Nama: _____ Tanggal: _____ Nilai: _____

Dasar Keamanan Siber & Pencegahan Ancaman Online

Ancaman keamanan siber, firewall jaringan, autentikasi multifaktor, kerangka kerja keamanan

GAMBARAN PEMBELAJARAN DASAR KEAMANAN SIBER

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 prinsip dasar keamanan siber dan pencegahan ancaman online. Anda akan mempelajari ancaman malware, autentikasi multifaktor, firewall jaringan, dan kerangka tanggap insiden.

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/

Peta Belajar Dasar Keamanan Siber Anda

- Kenali jalur umum malware, phishing, dan penyusupan jaringan perusahaan.
- Terapkan kontrol keamanan siber standar seperti MFA, firewall, dan pertahanan endpoint.
- Nilai prosedur tanggap insiden untuk mengurangi dampak kebocoran data.
- Analisis faktor risiko organisasi dan keselarasan keamanan dengan pedoman NIST.
- Terapkan kebiasaan keamanan yang baik untuk menangkal credential stuffing otomatis.

PETUNJUK PANDUAN KEAMANAN SIBER

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 pencegahan ancaman. Akhiri dengan aktivitas bonus Berpikir Cepat.

DASAR KEAMANAN SIBER & PENCEGAHAN ANCAMAN (PENGANTAR)

Keamanan siber melindungi jaringan, sistem, dan data dari serangan digital tanpa izin. Kebiasaan keamanan yang kuat, pengaturan firewall, kewajiban autentikasi multifaktor, dan pelatihan staf mengenali ancaman adalah komponen penting pertahanan jaringan perusahaan.

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

Pos 1: Tantangan Pilihan Ganda

1. **1. Apa tujuan utama serangan phishing?**
   - A. Mencuri kredensial dan data sensitif pengguna
   - B. Meningkatkan visibilitas situs di mesin pencari
   - C. Menambah kapasitas bandwidth jaringan
   - D. Mengelola replikasi pusat data cadangan

2. **2. Mekanisme mana yang memberi perlindungan akun terkuat?**
   - A. Autentikasi multifaktor dengan kunci perangkat keras
   - B. Kata sandi rumit yang diganti setiap tiga puluh hari
   - C. Membatasi login akun pada jam kerja
   - D. Menyembunyikan nama pengguna dari direktori publik

3. **3. Apa ciri muatan infeksi ransomware?**
   - A. Mengenkripsi berkas sistem dan meminta tebusan
   - B. Diam-diam merekam ketikan ke server jarak jauh
   - C. Menyisipkan iklan tanpa izin ke browser
   - D. Memakai CPU lokal untuk menambang mata uang kripto

4. **4. Bagaimana exploit zero-day memengaruhi pertahanan keamanan?**
   - A. Menyasar celah yang belum diketahui dan belum ditambal
   - B. Otomatis mematikan firewall perusahaan
   - C. Memaksa sistem melakukan reboot paksa
   - D. Tidak memerlukan anggaran untuk diperbaiki

5. **5. Kerangka mana yang mengatur kontrol keamanan perusahaan?**
   - A. Pedoman NIST Cybersecurity Framework
   - B. Spesifikasi skema dokumen HTML5 W3C
   - C. Panduan pemasangan driver printer
   - D. Definisi protokol perutean IETF

Pos 2: Tantangan Benar atau Salah

6 Pertanyaan 6

6. Serangan phishing hanya menyasar akun email pribadi.

Benar Salah

7 Pertanyaan 7

7. Autentikasi multifaktor membantu memblokir serangan credential stuffing.

Benar Salah

8 Pertanyaan 8

8. Firewall memeriksa lalu lintas jaringan untuk memblokir akses port tanpa izin.

Benar Salah

9 Pertanyaan 9

9. Mengatasi exploit zero-day cukup dengan pembaruan definisi antivirus standar.

Benar Salah

10 Pertanyaan 10

10. Honeypot adalah server umpan untuk memancing penjahat siber.

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. Administrator jaringan memasang _____ untuk menyaring lalu lintas masuk.

