Nama: _____ Tanggal: _____ Nilai: _____

Kebocoran Kata Sandi & Keamanan Kredensial

Credential stuffing, kebocoran data, algoritme hash, autentikasi multifaktor, dan keamanan kata sandi.

GAMBARAN PEMBELAJARAN KEBOCORAN KATA SANDI

TERAMANKAN
ENKRIPSI DATA
Standar AES 256-bit

PATUH
STANDAR GLOBAL
Kerangka GDPR & CCPA

ZERO TRUST
KEBIJAKAN AKSES
Autentikasi Multifaktor

Selamat datang! Paket aktivitas ini memandu Anda mempelajari kebocoran kata sandi dan keamanan kredensial. Anda akan mempelajari credential stuffing, pembobolan data, algoritme hash, autentikasi multifaktor, dan pengelola kata sandi.

POS-POS LEMBAR KERJA

- [ ] **Bagian 1-4: Kuasai keamanan siber dan pencegahan ancaman.**
- [ ] **Bagian 5-7: Selesaikan teka-teki silang & pencarian kata.**
- [ ] **Bagian 8-9: Selesaikan studi kasus & tantangan sandi.**
- [ ] **Bagian 10: Pelajari halaman FAQ dasar & lanjutan.**
- [ ] **Bagian 11: Jelajahi 10 fakta menarik dari dunia nyata.**
- [ ] **Bonus: Tantangan Berpikir Cepat.**

Buka Panduan Keamanan Siber VPN.com

URL: https://www.vpn.com/cybersecurity/passwords-leak/

Peta Belajar Keamanan Kata Sandi Anda

- Pahami risiko terbukanya kredensial di forum dark web.
- Terapkan autentikasi multifaktor (MFA) dan pemantauan kredensial yang telah dibobol.
- Rancang pertahanan keamanan perusahaan terhadap penipuan rekayasa sosial yang terarah.

PETUNJUK PANDUAN KEBOCORAN KATA SANDI

Jawab soal pilihan ganda dan benar/salah, lengkapi kalimat rumpang dengan bank kata, cocokkan definisi, serta selesaikan teka-teki silang dan pencarian kata. Terapkan pengetahuan Anda tentang perlindungan kredensial. Akhiri dengan aktivitas bonus Berpikir Cepat.

KEBOCORAN KATA SANDI & KEAMANAN KREDENSIAL (PENGANTAR)

Kebocoran kata sandi mengekspos kredensial pengguna di situs publik dan dark web. Kata sandi unik dari pengelola kata sandi, penyaringan kata sandi yang bocor, dan autentikasi multifaktor (MFA) mengurangi risiko credential stuffing, sementara hashing kata sandi yang lambat dan diberi salt membatasi kerusakan jika basis data kata sandi dicuri.

BACA SETIAP POS DENGAN SAKSAMA DAN PILIH ATAU TULIS JAWABAN YANG BENAR.

Pos 1: Tantangan Pilihan Ganda

1. **1. Apa itu credential stuffing?**
   - A. Mencoba kombinasi nama pengguna/kata sandi yang bocor di banyak situs secara otomatis
   - B. Mengenkripsi berkas basis data lokal
   - C. Membanjiri server web dengan lalu lintas
   - D. Memantau ketikan keyboard diam-diam

2. **2. Algoritma mana yang saat ini dicantumkan OWASP sebagai pilihan pertama untuk menyimpan kata sandi?**
   - A. Argon2id
   - B. MD5
   - C. SHA-1
   - D. ROT13

3. **3. Bagaimana autentikasi multifaktor (MFA) mengurangi risiko kebocoran kata sandi?**
   - A. MFA mewajibkan faktor verifikasi tambahan, sehingga kata sandi curian saja tidak cukup
   - B. MFA otomatis mengganti kata sandi setiap jam
   - C. MFA mengenkripsi nama pengguna selama transmisi
   - D. MFA memberi tahu biro kredit tentang permintaan yang curang

