Nama: _____ Tanggal: _____ Nilai: _____

Keamanan & Enkripsi Wi-Fi Publik

Serangan man-in-the-middle, titik akses palsu, packet sniffing, terowongan VPN, dan enkripsi HTTPS.

GAMBARAN PEMBELAJARAN KEAMANAN WI-FI PUBLIK

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 keamanan Wi-Fi publik. Anda akan mempelajari jaringan tanpa enkripsi, serangan man-in-the-middle (MitM), titik akses palsu, packet sniffing, terowongan VPN, dan keamanan transit HTTPS.

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/public-wifi-security/

Peta Belajar Keamanan Wi-Fi Publik Anda

- Kenali risiko umum Wi-Fi publik, termasuk packet sniffing dan titik akses palsu.
- Terapkan terowongan enkripsi VPN untuk mengamankan data yang dikirim.
- Wajibkan HTTPS dan pengaturan browser yang aman bagi pekerja jarak jauh.

PETUNJUK PANDUAN KEAMANAN WI-FI PUBLIK

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 keamanan akses jarak jauh. Akhiri dengan aktivitas bonus Berpikir Cepat.

KEAMANAN WI-FI PUBLIK & PERLINDUNGAN TRANSIT (PENGANTAR)

Hotspot Wi-Fi publik tanpa enkripsi membuat lalu lintas rentan terhadap packet sniffing dan pemalsuan Evil Twin. Memaksa lalu lintas lewat terowongan enkripsi VPN dan menerapkan aturan HSTS khusus HTTPS melindungi sesi dari penyadapan di jaringan lokal.

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

Pos 1: Tantangan Pilihan Ganda

1. **1. Apa itu serangan Man-in-the-Middle (MitM)?**
   - A. Menyadap dan mengubah komunikasi dua pihak di jaringan bersama
   - B. Teknik mengambil data pengguna dari basis data
   - C. Membanjiri server web dengan lalu lintas
   - D. Menghapus isi hard drive lokal

2. **2. Apa itu titik akses palsu (Evil Twin)?**
   - A. Hotspot Wi-Fi jahat dengan SSID yang sama dengan jaringan asli
   - B. Alat admin untuk memantau cadangan basis data
   - C. Konfigurasi gateway VPN yang aman
   - D. Catatan DNS berisi server email resmi

3. **3. Bagaimana VPN melindungi lalu lintas Wi-Fi publik?**
   - A. Membungkus semua paket dalam terowongan terenkripsi sehingga tak terbaca penyadap
   - B. Otomatis memblokir semua permintaan koneksi masuk
   - C. Mengganti alamat MAC kartu jaringan
   - D. Menghapus cookie tersimpan di browser

4. **4. Apa itu packet sniffing?**
   - A. Memakai alat perangkat keras atau lunak untuk menangkap dan mencatat paket jaringan
   - B. Memindai direktori lokal untuk berkas ganda
   - C. Membatasi hak baca basis data sesuai peran
   - D. Mengenkripsi drive dengan kunci AES-256

5. **5. Apa peran HTTPS?**
   - A. Mengenkripsi lalu lintas sesi antara browser dan server web
   - B. Menyaring email masuk di gerbang
   - C. Mengompresi gambar agar halaman lebih cepat dimuat
   - D. Mengelola struktur berkas di penyimpanan jaringan

