Nama: _____ Tanggal: _____ Nilai: _____

Dark Web vs. Deep Web: Keamanan & Perbedaannya

Pengindeksan mesin pencari, basis data deep web, onion routing Tor, anonimitas jaringan dan risikonya

GAMBARAN PEMBELAJARAN DARK WEB VS DEEP WEB

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 perbedaan antara Deep Web dan Dark Web. Anda akan mempelajari basis data tak terindeks, Onion Routing di browser Tor, domain kriptografis .onion, dan risiko keamanan anonimitas.

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/dark-web-vs-deep-web/

Peta Belajar Strategi Deep & Dark Web Anda

- Bandingkan deep web (basis data tak terindeks) dengan dark web (layanan onion).
- Pahami cara Onion Routing mengenkripsi dan meneruskan lalu lintas jaringan.
- Nilai risiko keamanan saat mengakses situs Tor yang belum terverifikasi.
- Terapkan gateway aman dan kebijakan sandbox untuk penelusuran intelijen ancaman.
- Analisis format alamat kriptografis domain layanan onion.

PETUNJUK PANDUAN DEEP & DARK WEB

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 privasi deep web dan dark web. Akhiri dengan aktivitas bonus Berpikir Cepat.

BASIS DATA DEEP WEB VS PERUTEAN ONION DARK WEB (PENGANTAR)

Deep web terdiri dari halaman tak terindeks di balik kata sandi dan login, seperti email pribadi atau portal bank perusahaan. Dark web adalah bagian dari deep web yang sengaja disembunyikan dan hanya bisa diakses secara anonim dengan browser khusus (seperti Tor) dan jaringan onion.

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

Pos 1: Tantangan Pilihan Ganda

1. Apa yang membedakan deep web dari surface web?

- A. Halaman deep web tidak diindeks mesin pencari publik
- B. Lalu lintas deep web ilegal dan dipantau penegak hukum
- C. Situs deep web memerlukan browser khusus seperti Tor
- D. Halaman deep web selalu dimuat lebih cepat daripada halaman surface web

2. Bagaimana dark web diakses?

- A. Lewat browser khusus yang memakai jaringan perutean onion
- B. Dengan mengatur DNS khusus di router biasa
- C. Lewat konsol pencarian surface web khusus undangan
- D. Dengan mencari lewat mesin pencari biasa seperti Google

3. Struktur apa yang membentuk bagian terbesar deep web?

- A. Basis data pengguna dan akun pribadi yang dilindungi kata sandi
- B. Forum pasar gelap yang memperdagangkan barang ilegal
- C. Protokol berbagi berkas peer-to-peer tanpa enkripsi
- D. Basis data cache mesin pencari publik

4. Apa yang dilakukan Onion Routing terhadap lalu lintas jaringan?

- A. Mengenkripsi paket dan merutekannya lewat beberapa relai
- B. Mempercepat unduhan dengan melewati node ISP
- C. Memetakan nomor seri perangkat ke catatan IP
- D. Menghapus cookie browser setiap kali mengklik

5. Akhiran domain mana yang khusus dipakai di jaringan Tor?

- A. Ekstensi tingkat atas kriptografis .onion
- B. Ekstensi komersial .com yang mapan
- C. Ekstensi blockchain terdesentralisasi Web3 .eth
- D. Ekstensi kode negara .ai untuk teknologi

Pos 2: Tantangan Benar atau Salah

6 Pertanyaan 6

6. Deep web dan dark web merujuk pada segmen jaringan yang sama.

○ Benar ○ Salah

7 Pertanyaan 7

7. Portal intranet perusahaan termasuk deep web.

○ Benar ○ Salah

8 Pertanyaan 8

8. Perutean onion mendekripsi paket data sepenuhnya di setiap node transit.

○ Benar ○ Salah

9 Pertanyaan 9

9. Mengakses dark web membuat perangkat berisiko tinggi terkena malware.

○ Benar ○ Salah

10 Pertanyaan 10

10. Mesin pencari web biasa menjelajahi dan mengindeks situs onion.

○ 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. Portal bank pribadi berada di segmen tak terindeks, yaitu _____ .
2. Node Tor khusus menampung layanan tersembunyi di _____ .
3. Situs web Tor memakai ekstensi tingkat atas kriptografis _____ .
4. Jalur lalu lintas terenkripsi berlapis disebut _____ .
5. Mesin pencari permukaan menjelajahi halaman yang secara publik _____ .
6. Jaringan onion mengenkripsi IP klien untuk menjaga _____ .

