5. Credential storage tool.
6. Multi-factor login check.
7. Precomputed table of password hashes.
8. Social engineering to steal logins.

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. G N I F F U T S

2. T P Y R C B

3. H C A E R B

4. G N I T L A S

5. R E G A N A M

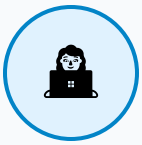
6. F M A

7. W O B N I A R

8. G N I H S I H P

Checkpoint 8: Cybersecurity Case Studies

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



CASE STUDY 1: ENTERPRISE CREDENTIAL LEAK REMEDIATION

Scenario: A dark web monitoring service alerts an organization that a database dump containing corporate system administrator passwords has been published online.

Discussion Question: Analyze the credentials leak risks, and propose an administrative reset strategy.

CASE STUDY 2: IMPLEMENTING PASSWORD HASHING STANDARDS

Scenario: An enterprise database currently stores user passwords using outdated MD5 hashes without cryptographic salt, making them vulnerable to rapid extraction.

Discussion Question: Design a migration strategy to upgrade the database hashing algorithm.

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

___ ___ ___ ___ ___ ___   ___ ___ ___ ___ ___ ___
19 5 3 21 18 5   12 5 1 11 5 4

___ ___ ___ ___ ___ ___ ___ ___ ___   ___ ___ ___ ___   ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___
16 1 19 19 23 15 18 4 19   23 9 20 8   13 21 12 20 9 6 1 3 20 15 18

___ ___ ___ ___ ___   ___ ___ ___ ___ ___ ___ ___ ___
12 15 7 9 14   3 15 14 20 18 15 12 19

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 a password leak?

A password leak occurs when user login credentials are exposed through data breaches or server misconfigurations.

Q2: How do hackers find leaked passwords?

Hackers scan dark web forums, public database dumps, and paste sites where breach data is published.

Q3: Is password reuse dangerous?

Yes, because if one site is compromised, hackers can test the same credentials across thousands of other platforms.

Q4: What is a cryptographic salt?

A salt is random data added to a password before hashing, making precomputed dictionary attacks ineffective.

Q5: Why is MD5 obsolete?

MD5 is fast to compute and suffers from collisions, allowing hackers to crack passwords in seconds using modern GPUs.

Checkpoint 10: Basic Cybersecurity FAQs (Part B)

Review common questions and answers regarding online threat mitigation.

Q6: How does a password manager protect users?

It auto-generates complex, unique credentials for every site, reducing human memory errors and reuse.

Q7: What is a brute force attack?

An attack that systematically tests every possible character combination until the correct password is found.

Q8: How does account lockout help?

It temporarily blocks a user account after a set number of failed login attempts, preventing automated brute-forcing.

Q9: Are master passwords secure?

They are secure if they are high-entropy passphrases that are never reused on other web systems.

Q10: Should passwords be changed regularly?

Modern standards advise changing them only upon suspected compromise, prioritizing password complexity and MFA instead.

Checkpoint 11: Advanced Security FAQs (Part A)

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

Q1: How does Argon2 compare to bcrypt?

Argon2 is the modern standard, offering configurable memory-hard options that protect against hardware-accelerated ASIC cracking.

Q2: What is key stretching?

A technique that loops a hashing algorithm thousands of times to slow down the password verification process, making cracking expensive.

Q3: How do rainbow tables work?

They are precomputed lookup databases of plaintext passwords and their corresponding hashes used to speed up decryption.

Q4: What is credential recycling?

The process of packaging old breach databases into new collections to sell to secondary attackers.

Q5: Can password managers be hacked?

Yes, but they use zero-knowledge local encryption, meaning even if their servers are breached, the master key remains safe on the client device.

Checkpoint 11: Advanced Security FAQs (Part B)

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

Q6: What is a dictionary attack?

A brute-force variant that tests common words, phrases, and historical leaked passwords rather than random letters.

Q7: Why are passphrases preferred?

Passphrases use multiple random words, creating high entropy that is easy for humans to remember but computationally expensive to crack.

Q8: How does single sign-on (SSO) affect password leaks?

SSO reduces the number of credentials employees manage, allowing teams to harden and audit a single secure entry point.

Q9: What is session hijacking?

An attacker stealing active authentication session tokens from browser memory, bypassing password logins entirely.

Q10: How do you detect password spraying?

By auditing login logs for single password attempts tested across thousands of different corporate usernames simultaneously.

Part 11: 10 Real-World Cybersecurity Facts & Insights

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

1. SECURITY INSIGHT

Over 80% of enterprise data breaches are caused by weak, compromised, or reused employee password credentials.

2. SECURITY INSIGHT

The 'Collection #1' breach database compiled over 773 million unique email and password combinations in a single dump.

3. SECURITY INSIGHT

A standard 8-character password using only lowercase letters can be cracked instantly by a consumer-grade desktop GPU.

4. SECURITY INSIGHT

ASIC hardware can calculate billions of SHA-256 hashes per second, making raw SHA hashing unsafe for user passwords.

5. SECURITY INSIGHT

Cryptographic salting ensures that two users with the exact same password will have completely different database hashes.

6. SECURITY INSIGHT

Enterprise password managers utilize AES-256 encryption keys derived from the user's master passphrase locally.

7. SECURITY INSIGHT

Credential stuffing bots account for over 40% of all login attempts on major global e-commerce and banking portals.

8. SECURITY INSIGHT

NIST Guidelines now discourage arbitrary periodic password resets, as they often lead users to create weaker patterns.

9. SECURITY INSIGHT

Adding a single uppercase letter and symbol to a short password does not stop modern automated GPU dictionary attacks.

