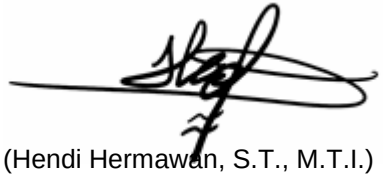
RENCANA TUGAS MAHASISWA (RTM)
PROGRAM STUDI INFORMATIKA
FAKULTAS TEKNOLOGI DAN DESAIN

SPT-I/02/BPP-LSE/POB-01/F-02

Issue/Revisi : R1

Mata Kuliah	Cyber Security	Tanggal	04 Agustus 2025
Kode MK	INF309	Rumpun MK	MKWP
Bobot (sks)	T (Teori) : 2 P (Praktik/Praktikum) : -	Semester	5
Dosen Pengembang RPS,  (Hendi Hermawan, S.T., M.T.I.)	Koordinator Keilmuan,  (Mohammad Nasucha, ST, MSc, Ph.D)	Kepala Program Studi,  (Dr. Ida Nurhaida, M.T)	Dekan  (Danto Sukmajati, ST, MSc, Ph.D)

NOMOR TUGAS
1
BENTUK TUGAS
Unjuk kerja (diskusi, tanya jawab, rancangan proyek)
JUDUL TUGAS
Serangan Phishing Melalui Email CEO Fraud (Business Email Compromise)
SUB CAPAIAN PEMBELAJARAN MATA KULIAH

SCPMK0419	Mampu menganalisis persoalan computing serta mengidentifikasi solusi setidaknya secara konseptual yang terkait dengan keamanan siber.
SCPMK0519	Mampu menguasai konsep teoritis dalam bidang Informatika/Ilmu Komputer untuk mendukung perancangan aplikasi teknologi yang sesuai dengan kebutuhan industri dan masyarakat yang terkait dengan keamanan siber.
SCPMK0835	Mampu mengimplementasikan metode/algoritma yang sesuai dengan kebutuhan computing pengguna yang terkait dengan keamanan siber.

DESKRIPSI TUGAS

Deskripsi Kasus:
Sebuah perusahaan keuangan menerima email dari seseorang yang mengaku sebagai CEO mereka, meminta transfer dana sebesar Rp250 juta ke rekening luar negeri dengan alasan transaksi investasi mendesak. Email tersebut terlihat sah karena menggunakan nama, tanda tangan digital, dan bahasa yang biasa digunakan oleh CEO.

Permasalahan:
Setelah dilakukan investigasi, diketahui bahwa email tersebut adalah hasil serangan **Business Email Compromise (BEC)** yang memanfaatkan **spear phishing** dan celah dalam konfigurasi **SPF/DKIM/DMARC** domain email organisasi.

METODE PENGERJAAN TUGAS

Tugas Mahasiswa:

1. Identifikasi jenis serangan dan teknik yang digunakan penyerang.
2. Jelaskan kerentanan yang diaminoalkane.
3. Analisis dampak terhadap sistem organisasi.
4. Berikan langkah mitigasi yang relevan untuk mencegah serangan serupa.

BENTUK DAN FORMAT LUARAN

Laporan analisis (maks. 5 halaman, font 11, spacing 1.15). Presentasi 5 menit

INDIKATOR, KRITERIA DAN BOBOT PENILAIAN

- Ketepatan identifikasi masalah (20%)
- Kesesuaian solusi/mitigasi yang diusulkan (30%)
- Kualitas analisis dan argumentasi (30%)
- Presentasi dan format laporan (20%)
- Bobot total: 10%

JADWAL PELAKSANAAN

Minggu ke-4 sampai ke-5

LAIN-LAIN

- Plagiarisme di atas 20% akan didiskualifikasi.
- AI Detection (zerogpt.com) di atas 20% akan didiskualifikasi.

DAFTAR RUJUKAN

Cisco Networking Academy. (2023). *Endpoint Security - Scope and Sequence v1.0*. Cisco. https://www.netacad.com/courses/endpoint-security

Ciampa, M. (2022). CompTIA Security+ Guide to Network Security Fundamentals (7th ed.). Cengage Learning.