BANK KATA KOSAKATA

ANONIMITAS | BASIS DATA | DARK WEB | DEEP WEB | GERBANG MASUK | ONION | ROUTING | TERINDEKS

Tulis jawaban Anda di sini:

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

Pos 4: Pencocokan Konsep Keamanan

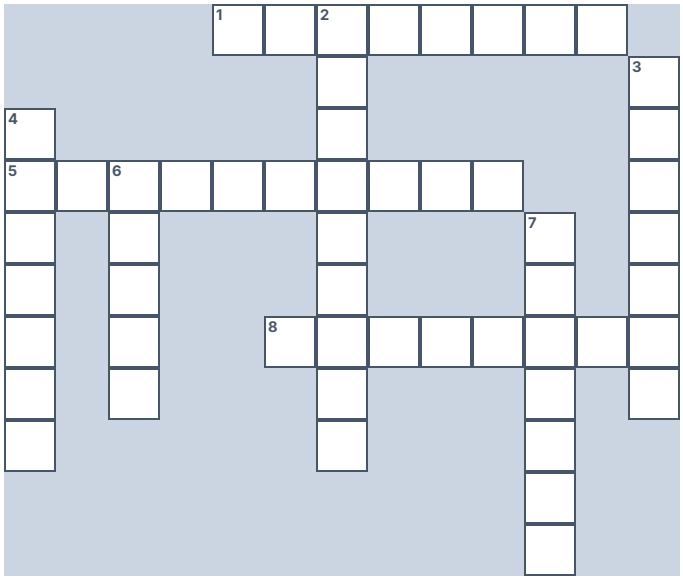
MENCOCOKKAN DEFINISI

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

☐	1. Segmen Deep Web	**A**	Segmen jaringan terenkripsi yang hanya bisa diakses lewat browser khusus.
☐	2. Portal Dark Web	**B**	Mengenkripsi data berlapis dan meneruskannya lewat tiga node.
☐	3. Ekstensi Onion	**C**	Penyimpanan backend aman berisi catatan sistem tak terindeks.
☐	4. Perutean Tor	**D**	Akhiran domain tingkat atas kriptografis yang dipakai di jaringan Tor.
☐	5. Halaman Terindeks	**E**	Node titik masuk untuk mengakses jaringan Tor.
☐	6. Anonimitas Pengguna	**F**	Konten surface web yang terhimpun dan dapat dicari di Google.
☐	7. Basis Data Pribadi	**G**	Menyembunyikan alamat IP publik klien dari server.
☐	8. Gerbang Masuk	**H**	Konten web tak terindeks seperti login pribadi, email, dan catatan basis data.

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. Penyimpanan catatan aman yang tidak dapat ditemukan mesin pencari (8)

5. Hal yang dijaga jaringan onion dengan menyembunyikan IP (10)

8. Pengiriman lalu lintas terenkripsi berlapis disebut ... onion (8)

PETUNJUK MENURUN

2. Syarat agar halaman dapat ditemukan mesin pencari biasa (9)

3. Node pertama yang dilewati lalu lintas saat masuk jaringan Tor (7)

4. Bagian tersembunyi yang hanya bisa diakses dengan browser khusus (7)

6. Domain tingkat atas kriptografis yang dipakai situs Tor (5)

7. Bagian web tak terindeks tempat perbankan online dan akun pribadi (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: Penyimpanan catatan aman yang tidak dapat ditemukan mesin pencari (8 huruf):

5 mendatar: Hal yang dijaga jaringan onion dengan menyembunyikan IP (10 huruf):

8 mendatar: Pengiriman lalu lintas terenkripsi berlapis disebut ... onion (8 huruf):

PETUNJUK MENURUN

2 menurun: Syarat agar halaman dapat ditemukan mesin pencari biasa (9 huruf):

3 menurun: Node pertama yang dilewati lalu lintas saat masuk jaringan Tor (7 huruf):

4 menurun: Bagian tersembunyi yang hanya bisa diakses dengan browser khusus (7 huruf):

6 menurun: Domain tingkat atas kriptografis yang dipakai situs Tor (5 huruf):

7 menurun: Bagian web tak terindeks tempat perbankan online dan akun pribadi (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.

