RENCANA PEMBELAJARAN SEMESTER (RPS)
MATA KULIAH : CYBERSECURITY
PROGRAM STUDI PENDIDIKAN TEKNOLOGI INFORMASI
FAKULTAS TARBIYAH DAN KEGURUAN UIN AR-RANIRY BANDA ACEH

A IDENTITAS

1	Prodi	Pendidikan Teknologi Informasi
2	Kode Mata kuliah	223PTI025
3	Nama Mata kuliah	Cybersecurity
4	Semester/SKS	5 / 2 sks
5	Jenis Mata Kuliah	MK KEAHLIAN DAN KETRAMPILAN (MKK)
6	Koordinator Mata Kuliah	1321059301 | Aulia Syarif Aziz, S.Kom., M.Sc.
7	Dosen Pengampu	Mulkan Fadli, M.T

B CAPAIAN PEMBELAJARAN LULUSAN (CPL-Prodi)

1 Sikap
   a S1-Bertakwa kepada Tuhan Yang Maha Esa dan mampu menunjukkan sikap religius;
   b S2-Menjunjung tinggi nilai kemanusiaan dalam menjalankan tugas berdasarkan agama,moral, dan etika;
   c S6-Bekerja sama dan memiliki kepekaan sosial serta kepedulian terhadap masyarakat dan lingkungan;
   d S8-Menginternalisasi nilai, norma, dan etika akademik
   e S11-Responsif perkembangan teknologi informasi dalam dunia pendidikan
2 Pengetahuan
   a P1-Menguasai konsep dan prinsip didaktik-pedagogik bidang Pendidikan Teknologi Informasi untuk merencanakan, melaksanakan dan mengevaluasi pembelajaran berbasis IPTEKS yang berorientasi pada kecakapan hidup (life skills)
   b P2-Menguasai konsep teoritis serta materi pembelajaran tentang Pendidikan Teknologi Informasi yang meliputi bidang rekaya perangkat lunak (RPL), TKJ, dan Multimedia
3 Keterampilan Umum
   a KU5-Mampu mengambil keputusan secara tepat dalam konteks penyelesaian masalah di bidang keahliannya, berdasarkan hasil analisis informasi dan data
   b KU6-Mampu memelihara dan mengembangkan jaringan kerja dengan pembimbing, kolega, sejawat baik di dalam maupun di luar lembaganya
   c KU8-Mampu melakukan proses evaluasi diri terhadap kelompok kerja yang berada dibawah tanggung jawabnya, dan mampu mengelola pembelajaran secara mandiri
4 Keterampilan Khusus
   a KK1-Mampu mengidentifikasi, menganalisis dan mendefinisikan kebutuhan pengembangan ilmu teknologi Informasi dalam dunia pendidikan
   b KK2-Mampu merancang, mengimplementasi dan mengevaluasi pemanfaatan sistem informasi, pengembangan aplikasi, jaringan komputer dan pengembangan multimedia sebagai bahan ajar pada Sekolah Menengah Kejuruan (SMK) Teknologi Informasi
   c KK4-Mampu mengidentifikasi dan menganalisis masalah mutu, relevansi, atau akses pembelajaran Pendidikan Teknologi Informasi dengan mengacu pada standar dan peraturan yang berlaku
   d KK5-Mampu mengaplikasikan ilmu Pendidikan teknologi informasi untuk menghasilkan rancangan bisnis/produk yang berorientasi pasar untuk menghasilkan peluang wirausaha.

C CAPAIAN PEMBELAJARAN MATA KULIAH (CPMK)

1 Membangun dan mengevaluasi sistem cyber security dalam berbagai area, termasuk yang berkaitan dengan ragam ancaman dan kerentanan, aset dan resiko, teknologi keamanan data, teknologi keamanan jaringan, atau tata kelola cyber security
2 Menguasai teori dan konsep yang mendasari ilmu komputer.khususnya cyber security
3 Menentukan pendekatan sistem cyber security yang sesuai dengan problem yang dihadapi, memilih representasi pengetahuan dan mekanisme penalarannya

D DESKRIPSI MATA KULIAH

Mata Kuliah ini memberikan pengetahuan kepada mahasiswa mengenai cyber security yang melingkupi prinsip-prinsipnya, melakukan perencanaan, perancangan model, infrastruktur dan aplikasi cyber security.