2. Penyerang memakai _____ zero-day untuk melewati patch sistem.

3. Penyerang mengirim email palsu untuk menjalankan kampanye _____ terhadap karyawan.

4. Ransomware adalah bentuk _____ yang merusak dan mengunci data pengguna.

5. Membangun _____ kata sandi yang kuat mengurangi risiko pencurian kredensial.

6. Untuk melindungi komunikasi sensitif, pengguna menerapkan _____ protokol.

BANK KATA KOSAKATA

ANCAMAN RANSOMWARE AUTENTIKASI MULTIFAKTOR ENKRIPSI EXPLOIT FIREWALL HIGIENE MALWARE PHISHING

Tulis jawaban Anda di sini:

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

Pos 4: Pencocokan Konsep Keamanan

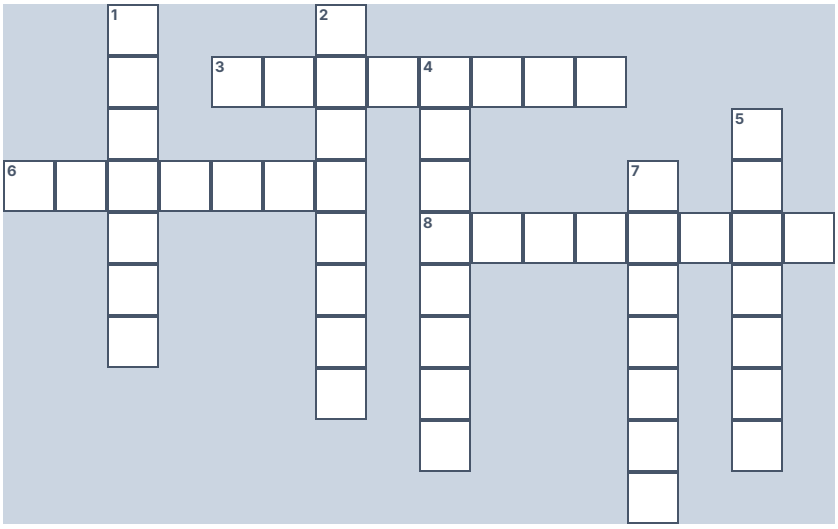
MENCOCOKKAN DEFINISI

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

☐	1. Ancaman Ransomware	A	Pedoman terstruktur seperti NIST untuk mengelola risiko siber.
☐	2. Autentikasi Multifaktor	B	Rencana terstruktur untuk menangani dan meredam pelanggaran keamanan.
☐	3. Exploit Zero-Day	C	Penghalang jaringan yang menyaring lalu lintas berdasarkan aturan keamanan.
☐	4. Honeypot Umpan	D	Malware yang mengenkripsi data dan meminta tebusan untuk dekripsi.
☐	5. Firewall Penyusupan	E	Eksploitasi celah sebelum vendor merilis patch.
☐	6. Tanggap Insiden	F	Praktik terbaik mengelola kredensial dan kunci autentikasi.
☐	7. Higiene Kata Sandi	G	Validasi keamanan yang memerlukan dua faktor autentikasi atau lebih.
☐	8. Kerangka Keamanan	H	Sistem umpan untuk memancing dan menganalisis pelaku jahat.

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

3. Email palsu untuk memancing karyawan membocorkan login (8)

6. Perangkat lunak berbahaya; ransomware salah satu bentuknya (7)

8. Perlindungan yang membuat komunikasi sensitif tak terbaca (8)

PETUNJUK MENURUN

1. Kode yang memanfaatkan celah sebelum ada perbaikan (7)

2. Penghalang yang menyaring lalu lintas masuk dengan aturan keamanan (8)

4. Server palsu untuk memancing dan mengungkap penjahat siber (8)

5. Kejadian keamanan yang ditangani dengan rencana tanggap (7)

7. Kebiasaan kata sandi yang baik untuk menekan risiko pencurian (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

3 mendatar: Email palsu untuk memancing karyawan membocorkan login (8 huruf):

