Nama: _____ Tanggal: _____ Nilai: _____

Analisis Malware & Mitigasi Ancaman Panduan

Trojan, ransomware, spyware, rootkit, sandbox virtualisasi, penahanan

GAMBARAN PEMBELAJARAN ANALISIS MALWARE

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 analisis dan pencegahan malware. Anda akan mempelajari spyware, trojan, muatan ransomware, alat rekayasa balik, perilaku rootkit, dan strategi penahanan.

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/malware/

Peta Belajar Mitigasi Malware Anda

- Bedakan jenis malware trojan, worm, dan rootkit.
- Terapkan eksekusi sandbox virtual untuk analisis kode.
- Rancang rencana penahanan dan pembersihan untuk muatan ransomware aktif.

PETUNJUK PANDUAN ANALISIS MALWARE

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 mitigasi malware. Akhiri dengan aktivitas bonus Berpikir Cepat.

ANALISIS MALWARE & PENAHANAN ANCAMAN (PENGANTAR)

Kode jahat seperti trojan, worm, dan ransomware adalah ancaman berdampak besar bagi endpoint dan server. Tim keamanan menganalisis malware di dalam sandbox virtual dan segera mengisolasi jaringan untuk menahan penyebaran muatan.

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

Pos 1: Tantangan Pilihan Ganda

1. Apa ciri khas kuda Troya (trojan)?

- A. Menyamar sebagai perangkat lunak sah agar pengguna menjalankannya
- B. Menggandakan diri otomatis di jaringan lokal
- C. Menginfeksi berkas di dalam sandbox virtual terisolasi
- D. Menyadap lalu lintas penyedia layanan internet

2. Jenis malware apa yang mengenkripsi berkas dan meminta tebusan?

- A. Ransomware
- B. Spyware
- C. Rootkit
- D. Adware

3. Apa yang dimaksud spyware?

- A. Malware yang diam-diam memantau ketikan dan aktivitas browser pengguna
- B. Kode program yang berjalan di wadah virtual sandbox
- C. Pembaruan anti-malware yang diunduh dari registri basis data
- D. Penyesuaian kecerahan layar otomatis

4. Mengapa pembuat malware memakai rootkit?

- A. Untuk menyembunyikan proses aktif dan berkas jahat dari sistem operasi
- B. Untuk mempercepat pemrosesan CPU di endpoint
- C. Untuk mencadangkan basis data ke penyimpanan cloud
- D. Untuk memperpanjang masa pakai baterai laptop

5. Apa arti sandboxing dalam analisis malware?

- A. Menjalankan berkas mencurigakan di ruang virtual terisolasi untuk mengamati perilakunya dengan aman
- B. Mencocokkan hash berkas dengan basis data ancaman
- C. Memulihkan cadangan basis data setelah penyusupan
- D. Memutus router lokal dari jaringan publik

Pos 2: Tantangan Benar atau Salah

6 Pertanyaan 6

6. Worm komputer memerlukan interaksi manusia untuk menyebar di jaringan lokal.

○ Benar ○ Salah

7 Pertanyaan 7

7. Adware selalu tidak berbahaya dan tidak melacak perilaku atau riwayat browser.

○ Benar ○ Salah

8 Pertanyaan 8

8. Memulihkan cadangan offline yang bersih memungkinkan korban mendapatkan kembali berkas terenkripsi tanpa membayar tebusan.

○ Benar ○ Salah

9 Pertanyaan 9

9. Antivirus berbasis signature dapat diandalkan untuk menghentikan malware zero-day sebelum ada signature untuknya.

○ Benar ○ Salah

10 Pertanyaan 10

10. Malware fileless menjalankan skrip jahat di memori sistem tanpa menulis berkas ke disk.

○ 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. **Malware yang menyamar sebagai program utilitas aman disebut** _____ .
2. **Muatan jahat yang mengunci sistem basis data demi uang disebut** _____ .
3. **Keylogger yang diam-diam merekam kata sandi tergolong** _____ .
4. **Bersembunyi jauh di dalam kernel sistem operasi memerlukan** _____ .
5. **Berkas mencurigakan dianalisis di ruang virtual terisolasi bernama** _____ .
6. **Menghentikan penyebaran malware aktif memerlukan tindakan jaringan segera berupa** _____ .