E MATRIKS KEGIATAN PEMBELAJARAN

NO	Kemampuan akhir yang diharapkan (Sub CPMK)	Bahan Kajian/Materi Perkuliahan	Bentuk Pembelajaran			Metode Pembelajaran	Alokasi Waktu	Pengalaman Belajar Mahasiswa	Penilaian (kriteria, indikator dan bobot)	Referensi
			Luring	Daring	Blanded					
1	Mahasiswa memahami kontrak perkuliahan dan RPS yang akan dilaksanakan dalam mata kuliah keamanan komputer	• Kontrak perkuliahan • RPS • Penjelasan tugas-tugas yang akan diberikan	X			Ceramah, Diskusi dan Tanya Jawab	2 x 50 menit	• Mendapatkan penjelasan dosen tentang kontrak kuliah • Mendapatkan penjelasan tentang materi yang akan dipelajari dalam perkuliahan • Mahasiswa berdiskusi terhadap materi ajar • Mahasiswa menjawab beberapa pertanyaan yang diajukan oleh dosen dan teman sejawat	• Kriteria dan indikator penilaian adalah ketepatan dan penguasaan materi • Ketepatan menjelaskan pengertian materi yang ditanyakan; • Mampu menguasai materi yang dipelajari minimal 80%	1. Andy Taylor, David Alexander, Amanda Finch, David Sutton, Information Security Management Principles, BCS, The Chartered Institute for IT; Updated edition (June 18, 2013) 2. Handbook for Computer Security Incident Response Teams http://www.cert.org/archive/pdf/csirt-handbook.pdf
2	• Menilai persyaratan etika dan hukum penilaian keamanan dan pengujian penetrasi dan menentukan strategi untuk memenuhi persyaratan ini. • Menganalisis berbagai fase peretasan dan merekomendasikan strategi untuk menggunakan peretasan etis untuk menilai keamanan berbagai komponen sistem informasi. • Bandingkan dan bandingkan berbagai teknik peretasan dan analisis implikasi hukum peretasan. • Memeriksa berbagai kerentanan, ancaman, dan serangan terhadap sistem informasi dan merekomendasikan penanggulangannya.	• Introduction to Ethical Hacking • Footprinting and Reconnaissance	X			Ceramah, Diskusi, Praktik	2 x 50 menit	• Mahasiswa mampu menjawab soal • Mahasiswa dapat mempraktikkan footprinting	• Kriteria dan indikator penilaian adalah ketepatan dan penguasaan materi • Ketepatan menjelaskan pengertian materi yang ditanyakan; • Mampu menguasai materi yang dipelajari minimal 80%	1. Andy Taylor, David Alexander, Amanda Finch, David Sutton, Information Security Management Principles, BCS, The Chartered Institute for IT; Updated edition (June 18, 2013) 2. Handbook for Computer Security Incident Response Teams http://www.cert.org/archive/pdf/csirt-handbook.pdf 3. Sheward, mike, Hands-on Incident Response and Digital Forensics, Imprint: BCS, The Chartered Institute for IT, 2018