6 mendatar: Perangkat lunak berbahaya; ransomware salah satu bentuknya (7 huruf):

8 mendatar: Perlindungan yang membuat komunikasi sensitif tak terbaca (8 huruf):

PETUNJUK MENURUN

1 menurun: Kode yang memanfaatkan celah sebelum ada perbaikan (7 huruf):

2 menurun: Penghalang yang menyaring lalu lintas masuk dengan aturan keamanan (8 huruf):

4 menurun: Server palsu untuk memancing dan mengungkap penjahat siber (8 huruf):

5 menurun: Kejadian keamanan yang ditangani dengan rencana tanggap (7 huruf):

7 menurun: Kebiasaan kata sandi yang baik untuk menekan risiko pencurian (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.

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

DAFTAR KOSAKATA

FIREWALL EXPLOIT PHISHING MALWARE HIGIENE ENKRIPSI HONEYPOT INSIDEN

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. FIREWALL
B. EXPLOIT
C. PHISHING
D. MALWARE
E. HIGIENE
F. ENKRIPSI
G. HONEYPOT
H. INSIDEN

DEFINISI & KOLOM PENCOCOKAN

_____ 1. Kebiasaan kata sandi yang baik untuk menekan risiko pencurian.

_____ 2. Perlindungan yang membuat komunikasi sensitif tak terbaca.

_____ 3. Penghalang yang menyaring lalu lintas masuk dengan aturan keamanan.

_____ 4. Kode yang memanfaatkan celah sebelum ada perbaikan.

_____ 5. Server palsu untuk memancing dan mengungkap penjahat siber.

_____ 6. Kejadian keamanan yang ditangani dengan rencana tanggap.

_____ 7. Email palsu untuk memancing karyawan membocorkan login.

_____ 8. Perangkat lunak berbahaya; ransomware salah satu bentuknya.

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. **LEWFAILR** _____
2. **SPGHNIHI** _____
3. **IHEEGNI** _____
4. **EOTPYHON** _____
5. **OTLPEIX** _____
6. **RLAMWEA** _____
7. **EIIPSNRK** _____
8. **NINIEDS** _____

Aktivitas Bonus: Berpikir Cepat

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

1	Pekerjaan di bidang keamanan siber			
2	Alasan memperbarui perangkat lunak			
3	Hal yang bisa diblokir firewall			
4	Tanda bahaya dalam email			
5	Hal yang Anda cadangkan			
6	Jenis serangan siber yang terkenal			
7	Hal yang bisa dipancing honeypot			
8	Informasi yang tidak boleh dibagikan			
9	Tanda komputer terinfeksi			
10	Film atau serial tentang peretas			
11	Lapisan keamanan yang bisa dibangun			
12	Hal yang dilatih dalam latihan keamanan			
13	Alat keamanan yang Anda ketahui			
14	Orang yang bisa dimintai bantuan TI			
15	Kata yang diawali 'siber'			

Pos 8: Studi Kasus Keamanan Siber

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

STUDI KASUS 1: STRATEGI PEMULIHAN RANSOMWARE



Skenario: Jaringan perusahaan terinfeksi ransomware yang mengunci basis data penting. Penyerang meminta tebusan $100.000 dalam mata uang kripto. Perusahaan punya cadangan offline dari 24 jam lalu.

Pertanyaan Diskusi: Analisis risiko membayar tebusan dan nilai strategi pemulihannya.

STUDI KASUS 2: PERTAHANAN CREDENTIAL STUFFING



Skenario: Sebuah layanan online diserang credential stuffing, dengan peretas mencoba jutaan pasangan nama pengguna/kata sandi curian dari situs lain.

Pertanyaan Diskusi: Jelaskan mekanisme serangan ini dan uraikan dua sistem pertahanan.