NOMOR TUGAS
2
BENTUK TUGAS
Unjuk kerja (diskusi, tanya jawab, rancangan proyek)
JUDUL TUGAS

Universitas Pembangunan Jaya	**RENCANA TUGAS MAHASISWA (RTM)** **PROGRAM STUDI INFORMATIKA** **FAKULTAS TEKNOLOGI DAN DESAIN**	**SPT-I/02/BPP-LSE/POB-01/F-02** Issue/Revisi : R1

Serangan Malware melalui USB Drive di Lingkungan Industri

SUB CAPAIAN PEMBELAJARAN MATA KULIAH

SCPMK0419	Mampu menganalisis persoalan computing serta mengidentifikasi solusi setidaknya secara konseptual yang terkait dengan keamanan siber.
SCPMK0519	Mampu menguasai konsep teoritis dalam bidang Informatika/Ilmu Komputer untuk mendukung perancangan aplikasi teknologi yang sesuai dengan kebutuhan industri dan masyarakat yang terkait dengan keamanan siber.
SCPMK0835	Mampu mengimplementasikan metode/algoritma yang sesuai dengan kebutuhan computing pengguna yang terkait dengan keamanan siber.

DESKRIPSI TUGAS

Deskripsi Kasus:
Seorang teknisi di pabrik manufaktur secara tidak sengaja menyambungkan flashdisk pribadi ke komputer kontrol sistem SCADA. Tak disangka, perangkat tersebut menyebarkan **malware** yang menyebabkan manipulasi data sensor dan berhentinya proses otomatisasi produksi selama 7 jam. Hasil audit menunjukkan bahwa malware menyebar karena tidak adanya endpoint protection dan kebijakan penggunaan removable media.

Permasalahan:
Serangan ini memanfaatkan kelalaian prosedur keamanan dan minimnya segmentasi jaringan antara komputer personal dan sistem kontrol industri.

METODE PENGERJAAN TUGAS

Tugas Mahasiswa:

1. Jelaskan bagaimana malware dapat menyebar dari USB ke sistem internal.
2. Identifikasi kesalahan sistem keamanan dan prosedur yang terjadi.
3. Evaluasi risiko dan dampaknya terhadap proses industri.
4. Susun rekomendasi kebijakan keamanan dan mitigasi teknis.

BENTUK DAN FORMAT LUARAN

Laporan analisis (maks. 5 halaman, font 11, spacing 1.15). Presentasi 5 menit

INDIKATOR, KRITERIA DAN BOBOT PENILAIAN

- Ketepatan identifikasi ancaman: 30%
- Relevansi solusi keamanan: 30%
- Kejelasan dan struktur laporan: 20%
- Orisinalitas dan argumentasi: 20%

JADWAL PELAKSANAAN

Minggu ke-12 sampai ke-13

LAIN-LAIN

- Plagiarisme di atas 20% akan didiskualifikasi.
- AI Detection (zerogpt.com) di atas 20% akan didiskualifikasi.

DAFTAR RUJUKAN

Cisco Networking Academy. (2023). *Endpoint Security - Scope and Sequence v1.0*. Cisco. https://www.netacad.com/courses/endpoint-security

Ciampa, M. (2022). CompTIA Security+ Guide to Network Security Fundamentals (7th ed.). Cengage Learning.