NO	Kemampuan akhir yang diharapkan (Sub CPMK)	Bahan Kajian/Materi Perkuliahan	Bentuk Pembelajaran			Metode Pembelajaran	Alokasi Waktu	Pengalaman Belajar Mahasiswa	Penilaian (kriteria, indikator dan bobot)	Referensi
			Luring	Daring	Blanded					
3	• Analisis berbagai fase peretasan dan rekomendasikan strategi untuk menggunakan peretasan etis untuk menilai keamanan berbagai komponen sistem informasi. • Bandingkan dan bandingkan berbagai teknik peretasan dan analisis implikasi hukum peretasan. • Memeriksa berbagai kerentanan, ancaman, dan serangan terhadap sistem informasi dan merekomendasikan penanggulangannya.	• Scanning Networks • Enumeration	X			Ceramah, Diskusi, Praktik	2 x 50 menit	• Mahasiswa dapat menjawab pertanyaan : Scanning Network dan Enumeration	• Sikap (Komunikasi dan santun) • Keaktifan dalam diskusi dan tanya jawab • Ketepatan dan kesempurnaan laporan penugasan • Bentuk penilaian Presentasi • Kriteria dan indikator penilaian adalah ketepatan dan penguasaan materi • Ketepatan menjelaskan pengertian materi yang ditanyakan; • Mampu menguasai materi yang dipelajari minimal 80%	1. Andy Taylor, David Alexander, Amanda Finch, David Sutton, Information Security Management Principles, BCS, The Chartered Institute for IT; Updated edition (June 18, 2013) 2. Handbook for Computer Security Incident Response Teams http://www.cert.org/archive/pdf/csirt-handbook.pdf 3. Sheward, mike, Hands-on Incident Response and Digital Forensics, Imprint: BCS, The Chartered Institute for IT, 2018
4	• Mempelajari cara mengidentifikasi celah keamanan di jaringan, infrastruktur komunikasi, dan sistem akhir organisasi target • Mempelajari berbagai Teknik metodologi — termasuk steganografi, serangan steganalisis, dan trek penutup — digunakan untuk menemukan kerentanan sistem dan jaringan.	• Vulneribility Analisys • System Hacking	X			Ceramah, Diskusi, Praktik	2 x 50 menit	Mahasiswa dapat menjawab pertanyaan : • Vulneribility Analisys • System Hacking	• Sikap (Komunikasi dan santun) • Keaktifan dalam diskusi dan tanya jawab • Ketepatan dan kesempurnaan laporan penugasan • Bentuk penilaian Presentasi • Kriteria dan indikator penilaian adalah ketepatan dan penguasaan materi • Ketepatan menjelaskan pengertian materi yang ditanyakan; • Mampu menguasai materi yang dipelajari minimal 80%	1. Andy Taylor, David Alexander, Amanda Finch, David Sutton, Information Security Management Principles, BCS, The Chartered Institute for IT; Updated edition (June 18, 2013) 2. Handbook for Computer Security Incident Response Teams http://www.cert.org/archive/pdf/csirt-handbook.pdf 3. Sheward, mike, Hands-on Incident Response and Digital Forensics, Imprint: BCS, The Chartered Institute for IT, 2018 4. *Aulia Syarif Aziz, Safriatullah Safriatullah, Perancangan Dan Analisis Keamanan Pada Sistem Autentikasi Terpusat Freeradius.* Jurnal of Informatics and computer sciences, Vol 7, No 2 (2021)