BANK KATA KOSAKATA

FILELESS | KUDA TROJAN | PENAHANAN | RANSOMWARE | ROOTKIT | SANDBOX | SPYWARE | WORM

Tulis jawaban Anda di sini:

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

Pos 4: Pencocokan Konsep Keamanan

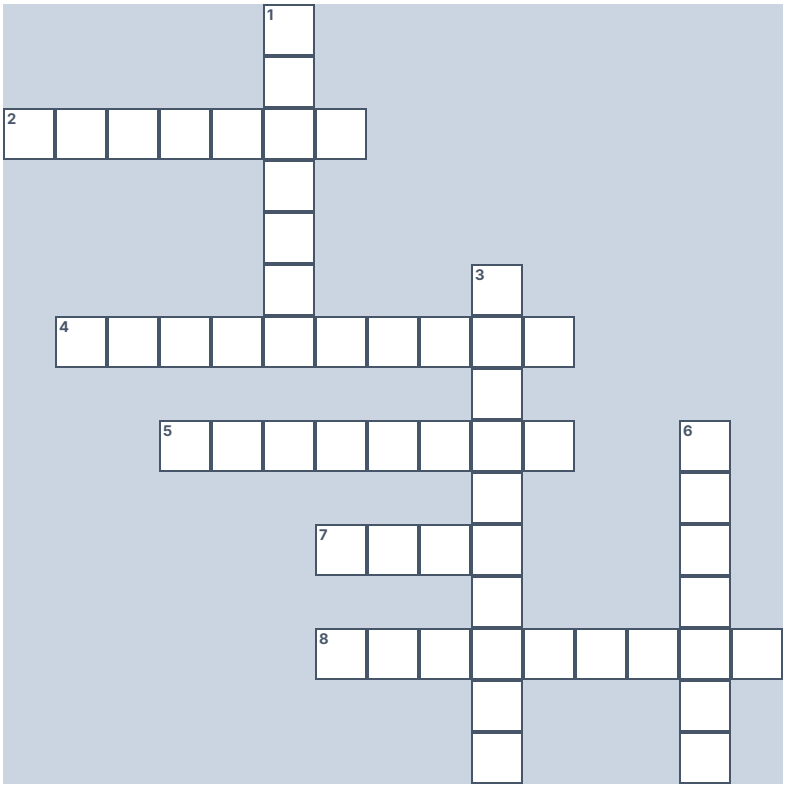
MENCOCOKKAN DEFINISI

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

☐	1. KUDA TROJAN	A	Program yang diam-diam memantau dan merekam aktivitas serta ketikan pengguna.
☐	2. RANSOMWARE	B	Malware yang berjalan langsung di RAM agar tidak terdeteksi pemindai disk.
☐	3. SPYWARE	C	Membatasi endpoint yang terinfeksi agar muatan ancaman tidak menyebar.
☐	4. ROOTKIT	D	Perangkat lunak jahat yang menyamar sebagai program utilitas yang aman atau berguna.
☐	5. SANDBOX	E	Malware yang menggandakan diri dan menyebar di jaringan tanpa tindakan manusia.
☐	6. PENAHANAN	F	Malware yang mengenkripsi penyimpanan sistem dan meminta bayaran untuk kuncinya.
☐	7. WORM	G	Lingkungan virtual terisolasi untuk menganalisis berkas jahat dengan aman.
☐	8. FILELESS	H	Malware tersembunyi di kernel sistem untuk mempertahankan kendali administratif.

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

2. Ruang virtual terisolasi untuk menganalisis berkas mencurigakan (7)

4. Malware yang menyamar sebagai program utilitas aman (10)

5. Malware yang berjalan langsung di RAM (8)

7. Malware yang menggandakan diri tanpa bantuan manusia (4)

8. Langkah segera untuk menghentikan penyebaran malware aktif (9)

PETUNJUK MENURUN

1. Malware tersembunyi jauh di dalam kernel sistem operasi (7)

3. Kode jahat yang mengunci data dan meminta tebusan (10)

6. Perangkat lunak yang diam-diam merekam ketikan dan kata sandi (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

2 mendatar: Ruang virtual terisolasi untuk menganalisis berkas mencurigakan (7 huruf):

4 mendatar: Malware yang menyamar sebagai program utilitas aman (10 huruf):

5 mendatar: Malware yang berjalan langsung di RAM (8 huruf):

7 mendatar: Malware yang menggandakan diri tanpa bantuan manusia (4 huruf):

8 mendatar: Langkah segera untuk menghentikan penyebaran malware aktif (9 huruf):

PETUNJUK MENURUN

1 menurun: Malware tersembunyi jauh di dalam kernel sistem operasi (7 huruf):

