Modul 1: Pengantar Digital Forensik & Incident Response

Deskripsi Modul:

Modul ini memperkenalkan konsep dasar forensik digital dan bagaimana proses incident response dilakukan dalam skenario nyata.

Topik Bahasan:

- Definisi dan peran Digital Forensics dalam keamanan siber
- Perbedaan antara DFIR dan Incident Handling
- Proses umum: Identifikasi, Akuisisi, Analisis, Pelaporan
- Tools pengantar: Autopsy, FTK Imager, Volatility, Wireshark

Latihan Praktik:

1. Studi kasus insiden malware sederhana.
2. Analisis log sistem untuk mendeteksi jejak digital.
3. Gunakan Wireshark untuk melihat komunikasi HTTP mencurigakan.

Tools yang Disarankan:

- Autopsy (https://www.sleuthkit.org/autopsy/)
- FTK Imager (https://accessdata.com/product-download/ftk-imager-version-4-2)
- Volatility Framework (https://www.volatilityfoundation.org/)
- Wireshark (https://www.wireshark.org/)

Referensi Tambahan:

- NIST SP 800-86: Guide to Integrating Forensic Techniques into Incident Response
- SANS DFIR Posters: https://www.sans.org/posters/

Tujuan Pembelajaran:

- Memahami dasar-dasar digital forensik

- Mampu mengidentifikasi langkah-langkah awal penanganan insiden

- Mengenali tool dasar yang umum digunakan dalam investigasi