NO	Kemampuan akhir yang diharapkan (Sub CPMK)	Bahan Kajian/Materi Perkuliahan	Bentuk Pembelajaran			Metode Pembelajaran	Alokasi Waktu	Pengalaman Belajar Mahasiswa	Penilaian (kriteria, indikator dan bobot)	Referensi
			Luring	Daring	Blanded					
5	• Memahami materi tentang berbagai jenis malware, seperti Trojan, virus, dan worm, serta audit sistem untuk serangan malware, analisis malware, dan penanggulangan. • mempelajari tentang teknik packet-sniffing dan cara menggunakannya untuk menemukan kerentanan jaringan, serta penanggulangan untuk bertahan dari serangan sniffing	• Malware Threats • Sniffing	X			Ceramah, Diskusi, Praktik	2 x 50 menit	Mahasiswa dapat menjawab pertanyaan : • Malware Threats • Sniffing	• Ketepatan menjelaskan pengertian materi yang ditanyakan; • Mampu menguasai materi yang dipelajari minimal 80%	1. Andy Taylor, David Alexander, Amanda Finch, David Sutton, Information Security Management Principles, BCS, The Chartered Institute for IT; Updated edition (June 18, 2013) 2. Handbook for Computer Security Incident Response Teams http://www.cert.org/archive/pdf/csirt-handbook.pdf 3. Sheward, mike, Hands-on Incident Response and Digital Forensics, Imprint: BCS, The Chartered Institute for IT, 2018 4. *Aulia Syarif Aziz, Safriatullah Safriatullah, Perancangan Dan Analisis Keamanan Pada Sistem Autentikasi Terpusat Freeradius.* Jurnal of Informatics and computer sciences, Vol 7, No 2 (2021)
6	• Mempelajari konsep dan teknik rekayasa sosial, termasuk cara mengidentifikasi upaya pencurian, mengaudit kerentanan tingkat manusia, dan menyarankan penanggulangan rekayasa sosial. • Mempelajari tentang berbagai teknik serangan Denial of Service (DoS) dan Distributed DoS (DDOS), serta alat yang digunakan untuk mengaudit target dan menyusun penanggulangan dan perlindungan DoS dan DDoS.	• Social engineering • Denial of Service (DoS)	X			Ceramah, Diskusi, Praktik	2 x 50 menit	Mahasiswa dapat menjawab pertanyaan : • Social engineering • Denial of Service (DoS)	• Ketepatan menjelaskan pengertian materi yang ditanyakan; • Mampu menguasai materi yang dipelajari minimal 80%	1. Andy Taylor, David Alexander, Amanda Finch, David Sutton, Information Security Management Principles, BCS, The Chartered Institute for IT; Updated edition (June 18, 2013) 2. Handbook for Computer Security Incident Response Teams http://www.cert.org/archive/pdf/csirt-handbook.pdf 3. Sheward, mike, Hands-on Incident Response and Digital Forensics, Imprint: BCS, The Chartered Institute for IT, 2018 4. *Aulia Syarif Aziz, Safriatullah Safriatullah, Perancangan Dan Analisis Keamanan Pada Sistem Autentikasi Terpusat Freeradius.* Jurnal of Informatics and computer sciences, Vol 7, No 2 (2021)
7	• Memahami berbagai teknik pembajakan (Hijacking) yang digunakan untuk menemukan manajemen sesi tingkat jaringan, autentikasi, otorisasi, dan kelemahan kriptografi serta penanggulangan terkait. • Pengenalan ke firewall, sistem deteksi intrusi, dan teknik penghindaran honeypot; alat yang digunakan untuk mengaudit kelemahan perimeter jaringan; dan penanggulangan.	• Evading IDS, Firewalls and Honeypots • Session Hijacking	X			Ceramah, Diskusi, Praktik	2 x 50 menit	Mahasiswa dapat menjawab pertanyaan : • Evading IDS, Firewalls and Honeypots • Session Hijacking	• Sikap (Komunikasi dan santun) • Keaktifan dalam diskusi dan tanya jawab • Ketepatan dan kesempurnaan laporan penugasan • Bentuk penilaian Presentasi • Kriteria dan indikator penilaian adalah ketepatan dan penguasaan materi • Ketepatan menjelaskan pengertian materi yang ditanyakan; • Mampu menguasai materi yang dipelajari minimal 80%	1. Andy Taylor, David Alexander, Amanda Finch, David Sutton, Information Security Management Principles, BCS, The Chartered Institute for IT; Updated edition (June 18, 2013) 2. Handbook for Computer Security Incident Response Teams http://www.cert.org/archive/pdf/csirt-handbook.pdf 3. Sheward, mike, Hands-on Incident Response and Digital Forensics, Imprint: BCS, The Chartered Institute for IT, 2018 4. E.Wheeler,2011,“Security Risk Management: Building an Information Security Risk Management Program from the Ground Up”, Syngress