Pos 2: Tantangan Benar atau Salah

6 Pertanyaan 6

6. Pengguna yang terhubung dapat dengan mudah menangkap data tanpa enkripsi di Wi-Fi publik terbuka.

○ Benar ○ Salah

7 Pertanyaan 7

7. Titik akses palsu (Evil Twin) selalu diizinkan administrator jaringan.

○ Benar ○ Salah

8 Pertanyaan 8

8. VPN tidak efektif melindungi lalu lintas dari packet sniffing di jaringan publik.

○ Benar ○ Salah

9 Pertanyaan 9

9. HTTPS hanya mengenkripsi jalur URL dan membiarkan muatan paket tanpa enkripsi.

○ Benar ○ Salah

10 Pertanyaan 10

10. Hotspot Wi-Fi dengan keamanan WPA3 lebih terlindung daripada jaringan terbuka tanpa kata sandi.

○ 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. Menangkap kata sandi pribadi di Wi-Fi publik disebut _____ .
2. Menganalisis paket mentah di jaringan lokal disebut packet _____ .
3. Hotspot palsu yang meniru Wi-Fi hotel disebut _____ .
4. Mengamankan lalu lintas web memerlukan enkripsi dengan _____ .
5. Mengenkripsi semua lalu lintas jaringan memakai klien _____ .
6. Jalur komunikasi terenkripsi melalui jaringan publik disebut _____ .

BANK KATA KOSAKATA

EVIL TWIN FIREWALL HTTPS PENYADAPAN SNIFFING TEROWONGAN VPN WPA3

Tulis jawaban Anda di sini:

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

Pos 4: Pencocokan Konsep Keamanan

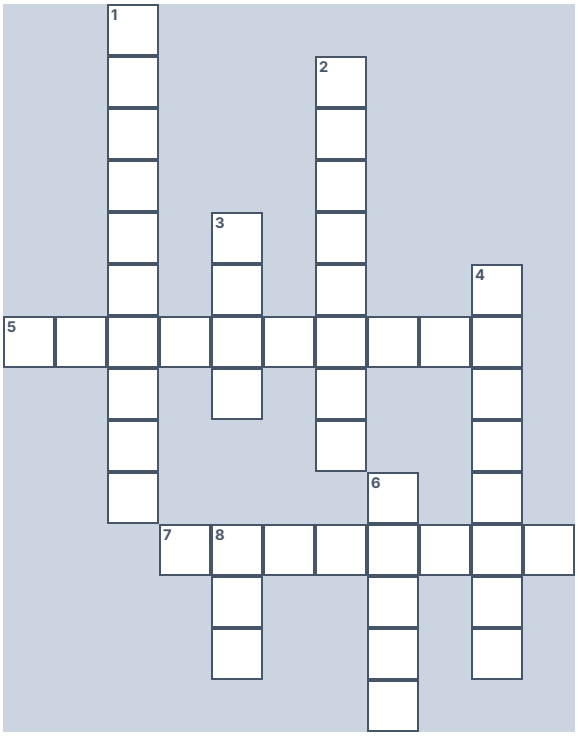
MENCOCOKKAN DEFINISI

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

☐	1. PENYADAPAN	A	Standar keamanan Wi-Fi modern.
☐	2. SNIFFING	B	Jalur data aman saat dikirim.
☐	3. EVIL TWIN	C	Menyaring lalu lintas masuk.
☐	4. HTTPS	D	Hotspot palsu yang meniru Wi-Fi.
☐	5. VPN	E	Membaca lalu lintas yang sedang dikirim.
☐	6. TEROWONGAN	F	Menangkap paket data jaringan.
☐	7. WPA3	G	Jaringan privat virtual terenkripsi.
☐	8. FIREWALL	H	Pengiriman web yang aman.

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

5. Menangkap kata sandi dan data orang lain di jaringan publik (10)

7. Hotspot palsu yang meniru jaringan asli dengan nama sama (8)

PETUNJUK MENURUN

1. Koneksi terenkripsi melalui jaringan publik (10)

2. Penghalang yang menyaring lalu lintas masuk (8)

3. Standar keamanan Wi-Fi terbaru (4)

4. Packet ...: menangkap dan menganalisis paket data mentah (8)

6. Protokol yang mengenkripsi lalu lintas antara browser dan server web (5)

8. Layanan yang mengenkripsi semua lalu lintas perangkat dalam terowongan (3)

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

5 mendatar: Menangkap kata sandi dan data orang lain di jaringan publik (10 huruf):

7 mendatar: Hotspot palsu yang meniru jaringan asli dengan nama sama (8 huruf):