4. **4. Apa itu bocoran data hasil pembobolan?**
   - A. Kumpulan kredensial bocor yang dipublikasikan atau dijual di forum peretas
   - B. Salinan cadangan basis data di lokasi lain
   - C. Cache sementara log server web
   - D. Alat admin untuk mengatur ulang kata sandi

5. **5. Apa peran pengelola kata sandi?**
   - A. Membuat dan menyimpan kata sandi unik yang kuat untuk tiap akun
   - B. Memantau lalu lintas jaringan untuk kebocoran kata sandi
   - C. Memblokir serangan brute-force otomatis di gerbang
   - D. Memindai basis data untuk kata sandi tanpa enkripsi

Pos 2: Tantangan Benar atau Salah

6 Pertanyaan 6

6. Memakai ulang kata sandi di banyak akun meningkatkan risiko credential stuffing.

Benar Salah

7 Pertanyaan 7

7. SHA-1 adalah fungsi hash yang disarankan untuk penyimpanan kata sandi modern.

Benar Salah

8 Pertanyaan 8

8. Mewajibkan kata sandi rumit saja (tanpa MFA) sepenuhnya menghentikan credential stuffing.

Benar Salah

9 Pertanyaan 9

9. Alat pemantau dark web memindai internet untuk kredensial perusahaan yang bocor.

Benar Salah

10 Pertanyaan 10

10. Hash dengan salt menambahkan data acak unik sebelum hashing untuk mengalahkan serangan rainbow table.

Benar Salah

Pos 3: Mengisi Istilah Kunci

Baca setiap kalimat di bawah ini dan isi bagian yang kosong dengan istilah yang tepat dari Bank Kata.

1. Menguji kredensial yang bocor di banyak aplikasi web disebut credential _____ .
2. Algoritma hashing kata sandi yang lambat dan adaptif serta masih diterima OWASP adalah _____ .
3. Terungkapnya file basis data rahasia di internet merupakan _____ data.
4. Menambahkan nilai acak pada kata sandi sebelum di-hash disebut _____ .
5. Basis data lokal yang aman untuk kredensial pengguna adalah _____ kata sandi.
6. Menambahkan langkah verifikasi login kedua memakai _____ .

BANK KATA KOSAKATA

BCRYPT KEBOCORAN MFA PENGELOLA PHISHING RAINBOW SALTING STUFFING

Tulis jawaban Anda di sini:

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

Pos 4: Pencocokan Konsep Keamanan

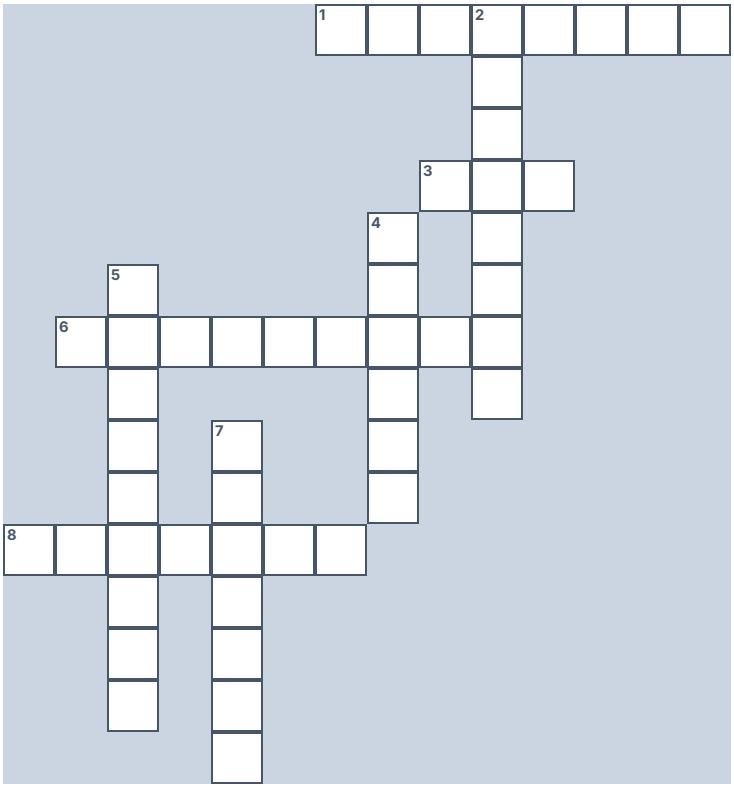
MENCOCOKKAN DEFINISI

Cocokkan setiap istilah di sebelah kiri dengan definisi yang benar di sebelah kanan dengan menulis huruf yang sesuai (A-H) di kotak isian.