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

13	6	1		13	5	14	7	8	5	14	20	9	11	1	14

19	5	2	1	7	9	1	14		2	5	19	1	18

19	5	18	1	14	7	1	14

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 tujuan utama keamanan siber?

Tujuan utamanya melindungi jaringan, perangkat, dan data dari akses tanpa izin, serangan, dan kerusakan tak disengaja.

Q2: Apa beda phishing dengan spear phishing?

Phishing adalah kampanye email luas yang menyasar pengguna acak, sedangkan spear phishing menyasar orang tertentu dengan data pribadi mereka.

Q3: Apa itu firewall jaringan?

Firewall adalah sistem keamanan jaringan yang memantau dan menyaring lalu lintas masuk dan keluar berdasarkan aturan keamanan yang ditetapkan.

Q4: Mengapa autentikasi multifaktor (MFA) diperlukan?

MFA menambah lapisan pertahanan penting sehingga akses tetap tertutup meski penyerang mencuri atau membobol kata sandi utama.

Q5: Apa ciri virus komputer?

Virus adalah malware yang menggandakan diri, menempel pada berkas bersih, dan menyebar ke sistem lain setelah dijalankan.

Pos 10: FAQ Dasar Keamanan Siber (Bagian B)

Pelajari pertanyaan dan jawaban umum tentang cara mengurangi ancaman online.

Q6: Bagaimana ransomware mengunci data lokal?

Ransomware memakai algoritme kriptografis untuk mengenkripsi berkas pengguna sehingga tak terbaca sampai kunci dekripsi dipakai.

Q7: Apa itu celah zero-day?

Zero-day adalah celah keamanan perangkat lunak yang belum diketahui vendor, sehingga tidak ada waktu membuat patch sebelum dieksploitasi.

Q8: Apa peran kerangka NIST?

Kerangka NIST menyediakan pedoman dan standar sukarela untuk membantu organisasi mengelola dan mengurangi risiko keamanan siber.

Q9: Apa itu rencana tanggap insiden keamanan?

Rencana ini adalah prosedur tertulis untuk mendeteksi, membendung, dan memulihkan diri dari pelanggaran keamanan dan jaringan yang dibobol.

Q10: Bagaimana rekayasa sosial memanfaatkan pengguna?

Rekayasa sosial memakai manipulasi psikologis untuk menipu karyawan agar membocorkan kata sandi atau mengunduh berkas berbahaya.

Pos 10: FAQ Lanjutan Keamanan (Bagian C)

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

Q1: Bagaimana serangan DDoS membanjiri server web?

Serangan DDoS mengerahkan jutaan perangkat botnet untuk membanjiri server dengan lalu lintas hingga bandwidth dan CPU habis.

Q2: Apa beda enkripsi simetris dan asimetris?

Enkripsi simetris memakai satu kunci untuk enkripsi dan dekripsi, sedangkan enkripsi asimetris memakai pasangan kunci publik dan privat.

Q3: Bagaimana peretas melakukan serangan SQL injection?

Penyerang memasukkan perintah SQL berbahaya ke kolom formulir sehingga basis data backend tertipu dan membocorkan catatan pengguna.

Q4: Apa itu pergerakan lateral dalam penyusupan jaringan?

Teknik ketika penyerang memanfaatkan akses awal ke satu server untuk membobol sistem lain yang terhubung di jaringan internal.

Q5: Bagaimana DNS spoofing mengalihkan lalu lintas web?

DNS spoofing mengubah catatan cache nameserver sehingga pengguna diarahkan ke situs tiruan berbahaya, bukan domain tujuan.

Pos 10: FAQ Lanjutan Keamanan (Bagian D)

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

Q6: Apa itu token keamanan perangkat keras?

Perangkat fisik (seperti YubiKey) yang menghasilkan bukti autentikasi kriptografis dan memberi pertahanan maksimal terhadap phishing jarak jauh.

Q7: Bagaimana tim keamanan memakai honeypot umpan?