NO	Kemampuan akhir yang diharapkan (Sub CPMK)	Bahan Kajian/Materi Perkuliahan	Bentuk Pembelajaran			Metode Pembelajaran	Alokasi Waktu	Pengalaman Belajar Mahasiswa	Penilaian (kriteria, indikator dan bobot)	Referensi
			Luring	Daring	Blanded					
8	UTS	pt 1 s/d 7	X			ujian	2 x 50 menit	• Mahasiswa menjawab soal-soal yang diujikan secara tertulis • Mahasiswa mengumpul-kan kertas jawaban KT Mahasiswa membahas soal UTS yang diujiankan dengan berpedoman pada bahan ajar KM Membaca referensi lain yang berkaitan dengan materi ajar dan membuat beberapa catatan penting terkait materi yang dibaca dan kaitannya dengan materi evaluasi	• Sikap (Komunikasi dan santun) • Keaktifan dalam diskusi dan tanya jawab • Ketepatan dan kesempurnaan laporan penugasan • Bentuk penilaian Presentasi • Kriteria dan indikator penilaian adalah ketepatan dan penguasaan materi • Ketepatan menjelaskan pengertian materi yang ditanyakan; • Mampu menguasai materi yang dipelajari minimal 80%	1. Andy Taylor, David Alexander, Amanda Finch, David Sutton, Information Security Management Principles, BCS, The Chartered Institute for IT; Updated edition (June 18, 2013) 2. Handbook for Computer Security Incident Response Teams http://www.cert.org/archive/pdf/csirt-handbook.pdf 3. Sheward, mike, Hands-on Incident Response and Digital Forensics, Imprint: BCS, The Chartered Institute for IT, 2018 4. E.Wheeler,2011,“Security Risk Management: Building an Information Security Risk Management Program from the Ground Up”, Syngress
9	• Mempelajari tentang serangan server web, termasuk metodologi serangan komprehensif yang digunakan untuk mengaudit kerentanan dalam infrastruktur dan penanggulangan server web. • Mempelajari tentang serangan aplikasi web, termasuk metodologi peretasan aplikasi web komprehensif yang digunakan untuk mengaudit kerentanan dalam aplikasi web dan penanggulangannya.	• Hacking Web Servers • Hacking Web Applications	X			Ceramah, Diskusi, Praktik	2 x 50 menit	Mahasiswa dapat menjawab pertanyaan : • Hacking Web Servers • Hacking Web Applications	• Sikap (Komunikasi dan santun) • Keaktifan dalam diskusi dan tanya jawab • Ketepatan dan kesempurnaan laporan penugasan • Bentuk penilaian Presentasi • Kriteria dan indikator penilaian adalah ketepatan dan penguasaan materi • Ketepatan menjelaskan pengertian materi yang ditanyakan; • Mampu menguasai materi yang dipelajari minimal 80%	1. Andy Taylor, David Alexander, Amanda Finch, David Sutton, Information Security Management Principles, BCS, The Chartered Institute for IT; Updated edition (June 18, 2013) 2. Handbook for Computer Security Incident Response Teams http://www.cert.org/archive/pdf/csirt-handbook.pdf 3. Sheward, mike, Hands-on Incident Response and Digital Forensics, Imprint: BCS, The Chartered Institute for IT, 2018 4. E.Wheeler,2011,“Security Risk Management: Building an Information Security Risk Management Program from the Ground Up”, Syngress