☐	1. STUFFING	A	Tabel hash kata sandi yang dihitung sebelumnya.
☐	2. BCRYPT	B	Pemeriksaan login multifaktor.
☐	3. KEBOCORAN	C	Alat penyimpan kredensial.
☐	4. SALTING	D	Terbukanya basis data tanpa izin.
☐	5. PENGELOLA	E	Rekayasa sosial untuk mencuri login.
☐	6. MFA	F	Mencoba kredensial bocor.
☐	7. RAINBOW	G	Menambahkan salt acak ke hash kata sandi.
☐	8. PHISHING	H	Algoritme hash kata sandi yang lambat.

Pos 5: Teka-Teki Silang

Selesaikan teka-teki silang dengan mengetik huruf di kotak putih yang aktif. Nomor-nomornya sesuai dengan petunjuk di bawah.



PETUNJUK MENDATAR

1. Rekayasa sosial untuk mencuri data login. (8)

3. Pemeriksaan login multifaktor. (3)

6. Paparan basis data tanpa izin. (9)

8. Menambahkan salt acak pada hash kata sandi. (7)

PETUNJUK MENURUN

2. Pengujian kredensial yang bocor. (8)

4. Algoritma hashing kata sandi yang lambat. (6)

5. Alat penyimpan kredensial. (9)

7. Tabel hash kata sandi yang dihitung sebelumnya. (7)

Alternatif Pos 5: Petunjuk Teka-Teki Silang yang Aksesibel

Pengguna pembaca layar dan keyboard dapat mengetik jawaban teka-teki silang langsung di kolom teks di bawah ini.

PETUNJUK MENDATAR

1 mendatar: Rekayasa sosial untuk mencuri data login. (8 huruf):

3 mendatar: Pemeriksaan login multifaktor. (3 huruf):

6 mendatar: Paparan basis data tanpa izin. (9 huruf):

8 mendatar: Menambahkan salt acak pada hash kata sandi. (7 huruf):

PETUNJUK MENURUN

2 menurun: Pengujian kredensial yang bocor. (8 huruf):

4 menurun: Algoritma hashing kata sandi yang lambat. (6 huruf):

5 menurun: Alat penyimpan kredensial. (9 huruf):

7 menurun: Tabel hash kata sandi yang dihitung sebelumnya. (7 huruf):

Pos 6: Mencari Kata Tersembunyi

Temukan 8 istilah kunci yang tersembunyi dalam kisi di bawah ini. Kata dapat tersusun mendatar, menurun, atau diagonal.

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

DAFTAR KOSAKATA

STUFFING BCRYPT KEBOCORAN SALTING PENGELOLA MFA RAINBOW PHISHING

Alternatif Pos 6: Pencocokan Kosakata yang Aksesibel

Cocokkan kedelapan istilah dari Pencarian Kata dengan definisi yang benar dengan menulis hurufnya (A-H) di tempat kosong.

ISTILAH KOSAKATA
A. STUFFING
B. BCRYPT
C. KEBOCORAN
D. SALTING
E. PENGELOLA
F. MFA
G. RAINBOW
H. PHISHING

DEFINISI & KOLOM PENCOCOKAN

1. Rekayasa sosial untuk mencuri data login.
2. Paparan basis data tanpa izin.
3. Algoritma hashing kata sandi yang lambat.
4. Tabel hash kata sandi yang dihitung sebelumnya.
5. Pengujian kredensial yang bocor.
6. Menambahkan salt acak pada hash kata sandi.
7. Alat penyimpan kredensial.
8. Pemeriksaan login multifaktor.