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

DAFTAR KOSAKATA

DEEPWEB DARKWEB ONION PERUTEAN TERINDEKS ANONIMITAS
DATABASE GERBANG

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. DEEPWEB
B. DARKWEB
C. ONION
D. PERUTEAN
E. TERINDEKS
F. ANONIMITAS
G. DATABASE
H. GERBANG

DEFINISI & KOLOM PENCOCOKAN

1. Hal yang dijaga jaringan onion dengan menyembunyikan IP.
2. Penyimpanan catatan aman yang tidak dapat ditemukan mesin pencari.
3. Pengiriman lalu lintas terenkripsi berlapis disebut ... onion.
4. Bagian web tak terindeks tempat perbankan online dan akun pribadi.
5. Bagian tersembunyi yang hanya bisa diakses dengan browser khusus.
6. Domain tingkat atas kriptografis yang dipakai situs Tor.
7. Node pertama yang dilewati lalu lintas saat masuk jaringan Tor.
8. Syarat agar halaman dapat ditemukan mesin pencari biasa.

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. **PEDWBEE** _____
2. **ONOIN** _____
3. **TDNEESIKR** _____
4. **ASEABDAT** _____
5. **WBKRDEA** _____
6. **ANUEPTER** _____
7. **NNAIMTASIO** _____
8. **EBGGNAR** _____

Aktivitas Bonus: Berpikir Cepat

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

1	Alasan menjauhi dark web			
2	Hal yang tidak bisa ditemukan mesin pencari			
3	Perangkat yang bisa diretas			
4	Alasan sah memakai Tor			
5	Alasan memperbarui perangkat lunak			
6	Tanda bahaya dalam email			
7	Barang ilegal yang dijual di dark web			
8	Orang yang bisa dimintai bantuan TI			
9	Kebiasaan aman yang bisa dimulai hari ini			
10	Hal yang dilakukan setelah kebocoran data			
11	Hal yang termasuk deep web			
12	Situs yang Anda pakai dengan login			
13	Kata yang berkaitan dengan anonimitas			
14	Informasi yang tidak boleh dibagikan			
15	Hal yang ada 'di bawah permukaan'			

Pos 8: Studi Kasus Keamanan Siber

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

STUDI KASUS 1: MENGIDENTIFIKASI KEBOCORAN DATA



Skenario: Audit keamanan perusahaan menemukan bahwa catatan basis data klien yang sensitif diperdagangkan di pasar onion. Data tersebut tidak terindeks di Google.

Pertanyaan Diskusi: Jelaskan segmen web mana yang terlibat dan bagaimana kebocoran ini terjadi.

STUDI KASUS 2: ANONIMITAS VS. RISIKO MALWARE



Skenario: Seorang analis ingin memeriksa umpan intelijen ancaman di situs Tor. Ia mengunduh browser Tor dan membuka situs tersebut.

Pertanyaan Diskusi: Nilai manfaat anonimitasnya dan uraikan langkah mitigasi malware.

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

20	15	18		13	5	14	25	5	13	2	21	14	25	9	11	1	14

1	12	1	13	1	20		9	16		1	14	4	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 deep web?

Deep web terdiri dari semua halaman yang tidak dapat diindeks mesin pencari, termasuk perbankan online, basis data email, dan jurnal berbayar.

Q2: Apa itu dark web?

Dark web adalah bagian kecil deep web yang sengaja disembunyikan dan hanya bisa diakses lewat browser khusus dengan jaringan onion.

Q3: Bagaimana mesin pencari mengindeks halaman?

Mesin pencari menjalankan program otomatis (spider) yang mengikuti tautan publik dan mengindeks halaman yang tidak memblokir penelusuran lewat direktif robot.

Q4: Mengapa perbankan online termasuk deep web?

Portal perbankan berada di balik login dan kata sandi, sehingga mesin pencari publik tidak bisa mengindeks halaman rekening.

Q5: Apa itu Onion Routing di browser Tor?

Onion routing adalah metode transmisi yang mengenkripsi lalu lintas berlapis dan meneruskannya lewat beberapa relai untuk menyamarkan alamat IP pengguna.

Pos 10: FAQ Dasar Keamanan Siber (Bagian B)

Pelajari pertanyaan dan jawaban umum tentang cara mengurangi ancaman online.

Q6: Apakah mengakses dark web ilegal?

Tidak. Mengakses dark web legal di sebagian besar negara, tetapi terlibat di pasar ilegal atau kejahatan siber dilarang.

Q7: Mengapa situs dark web lambat dimuat?

Lalu lintas dirutekan dan didekripsi lewat setidaknya tiga relai global (masuk, tengah, keluar), sehingga latensi bertambah.

