Malware Forensics & Reverse Engineering

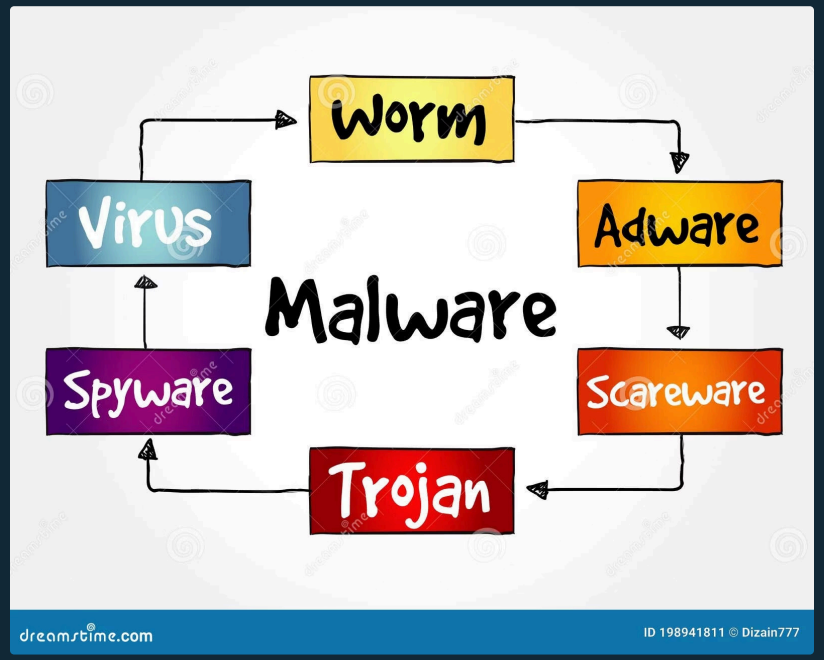
Modul Pelatihan Analisis Malware Tingkat Pemula hingga Menengah

Author: Edy Susanto | Durasi: 4–6 Jam

Tentang Modul Ini

Modul ini dirancang khusus untuk profesional keamanan siber yang ingin menguasai analisis malware secara aman dan terstruktur. Menggunakan kombinasi metode forensik dan teknik reverse engineering tingkat dasar, peserta akan mempelajari cara mengidentifikasi perilaku berbahaya dari executable, memahami struktur internal file malware, serta menghasilkan indikator kompromi (IOC) yang dapat diterapkan langsung dalam operasi deteksi dan respons insiden.

Pendekatan praktis dan hands-on memastikan peserta tidak hanya memahami teori, tetapi juga mampu menerapkan teknik analisis dalam lingkungan kerja nyata.



Tujuan Pembelajaran

Analisis Mendalam

Mampu mengidentifikasi asal, fungsi, dan dampak dari executable berbahaya menggunakan pendekatan forensik

Deteksi Proaktif

Menghasilkan IOC berkualitas tinggi untuk sistem SIEM, EDR rules, dan threat hunting

Praktik Aman

Melakukan analisis malware dalam lingkungan terisolasi dengan prosedur keamanan yang ketat

Agenda Pembelajaran

01

Konsep Inti Malware Forensics

Dasar-dasar analisis malware dan pendekatan forensik

02

Toolset Utama

Pengenalan tools industri untuk identifikasi dan reverse engineering

03

Teknik IOC Extraction

Metode menghasilkan dan mendokumentasikan artefak keamanan

04

Praktik Lab Aman

Simulasi hands-on dalam lingkungan virtual terisolasi

Konsep Inti Malware Forensics

Malware forensics adalah disiplin ilmu yang menggabungkan teknik forensik digital dengan analisis keamanan untuk memahami cara kerja perangkat lunak berbahaya. Pendekatan forensik memungkinkan analis untuk mengidentifikasi tidak hanya *apa* yang dilakukan malware, tetapi juga *bagaimana* dan *mengapa* hal tersebut terjadi.

Dalam modul ini, peserta akan mempelajari tiga pendekatan utama yang membentuk fondasi analisis malware modern: static analysis, dynamic analysis, dan sandboxing. Ketiga metode ini saling melengkapi dan memberikan gambaran komprehensif tentang perilaku dan struktur malware.

Tiga Pilar Analisis Malware

1

Static Analysis

Pemeriksaan file malware tanpa menjalankannya. Analisis meliputi struktur header PE (Portable Executable), string menarik yang tersimpan dalam file, nilai hash untuk identifikasi, entropi file untuk deteksi packing, dan signature yang mencurigakan.