Pos 7: Tantangan Kata Acak

Susun ulang huruf di bawah ini untuk menemukan konsep dan istilah kunci keamanan siber. Tulis jawaban Anda di kotak isian yang tersedia.

1. **NFFSITGU** _____
2. **NKAOEORCB** _____
3. **PLEEOAGLN** _____
4. **WABNORI** _____
5. **YRTBPC** _____
6. **NLISTGA** _____
7. **AFM** _____
8. **SHHGPNII** _____

Aktivitas Bonus: Berpikir Cepat

3 JAWABAN UNTUK SETIAP KATEGORI. ORANG PERTAMA YANG MELENGKAPI DAFTAR MENANG.

1	Kebiasaan aman yang bisa dimulai hari ini			
2	Aturan kata sandi yang kuat			
3	Pengelola kata sandi yang Anda ketahui			
4	Alat keamanan yang Anda ketahui			
5	Tanda bahaya dalam email			
6	Kata lucu untuk frasa sandi panjang			
7	Cara masuk tanpa kata sandi			
8	Informasi yang tidak boleh dibagikan			
9	Alasan memperbarui perangkat lunak			
10	Hal yang dilakukan saat kata sandi bocor			
11	Akun yang butuh MFA			
12	Tempat kata sandi tidak boleh disimpan			
13	Tanda komputer terinfeksi			
14	Kata sandi buruk yang sering dipakai			
15	Hal yang Anda cadangkan			

Pos 8: Studi Kasus Keamanan Siber

Terapkan konsep yang telah Anda pelajari untuk menyelesaikan skenario nyata di bawah ini.

STUDI KASUS 1: MENANGANI KEBOCORAN KREDENSIAL PERUSAHAAN

👷

Skenario: Layanan pemantau dark web memberi tahu sebuah organisasi bahwa bocoran basis data berisi kata sandi administrator sistem perusahaan telah dipublikasikan online.

Pertanyaan Diskusi: Analisis risiko kebocoran kredensial, dan usulkan strategi pengaturan ulang akun admin.

STUDI KASUS 2: MENERAPKAN STANDAR HASH KATA SANDI

👷

Skenario: Basis data sebuah perusahaan menyimpan kata sandi pengguna dengan hash MD5 usang tanpa salt kriptografis, sehingga mudah dibongkar dengan cepat.

Pertanyaan Diskusi: Rancang strategi migrasi untuk meningkatkan algoritme hash basis data.

Pos 9: Memecahkan Sandi

Seorang profesional keamanan siber melindungi aset jaringan dari pelaku ancaman online. Gunakan kunci Huruf-ke-Angka di bawah untuk memecahkan pesan dengan menulis huruf yang sesuai di tempat kosong.

KUNCI ENKRIPSI HURUF-KE-ANGKA

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

16	1	11	1	9		11	1	20	1		19	1	14	4	9		21	14	9	11
							4	1	14		13	6	1							

Pesan yang dipecahkan:

TIPS: SETIAP ANGKA MEWAKILI POSISI HURUF TERSEBUT DALAM ALFABET (MISALNYA 1 = A, 2 = B, 26 = Z).

Pos 10: FAQ Dasar Keamanan Siber (Bagian A)

Pelajari pertanyaan dan jawaban umum tentang cara mengurangi ancaman online.

Q1: Apa itu kebocoran kata sandi?

Kebocoran kata sandi terjadi saat kredensial login pengguna terbuka akibat pembobolan data atau salah konfigurasi server.

Q2: Bagaimana peretas menemukan kata sandi yang bocor?

Peretas memindai forum dark web, dump basis data publik, dan situs paste tempat data pembobolan dipublikasikan [8].

Q3: Apakah memakai ulang kata sandi berbahaya?

Ya, karena jika satu situs dibobol, peretas dapat menguji kredensial yang sama di ribuan platform lain [3].

Q4: Apa itu salt kriptografis?

Salt adalah data acak yang ditambahkan ke kata sandi sebelum hashing, sehingga serangan tabel pencarian prakomputasi menjadi tidak efektif [2].

Q5: Mengapa MD5 sudah usang?