NO	Kemampuan akhir yang diharapkan (Sub CPMK)	Bahan Kajian/Materi Perkuliahan	Bentuk Pembelajaran			Metode Pembelajaran	Alokasi Waktu	Pengalaman Belajar Mahasiswa	Penilaian (kriteria, indikator dan bobot)	Referensi
			Luring	Daring	Blanded					
10	• Mempelajari tentang teknik serangan injeksi SQL, alat deteksi injeksi, dan penanggulangan untuk mendeteksi dan bertahan dari upaya injeksi SQL.	• Teknik serangan injeksi SQL	X			Ceramah, Diskusi, Praktik	2 x 50 menit	Mahasiswa dapat menjawab pertanyaan : • Teknik serangan injeksi SQL	• Sikap (Komunikasi dan santun) • Keaktifan dalam diskusi dan tanya jawab • Ketepatan dan kesempurnaan laporan penugasan • Bentuk penilaian Presentasi • Kriteria dan indikator penilaian adalah ketepatan dan penguasaan materi • Ketepatan menjelaskan pengertian materi yang ditanyakan; • Mampu menguasai materi yang dipelajari minimal 80%	1. Andy Taylor, David Alexander, Amanda Finch, David Sutton, Information Security Management Principles, BCS, The Chartered Institute for IT; Updated edition (June 18, 2013) 2. Handbook for Computer Security Incident Response Teams http://www.cert.org/archive/pdf/csirt-handbook.pdf 3. Sheward, mike, Hands-on Incident Response and Digital Forensics, Imprint: BCS, The Chartered Institute for IT, 2018 4. E.Wheeler,2011,“Security Risk Management: Building an Information Security Risk Management Program from the Ground Up”, Syngress
11	• Mempelajari tentang enkripsi nirkabel, metodologi dan alat peretasan nirkabel, dan alat keamanan Wi-Fi.	• Hacking Wireless Networks	X			Ceramah, Diskusi, Praktik	2 x 50 menit	Mahasiswa dapat menjawab pertanyaan : • Hacking Wireless Networks	• Mampu menguasai materi yang dipelajari minimal 80%	1. Andy Taylor, David Alexander, Amanda Finch, David Sutton, Information Security Management Principles, BCS, The Chartered Institute for IT; Updated edition (June 18, 2013) 2. Handbook for Computer Security Incident Response Teams http://www.cert.org/archive/pdf/csirt-handbook.pdf 3. Sheward, mike, Hands-on Incident Response and Digital Forensics, Imprint: BCS, The Chartered Institute for IT, 2018 4. E.Wheeler,2011,“Security Risk Management: Building an Information Security Risk Management Program from the Ground Up”, Syngress
12	• Mempelajari tentang vektor serangan platform seluler, eksploitasi kerentanan Android, serta pedoman dan alat keamanan seluler.	• Hacking Mobile Platforms	X			Ceramah, Diskusi, Praktik	2 x50 menit	Mahasiswa dapat menjawab pertanyaan : • Hacking Mobile Platforms	• Mampu menguasai materi yang dipelajari minimal 80%	1. Andy Taylor, David Alexander, Amanda Finch, David Sutton, Information Security Management Principles, BCS, The Chartered Institute for IT; Updated edition (June 18, 2013) 2. Handbook for Computer Security Incident Response Teams http://www.cert.org/archive/pdf/csirt-handbook.pdf 3. Sheward, mike, Hands-on Incident Response and Digital Forensics, Imprint: BCS, The Chartered Institute for IT, 2018 4. E.Wheeler,2011,“Security Risk Management: Building an Information Security Risk Management Program from the Ground Up”, Syngress