Tim memasang server umpan non-produksi untuk mendeteksi penyusupan sejak dini dan menganalisis pola serangan pelaku.

Q8: Apa itu prinsip hak akses minimum?

Standar keamanan yang membatasi hak akses pengguna seminimal mungkin sesuai kebutuhan pekerjaannya.

Q9: Bagaimana serangan Man-in-the-Middle memanfaatkan koneksi?

Penyerang menyadap dan mengubah komunikasi antara dua perangkat di jaringan tanpa enkripsi, lalu mencuri token sesi dan kredensial.

Q10: Apa itu indikator kompromi (IOC)?

IOC adalah petunjuk forensik, seperti perubahan registri yang tidak wajar atau lalu lintas IP mencurigakan, yang menunjukkan sistem telah dibobol.

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

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

1. WAWASAN KEAMANAN

Penyerang terus-menerus memindai internet untuk mencari server yang rentan dan mengirim email phishing ke kotak masuk karyawan.

2. WAWASAN KEAMANAN

Kesalahan manusia, seperti mengeklik tautan phishing, adalah faktor umum dalam kebocoran data, itulah sebabnya pelatihan itu penting.

3. WAWASAN KEAMANAN

Biaya kebocoran data mencakup denda hukum, hilangnya pelanggan, investigasi, dan perbaikan, dan bisa mencapai jutaan dolar.

4. WAWASAN KEAMANAN

MFA yang tahan phishing, seperti kunci keamanan perangkat keras, adalah jenis MFA terkuat dan standar yang didorong oleh CISA. [2]

5. WAWASAN KEAMANAN

Ransomware tetap menjadi ancaman besar bagi jaringan perusahaan, dan CISA mendorong cadangan offline yang terenkripsi sebagai pertahanan utama. [4]

6. WAWASAN KEAMANAN

NIST Cybersecurity Framework 2.0 (2024) memiliki enam fungsi inti: Govern, Identify, Protect, Detect, Respond, Recover. [1]

7. WAWASAN KEAMANAN

Bot credential stuffing menguji pasangan nama pengguna dan kata sandi yang bocor secara massal terhadap portal login perbankan dan e-commerce.

8. WAWASAN KEAMANAN

Pasar exploit zero-day ada di seluruh dunia, tempat kerentanan dengan tingkat keparahan tinggi dapat terjual dengan harga besar sebelum ditambal.

9. WAWASAN KEAMANAN

Sistem umpan honeypot langsung melaporkan penyusupan karena pengguna sah tidak punya alasan mengaksesnya.

10. WAWASAN KEAMANAN

Transport Layer Security (TLS) mengenkripsi sesi browser sehingga penyadapan paket di Wi-Fi publik tercegah.

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. (2024). The NIST Cybersecurity Framework (CSF) 2.0.
https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

[2] CISA. (n.d.). More than a Password.
https://www.cisa.gov/MFA

[3] 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

[4] CISA. (2023). #StopRansomware Guide.
https://www.cisa.gov/stopransomware/ransomware-guide

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

[6] NIST. (2025). SP 800-61 Rev. 3, Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile.
https://csrc.nist.gov/pubs/sp/800/61/r3/final

[7] NIST. (2025). SP 800-63B-4: Digital Identity Guidelines: Authentication and Authenticator Management.
https://pages.nist.gov/800-63-4/sp800-63b.html

[8] OWASP. (n.d.). SQL Injection.
https://owasp.org/www-community/attacks/SQL_Injection

Kunci Jawaban: Pos 1 - Pilihan Ganda

1 **Serangan Phishing** PHISHING — **Jawaban Benar: A**

CATATAN PENGAJAR

Kampanye phishing berusaha mencuri kredensial dan data sensitif pengguna dengan email palsu.

2 **Perlindungan Akun** KUNCI MFA — **Jawaban Benar: A**

CATATAN PENGAJAR

Autentikasi multifaktor (MFA) dengan token perangkat keras memberi pertahanan akses akun terkuat.