PETUNJUK MENURUN

1 menurun: Koneksi terenkripsi melalui jaringan publik (10 huruf):

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

3 menurun: Standar keamanan Wi-Fi terbaru (4 huruf):

4 menurun: Packet ...: menangkap dan menganalisis paket data mentah (8 huruf):

6 menurun: Protokol yang mengenkripsi lalu lintas antara browser dan server web (5 huruf):

8 menurun: Layanan yang mengenkripsi semua lalu lintas perangkat dalam terowongan (3 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 I G N R M F P X Q O C U S
T E L J B A B I C P H X L K Y
N K 3 X T K D R Q M T J D I N
A N A K Q P G E M M T Q R S T
G T P G C P S W Q O P H S S B
N W W D S E Z A V C S Z W N F
O K H Z D N N L E D Q X P I C
W U B A Z Y N L V D K A D F O
O D F H I A D R I Q M E I F R
R Z S F Q D V V L F A A Q I O
E N P T X A P Q T K R U S N D
T N Y B F P N S W X W J A G R
Z Y Y L G A I M I R J M L T O
H Q Q H Z N A O N V G U B Y R
Y B H L Z G J O P N W C M Z Y

DAFTAR KOSAKATA

PENYADAPAN SNIFFING EVILTWIN HTTPS VPN TEROWONGAN WPA3 FIREWALL

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. PENYADAPAN
B. SNIFFING
C. EVILTWIN
D. HTTPS
E. VPN
F. TEROWONGAN
G. WPA3
H. FIREWALL

DEFINISI & KOLOM PENCOCOKAN

1. Standar keamanan Wi-Fi terbaru.
2. Hotspot palsu yang meniru jaringan asli dengan nama sama.
3. Packet ...: menangkap dan menganalisis paket data mentah.
4. Koneksi terenkripsi melalui jaringan publik.
5. Penghalang yang menyaring lalu lintas masuk.
6. Menangkap kata sandi dan data orang lain di jaringan publik.
7. Layanan yang mengenkripsi semua lalu lintas perangkat dalam terowongan.
8. Protokol yang mengenkripsi lalu lintas antara browser dan server web.

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. A A D A E P P N Y N _____
2. L E N V I W T I _____
3. N P V _____
4. 3 A W P _____
5. F I N G F S N I _____
6. P H T S T _____
7. E O T N O G A N W R _____
8. E I W L F L A R _____

Aktivitas Bonus: Berpikir Cepat

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

1	Alasan memperbarui perangkat lunak			
2	Perangkat yang tersambung otomatis ke Wi-Fi			
3	Informasi yang tidak boleh dibagikan			
4	Kebiasaan aman yang bisa dimulai hari ini			
5	Cara tetap aman di kafe			
6	Perangkat yang bisa diretas			
7	Hal yang bisa dilihat peretas di Wi-Fi terbuka			
8	Tanda jaringan Wi-Fi palsu			
9	Alternatif selain Wi-Fi publik			
10	Tanda bahaya dalam email			
11	Hal yang tidak dilakukan di Wi-Fi publik			
12	Tempat dengan Wi-Fi gratis			
13	Cara melindungi akun Anda			
14	Tanda komputer terinfeksi			
15	Nama Wi-Fi yang mencurigakan			

Pos 8: Studi Kasus Keamanan Siber

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

STUDI KASUS 1: MENAHAN PACKET SNIFFING DI WI-FI PUBLIK



Skenario: Seorang eksekutif penjualan yang terhubung ke Wi-Fi publik bandara mendapati beberapa email bisnis sensitif bocor tak lama setelah dikirim tanpa enkripsi.

Pertanyaan Diskusi: Analisis risiko jaringan publik, dan uraikan solusi enkripsi lalu lintas.

STUDI KASUS 2: PERTAHANAN DARI HOTSPOT PALSU EVIL TWIN



Skenario: Penyerang memasang titik akses nirkabel palsu bernama 'CoffeeShop_Guest' yang meniru hotspot kafe asli dan menangkap lalu lintas tamu yang tidak curiga.