3 menurun: Kode jahat yang mengunci data dan meminta tebusan (10 huruf):

6 menurun: Perangkat lunak yang diam-diam merekam ketikan dan kata sandi (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 R P L C R I G N
R M P X Q O C O U S S T E L J
B A M B C P X O L K A Y K X T
N K R D Q M J T D I N N N K Q
A P O G M K M K Q R D S T F T
N G W C S U Q I O H B S B I W
A D S Z V D C T S Z O W F L K
H H Z D N A D Q P X X P C E U
A B A Z N T D K Y A D O D L F
N H I D R R Q M W E I R Z E S
E R A N S O M W A R E F Q S V
P F A A Q J O N R P T X Q S K
R U S D N A Y B E F S X W J A
R Z Y Y L N G I M R J M L T O
H Q Q H Z A O V G U B Y R Y B

DAFTAR KOSAKATA

KUDATROJAN RANSOMWARE SPYWARE ROOTKIT SANDBOX PENAHANAN WORM FILELESS

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. KUDATROJAN
B. RANSOMWARE
C. SPYWARE
D. ROOTKIT
E. SANDBOX
F. PENAHANAN
G. WORM
H. FILELESS

DEFINISI & KOLOM PENCOCOKAN

1. Malware tersembunyi jauh di dalam kernel sistem operasi.
2. Langkah segera untuk menghentikan penyebaran malware aktif.
3. Malware yang berjalan langsung di RAM.
4. Malware yang menggandakan diri tanpa bantuan manusia.
5. Kode jahat yang mengunci data dan meminta tebusan.
6. Perangkat lunak yang diam-diam merekam ketikan dan kata sandi.
7. Malware yang menyamar sebagai program utilitas aman.
8. Ruang virtual terisolasi untuk menganalisis berkas mencurigakan.

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. AORTUKJNAD
2. SYERAWP
3. DSBXNOA
4. MRWO
5. AMEASWORRN
6. IOKRTTO
7. APANNAEHN
8. EILSFSEL

Aktivitas Bonus: Berpikir Cepat

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

1	Tempat mengunduh aplikasi yang aman			
2	Perangkat yang bisa diretas			
3	Hal yang Anda cadangkan			
4	Tanda bahaya dalam email			
5	Tanda ponsel terkena malware			
6	Jenis malware yang Anda ketahui			
7	Jenis file yang perlu diwaspadai			
8	Cara malware masuk ke komputer			
9	Kebiasaan aman yang bisa dimulai hari ini			
10	Kata yang berkaitan dengan keamanan siber			
11	Hal yang dilakukan setelah kebocoran data			
12	Alasan memperbarui perangkat lunak			
13	Hewan atau tokoh yang namanya seperti malware			
14	Hal yang bisa dicuri malware			
15	Hal yang dilakukan jika salah klik			

Pos 8: Studi Kasus Keamanan Siber

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

STUDI KASUS 1: PENAHANAN MUATAN RANSOMWARE PERUSAHAAN



Skenario: Jaringan lokal sebuah perusahaan dibobol ransomware yang aktif. Server berkas utama mulai menampilkan ekstensi .locked. Tetapkan kebijakan penahanan.

Pertanyaan Diskusi: Uraikan langkah penahanan, dan susun rencana pemulihan protokol.

STUDI KASUS 2: INJEKSI MEMORI MALWARE FILELESS



Skenario: Seorang analis mendeteksi pola skrip mencurigakan yang berjalan langsung di RAM sistem memakai alat administratif standar, tetapi tidak ada berkas jahat di disk.

Pertanyaan Diskusi: Jelaskan strategi analisis memori, dan sebutkan alat untuk memblokir eksekusi fileless.

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

9	19	15	12	1	19	9		16	5	18	1	14	7	11	1	20

20	5	18	9	14	6	5	11	19	9		19	5	7	5	18	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 malware?

Perangkat lunak jahat buatan pelaku ancaman untuk merusak, membajak, atau mencuri data dari perangkat dan jaringan.

Q2: Apa beda virus dan worm?

Virus butuh tindakan manusia (seperti membuka berkas) untuk menyebar, sedangkan worm menyebar otomatis di jaringan.

Q3: Bagaimana trojan menginfeksi komputer?

Trojan menipu pengguna dengan menyamar sebagai program aman sambil menyembunyikan muatan jahat di dalamnya.

Q4: Apa itu ransomware?

Jenis malware yang mengenkripsi berkas di sistem sasaran dan meminta bayaran sebagai ganti kunci dekripsi. [1]

Q5: Apa itu spyware?