Q8: Apa arti akhiran domain .onion?

Akhiran domain tingkat atas khusus di jaringan Tor yang menunjuk ke alamat hasil kriptografi, bukan ke server DNS biasa.

Q9: Apa risiko tautan dark web?

Situsnya tidak disaring keamanannya, sehingga pengguna berisiko tinggi terkena malware, skrip phishing, dan penipuan transaksi.

Q10: Siapa pencipta protokol perutean jaringan Tor?

Teknologi ini awalnya dikembangkan U.S. Naval Research Laboratory pada 1990-an untuk melindungi komunikasi pemerintah.

Pos 10: FAQ Lanjutan Keamanan (Bagian C)

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

Q1: Bagaimana node perantara melindungi anonimitas Tor?

Setiap node hanya mendekripsi satu lapisan data perutean, sehingga hanya tahu lompatan sebelum dan sesudahnya, tidak pernah sumber dan tujuan sekaligus.

Q2: Apa peran exit node?

Exit node mendekripsi lapisan enkripsi terakhir dan mengirim lalu lintas ke server tujuan publik atau server onion.

Q3: Apa itu gateway bridge Tor?

Bridge adalah relai masuk Tor yang tidak tercantum untuk menembus blokir ISP dan sensor di wilayah yang membatasi browser Tor.

Q4: Bagaimana pelaku dark web memanfaatkan mata uang kripto?

Pelaku memakai mata uang kripto anonim untuk bertransaksi di pasar gelap, menghindari pemeriksaan transaksi perbankan biasa.

Q5: Mengapa mesin pencari biasa tidak bisa menelusuri basis data deep web?

Crawler tidak bisa memasukkan kredensial login, menyelesaikan CAPTCHA, atau menjalankan kueri SQL backend yang diperlukan untuk mengakses basis data deep web.

Pos 10: FAQ Lanjutan Keamanan (Bagian D)

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

Q6: Apa itu server direktori di jaringan Tor?

Server tepercaya yang menyimpan daftar relai masuk, tengah, dan keluar yang aktif untuk dipakai klien menyusun jalur perutean.

Q7: Bagaimana pelaku jahat menyadap lewat exit node?

Operator exit node nakal dapat menyadap lalu lintas HTTP tanpa enkripsi saat keluar dari jaringan Tor, lalu mencuri nama pengguna dan cookie.

Q8: Apa beda Tor dan I2P?

Tor memakai direktori relai terpusat dan exit node untuk akses web publik, sedangkan I2P memakai struktur peer-to-peer terdesentralisasi untuk hosting internal.

Q9: Bagaimana penegak hukum melacak pasar dark web?

Aparat memakai analisis blockchain, melacak lokasi fisik server, dan menjalankan operasi penyamaran untuk mengidentifikasi operator.

Q10: Bagaimana kebocoran DNS membahayakan anonimitas klien?

Kebocoran DNS terjadi saat kueri DNS browser dikirim langsung lewat ISP lokal, bukan lewat jaringan Tor yang terenkripsi.

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

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

1. WAWASAN KEAMANAN

Deep web jauh lebih besar daripada surface web yang dapat dicari, karena sebagian besar kontennya berada di balik login dan database.

2. WAWASAN KEAMANAN

Dark web adalah bagian kecil dari deep web yang sengaja disembunyikan, dan diakses dengan alat seperti Tor.

3. WAWASAN KEAMANAN

Perutean Tor mengenkripsi paket data tiga kali dan mengupas lapisan enkripsi seperti bawang di setiap node relai.

4. WAWASAN KEAMANAN

Tor berawal dari proyek onion routing yang dijalankan U.S. Naval Research Lab, dan kodenya dirilis sebagai perangkat lunak bebas. [1]

5. WAWASAN KEAMANAN

Alamat onion adalah rangkaian alfanumerik 56 karakter yang dihasilkan secara kriptografis dari pasangan kunci publik.

6. WAWASAN KEAMANAN

Exit node dapat membaca lalu lintas teks biasa, jadi TLS/HTTPS tetap diperlukan di Tor untuk data sesi yang aman.

7. WAWASAN KEAMANAN

Situs intranet, drive cloud, dan basis data pribadi adalah segmen penyimpanan data terbesar di deep web.

8. WAWASAN KEAMANAN

Mesin pencari khusus seperti DuckDuckGo menjalankan portal onion untuk pencarian anonim di jaringan Tor.