Pertanyaan Diskusi: Uraikan langkah verifikasi untuk mendeteksi dan memblokir titik akses palsu.

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

19	5	12	1	12	21		16	1	11	1	9		22	16	14		4	9

10	1	18	9	14	7	1	14		16	21	2	12	9	11

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: Mengapa Wi-Fi publik tidak aman?

Wi-Fi publik yang terbuka tidak mengenkripsi lalu lintas di udara, sehingga orang lain di sekitar dapat menangkap data apa pun yang tidak terlindungi. [2]

Q2: Apa itu packet sniffing?

Packet sniffer menangkap data mentah di antarmuka jaringan dan membuka kata sandi tanpa enkripsi serta detail lalu lintas.

Q3: Apa itu Evil Twin?

Titik akses palsu buatan peretas yang meniru nama dan pengaturan hotspot Wi-Fi lokal tepercaya.

Q4: Bagaimana VPN melindungi saya?

VPN merutekan lalu lintas lewat terowongan terenkripsi sehingga aktivitas Anda tersembunyi dari penyadap jaringan lokal.

Q5: Apakah HTTPS melindungi saya di Wi-Fi publik?

Ya, HTTPS mengenkripsi data yang dipertukarkan antara browser Anda dan situs web, dan VPN menambahkan lapisan perlindungan lain.

Pos 10: FAQ Dasar Keamanan Siber (Bagian B)

Pelajari pertanyaan dan jawaban umum tentang cara mengurangi ancaman online.

Q6: Apa itu WPA3?

Standar Wi-Fi Protected Access modern dengan enkripsi lebih kuat dan perlindungan dari serangan kamus offline. [1]

Q7: Bisakah Wi-Fi publik menyebarkan malware?

Bisa, penyerang dapat menyadap lalu lintas dan menyisipkan unduhan berbahaya (drive-by download) ke sesi browser Anda.

Q8: Apa risiko berbagi berkas?

Jika berbagi berkas aktif, pengguna lain di jaringan publik dapat membaca atau mengubah folder lokal Anda.

Q9: Apa itu captive portal?

Halaman login jaringan hotel atau kafe untuk memberi akses internet, yang terkadang dipalsukan penyerang.

Q10: Perlukah Wi-Fi dimatikan saat tidak dipakai?

Perlu, mematikan Wi-Fi mencegah perangkat otomatis terhubung ke jaringan tak tepercaya.

Pos 10: FAQ Lanjutan Keamanan (Bagian C)

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

Q1: Bagaimana serangan Man-in-the-Middle memanfaatkan DNS?

Dengan pemalsuan DNS di router palsu untuk mengarahkan browser ke halaman phishing tiruan, bukan domain tujuan.

Q2: Apa itu pembajakan sesi?

Penyerang menyadap cookie sesi tanpa enkripsi di Wi-Fi publik lalu memakainya untuk melewati login.

Q3: Apa itu SSL stripping?

Serangan MitM yang menurunkan permintaan HTTPS aman menjadi HTTP tanpa enkripsi untuk menangkap login.

Q4: Bagaimana HSTS melindungi dari SSL stripping?

HTTP Strict Transport Security memaksa browser hanya terhubung lewat HTTPS dan menolak beralih ke HTTP. [3]

Q5: Apa itu VPN split-tunnel?

Konfigurasi yang hanya merutekan lalu lintas perusahaan lewat VPN dan mengirim data internet publik langsung, yang berisiko membuka jalur kebocoran.

Pos 10: FAQ Lanjutan Keamanan (Bagian D)

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

Q6: Mengapa WPA2 rentan terhadap KRACK?

Key Reinstallation Attack memanfaatkan handshake empat arah WPA2 untuk mendekripsi paket tanpa kata sandi Wi-Fi.

Q7: Apa itu isolasi klien?

Pengaturan keamanan router yang mencegah perangkat Wi-Fi saling berkomunikasi langsung, sehingga penyadapan lokal terblokir.