10. SECURITY INSIGHT

Multi-factor authentication prevents up to 99.9% of automated credential stuffing attacks even if passwords are leaked.

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 Brokerage Function

BROKERAGE

Correct Answer: A

TEACHING NOTE

Domain brokers act as confidential negotiators representing buyers and sellers to reach fair market transactions.

Citation: ICANN Transfer Policy [Ref 1].

2 Stealth Strategy

STEALTH

Correct Answer: A

TEACHING NOTE

Stealth acquisition conceals corporate buyer identity to prevent sellers from inflating asking prices.

Citation: Escrow.com Protocol [Ref 7].

3 Escrow Protection

ESCROW

Correct Answer: A

TEACHING NOTE

Licensed third-party escrow holds funds safely until ownership transfer verification is complete.

Citation: Escrow.com Protocol [Ref 7].

4 Domain Appraisal

VALUATION

Correct Answer: A

TEACHING NOTE

Short 2-letter and 1-word .com domains carry extreme global brand scarcity and liquidity.

Citation: WIPO UDRP Guide [Ref 3].

5 Dispute Resolution

UDRP POLICY

Correct Answer: A

TEACHING NOTE

ICANN's Uniform Domain-Name Dispute-Resolution Policy (UDRP) governs administrative trademark disputes.

Citation: WIPO Dispute Rules [Ref 2].

Answer Key: Checkpoint 2 - True or False

6 Confidential NDAs NDAS — Correct Answer: True

TEACHING NOTE

Professional domain brokers operate under non-disclosure agreements to protect buyer corporate strategy.

Citation: CIS Controls [Ref 8].

7 Escrow Delivery ESCROW — Correct Answer: False

TEACHING NOTE

Escrow holding accounts disburse funds only after full domain ownership transfer is verified by the buyer.

Citation: Escrow.com Protocol [Ref 7].

8 Digital Real Estate ASSETS — Correct Answer: False

TEACHING NOTE

Short 2-letter and 3-letter .com domains function as high-value, liquid digital property assets.

Citation: NIST Guidelines [Ref 9].

9 Stealth Negotiation STRATEGY — Correct Answer: True

TEACHING NOTE

Direct corporate buyer outreach often causes sellers to inflate asking prices significantly.

Citation: WIPO UDRP Guide [Ref 3].

10 EPP Authorization EPP CODE — Correct Answer: True

TEACHING NOTE

EPP codes are unique security passcodes generated by registrars to authorize domain transfers.

Citation: IETF RFC 5730 [Ref 4].

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 STUFFING	B BCRYPT	C BREACH	D SALTING
E MANAGER	F MFA	G RAINBOW	H PHISHING

CHECKPOINT 3: KEY TERM KEY

1 STUFFING	2 BCRYPT	3 BREACH
4 SALTING	5 MANAGER	6 MFA

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).

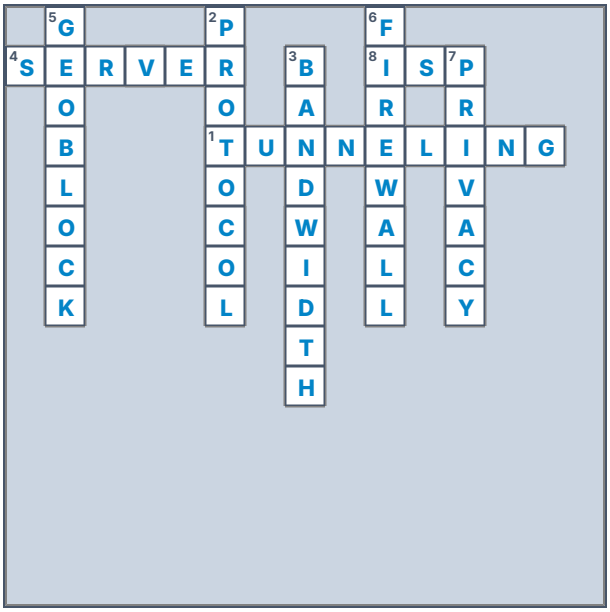
Regulatory Compliance:
Highlight user consent, data minimization, encryption at-rest and in-transit, and global frameworks like GDPR/CCPA.

Puzzles Keys & Instructor Notes

WORD SEARCH SOLUTION

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

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. G N I F F U T S
   STUFFING

2. T P Y R C B
   BCRYPT

3. H C A E R B
   BREACH

4. G N I T L A S
   SALTING

5. R E G A N A M
   MANAGER

6. F M A
   MFA

7. W O B N I A R
   RAINBOW

8. G N I H S I H P
   PHISHING

SECRET CIPHER CHALLENGE KEY

"SECURE LEAKED PASSWORDS WITH MULTIFACTOR LOGIN CONTROLS"

Domain Brokerage Case Studies Solution Key

A Case Study 1: Enterprise Credential Leak Remediation

Instructor Solution

GRADING GUIDELINE

Student answers should cover the following points:

- **Scenario Analysis:** A dark web monitoring service alerts an organization that a database dump containing corporate system administrator passwords has been published online.
- **Recommended Strategy & Solution:** Revoke all active administrator sessions immediately. Initiate a mandatory password reset using a high-entropy generator, and enforce hardware key MFA for all administrative portals.

B Case Study 2: Implementing Password Hashing Standards

Instructor Solution

GRADING GUIDELINE

Student answers should cover the following points:

- **Scenario Analysis:** An enterprise database currently stores user passwords using outdated MD5 hashes without cryptographic salt, making them vulnerable to rapid extraction.
- **Recommended Strategy & Solution:** Implement bcrypt password hashing. Generate a unique random cryptographic salt for each user. Update database records dynamically when users log in by capturing and rehashing their plaintext passwords.