- Risiko rendah: file tidak dieksekusi
- Mengungkap struktur dan metadata
- Identifikasi awal sebelum dynamic analysis

2

Dynamic Analysis

Mengamati perilaku malware saat dijalankan dalam lingkungan terisolasi. Fokus pada aktivitas proses, perubahan registry, modifikasi file system, komunikasi network, dan mekanisme persistence yang digunakan malware untuk bertahan.

- Mengungkap perilaku runtime sebenarnya
- Deteksi teknik evasion dan obfuscation
- Memerlukan lingkungan aman dan terkontrol

3

Sandboxing

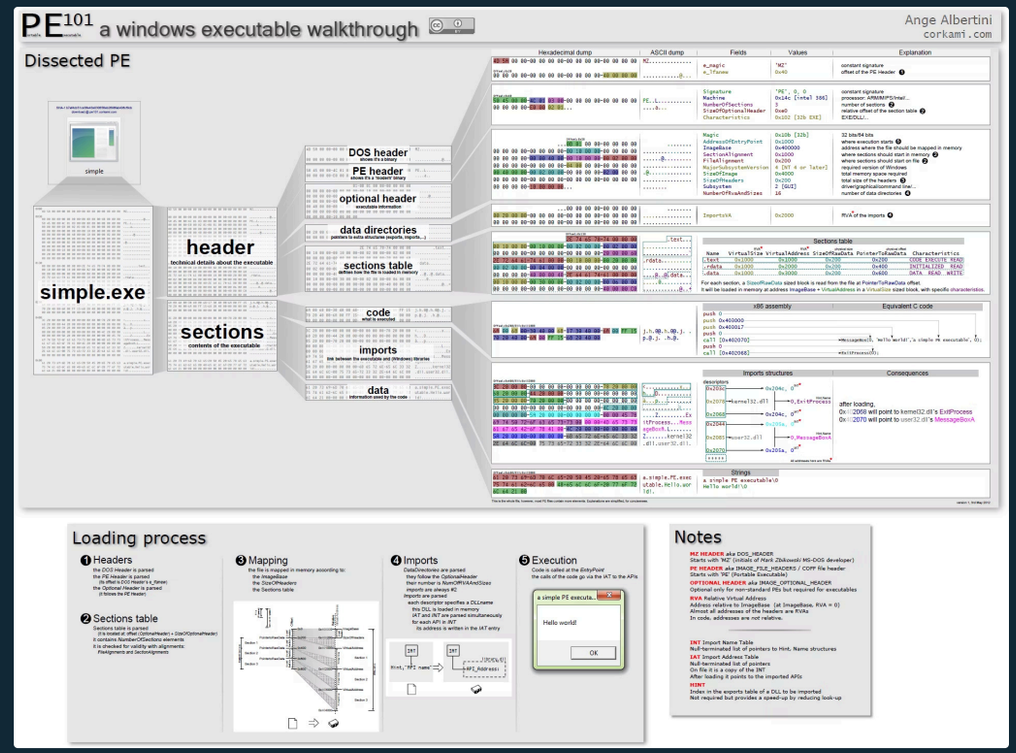
Menggunakan lingkungan virtual terkontrol untuk mengeksekusi malware secara aman dan memantau seluruh tindakan otomatis. Sandbox modern dapat mendeteksi anti-analysis techniques dan menyediakan laporan komprehensif tentang aktivitas malware.

- Automasi proses dynamic analysis
- Isolasi penuh dari sistem produksi
- Menghasilkan laporan terstruktur

Static Analysis: Membedah Tanpa Menjalankan

Komponen Analisis

- **Header PE:** Struktur file executable Windows, termasuk sections, imports, dan exports
- **String Analysis:** Ekstraksi teks untuk menemukan URL, command, API calls, atau pesan error
- **Hashing:** MD5/SHA256 untuk identifikasi dan pencarian reputasi di threat intelligence
- **Entropi File:** Deteksi packing atau enkripsi pada executable
- **Signature Matching:** Identifikasi pattern known-malware



Keuntungan Utama: Static analysis dapat dilakukan dengan aman tanpa risiko eksekusi kode berbahaya, memberikan insight awal yang berharga sebelum melangkah ke dynamic analysis.