Q8: Bagaimana penyerang memakai server DNS palsu?

Mereka mengatur router palsu agar memberi server DNS palsu kepada klien, sehingga semua pencarian web bisa disadap dan diubah.

Q9: Bisakah VPN menyembunyikan alamat MAC lokal saya?

Tidak. Alamat MAC adalah pengidentifikasi lokal lapisan 2; gunakan pengaturan pengacakan MAC bawaan perangkat Anda (alamat privat) sebagai gantinya.

Q10: Apa itu serangan pemalsuan captive portal?

Penyerang memasang portal login palsu di hotspot tiruan untuk mencuri kredensial dengan dalih Wi-Fi gratis.

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

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

1. WAWASAN KEAMANAN

Pekerja jarak jauh sering menggunakan Wi-Fi di kafe, hotel, dan bandara, tempat mereka tidak dapat mengendalikan keamanan jaringan.

2. WAWASAN KEAMANAN

Hotspot palsu Evil Twin dapat meniru persis nama dan alamat MAC jaringan tepercaya sehingga perangkat tertipu.

3. WAWASAN KEAMANAN

Perangkat lunak packet sniffing seperti Wireshark gratis dan dapat menampilkan kata sandi HTTP tanpa enkripsi.

4. WAWASAN KEAMANAN

Keamanan WPA3 memakai Simultaneous Authentication of Equals (SAE) untuk melindungi dari serangan brute force lokal.

5. WAWASAN KEAMANAN

Serangan SSL stripping melewati perlindungan HTTPS dasar dengan mencegat pengalihan HTTP awal di gerbang.

6. WAWASAN KEAMANAN

Header respons HTTP Strict Transport Security (HSTS) mencegah browser kembali ke koneksi HTTP yang tidak terenkripsi. [3]

7. WAWASAN KEAMANAN

Mematikan 'Auto-Connect' mencegah ponsel terhubung ke jaringan palsu yang mirip di tempat umum.

8. WAWASAN KEAMANAN

Konfigurasi VPN perusahaan 'selalu aktif' memaksa semua lalu lintas pekerja jarak jauh melewati firewall perusahaan.

9. WAWASAN KEAMANAN

Titik akses palsu dapat memberikan jawaban DNS palsu, yang mengalihkan domain sasaran ke server phishing.

10. WAWASAN KEAMANAN

Tanpa VPN, pengguna lain di hotspot terbuka dapat melihat situs dan server mana yang dihubungi perangkat Anda.

Referensi & Sumber Teknis

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

REFERENSI AKADEMIK & INDUSTRI

[1] Wi-Fi Alliance. (n.d.). Security.

https://www.wi-fi.org/discover-wi-fi/security

[2] Federal Trade Commission. (2023). Are Public Wi-Fi Networks Safe? What You Need To Know.

https://consumer.ftc.gov/articles/are-public-wi-fi-networks-safe-what-you-need-know

[3] MDN Web Docs. (n.d.). Strict-Transport-Security header.

https://developer.mozilla.org/en-US/docs/Web/HTTP/Reference/Headers/Strict-Transport-Security

[4] 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

[5] CISA. (n.d.). Malware, Phishing, and Ransomware.

https://www.cisa.gov/topics/cyber-threats-and-advisories/malware-phishing-and-ransomware

Kunci Jawaban: Pos 1 - Pilihan Ganda

1 Soal 1

Jawaban Benar: A

CATATAN PENGAJAR

Apa itu serangan Man-in-the-Middle (MitM)? → Menyadap dan mengubah komunikasi dua pihak di jaringan bersama

2 Soal 2

Jawaban Benar: A

CATATAN PENGAJAR

Apa itu titik akses palsu (Evil Twin)? → Hotspot Wi-Fi jahat dengan SSID yang sama dengan jaringan asli

3 Soal 3

Jawaban Benar: A

CATATAN PENGAJAR

Bagaimana VPN melindungi lalu lintas Wi-Fi publik? → Membungkus semua paket dalam terowongan terenkripsi sehingga tak terbaca penyadap