MD5 adalah hash serbaguna yang cepat dan usang, sehingga penyerang dapat menguji tebakan kata sandi dengan sangat cepat, terutama jika hash tidak diberi salt [2].

Pos 10: FAQ Dasar Keamanan Siber (Bagian B)

Pelajari pertanyaan dan jawaban umum tentang cara mengurangi ancaman online.

Q6: Bagaimana pengelola kata sandi melindungi pengguna?

Pengelola kata sandi otomatis membuat kredensial rumit dan unik untuk tiap situs, mengurangi lupa dan pemakaian ulang.

Q7: Apa itu serangan brute force?

Serangan yang secara sistematis menguji setiap kemungkinan kombinasi karakter hingga kata sandi yang benar ditemukan [4].

Q8: Apa manfaat penguncian akun?

Penguncian akun atau pembatasan laju memperlambat tebakan online berulang dan, bersama pemantauan dan MFA, mengurangi risiko brute force [4].

Q9: Apakah kata sandi utama aman?

Aman jika berupa frasa sandi berentropi tinggi yang tidak pernah dipakai di sistem lain.

Q10: Perlukah kata sandi diganti rutin?

NIST menyatakan agar tidak memaksa penggantian berkala; ganti kata sandi bila ada bukti pembobolan dan prioritaskan panjang, daftar blokir, dan MFA [1].

Pos 10: FAQ Lanjutan Keamanan (Bagian C)

Jelajahi aspek teknis lanjutan dari kerangka keamanan, analisis malware, dan kepatuhan data.

Q1: Bagaimana Argon2 dibanding bcrypt?

OWASP mencantumkan Argon2id sebagai pilihan pertama; pengaturan memory-hard-nya lebih tahan terhadap pembobolan GPU dan ASIC daripada bcrypt [2].

Q2: Apa itu key stretching?

Teknik yang mengulang algoritma hashing ribuan kali untuk memperlambat proses verifikasi kata sandi, sehingga pembobolan menjadi mahal [2].

Q3: Bagaimana rainbow table bekerja?

Tabel pencarian prakomputasi yang menghubungkan kata sandi teks biasa dengan hash-nya, digunakan untuk membalikkan hash tanpa salt dengan cepat [2].

Q4: Apa itu daur ulang kredensial?

Menggunakan kembali pasangan nama pengguna/kata sandi curian dari satu pembobolan untuk mencoba mengakses layanan lain, terutama jika orang memakai ulang kata sandi [3].

Q5: Bisakah pengelola kata sandi diretas?

Ya. Banyak yang menggunakan enkripsi zero-knowledge, sehingga kebocoran server hanya membuka brankas yang terenkripsi, tetapi kata sandi utama yang lemah tetap dapat dibobol secara offline.

Pos 10: FAQ Lanjutan Keamanan (Bagian D)

Jelajahi aspek teknis lanjutan dari kerangka keamanan, analisis malware, dan kepatuhan data.

Q6: Apa itu serangan kamus?

Varian brute force yang mencoba kata umum, frasa, dan kata sandi bocor, bukan huruf acak.

Q7: Mengapa frasa sandi lebih disukai?

Frasa sandi menggunakan beberapa kata acak, menghasilkan entropi tinggi yang mudah diingat manusia tetapi mahal secara komputasi untuk dibobol [1].

Q8: Bagaimana single sign-on (SSO) memengaruhi kebocoran kata sandi?

SSO mengurangi penyebaran kata sandi, tetapi penyedia identitas menjadi target bernilai tinggi yang memerlukan MFA kuat, sebaiknya yang tahan phishing [6].

Q9: Apa itu pembajakan sesi?

Penyerang memperoleh atau menyalahgunakan token sesi yang valid untuk menyamar sebagai pengguna yang sedang masuk tanpa perlu kata sandi lagi [5].

Q10: Bagaimana mendeteksi password spraying?

Dengan mencari beberapa kata sandi yang sama yang dicoba di banyak akun, sering kali secara perlahan agar tetap di bawah ambang penguncian [7].