Dynamic Analysis: Observasi Perilaku Aktif

Eksekusi Terkontrol

Malware dijalankan dalam VM atau sandbox yang terisolasi dari jaringan produksi

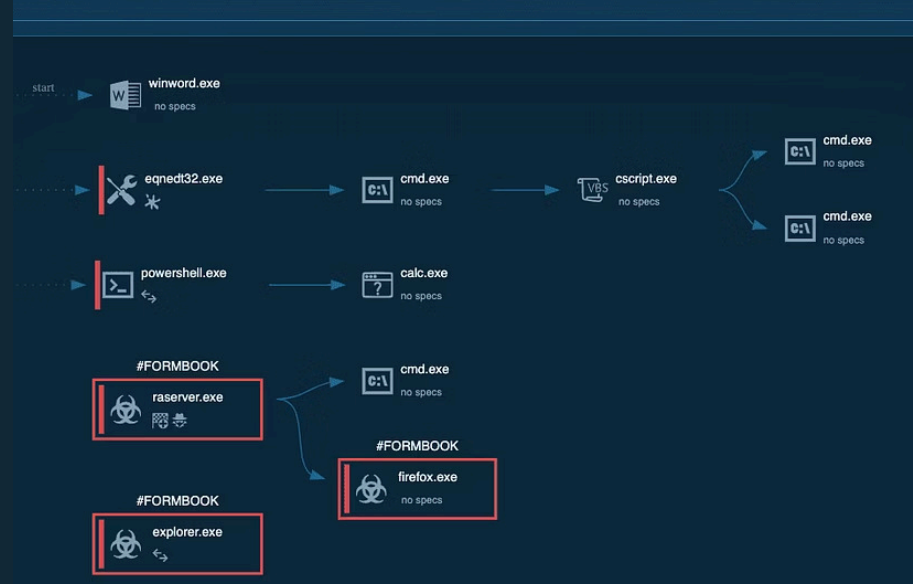
Monitoring Komprehensif

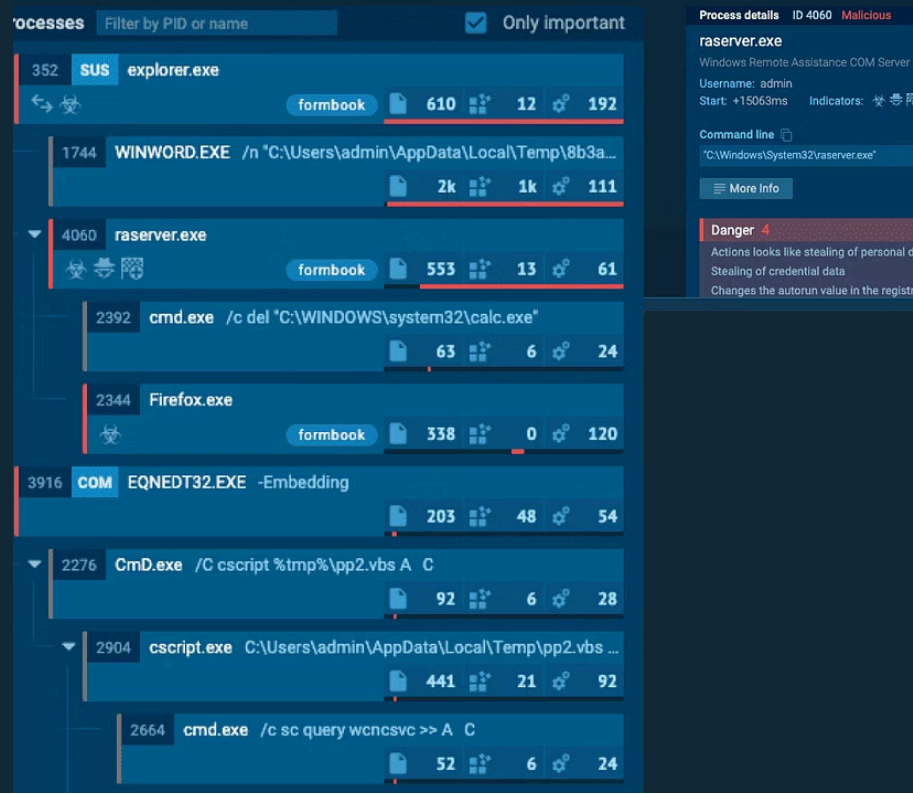
Pantau semua aktivitas: process creation, registry changes, file operations, network connections