Perangkat lunak jahat yang diam-diam merekam ketikan, kata sandi, dan kebiasaan menjelajah lalu mengirimnya ke penyerang.

Pos 10: FAQ Dasar Keamanan Siber (Bagian B)

Pelajari pertanyaan dan jawaban umum tentang cara mengurangi ancaman online.

Q6: Apa arti sandboxing?

Menjalankan berkas mencurigakan di lingkungan virtual terisolasi yang aman untuk mengamati perilakunya tanpa membahayakan sistem produksi.

Q7: Apa itu malware fileless?

Malware yang berjalan langsung di memori sistem (RAM) memakai utilitas sah, tanpa menulis berkas ke disk agar lolos dari pemindai dasar.

Q8: Bagaimana rootkit melindungi malware?

Rootkit menyembunyikan proses dan file berbahaya, sering kali dengan menyusupi kernel sistem operasi, sehingga pemindai antivirus bisa melewatkannya.

Q9: Apa itu pemantauan perilaku dinamis?

Pemindaian antivirus yang memantau proses aktif secara real time untuk memblokir tindakan khas malware, seperti enkripsi berkas massal.

Q10: Mengapa penahanan (containment) mendesak selama respons insiden?

Mengisolasi endpoint yang dibobol mencegah muatan malware aktif menyebar ke perangkat jaringan lain.

Pos 10: FAQ Lanjutan Keamanan (Bagian C)

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

Q1: Bagaimana pembuat malware lolos dari antivirus berbasis tanda tangan?

Mereka memakai polimorfisme, mengubah hash dan struktur kode di setiap infeksi sambil mempertahankan perilaku jahatnya.

Q2: Apa risiko alat serbaguna dalam kampanye malware?

Penyerang memakai alat administratif sah (seperti PowerShell atau Sysinternals) agar berbaur dengan lalu lintas normal, sehingga sulit dideteksi.

Q3: Bagaimana process hollowing menjalankan muatan jahat?

Teknik ini menjalankan proses sistem yang sah dalam keadaan tertunda, mengganti kode memorinya dengan malware, lalu melanjutkan eksekusi.

Q4: Apa peran server Command and Control (C2)?

Server jarak jauh milik peretas untuk mengirim perintah dan muatan ke malware di mesin yang dibobol.

Q5: Mengapa keylogging sulit dideteksi?

Keylogger sederhana memakai sedikit sumber daya CPU dan menyembunyikan prosesnya di dalam utilitas ruang pengguna yang sah.

Pos 10: FAQ Lanjutan Keamanan (Bagian D)

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

Q6: Bagaimana obfuskasi kode memperlambat analisis malware?

Obfuskasi mengenkripsi atau menyusun ulang kode sumber sehingga tak terbaca oleh alat analis dan pemindai keamanan.

Q7: Apa fungsi bootkit?

Rootkit yang menginfeksi proses boot (MBR, boot sector, atau firmware UEFI), sehingga berjalan sebelum sistem operasi dimuat.

Q8: Bagaimana pemindaian heuristik mengenali ancaman zero-day?

Pemindaian ini mencari pola kode dan perintah administratif yang mencurigakan, bukan hash yang cocok di basis data.

Q9: Apa ancaman DLL hijacking?

Memaksa aplikasi sah memuat dynamic link library (DLL) jahat dengan menaruhnya di direktori aplikasi.

Q10: Bagaimana alur analisis malware otomatis memakai virtualisasi?

Berkas mencurigakan dijalankan di beberapa VM sistem operasi yang otomatis membuat log perilaku dan berkas PCAP jaringan.

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

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

1. WAWASAN KEAMANAN

Kuda Troya tetap menjadi metode infeksi yang umum karena menyembunyikan kode berbahaya di dalam program yang tampak tidak berbahaya.

2. WAWASAN KEAMANAN

IC3 milik FBI menerima lebih dari 3,600 pengaduan ransomware pada 2025, dengan kerugian yang dilaporkan melebihi $32 juta. [3]

3. WAWASAN KEAMANAN

Worm dapat menyebar dengan cepat di seluruh jaringan dengan mengeksploitasi kerentanan protokol yang belum ditambal, seperti EternalBlue pada SMB.

4. WAWASAN KEAMANAN

Malware fileless sulit dideteksi karena berjalan di memori melalui alat yang sah dan hanya meninggalkan sedikit jejak di disk.