NOMOR TUGAS

3

BENTUK TUGAS

Unjuk kerja (diskusi, tanya jawab, rancangan proyek)

JUDUL TUGAS

Proyek Akhir: Insiden Ransomware pada Sistem Informasi Rumah Sakit

Universitas Pembangunan Jaya	**RENCANA TUGAS MAHASISWA (RTM)** **PROGRAM STUDI INFORMATIKA** **FAKULTAS TEKNOLOGI DAN DESAIN**	**SPT-I/02/BPP-LSE/POB-01/F-02** Issue/Revisi : R1

SUB CAPAIAN PEMBELAJARAN MATA KULIAH	
SCPMK0419	Mampu menganalisis persoalan computing serta mengidentifikasi solusi setidaknya secara konseptual yang terkait dengan keamanan siber.
SCPMK0519	Mampu menguasai konsep teoritis dalam bidang Informatika/Ilmu Komputer untuk mendukung perancangan aplikasi teknologi yang sesuai dengan kebutuhan industri dan masyarakat yang terkait dengan keamanan siber.
SCPMK0835	Mampu mengimplementasikan metode/algoritma yang sesuai dengan kebutuhan computing pengguna yang terkait dengan keamanan siber.

DESKRIPSI TUGAS

Latar Belakang Kasus:
Sebuah rumah sakit swasta di Indonesia mengalami gangguan sistem besar-besaran setelah serangan **ransomware** yang berhasil mengenkripsi seluruh data pasien, rekam medis, dan jadwal tindakan di server pusat. Sistem tidak dapat diakses selama lebih dari 48 jam. Penyerang meminta tebusan sebesar 5 BTC agar kunci dekripsi diberikan. Serangan diduga terjadi melalui file PDF yang dikirim melalui email palsu dari “Dinas Kesehatan”, yang dibuka oleh staf bagian administrasi.

Fakta-Fakta Teknis:

- Tidak ada sistem backup otomatis harian yang aktif.
- Tidak ada endpoint protection pada perangkat kerja staf administrasi.
- Server aplikasi menggunakan sistem operasi Windows tanpa patch keamanan terbaru.
- Tidak ada segmentasi jaringan antara komputer publik dan sistem rekam medis.

METODE PENGERJAAN TUGAS

Tugas Mahasiswa (dalam Tim/Kelompok):

1. **Analisis Kronologi Insiden:**
    - Bagaimana serangan masuk?
    - Apa yang memungkinkan malware mengenkripsi sistem utama?
2. **Identifikasi Kerentanan dan Kesalahan Prosedur:**

- Jelaskan titik-titik lemah teknis dan manajerial dalam sistem rumah sakit.

3. **Evaluasi Dampak Keamanan:**
   - Apa akibatnya secara teknis dan operasional?
   - Bagaimana pelanggaran ini berhubungan dengan prinsip CIA?
4. **Simulasi Tanggapan Insiden:**
   - Rancang prosedur tanggap insiden: isolasi, forensik, pemulihan.
   - Usulkan perbaikan kebijakan keamanan dan teknologi (teknis dan non-teknis).
5. **Presentasi Temuan:**
   - Visualisasi alur serangan dan skenario pemulihan sistem.
   - Paparkan rekomendasi kebijakan baru agar insiden serupa tidak terulang.

BENTUK DAN FORMAT LUARAN

- Laporan akhir kelompok: 6–8 halaman (Times New Roman 11, spasi 1.15)
- Slide presentasi: maksimal 10 slide
- Presentasi: 7 menit + 3 menit tanya jawab

INDIKATOR, KRITERIA DAN BOBOT PENILAIAN

- Ketepatan pemilihan solusi: 30%
- Kesesuaian solusi dengan kebutuhan pengguna: 30%
- Kualitas dokumentasi: 20%

- Orisinalitas rancangan dan argumentasi: 20%

JADWAL PELAKSANAAN

Minggu ke-14 sampai ke-15

LAIN-LAIN

- Plagiarisme di atas 20% akan didiskualifikasi.
- AI Detection (zerogpt.com) di atas 20% akan didiskualifikasi.
- Harus mencantumkan referensi dan dasar pemilihan solusi.

DAFTAR RUJUKAN

Cisco Networking Academy. (2020). Cybersecurity Operations (CyberOps) Associate v1.0 – Course Material. Cisco Press.

Ciampa, M. (2022). Security+ Guide to Network Security Fundamentals (7th ed.). Cengage Learning.