Bagian 11: 10 Fakta & Wawasan Keamanan Siber di Dunia Nyata

Pelajari fakta nyata tentang pelanggaran keamanan, mekanisme pertahanan, dan standar kepatuhan.

1. WAWASAN KEAMANAN

NIST SP 800-63B mewajibkan kata sandi baru diperiksa terhadap daftar blokir kata sandi umum dan kata sandi yang telah dibobol [1].

2. WAWASAN KEAMANAN

Dump 'Collection #1' tahun 2019 menggabungkan data dari banyak pembobolan sebelumnya ke dalam satu file besar berisi pasangan email dan kata sandi [8].

3. WAWASAN KEAMANAN

NIST kini mewajibkan kata sandi yang digunakan sebagai satu-satunya faktor autentikasi memiliki panjang minimal 15 karakter [1].

4. WAWASAN KEAMANAN

Perangkat keras ASIC dapat menghitung miliaran hash SHA-256 per detik, sehingga hashing SHA mentah tidak aman untuk kata sandi pengguna [2].

5. WAWASAN KEAMANAN

Salt unik berarti dua pengguna dengan kata sandi yang persis sama mendapatkan hash yang berbeda di basis data [2].

6. WAWASAN KEAMANAN

Banyak pengelola kata sandi mengenkripsi data brankas secara lokal dengan kriptografi kuat yang diturunkan dari kata sandi utama pengguna.

7. WAWASAN KEAMANAN

Credential stuffing berhasil karena banyak orang memakai ulang kata sandi yang sama untuk akun e-commerce, perbankan, dan email [3].

8. WAWASAN KEAMANAN

NIST SP 800-63B menyatakan bahwa verifikator tidak boleh mewajibkan penggantian kata sandi berkala, hanya penggantian setelah ada bukti pembobolan [1].

9. WAWASAN KEAMANAN

Menambahkan satu huruf besar dan simbol ke kata sandi pendek tidak menghentikan serangan kamus GPU otomatis modern [1].

10. WAWASAN KEAMANAN

MFA dapat memblokir banyak upaya credential stuffing bahkan setelah kata sandi bocor; MFA tahan phishing lebih kuat daripada kode SMS [3].

Referensi & Sumber Teknis

Panduan belajar dan teka-teki interaktif ini disusun berdasarkan standar global NIST, OWASP, dan kepatuhan privasi data.

REFERENSI AKADEMIK & INDUSTRI

[1] NIST. (2025). SP 800-63B-4: Digital Identity Guidelines: Authentication and Authenticator Management.

https://pages.nist.gov/800-63-4/sp800-63b.html

[2] OWASP. (n.d.). Password Storage Cheat Sheet.

https://cheatsheetseries.owasp.org/cheatsheets/Password_Storage_Cheat_Sheet.html

[3] OWASP. (n.d.). Credential Stuffing Prevention Cheat Sheet.

https://cheatsheetseries.owasp.org/cheatsheets/Credential_Stuffing_Prevention_Cheat_Sheet.html

[4] OWASP. (n.d.). Authentication Cheat Sheet.

https://cheatsheetseries.owasp.org/cheatsheets/Authentication_Cheat_Sheet.html

[5] OWASP. (n.d.). Session Management Cheat Sheet.

https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html

[6] CISA. (2022). Implementing Phishing-Resistant MFA (fact sheet).

https://www.cisa.gov/sites/default/files/publications/fact-sheet-implementing-phishing-resistant-mfa-508c.pdf

[7] CISA. (2018). Brute Force Attacks Conducted by Cyber Actors (Alert TA18-086A).

https://www.cisa.gov/news-events/alerts/2018/03/27/brute-force-attacks-conducted-cyber-actors

[8] Hunt, T. (2019). The 773 Million Record "Collection #1" Data Breach. Troy Hunt.

https://www.troyhunt.com/the-773-million-record-collection-1-data-reach/

Kunci Jawaban: Pos 1 - Pilihan Ganda

1 Soal 1

Jawaban Benar: A

CATATAN PENGAJAR

Credential stuffing menggunakan otomatisasi untuk mencoba pasangan nama pengguna/kata sandi yang bocor di situs lain [3].