9. WAWASAN KEAMANAN

Lebih dari 2 juta pengguna terhubung ke jaringan Tor setiap hari untuk menembus sensor dan menjaga privasi komunikasi.

10. WAWASAN KEAMANAN

Operasi penegak hukum global (seperti Operation Bayonet) menutup pasar gelap besar dengan menyita perangkat keras hosting.

Referensi & Sumber Teknis

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

REFERENSI AKADEMIK & INDUSTRI

[1] Tor Project. (n.d.). Why is it called Tor?
https://support.torproject.org/about/why-is-it-called-tor/

[2] Tor Project. (n.d.). How do Onion Services work?
https://community.torproject.org/onion-services/overview/

[3] Tor Project. (n.d.). Users – Tor Metrics.
https://metrics.torproject.org/userstats-relay-country.html

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

[5] 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

Kunci Jawaban: Pos 1 - Pilihan Ganda

1 **Pengindeksan Pencarian** DEEP WEB — Jawaban Benar: A

CATATAN PENGAJAR

Halaman deep web berada di balik login dan basis data, sehingga spider mesin pencari tidak bisa menelusurinya.

2 **Akses Tor** DARK WEB — Jawaban Benar: A

CATATAN PENGAJAR

Dark web terdiri dari layanan onion tersembunyi yang hanya bisa diakses lewat browser seperti Tor.

3 **Basis Data Deep Web** BASIS DATA — Jawaban Benar: A

CATATAN PENGAJAR

Akun yang dilindungi kata sandi dan catatan perusahaan membentuk segmen terbesar deep web.

4 **Perutean Onion** JARINGAN TOR — Jawaban Benar: A

CATATAN PENGAJAR

Perutean onion mengenkripsi paket data berlapis dan meneruskannya lewat beberapa node demi anonimitas.

5 **Domain Onion** AKHIRAN — Jawaban Benar: A

CATATAN PENGAJAR

Akhiran domain kriptografis.onion merutekan lalu lintas secara internal di Tor tanpa DNS publik.

Kunci Jawaban: Pos 2 - Benar atau Salah

6 **Segmen Web** STRUKTUR — Jawaban Benar: Salah

CATATAN PENGAJAR

Deep web mencakup semua halaman tak terindeks, sedangkan dark web adalah subsegmen onion kecil yang terenkripsi.

7 **Intranet Perusahaan** DEEP WEB — Jawaban Benar: Benar

CATATAN PENGAJAR

Situs intranet berada di balik portal kata sandi dan tidak terindeks, sehingga termasuk deep web.

8 **Enkripsi Berlapis** RELAI — Jawaban Benar: Salah

CATATAN PENGAJAR

Relai onion hanya mendekripsi satu lapisan perutean untuk melindungi anonimitas pengguna, tidak pernah seluruh paket.

9 **Paparan Malware** ANCAMAN — Jawaban Benar: Benar

CATATAN PENGAJAR

Pasar dark web tidak punya penyaringan keamanan, sehingga risiko infeksi malware sangat tinggi.

10 **Soal 10** — Jawaban Benar: Salah

CATATAN PENGAJAR

Crawler mesin pencari biasa tidak menggunakan Tor, sehingga tidak dapat menjangkau atau mengindeks situs .onion.

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

H 1. Segmen Deep Web	A 2. Portal Dark Web	D 3. Ekstensi Onion	B 4. Perutean Tor
F 5. Halaman Terindeks	G 6. Anonimitas Pengguna	C 7. Basis Data Pribadi	E 8. Gerbang Masuk

POS 3: KUNCI ISTILAH KUNCI

1 DEEP WEB	2 DARK WEB	3 ONION	4 ROUTING
5 TERINDEKS	6 ANONIMITAS		

ALTERNATIF POS 6: KUNCI PENCOCOKAN KOSAKATA

1 F – ANONIMITAS	2 G – DATABASE	3 D – PERUTEAN	4 A – DEEPWEB
5 B – DARKWEB	6 C – ONION	7 H – GERBANG	8 E – TERINDEKS

CATATAN DISKUSI UNTUK PENGAJAR

Istilah Kunci:
Pastikan siswa dapat menjelaskan Segmen Deep Web, Portal Dark Web, dan Ekstensi Onion dengan kata-kata sendiri serta memberi contoh untuk setiap istilah.