3 **Ancaman Ransomware** RANSOMWARE — **Jawaban Benar: A**

CATATAN PENGAJAR

Ransomware mengenkripsi sistem dan data penting, lalu meminta tebusan mata uang kripto untuk kunci dekripsi.

4 **Celah Zero-Day** ZERO-DAY — **Jawaban Benar: A**

CATATAN PENGAJAR

Ancaman zero-day mengeksploitasi celah yang belum diketahui dan belum ditambal sebelum vendor merilis patch.

5 **Kerangka Keamanan** KERANGKA — **Jawaban Benar: A**

CATATAN PENGAJAR

Kerangka seperti NIST menyediakan pedoman terstruktur untuk membantu organisasi mengelola dan mengurangi risiko siber.

Kunci Jawaban: Pos 2 - Benar atau Salah

6 **Sasaran Phishing** PHISHING — **Jawaban Benar: Salah**

CATATAN PENGAJAR

Serangan phishing menyasar jaringan perusahaan maupun akun pribadi untuk memperluas jalur eksploitasi.

7 **Soal 7** — **Jawaban Benar: Benar**

CATATAN PENGAJAR

MFA memerlukan faktor kedua, sehingga kata sandi curian saja biasanya tidak cukup untuk login.

8 **Firewall Lalu Lintas** FIREWALL — **Jawaban Benar: Benar**

CATATAN PENGAJAR

Firewall memeriksa dan memblokir lalu lintas di port tertentu untuk menyaring koneksi tanpa izin.

9 **Tanggapan Zero-Day** ZERO-DAY — **Jawaban Benar: Salah**

CATATAN PENGAJAR

Mengatasi celah zero-day memerlukan patch kode dan penyaringan WAF karena signature-nya belum ada.

10 **Honeypot Umpan** HONEYPOT — **Jawaban Benar: Benar**

CATATAN PENGAJAR

Honeypot adalah server tipuan yang dipakai tim keamanan untuk memancing, memberi peringatan, dan mempelajari pelaku jahat.

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

D 1. Ancaman Ransomware	G 2. Autentikasi Multifaktor	E 3. Exploit Zero-Day	H 4. Honeypot Umpan
C 5. Firewall Penyusupan	B 6. Tanggap Insiden	F 7. Higiene Kata Sandi	A 8. Kerangka Keamanan

POS 3: KUNCI ISTILAH KUNCI

1 FIREWALL	2 EXPLOIT	3 PHISHING	4 MALWARE
5 HIGIENE	6 ENKRIPSI		

ALTERNATIF POS 6: KUNCI PENCOCOKAN KOSAKATA

1 E – HIGIENE	2 F – ENKRIPSI	3 A – FIREWALL	4 B – EXPLOIT
5 G – HONEYPOT	6 H – INSIDEN	7 C – PHISHING	8 D – MALWARE

CATATAN DISKUSI UNTUK PENGAJAR

Istilah Kunci:
Pastikan siswa dapat menjelaskan Ancaman Ransomware, Autentikasi Multifaktor, dan Exploit Zero-Day dengan kata-kata sendiri serta memberi contoh untuk setiap istilah.

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

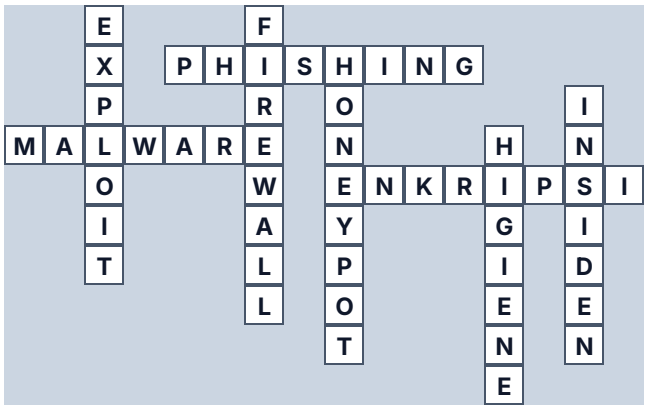
Evaluasi Sumber:
Minta siswa memeriksa setidaknya satu klaim terhadap referensi di lembar kerja, lalu diskusikan mengapa angka, harga, dan aturan dapat berubah seiring waktu.