2 Soal 2

Jawaban Benar: A

CATATAN PENGAJAR

OWASP merekomendasikan Argon2id terlebih dahulu; bcrypt terutama untuk sistem lama yang tidak memiliki Argon2id atau scrypt [2].

3 Soal 3

Jawaban Benar: A

CATATAN PENGAJAR

MFA mewajibkan faktor tambahan, sehingga kata sandi curian saja tidak dapat membuka akun.

4 Soal 4

Jawaban Benar: A

CATATAN PENGAJAR

Dump pembobolan adalah kumpulan kredensial yang bocor, seperti kompilasi Collection #1 tahun 2019 [8].

5 Soal 5

Jawaban Benar: A

CATATAN PENGAJAR

Pengelola kata sandi membuat dan menyimpan kata sandi yang unik dan kuat untuk setiap akun, sehingga mencegah pemakaian ulang [3].

Kunci Jawaban: Pos 2 - Benar atau Salah

6 Soal 6

Jawaban Benar: Benar

CATATAN PENGAJAR

Benar: kata sandi yang dipakai ulang memungkinkan penyerang memutar ulang kredensial bocor dari satu situs di situs lain [3].

7 Soal 7

Jawaban Benar: Salah

CATATAN PENGAJAR

Salah: SHA-1 adalah hash cepat; OWASP merekomendasikan Argon2id, scrypt, bcrypt, atau PBKDF2 sebagai gantinya.

8 Soal 8

Jawaban Benar: Salah

CATATAN PENGAJAR

Salah: aturan kerumitan saja tidak dapat menghentikan stuffing dengan kata sandi bocor yang dipakai ulang; MFA tetap diperlukan.

9 Soal 9

Jawaban Benar: Benar

CATATAN PENGAJAR

Benar: layanan pemantauan menelusuri dump pembobolan dan sumber dark web untuk mencari kredensial yang terekspos [8].

10 Soal 10

Jawaban Benar: Benar

CATATAN PENGAJAR

Benar: salt unik per kata sandi membuat rainbow table prakomputasi tidak efektif [2].

Kunci Kosakata & Rubrik Penilaian

Rubrik Penilaian Pengajar: Berikan 1 poin untuk setiap pencocokan yang benar (total 8 poin) dan setiap istilah konteks yang benar (total 6 poin).

POS 4: KUNCI PENCOCOKAN KONSEP

F 1. STUFFING	H 2. BCRYPT	D 3. KEBOCORAN	G 4. SALTING
C 5. PENGELOLA	B 6. MFA	A 7. RAINBOW	E 8. PHISHING

POS 3: KUNCI ISTILAH KUNCI

1 STUFFING	2 BCRYPT	3 KEBOCORAN	4 SALTING
5 PENGELOLA	6 MFA		

ALTERNATIF POS 6: KUNCI PENCOCOKAN KOSAKATA

1 H – PHISHING	2 C – KEBOCORAN	3 B – BCRYPT	4 G – RAINBOW
5 A – STUFFING	6 D – SALTING	7 E – PENGELOLA	8 F – MFA

CATATAN DISKUSI UNTUK PENGAJAR

Istilah Kunci:
Pastikan siswa dapat menjelaskan STUFFING, BCRYPT, dan KEBOCORAN dengan kata-kata sendiri serta memberi contoh untuk setiap istilah.

Studi Kasus:
Minta siswa mendukung rekomendasi mereka dengan fakta dari lembar kerja, bukan asumsi.