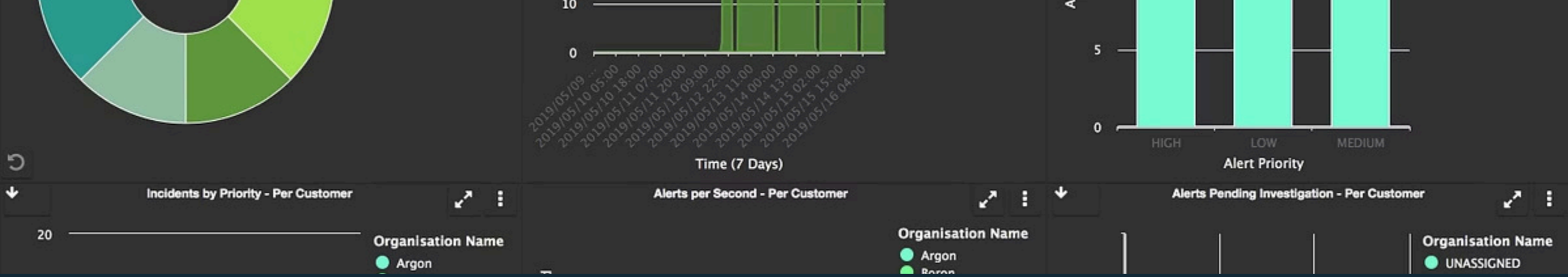
Dokumentasi Behavior

Catat persistence mechanisms, C2 communications, dan payload delivery methods

Dynamic analysis mengungkap **perilaku aktual malware** yang sering tersembunyi melalui obfuscation atau encryption dalam static analysis. Teknik ini krusial untuk memahami intent sebenarnya dari malware dan mengidentifikasi teknik evasion yang digunakan.







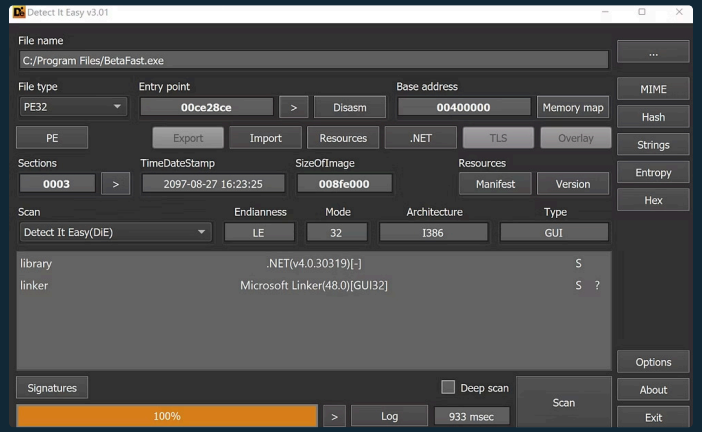
Toolset Utama untuk Analisis Malware

Profesional malware forensics menggunakan kombinasi tools specialized untuk setiap tahap analisis. Berikut adalah toolset esensial yang akan dipelajari dalam modul ini:

Tools untuk Static Analysis

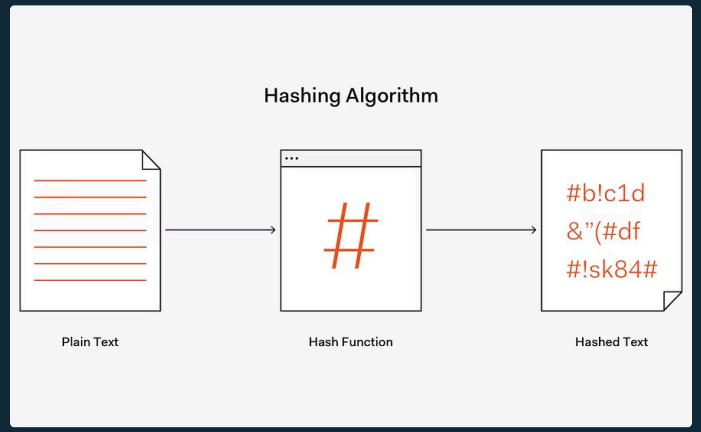
strings

Ekstraksi teks dari binary untuk mengidentifikasi URL, command-line arguments, API calls, atau pesan yang di-hardcode dalam executable



PEview / Detect It Easy

Visualisasi struktur PE file dan deteksi otomatis packer/crypter yang digunakan untuk obfuscate malware



Hashing Tools

Generasi MD5/SHA256 untuk fingerprinting file dan cross-reference dengan threat intelligence databases seperti VirusTotal

Tools untuk Dynamic Analysis & Reverse Engineering

1

Procmon (Process Monitor)

Tool Sysinternals yang powerful untuk real-time monitoring aktivitas system, termasuk registry operations, file system changes, process/thread activity, dan network operations. Sangat berguna untuk melihat jejak yang ditinggalkan malware.

