MALWARE ANALISIS

Always The First

Definisi Malware

- Malware suatu perangkat lunak berbahaya, yang dirancang untuk merusak, mengeksploitasi, atau mengkompromikan sistem komputer atau jaringan.
- Jenis-jenis malware meliputi :
  - Worm
  - Trojan
  - Ransomware
  - Spyware
  - Adware

Tujuan Analisis Malware

- Tujuan utama analisis malware adalah
  - Mengidentifikasi jenis dan perilaku malware
  - Memahami dampaknya terhadap sistem
  - Mengembangkan metode untuk deteksi dan penghapusan
  - Mengumpulkan informasi tentang penyerang
  - Meningkatkan langkah-langkah keamanan untuk mencegah serangan di masa mendatang

Jenis-jenis Analisa Malware

- **1. Analisis Statik**

  Memeriksa malware tanpa mengeksekusinya. Ini termasuk meninjau kode, string, dan header.

- **2. Analisis Dinamik**

  Melibatkan eksekusi malware dalam lingkungan terkontrol untuk mengamati perilakunya dan dampak yang ditimbulkan.

- **3. Analisis Perilaku**

  Fokus pada bagaimana malware berinteraksi dengan sistem selama eksekusi, termasuk modifikasi file, aktivitas jaringan, dan perubahan registri.

Analisis Statik

- **Disassembly**

  Mengonversi kode mesin menjadi bahasa assembly untuk memahami alur program.
- **Analisis String**

  Mencari string yang dapat dibaca yang mungkin mengungkapkan fungsionalitas atau target.
- **Analisis File dan Header**

  Memeriksa struktur file dan metadata untuk anomali.

Teknik Analisis Statik

- **Analisis File dan Metadata**
- **ExifTool** → Untuk menampilkan metadata dan informasi lainnya yang terkandung dalam file.
  - **Command line :** `exiftool nama_file_malware`
- **Analisis Strin**g
- **Strings** → Menampilkan string ASCII atau Unicode didalam file untuk membantu menemukan petunjuk seperti URL, IP Address, atau pesan tersembunyi.
  - **Command line :** `strings nama_file_malware`

Teknik Analisis Statik

- **Disassembly**
- **Objdump** → Menyediakan disassembly dari file biner, untuk membantu analisis kode assembly dalam file malware.
  - **Command line :** `objdump -d nama_file_malware`
- **Radare2** → Tools disassembler untuk analisis lebih lanjut.
  - **Command line :** `radare2 -A nama_file_malware`

Analisis Dinamic

- **Sandboxing**

  Menjalankan malware di lingkungan yang aman untuk memantau perilakunya tanpa risiko.
- **Analisis Jaringan**

  Memantau lalu lintas jaringan untuk mengidentifikasi komunikasi dengan server perintah dan kontrol.
- **Pemantauan Proses**

  Mengamati proses sistem dan interaksinya dengan sistem operasi.

Teknik Analisis Dinamic

- Analisis dinamis melibatkan eksekusi malware di lingkungan terisolasi untuk memantau perilakunya. Karena risiko tinggi, disarankan untuk menggunakan sandbox atau mesin virtual.
- **Sandboxing dengan Cuckoo**
  - **Cuckoo Sandbox →** Kali Linux mendukung integrasi dengan Cuckoo untuk analisis dinamis. Setelah instalasi dan konfigurasi, dapat menjalankan file dalam sandbox dan memonitor aktivitas malware seperti perubahan file, registri, dan lalu lintas jaringan.
- **Pemantauan Proses dan Sistem**
  - **Sysdig →** Digunakan untuk memonitor aktivitas sistem selama eksekusi malware. Sysdig dapat merekam semua kejadian dalam sistem, seperti penggunaan file, jaringan, dan proses.
  - **Command line :** `sysdig`

Teknik Analisis Dinamic

- **Strace →** Untuk memonitor sistem call yang dilakukan oleh program. Strace memungkinkan melihat bagaimana malware berinteraksi dengan sistem operasi.
  - **Command line :** `strace -o output.txt ./nama_file_malware`
- **Analisis Jaringan**
- Wireshark: Alat penganalisa jaringan untuk menangkap dan menganalisis lalu lintas jaringan. Ini berguna untuk mengidentifikasi komunikasi jaringan yang dilakukan oleh malware.
- **Tcpdump →** Tools Alternatif untuk Wireshark didalam menganalisis jaringan.
  - **Command line :** `tcpdump -i eth0 -w capture.pcap`

Tools Analisis Malware

- **IDA Pro**

  Disassembler yang bagus untuk reverse engineering.
- **OllyDbg**

  Debugger tingkat assembler untuk aplikasi Windows.
- **Wireshark**

  Analyzer protokol jaringan untuk capture paket.
- **Cuckoo Sandbox**

  Sistem analisis malware otomatis.
- **VirusTotal**

  Layanan untuk memindai file dan URL untuk malware.

Tools Analisis Malware Tambahan

- **Binwalk →** Tools untuk mengekstrak file terkompresi atau file yang tersembunyi dalam malware, khususnya dalam firmware atau file yang memiliki banyak jenis data.
  - **Command line :** `binwalk -e nama_file_malware`
- **YARA →** Tools yang digunakan untuk membuat aturan mendeteksi malware berdasarkan pola dalam file biner. Teknik membuat aturan YARA untuk mendeteksi karakteristik malware dan jalankan dengan perintah:
  - **Command line :** `yara -r rules.yar nama_file_malware`
- **Volatility →** Volatility digunakan untuk menganalisis image memori dan digunakan untuk menemukan proses atau jaringan yang aktif dan terinfeksi.

Single Degree Program

S2 - Sistem Informasi (M.Kom.)
S1 - Sistem Komputer (S.Kom.)
S1 - Sistem Informasi (S.Kom.)
S1 - Teknologi Informasi (S.Kom.)
S1 - Bisnis Digital (S.Bns.)
D3 - Manajemen Informatika (A.Md.Kom.)

Dual Degree International Program

S1 - Sistem Informasi (S.Kom., B.IT.)
(collaboration with HELP University)
S1 - Bisnis Digital (S.Bns., B.M.)
(collaboration with DNUI University)

Dual Degree National Program

S1 - Sistem Informasi (S.Kom., S.Ds.)
(collaboration with Universitas Teknologi Bandung)

www.stikom-bali.ac.id info@stikom-bali.ac.id (0361) 244445

STIKOMERS TV STIKOM Bali @stikombali

Always The First