5. WAWASAN KEAMANAN

Sandbox analisis biasanya kembali ke snapshot bersih setelah setiap eksekusi sehingga setiap pengujian dimulai dari kondisi yang diketahui.

6. WAWASAN KEAMANAN

Rootkit dapat mengubah panggilan sistem kernel dan memberi hasil diagnostik palsu kepada pemindai anti-malware.

7. WAWASAN KEAMANAN

Obfuskasi kode memakai utilitas packer untuk memampatkan dan menyembunyikan struktur biner asli malware.

8. WAWASAN KEAMANAN

Malware polimorfik mengubah kodenya, dan dengan demikian hash filenya, di setiap salinan baru untuk menghindari pemeriksaan signature.

9. WAWASAN KEAMANAN

DLL hijacking memanfaatkan urutan pencarian pustaka di sistem operasi standar seperti Windows.

10. WAWASAN KEAMANAN

Vendor keamanan menemukan sangat banyak sampel malware baru setiap hari, sehingga signature perlu terus diperbarui.

Referensi & Sumber Teknis

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

REFERENSI AKADEMIK & INDUSTRI

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

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

[3] FBI Internet Crime Complaint Center. (2026). 2025 IC3 Annual Report.
https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf

[4] FBI Internet Crime Complaint Center. (n.d.). Ransomware.
https://www.ic3.gov/CrimeInfo/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 Soal 1

Jawaban Benar: A

CATATAN PENGAJAR

Apa ciri khas kuda Troya (trojan)? → Menyamar sebagai perangkat lunak sah agar pengguna menjalankannya

2 Soal 2

Jawaban Benar: A

CATATAN PENGAJAR

Jenis malware apa yang mengenkripsi berkas dan meminta tebusan? → Ransomware [1]

3 Soal 3

Jawaban Benar: A

CATATAN PENGAJAR

Apa yang dimaksud spyware? → Malware yang diam-diam memantau ketikan dan aktivitas browser pengguna

4 Soal 4

Jawaban Benar: A

CATATAN PENGAJAR

Mengapa pembuat malware memakai rootkit? → Untuk menyembunyikan proses aktif dan berkas jahat dari sistem operasi

5 Soal 5

Jawaban Benar: A

CATATAN PENGAJAR

Apa arti sandboxing dalam analisis malware? → Menjalankan berkas mencurigakan di ruang virtual terisolasi untuk mengamati perilakunya dengan aman

Kunci Jawaban: Pos 2 - Benar atau Salah

6 Soal 6

Jawaban Benar: Salah

CATATAN PENGAJAR

Salah: worm menggandakan diri dan menyebar di jaringan tanpa tindakan apa pun dari pengguna.

7 Soal 7

Jawaban Benar: Salah

CATATAN PENGAJAR

Salah: adware tidak selalu tidak berbahaya; banyak adware melacak aktivitas penjelajahan untuk menargetkan iklan.

8 Soal 8

Jawaban Benar: Benar

CATATAN PENGAJAR

Benar: cadangan offline yang bersih memulihkan berkas terenkripsi tanpa membayar, meskipun data yang dicuri tetap bisa bocor.

9 Soal 9

Jawaban Benar: Salah

CATATAN PENGAJAR

Salah: pemindai signature memerlukan sampel yang sudah dikenal, sehingga malware zero-day yang benar-benar baru dapat lolos.

10 Soal 10

Jawaban Benar: Benar

CATATAN PENGAJAR

Malware fileless menjalankan skrip jahat di memori sistem tanpa menulis berkas ke disk.

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. KUDA TROJAN	F 2. RANSOMWARE	A 3. SPYWARE	H 4. ROOTKIT
G 5. SANDBOX	C 6. PENAHANAN	E 7. WORM	B 8. FILELESS

POS 3: KUNCI ISTILAH KUNCI

1 KUDA TROJAN	2 RANSOMWARE	3 SPYWARE	4 ROOTKIT
5 SANDBOX	6 PENAHANAN		

ALTERNATIF POS 6: KUNCI PENCOCOKAN KOSAKATA

1 D – ROOTKIT	2 F – PENAHANAN	3 H – FILELESS	4 G – WORM
5 B – RANSOMWARE	6 C – SPYWARE	7 A – KUDATROJAN	8 E – SANDBOX

CATATAN DISKUSI UNTUK PENGAJAR

Istilah Kunci:
Pastikan siswa dapat menjelaskan KUDA TROJAN, RANSOMWARE, dan SPYWARE dengan kata-kata sendiri serta memberi contoh untuk setiap istilah.

