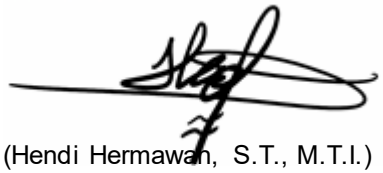
RENCANA TUGAS MAHASISWA (RTM)
PROGRAM STUDI INFORMATIKA
INF515- IT FUNDAMENTALS FOR CYBERSECURITY

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

Issue/Revisi : R1

Mata Kuliah	IT Fundamentals for Cyber Security	Tanggal	04 Agustus 2025
Kode MK	INF515	Rumpun MK	MKP
Bobot (sks)	T (Teori) : 2 P (Praktik/Praktikum) : 1	Semester	7
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
Analisis dan Identifikasi Ancaman Siber dalam Infrastruktur TI
SUB CAPAIAN PEMBELAJARAN MATA KULIAH

RENCANA TUGAS MAHASISWA (RTM)
PROGRAM STUDI INFORMATIKA
INF515- IT FUNDAMENTALS FOR CYBERSECURITY

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

Issue/Revisi : R1

SCPMK0326 - Mampu **menerapkan** pengetahuan-pengetahuan dalam ranah ***Cyber Security*** untuk memecahkan masalah.
SCPMK0819 - Mampu mengidentifikasi kebutuhan computing pengguna dengan benar, **khususnya pada ranah terkait dengan metode/algoritma yang dipilih**
SCPMK0829 - Mampu **memilih solusi** yang sesuai dengan kebutuhan pengguna, khususnya yang terkait dengan ***Cyber Security.***
SCPMK0839 - Mampu **mengimplementasikan solusi** untuk memecahkan masalah pengguna, khususnya dalam ranah ***Cyber Security.***

DESKRIPSI TUGAS

Mahasiswa diminta untuk menganalisis sebuah studi kasus insiden siber yang terjadi di organisasi nyata. Tugas ini mencakup identifikasi kerentanan, tipe serangan, dampak terhadap sistem, serta penyusunan rekomendasi langkah mitigasi awal.

METODE PENGERJAAN TUGAS

Diskusi kelompok, penelusuran referensi pustaka dan studi kasus, serta penulisan laporan individu.

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-2 sampai ke-3

LAIN-LAIN

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

Universitas Pembangunan Jaya	**RENCANA TUGAS MAHASISWA (RTM)** **PROGRAM STUDI INFORMATIKA** **INF515- IT FUNDAMENTALS FOR CYBERSECURITY**	**SPT-I/02/BPP-LSE/POB-01/F-02** Issue/Revisi : R1

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. NIST. (2020). Framework for Improving Critical Infrastructure Cybersecurity – NIST SP 800-53. United States Department of Commerce.

NOMOR TUGAS
2
BENTUK TUGAS
Unjuk kerja (diskusi, tanya jawab, rancangan proyek)
JUDUL TUGAS
Analisis Keamanan Jaringan Dasar
SUB CAPAIAN PEMBELAJARAN MATA KULIAH
SCPMK0326 - Mampu **menerapkan** pengetahuan-pengetahuan dalam ranah ***Cyber Security*** untuk memecahkan masalah. SCPMK0819 - Mampu mengidentifikasi kebutuhan computing pengguna dengan benar, **khususnya pada ranah terkait dengan metode/algoritma yang dipilih** SCPMK0829 - Mampu **memilih solusi** yang sesuai dengan kebutuhan pengguna, khususnya yang terkait dengan ***Cyber Security.*** SCPMK0839 - Mampu **mengimplementasikan solusi** untuk memecahkan masalah pengguna, khususnya dalam ranah ***Cyber Security.***
DESKRIPSI TUGAS
Mahasiswa diminta menganalisis kebutuhan keamanan jaringan pada sebuah organisasi kecil atau simulasi kasus, dengan memetakan potensi ancaman dan kebutuhan proteksi dasar.
METODE PENGERJAAN TUGAS

Universitas Pembangunan Jaya	**RENCANA TUGAS MAHASISWA (RTM)** **PROGRAM STUDI INFORMATIKA** **INF515- IT FUNDAMENTALS FOR CYBERSECURITY**	**SPT-I/02/BPP-LSE/POB-01/F-02** Issue/Revisi : R1

Individu atau kelompok kecil (maksimal 3 orang), pengumpulan dalam bentuk dokumen analisis PDF.

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-11

LAIN-LAIN

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

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.

NIST. (2020). Framework for Improving Critical Infrastructure Cybersecurity – NIST SP 800-53. United States Department of Commerce.

NOMOR TUGAS

3

BENTUK TUGAS

Unjuk kerja (diskusi, tanya jawab, rancangan proyek)

JUDUL TUGAS

Perancangan Sistem Keamanan Endpoint

SUB CAPAIAN PEMBELAJARAN MATA KULIAH

SCPMK0326 - Mampu **menerapkan** pengetahuan-pengetahuan dalam ranah ***Cyber Security*** untuk memecahkan masalah.
SCPMK0819 - Mampu mengidentifikasi kebutuhan computing pengguna dengan benar, **khususnya pada ranah terkait dengan metode/algoritma yang dipilih**
SCPMK0829 - Mampu **memilih solusi** yang sesuai dengan kebutuhan pengguna, khususnya yang terkait dengan ***Cyber Security.***
SCPMK0839 - Mampu **mengimplementasikan solusi** untuk memecahkan masalah pengguna, khususnya dalam ranah ***Cyber Security.***

DESKRIPSI TUGAS

Mahasiswa diminta merancang sistem keamanan endpoint (komputer pengguna) berdasarkan skenario kasus penggunaan di sebuah institusi, dengan memp ertimbangkan perangkat lunak dan kebijakan yang relevan.

METODE PENGERJAAN TUGAS

Kelompok (maksimal 3 orang), pengumpulan dalam bentuk dokumen desain sistem keamanan.

BENTUK DAN FORMAT LUARAN

Dokumen rencana sistem keamanan endpoint, dilengkapi dengan skema arsitektur dan kebijakan yang diusulkan.

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

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.

NIST. (2020). Framework for Improving Critical Infrastructure Cybersecurity – NIST SP 800-53. United States Department of Commerce.