2

Ghidra / IDA Free

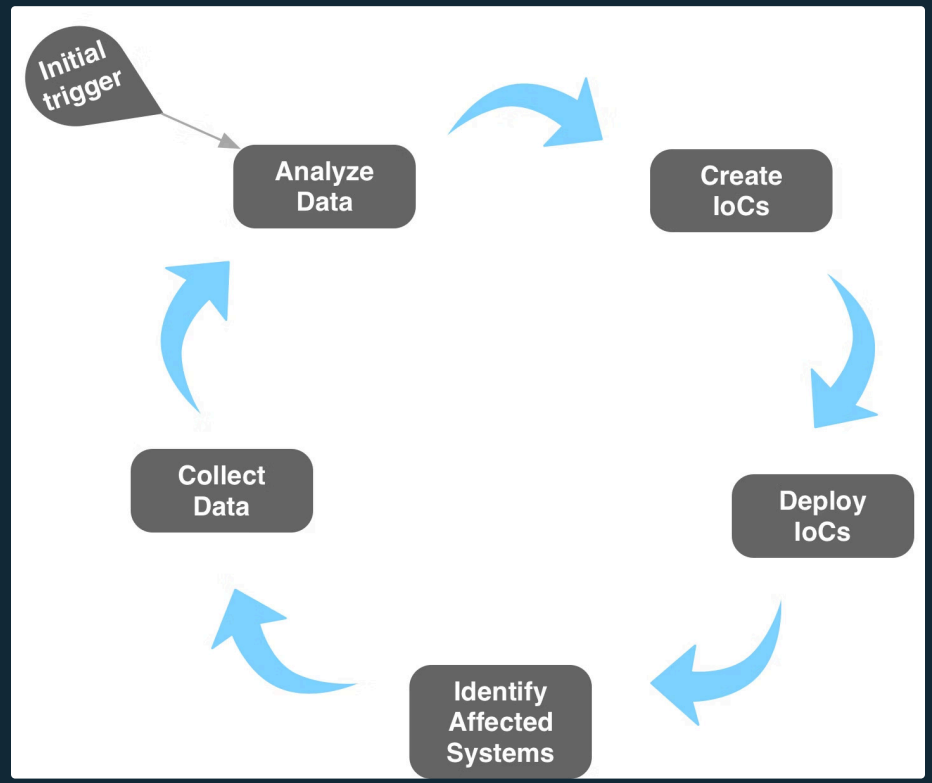
Disassembler dan decompiler tingkat enterprise yang memungkinkan analis melihat assembly code dan pseudo-code dari executable. Meskipun advance, overview dasar akan membantu peserta memahami struktur internal malware.

Teknik IOC Extraction

Indicators of Compromise (IOC) adalah artefak forensik yang tersisa setelah sistem terinfeksi malware. IOC berkualitas tinggi memungkinkan tim security untuk:

- Mendeteksi infeksi serupa di lingkungan lain
- Membuat detection rules untuk SIEM dan EDR
- Melakukan threat hunting proaktif
- Berbagi intelligence dengan komunitas security

Ekstraksi IOC yang akurat adalah **output paling berharga** dari proses analisis malware, mengubah investigasi menjadi actionable defense.



Jenis-Jenis IOC yang Diekstraksi

File System IOCs

File paths yang dimodifikasi, file baru yang dibuat, DLL yang di-drop, dan executables yang di-inject

Registry IOCs

Registry keys untuk persistence (Run, RunOnce), service entries, dan configuration values

Behavioral IOCs

Mutex names, process behavior patterns, injection techniques, dan API call sequences

Network IOCs

Domain/IP yang dihubungi, HTTP beacon patterns, C2 server addresses, dan port komunikasi

Workflow Ekstraksi IOC

Collection

Kumpulkan semua data dari static dan dynamic analysis: logs, screenshots, network captures, dan process traces

1

Normalization

2

Standarisasi format IOC (IP addresses, domain names, hash values) sesuai dengan format STIX atau OpenIOC

Validation

3

Verifikasi IOC untuk menghindari false positives dan pastikan relevansi dengan malware family