4 Soal 4

Jawaban Benar: A

CATATAN PENGAJAR

Apa itu packet sniffing? → Memakai alat perangkat keras atau lunak untuk menangkap dan mencatat paket jaringan

5 Soal 5

Jawaban Benar: A

CATATAN PENGAJAR

Apa peran HTTPS? → Mengenkripsi lalu lintas sesi antara browser dan server web

Kunci Jawaban: Pos 2 - Benar atau Salah

6 **Soal 6** — **Jawaban Benar: Benar**

CATATAN PENGAJAR

Pengguna yang terhubung dapat dengan mudah menangkap data tanpa enkripsi di Wi-Fi publik terbuka.

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

CATATAN PENGAJAR

Salah: Evil Twin adalah hotspot tidak resmi yang dipasang penyerang untuk meniru hotspot asli.

8 **Soal 8** — **Jawaban Benar: Salah**

CATATAN PENGAJAR

Salah: VPN mengenkripsi lalu lintas di dalam terowongan, sehingga penyadap lokal tidak dapat membacanya.

9 **Soal 9** — **Jawaban Benar: Salah**

CATATAN PENGAJAR

Salah: HTTPS mengenkripsi seluruh pertukaran HTTP, termasuk jalur URL dan isi halaman.

10 **Soal 10** — **Jawaban Benar: Benar**

CATATAN PENGAJAR

Hotspot Wi-Fi dengan keamanan WPA3 lebih terlindung daripada jaringan terbuka tanpa kata sandi.

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

E 1. PENYADAPAN	F 2. SNIFFING	D 3. EVIL TWIN	H 4. HTTPS
G 5. VPN	B 6. TEROWONGAN	A 7. WPA3	C 8. FIREWALL

POS 3: KUNCI ISTILAH KUNCI

1 PENYADAPAN	2 SNIFFING	3 EVIL TWIN	4 HTTPS
5 VPN	6 TEROWONGAN		

ALTERNATIF POS 6: KUNCI PENCOCOKAN KOSAKATA

1 G – WPA3	2 C – EVILTWIN	3 B – SNIFFING	4 F – TEROWONGAN
5 H – FIREWALL	6 A – PENYADAPAN	7 E – VPN	8 D – HTTPS

CATATAN DISKUSI UNTUK PENGAJAR

Istilah Kunci:
Pastikan siswa dapat menjelaskan PENYADAPAN, SNIFFING, dan EVIL TWIN dengan kata-kata sendiri serta memberi contoh untuk setiap istilah.

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

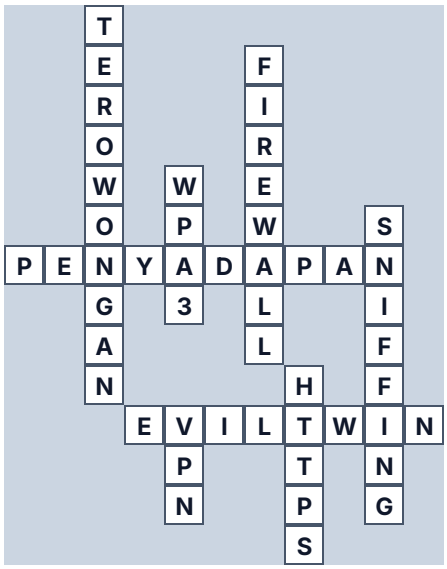
Evaluasi Sumber:
Minta siswa memeriksa setidaknya satu klaim terhadap referensi di lembar kerja, lalu diskusikan mengapa angka, harga, dan aturan dapat berubah seiring waktu.