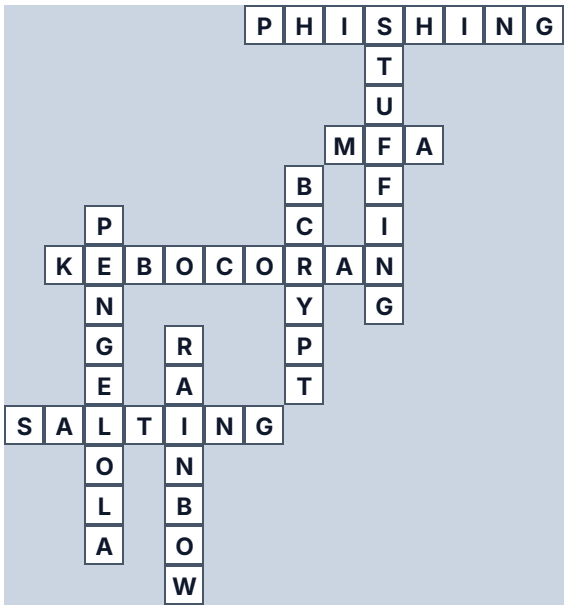
Evaluasi Sumber:
Minta siswa memeriksa setidaknya satu klaim terhadap referensi di lembar kerja, lalu diskusikan mengapa angka, harga, dan aturan dapat berubah seiring waktu.

Kunci Teka-Teki & Catatan Pengajar

JAWABAN PENCARIAN KATA

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

JAWABAN TEKA-TEKI SILANG



PANDUAN PENGAJAR UNTUK JAWABAN TEKA-TEKI SILANG

PETUNJUK MENDATAR

1 mendatar: PHISHING Rekayasa sosial untuk mencuri data login. (8 huruf)

3 mendatar: MFA Pemeriksaan login multifaktor. (3 huruf)

6 mendatar: KEBOCORAN Paparan basis data tanpa izin. (9 huruf)

8 mendatar: SALTING Menambahkan salt acak pada hash kata sandi. (7 huruf)

PETUNJUK MENURUN

2 menurun: STUFFING Pengujian kredensial yang bocor. (8 huruf)

4 menurun: BCRYPT Algoritma hashing kata sandi yang lambat. (6 huruf)

5 menurun: PENGELOLA Alat penyimpan kredensial. (9 huruf)

7 menurun: RAINBOW Tabel hash kata sandi yang dihitung sebelumnya. (7 huruf)

Kunci Jawaban Kata Acak & Sandi

Kunci penilaian untuk aktivitas menyusun kata acak dan Tantangan Sandi Rahasia.

KUNCI KATA ACAK

1.	NFFSITGU	STUFFING	5.	YRTBPC	BCRYPT
2.	NKAOEORCB	KEBOCORAN	6.	NLISTGA	SALTING
3.	PLEEOAGLN	PENGELOLA	7.	AFM	MFA
4.	WABNORI	RAINBOW	8.	SHHGPNII	PHISHING

KUNCI TANTANGAN SANDI RAHASIA

"PAKAI KATA SANDI UNIK DAN MFA"

Kunci Jawaban Studi Kasus

A Studi Kasus 1: Menangani Kebocoran Kredensial Perusahaan

Jawaban Pengajar

PEDOMAN PENILAIAN

Jawaban siswa harus mencakup poin-poin berikut:

- Analisis Skenario: Layanan pemantau dark web memberi tahu sebuah organisasi bahwa bocoran basis data berisi kata sandi administrator sistem perusahaan telah dipublikasikan online.
- Strategi & Solusi yang Direkomendasikan: Cabut semua sesi administrator yang aktif dan setel ulang kredensial dengan generator berentropi tinggi. Terapkan MFA tahan phishing di portal admin [6], rotasi kunci API yang terdampak, tinjau log login, temukan paparan awal, dan periksa akun istimewa lainnya.

B Studi Kasus 2: Menerapkan Standar Hash Kata Sandi

Jawaban Pengajar

PEDOMAN PENILAIAN

Jawaban siswa harus mencakup poin-poin berikut:

- Analisis Skenario: Basis data sebuah perusahaan menyimpan kata sandi pengguna dengan hash MD5 usang tanpa salt kriptografis, sehingga mudah dibongkar dengan cepat.
- Strategi & Solusi yang Direkomendasikan: Gunakan Argon2id (atau bcrypt pada sistem lama) dengan salt unik per pengguna [2]. Bungkus hash MD5 yang ada dengan algoritma baru sekarang, lakukan hash ulang langsung saat setiap pengguna login berikutnya, dan paksa reset untuk akun yang lama tidak aktif.