Documentation

4

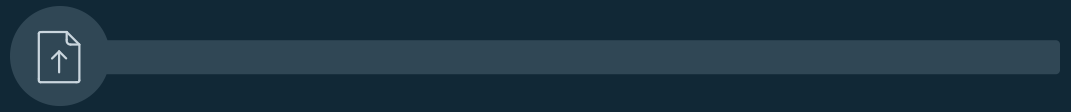
Buat IOC report dengan context, confidence level, dan recommended actions

Praktik Lab Aman: Hands-On Analysis

Komponen paling krusial dari modul ini adalah praktik langsung dalam lingkungan yang aman dan terisolasi. Peserta akan melakukan analisis malware nyata (atau sample yang di-sanitize) menggunakan metodologi profesional.

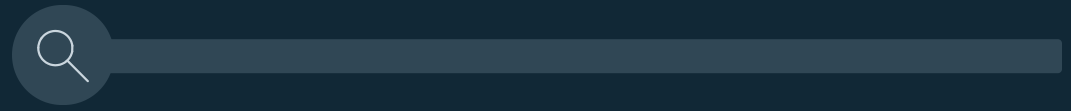
Semua aktivitas lab dilakukan dalam VM yang terisolasi dari jaringan produksi, dengan snapshot untuk recovery cepat. Pendekatan ini memastikan peserta mendapatkan pengalaman praktis tanpa risiko keamanan.

Lab Exercise 1: Static Analysis



Persiapan Sample

Download malware sample ke isolated VM. Verifikasi hash dan buat working copy untuk analysis



Initial Triage

Gunakan **strings** untuk ekstraksi text, **DIE/PEview** untuk analisis struktur PE, dan hash tools untuk fingerprinting

Identify Indicators

Cari suspicious imports (CreateRemoteThread, WriteProcessMemory), embedded URLs, atau evidence of packing/obfuscation

Document Findings

Catat semua temuan dalam lab notebook: file metadata, suspicious strings, PE characteristics, dan initial hypotheses

Lab Exercise 2: Dynamic Analysis

Persiapan Lingkungan

1. Buat snapshot VM sebelum eksekusi
2. Launch Procmon dengan filter yang sesuai
3. Setup network capture tools (Wireshark)
4. Disable network atau gunakan fake network

Eksekusi & Monitoring

1. Jalankan malware dalam VM
2. Monitor aktivitas selama 5-10 menit
3. Observasi process creation dan injection
4. Catat network connection attempts

Analisis Behavior

- **File System:** File baru, modification, deletion
- **Registry:** Persistence keys, configuration
- **Process:** Injection, hollowing, spawning
- **Network:** C2 beaconing, data exfiltration

Lab Exercise 3: IOC Extraction & Documentation

Tahap final lab adalah mengkonsolidasikan semua temuan dari static dan dynamic analysis menjadi IOC report yang actionable.

Kumpulkan Data

Agregasi hash values, file paths, registry keys, network indicators, dan mutex names dari kedua fase analisis

Format IOC

Struktur IOC dalam format yang dapat digunakan: STIX, CSV, atau format custom untuk SIEM/EDR

Validate & Test

Verifikasi IOC tidak menghasilkan false positives dan test detection rules di lab environment

Deliverable: Peserta akan menghasilkan IOC report komprehensif yang mencakup technical indicators, malware behavior summary, dan recommended detection/mitigation strategies.

Hasil Akhir Modul

3

Metodologi Analisis

Static, dynamic, dan sandboxing untuk comprehensive malware investigation

6+

Professional Tools

Hands-on experience dengan industry-standard tools untuk forensics dan reverse engineering

100%

Practical Skills

Kemampuan melakukan analisis malware end-to-end dan menghasilkan actionable IOCs

---

Setelah menyelesaikan modul ini, peserta akan memiliki **pemahaman solid** tentang konsep reverse engineering, mampu melakukan analisis malware tingkat pemula hingga menengah, dan menghasilkan IOC yang dapat diterapkan secara operasional dalam incident response dan detection engineering.

Terima Kasih

Malware Forensics & Reverse Engineering

Modul Pelatihan oleh **Edy Susanto**

> *"The best defense is understanding the offense. Through malware analysis, we turn threats into intelligence and fear into preparation."*

Untuk pertanyaan lebih lanjut atau diskusi mendalam tentang teknik malware analysis, silakan hubungi instructor.