Kunci Teka-Teki & Catatan Pengajar

JAWABAN PENCARIAN KATA

C	R	I	G	N	R	M	F	P	X	Q	O	C	U	S
T	E	L	J	B	A	B	I	C	P	H	X	L	K	Y
N	K	3	X	T	K	D	R	Q	M	T	J	D	I	N
A	N	A	K	Q	P	G	E	M	M	T	Q	R	S	T
G	T	P	G	C	P	S	W	Q	O	P	H	S	S	B
N	W	W	D	S	E	Z	A	V	C	S	Z	W	N	F
O	K	H	Z	D	N	N	L	E	D	Q	X	P	I	C
W	U	B	A	Z	Y	N	L	V	D	K	A	D	F	O
O	D	F	H	I	A	D	R	I	Q	M	E	I	F	R
R	Z	S	F	Q	D	V	V	L	F	A	A	Q	I	O
E	N	P	T	X	A	P	Q	T	K	R	U	S	N	D
T	N	Y	B	F	P	N	S	W	X	W	J	A	G	R
Z	Y	Y	L	G	A	I	M	I	R	J	M	L	T	O
H	Q	Q	H	Z	N	A	O	N	V	G	U	B	Y	R
Y	B	H	L	Z	G	J	O	P	N	W	C	M	Z	Y

JAWABAN TEKA-TEKI SILANG



PANDUAN PENGAJAR UNTUK JAWABAN TEKA-TEKI SILANG

PETUNJUK MENDATAR

5 mendatar: PENYADAPAN Menangkap kata sandi dan data orang lain di jaringan publik (10 huruf)

7 mendatar: EVILTWIN Hotspot palsu yang meniru jaringan asli dengan nama sama (8 huruf)

PETUNJUK MENURUN

1 menurun: TEROWONGAN Koneksi terenkripsi melalui jaringan publik (10 huruf)

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

3 menurun: WPA3 Standar keamanan Wi-Fi terbaru (4 huruf)

4 menurun: SNIFFING Packet ...: menangkap dan menganalisis paket data mentah (8 huruf)

6 menurun: HTTPS Protokol yang mengenkripsi lalu lintas antara browser dan server web (5 huruf)

8 menurun: VPN Layanan yang mengenkripsi semua lalu lintas perangkat dalam terowongan (3 huruf)

Kunci Jawaban Kata Acak & Sandi

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

KUNCI KATA ACAK

1.	A A D A E P P N Y N	PENYADAPAN	5.	F I N G F S N I	SNIFFING
2.	L E N V I W T I	EVILTWIN	6.	P H T S T	HTTPS
3.	N P V	VPN	7.	E O T N O G A N W R	TEROWONGAN
4.	3 A W P	WPA3	8.	E I W L F L A R	FIREWALL

KUNCI TANTANGAN SANDI RAHASIA

"SELALU PAKAI VPN DI JARINGAN PUBLIK"

Kunci Jawaban Studi Kasus

A Studi Kasus 1: Menahan Packet Sniffing di Wi-Fi Publik

Jawaban Pengajar

PEDOMAN PENILAIAN

Jawaban siswa harus mencakup poin-poin berikut:

- Analisis Skenario: Seorang eksekutif penjualan yang terhubung ke Wi-Fi publik bandara mendapati beberapa email bisnis sensitif bocor tak lama setelah dikirim tanpa enkripsi.
- Strategi & Solusi yang Disarankan: Wajibkan klien VPN perusahaan di semua komputer jarak jauh. Terapkan ekstensi browser khusus HTTPS, dan blokir protokol tanpa enkripsi (seperti HTTP dan FTP) di firewall klien.

B Studi Kasus 2: Pertahanan dari Hotspot Palsu Evil Twin

Jawaban Pengajar

PEDOMAN PENILAIAN

Jawaban siswa harus mencakup poin-poin berikut:

- Analisis Skenario: Penyerang memasang titik akses nirkabel palsu bernama 'CoffeeShop_Guest' yang meniru hotspot kafe asli dan menangkap lalu lintas tamu yang tidak curiga.
- Strategi & Solusi yang Disarankan: Periksa alamat MAC BSSID titik akses untuk memastikan jaringan asli. Terapkan validasi kondisi perangkat untuk memblokir koneksi ke jaringan terbuka, dan wajibkan hotspot seluler untuk pekerjaan sensitif.