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

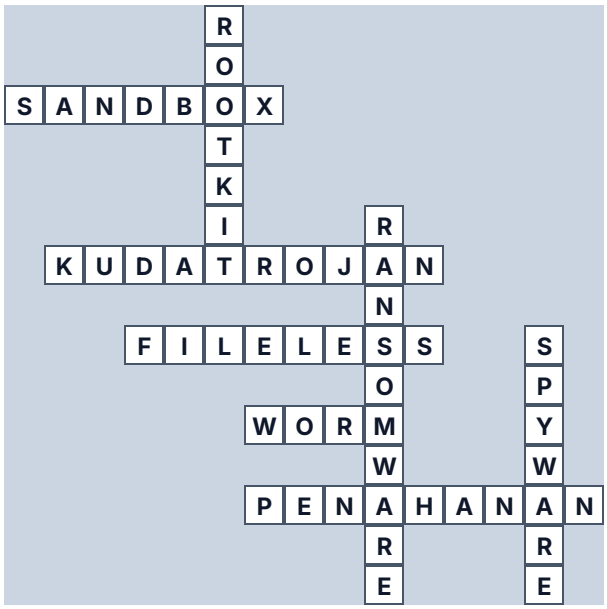
Evaluasi Sumber:
Minta siswa memeriksa setidaknya satu klaim terhadap referensi di lembar kerja, lalu diskusikan mengapa angka, harga, dan aturan dapat berubah seiring waktu.

Kunci Teka-Teki & Catatan Pengajar

JAWABAN PENCARIAN KATA

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

2 mendatar: SANDBOX Ruang virtual terisolasi untuk menganalisis berkas mencurigakan (7 huruf)

4 mendatar: KUDATROJAN Malware yang menyamar sebagai program utilitas aman (10 huruf)

5 mendatar: FILELESS Malware yang berjalan langsung di RAM (8 huruf)

7 mendatar: WORM Malware yang menggandakan diri tanpa bantuan manusia (4 huruf)

8 mendatar: PENAHANAN Langkah segera untuk menghentikan penyebaran malware aktif (9 huruf)

PETUNJUK MENURUN

1 menurun: ROOTKIT Malware tersembunyi jauh di dalam kernel sistem operasi (7 huruf)

3 menurun: RANSOMWARE Kode jahat yang mengunci data dan meminta tebusan (10 huruf)

6 menurun: SPYWARE Perangkat lunak yang diam-diam merekam ketikan dan kata sandi (7 huruf)

Kunci Jawaban Kata Acak & Sandi

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

KUNCI KATA ACAK

1.	A O R T U K J N A D	KUDATROJAN	5.	A M E A S W O R R N	RANSOMWARE
2.	S Y E R A W P	SPYWARE	6.	I O K R T T O	ROOTKIT
3.	D S B X N O A	SANDBOX	7.	A P A N N A E H N	PENAHANAN
4.	M R W O	WORM	8.	E I L S F S E L	FILELESS

KUNCI TANTANGAN SANDI RAHASIA

"ISOLASI PERANGKAT TERINFEKSI SEGERA"

Kunci Jawaban Studi Kasus

A Studi Kasus 1: Penahanan Muatan Ransomware Perusahaan

Jawaban Pengajar

PEDOMAN PENILAIAN

Jawaban siswa harus mencakup poin-poin berikut:

- Analisis Skenario: Jaringan lokal sebuah perusahaan dibobol ransomware yang aktif. Server berkas utama mulai menampilkan ekstensi .locked. Tetapkan kebijakan penahanan.
- Strategi & Solusi yang Disarankan: Putuskan semua server terdampak dari jaringan lokal. Hentikan sesi administratif yang aktif. Pulihkan berkas yang tidak terdampak dari sistem cadangan offline yang aman dan terkunci dari penulisan.

B Studi Kasus 2: Injeksi Memori Malware Fileless

Jawaban Pengajar

PEDOMAN PENILAIAN

Jawaban siswa harus mencakup poin-poin berikut:

- Analisis Skenario: Seorang analis mendeteksi pola skrip mencurigakan yang berjalan langsung di RAM sistem memakai alat administratif standar, tetapi tidak ada berkas jahat di disk.
- Strategi & Solusi yang Direkomendasikan: Isolasi endpoint yang terdampak dan ambil citra memori terlebih dahulu. Tinjau log PowerShell dan WMI, blokir skrip yang tidak disetujui dengan AppLocker, lalu lakukan reboot untuk membersihkan muatan.