TUGAS VCLASS 2

NAMA : ALI AKBAR SAID
NPM : 50421119
KELAS : 4IA03
MATERI : MALWARE FORENSIK
MATA PRAKTIKUM : FORENSIK TEKNOLOGI INFORMASI
JENIS TUGAS : PRE TEST

PILIHAN GANDA

1. Apa tujuan utama dari malware forensik?
   a. Menghapus malware dari sistem korban
   b. Mengidentifikasi jenis malware dan perilakunya
   c. Mengembalikan file yang hilang akibat malware
   d. Meningkatkan performa sistem setelah serangan
2. Manakah dari berikut ini yang termasuk teknik analisis malware?
   a. Static Analysis b. Penetration Testing c. Dynamic Analysis **d. Both a and c**
3. Apa yang dimaksud dengan "obfuscation" dalam malware?
   a. Teknik malware untuk memanipulasi jaringan korban
   b. Proses pengamanan data oleh pengguna
   c. Upaya malware untuk menyembunyikan kode atau fungsinya
   d. Metode enkripsi file oleh ransomware
4. File dengan ekstensi .dll yang mencurigakan ditemukan di sistem. Langkah pertama dalam analisis file ini adalah:
   a. Menghapus file dari sistem
   b. Membuka file dengan teks editor untuk mencari string mencurigakan
   c. Menjalankan file di sistem produksi
   d. Mengirim file ke antivirus untuk pemindaian

SOAL ESAI

5. Jelaskan perbedaan antara analisis statis dan analisis dinamis dalam malware forensik.

- **Analisis statis:** metode memeriksa malware tanpa menjalankannya, biasanya dengan menganalisis kode biner, strings, dan struktur file.
- **Analisis dinamis:** metode menganalisis malware dengan menjalankannya di lingkungan yang terkontrol untuk mengamati perilaku langsungnya, seperti komunikasi jaringan atau modifikasi sistem.

6. Sebutkan tiga alat yang sering digunakan dalam analisis malware, serta fungsinya masing-masing.

- **IDA Pro:** Untuk membedah dan menganalisis kode biner malware secara mendalam.
- **Wireshark:** Untuk memantau dan menganalisis lalu lintas jaringan yang dihasilkan oleh malware.
- **Sandbox (ex.: Cucko Sandbox):** Untuk menjalankan malware dalam lingkungan aman dan memantau perilakunya secara real-time.

7. Apa fungsi dari hashing (misalnya, menggunakan SHA-256) dalam malware forensik?

- Menghasilkan sidik jari unik dari sebuah file, sehingga file tersebut dapat diidentifikasi dan dibandingkan dengan basis data malware yang sudah dikenal atau digunakan untuk memverifikasi integritas file.

STUDI KASUS

Kasus: Anda menemukan file eksekusi yang mencurigakan di komputer korban. File ini memiliki nama legitcheck.exe dan tidak terdeteksi oleh antivirus. Setelah diunggah ke layanan analisis online, ditemukan bahwa file ini mengandung payload berbahaya.

Analisis:

8. Jelaskan langkah-langkah yang perlu Anda lakukan untuk menganalisis file ini secara lengkap, mulai dari identifikasi hingga pelaporan.

a. Identifikasi Awal:

- Periksa nama file, metadata, dan lokasi file.
- Gunakan hashing (SHA-256) untuk memeriksa apakah file sudah terdaftar dalam database malware seperti VirusTotal.

b. Analisis Statis:

- Gunakan strings atau Hex Editor untuk mencari teks atau pola mencurigakan.
- Periksa header file untuk memahami apakah file sudah dimodifikasi atau abnormal.
- Analisis file menggunakan IDA Pro atau Ghidra untuk membongkar kode.

c. Analisis Dinamis:

- Jalankan file di sandbox seperti Cuckoo Sandbox untuk mengamati aktivitasnya, termasuk perubahan file, komunikasi jaringan, dan penggunaan API.
- Gunakan Wireshark untuk menangkap dan memeriksa lalu lintas jaringan yang dihasilkan oleh file.

d. Dokumentasi dan Pelaporan:

- Catat hasil analisis, termasuk perilaku berbahaya seperti komunikasi dengan server command-and-control (C2).
- Buat laporan yang mencakup ringkasan teknis, indikator kompromi (IoC), dan rekomendasi mitigasi.

e. Tindakan Tindak Lanjut:

- Kirim laporan ke tim keamanan atau pihak terkait.
- Pastikan sistem korban diperiksa untuk tanda-tanda infeksi lebih lanjut.
- Terapkan kebijakan keamanan untuk mencegah insiden serupa di masa depan.