Kunci Teka-Teki & Catatan Pengajar

JAWABAN PENCARIAN KATA

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

JAWABAN TEKA-TEKI SILANG



PANDUAN PENGAJAR UNTUK JAWABAN TEKA-TEKI SILANG

PETUNJUK MENDATAR

3 mendatar: PHISHING Email palsu untuk memancing karyawan membocorkan login (8 huruf)

6 mendatar: MALWARE Perangkat lunak berbahaya; ransomware salah satu bentuknya (7 huruf)

8 mendatar: ENKRIPSI Perlindungan yang membuat komunikasi sensitif tak terbaca (8 huruf)

PETUNJUK MENURUN

1 menurun: EXPLOIT Kode yang memanfaatkan celah sebelum ada perbaikan (7 huruf)

2 menurun: FIREWALL Penghalang yang menyaring lalu lintas masuk dengan aturan keamanan (8 huruf)

4 menurun: HONEYPOT Server palsu untuk memancing dan mengungkap penjahat siber (8 huruf)

5 menurun: INSIDEN Kejadian keamanan yang ditangani dengan rencana tanggap (7 huruf)

7 menurun: HIGIENE Kebiasaan kata sandi yang baik untuk menekan risiko pencurian (7 huruf)

Kunci Jawaban Kata Acak & Sandi

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

KUNCI KATA ACAK

1.	L E W F A I L R	FIREWALL	5.	O T L P E I X	EXPLOIT
2.	S P G H N I H I	PHISHING	6.	R L A M W E A	MALWARE
3.	I H E E G N I	HIGIENE	7.	E I I P S N R K	ENKRIPSI
4.	E O T P Y H O N	HONEYPOT	8.	N I N I E D S	INSIDEN

KUNCI TANTANGAN SANDI RAHASIA

"MFA MENGHENTIKAN SEBAGIAN BESAR SERANGAN"

Kunci Jawaban Studi Kasus

A Studi Kasus 1: Strategi Pemulihan Ransomware

Jawaban Pengajar

PEDOMAN PENILAIAN

Jawaban siswa harus mencakup poin-poin berikut:

- Analisis Skenario: Jaringan perusahaan terinfeksi ransomware yang mengunci basis data penting. Penyerang meminta tebusan $100.000 dalam mata uang kripto. Perusahaan punya cadangan offline dari 24 jam lalu.
- Strategi & Solusi yang Disarankan: Risiko Membayar: Membayar tidak menjamin berkas terdekripsi, menandai perusahaan sebagai sasaran yang mau membayar, dan mendanai kejahatan. Strategi Pemulihan: Tim harus mengisolasi host yang terinfeksi, menghapus server yang dibobol, dan memulihkan data dari cadangan offline. Jalur akses awal (phishing atau exploit) harus ditambal agar tidak langsung terinfeksi lagi.

B Studi Kasus 2: Pertahanan Credential Stuffing

Jawaban Pengajar

PEDOMAN PENILAIAN

Jawaban siswa harus mencakup poin-poin berikut:

- Analisis Skenario: Sebuah layanan online diserang credential stuffing, dengan peretas mencoba jutaan pasangan nama pengguna/kata sandi curian dari situs lain.
- Strategi & Solusi yang Disarankan: Mekanisme: Penyerang memanfaatkan kata sandi yang dipakai ulang di banyak situs dan memakai bot otomatis untuk masuk ke akun pengguna. Pertahanan: 1. Autentikasi multifaktor (MFA) memblokir upaya login meski kata sandinya benar. 2. Pembatasan laju dan CAPTCHA memblokir lalu lintas bot yang membanjiri halaman login.