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

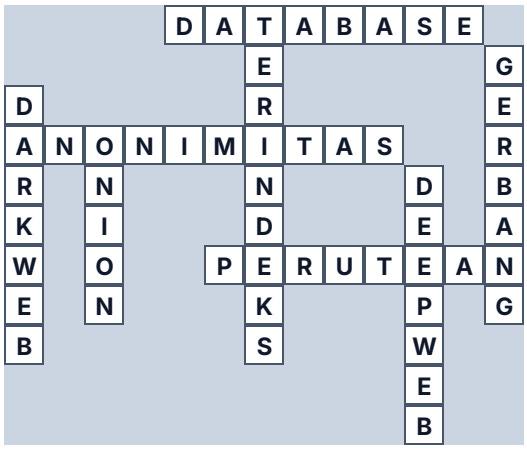
Evaluasi Sumber:
Minta siswa memeriksa setidaknya satu klaim terhadap referensi di lembar kerja, lalu diskusikan mengapa angka, harga, dan aturan dapat berubah seiring waktu.

Kunci Teka-Teki & Catatan Pengajar

JAWABAN PENCARIAN KATA

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

JAWABAN TEKA-TEKI SILANG



PANDUAN PENGAJAR UNTUK JAWABAN TEKA-TEKI SILANG

PETUNJUK MENDATAR

1 mendatar: DATABASE Penyimpanan catatan aman yang tidak dapat ditemukan mesin pencari (8 huruf)

5 mendatar: ANONIMITAS Hal yang dijaga jaringan onion dengan menyembunyikan IP (10 huruf)

8 mendatar: PERUTEAN Pengiriman lalu lintas terenkripsi berlapis disebut ... onion (8 huruf)

PETUNJUK MENURUN

2 menurun: TERINDEKS Syarat agar halaman dapat ditemukan mesin pencari biasa (9 huruf)

3 menurun: GERBANG Node pertama yang dilewati lalu lintas saat masuk jaringan Tor (7 huruf)

4 menurun: DARKWEB Bagian tersembunyi yang hanya bisa diakses dengan browser khusus (7 huruf)

6 menurun: ONION Domain tingkat atas kriptografis yang dipakai situs Tor (5 huruf)

7 menurun: DEEPWEB Bagian web tak terindeks tempat perbankan online dan akun pribadi (7 huruf)

Kunci Jawaban Kata Acak & Sandi

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

KUNCI KATA ACAK

1. PEDWBEE	DEEPWEB	5. WBKRDEA	DARKWEB
2. ONOIN	ONION	6. ANUEPTER	PERUTEAN
3. TDNEESIKR	TERINDEKS	7. NNAIMTASIO	ANONIMITAS
4. ASEABDAT	DATABASE	8. EBGGNAR	GERBANG

KUNCI TANTANGAN SANDI RAHASIA

"TOR MENYEMBUNYIKAN ALAMAT IP ANDA"

Kunci Jawaban Studi Kasus

A Studi Kasus 1: Mengidentifikasi Kebocoran Data

Jawaban Pengajar

PEDOMAN PENILAIAN

Jawaban siswa harus mencakup poin-poin berikut:

- Analisis Skenario: Audit keamanan perusahaan menemukan bahwa catatan basis data klien yang sensitif diperdagangkan di pasar onion. Data tersebut tidak terindeks di Google.
- Strategi & Solusi yang Disarankan: Segmen yang Terlibat: Basis data pribadi termasuk deep web (tak terindeks tetapi aman). Pasar yang memperdagangkan data curian berada di dark web (jaringan onion). Cara Terjadinya: Peretas menembus pertahanan server, mencuri basis data dari deep web, lalu menjualnya secara anonim di dark web agar lolos dari pelacakan aparat.

B Studi Kasus 2: Anonimitas vs. Risiko Malware

Jawaban Pengajar

PEDOMAN PENILAIAN

Jawaban siswa harus mencakup poin-poin berikut:

- Analisis Skenario: Seorang analis ingin memeriksa umpan intelijen ancaman di situs Tor. Ia mengunduh browser Tor dan membuka situs tersebut.
- Strategi & Solusi yang Disarankan: Manfaat: Tor merutekan lalu lintas lewat tiga node sehingga IP perusahaan analis tersamarkan. Risiko & Mitigasi: Tautan dark web tidak disaring reputasinya. Analis harus menjalankan Tor di mesin virtual (VM) terisolasi, mematikan JavaScript di pengaturan Tor, dan tidak mengunduh berkas apa pun demi melindungi jaringan perusahaan.