NO	Kemampuan akhir yang diharapkan (Sub CPMK)	Bahan Kajian/Materi Perkuliahan	Bentuk Pembelajaran			Metode Pembelajaran	Alokasi Waktu	Pengalaman Belajar Mahasiswa	Penilaian (kriteria, indikator dan bobot)	Referensi
			Luring	Daring	Blanded					
13	• Mempelajari tentang teknik packet-sniffing dan cara menggunakannya untuk menemukan kerentanan jaringan, serta penanggulangan untuk bertahan dari serangan sniffing	• Hacking IoT (internet of things) and OT (Operational Technology)	X			Ceramah, Diskusi, Praktik	2 x 50 menit	Mahasiswa dapat menjawab pertanyaan : • Hacking IoT (internet of things) and OT (Operational Technology)	• Mampu menguasai materi yang dipelajari minimal 80%	1. Andy Taylor, David Alexander, Amanda Finch, David Sutton, Information Security Management Principles, BCS, The Chartered Institute for IT; Updated edition (June 18, 2013) 2. Handbook for Computer Security Incident Response Teams http://www.cert.org/archive/pdf/csirt-handbook.pdf 3. Sheward, mike, Hands-on Incident Response and Digital Forensics, Imprint: BCS, The Chartered Institute for IT, 2018 4. E.Wheeler,2011,“Security Risk Management: Building an Information Security Risk Management Program from the Ground Up”, Syngress
14	Mempelajari berbagai konsep komputasi cloud, seperti teknologi kontainer dan komputasi tanpa server, berbagai ancaman dan serangan berbasis cloud, serta teknik dan alat keamanan cloud.	• Cloud Computing	X			Ceramah, Diskusi, Praktik	2 x 50 menit	Mahasiswa dapat menjawab pertanyaan : • Cloud Computing	• Mampu menguasai materi yang dipelajari minimal 80%	1. Andy Taylor, David Alexander, Amanda Finch, David Sutton, Information Security Management Principles, BCS, The Chartered Institute for IT; Updated edition (June 18, 2013) 2. Handbook for Computer Security Incident Response Teams http://www.cert.org/archive/pdf/csirt-handbook.pdf 3. Sheward, mike, Hands-on Incident Response and Digital Forensics, Imprint: BCS, The Chartered Institute for IT, 2018 4. E.Wheeler,2011,“Security Risk Management: Building an Information Security Risk Management Program from the Ground Up”, Syngress
15	• Mempelajari tentang kriptografi dan penyandian, infrastruktur kunci publik,	• Kriptographi	X			ceramah diskusi dan tanya jawab	2 x 50 menit	Mahasiswa dapat menjawab pertanyaan : • Kriptographi	• Mampu menguasai materi yang dipelajari minimal 80%	1. Andy Taylor, David Alexander, Amanda Finch, David Sutton, Information Security Management Principles, BCS, The Chartered Institute for IT; Updated edition (June 18, 2013) 2. Handbook for Computer Security Incident Response Teams http://www.cert.org/archive/pdf/csirt-handbook.pdf 3. Sheward, mike, Hands-on Incident Response and Digital Forensics, Imprint: BCS, The Chartered Institute for IT, 2018 4. E.Wheeler,2011,“Security Risk Management: Building an Information Security Risk Management Program from the Ground Up”, Syngress
16	Ujian Akhir Semester		X				2 x 50 menit			
17										
18										
19										
20										

F REFERENSI

1 Wajib

a Andy Taylor, David Alexander, Amanda Finch, David Sutton, Information Security Management Principles, BCS, The Chartered Institute for IT; Updated edition (June 18, 2013)

b Handbook for Computer Security Incident Response Teams http://www.cert.org/archive/pdf/csirt-handbook.pdf

2 Pendukung

a E.Wheeler,2011,“Security Risk Management: Building an Information Security Risk Management Program from the Ground Up”, Syngress

b Gurjar, L.R., 2009, Cyber securities and Cyber Terrorism, Vardhaman Mahaveer Open

c Sheward, mike, Hands-on Incident Response and Digital Forensics, Imprint: BCS, The Chartered Institute for IT, 2018

d Handbook of Security, Cryptography and Digital Signature by P. Ramchandaran & S.M. Bhaskar (Viva Book Pvt. Ltd.)

e *Aulia Syarif Aziz, Safriatullah Safriatullah, Perancangan Dan Analisis Keamanan Pada Sistem Autentikasi Terpusat Freeradius.* Jurnal of Informatics and computer sciences, Vol 7, No 2 (2021)

Mengetahui:
Ketua Prodi Pendidikan Teknologi Informasi

Mira Maisura, M.Sc.
NIDN : 2027058602

Banda Aceh, 06 Februari 2024
Koordinator/Dosen Mata Kuliah

Aulia Syarif Aziz, S.Kom., M.Sc.
NIDN : 1321059301

TUGAS KEGIATAN TERSTRUKTUR (TKT)

Nama Mata Kuliah	Cybersecurity
Kode mata Kuliah	223PTI025
Semester/SKS	5/2 sks

1 Tujuan Tugas — Mahasiswa mampu menguasai konsep dasar tentang keamanan komputer (cyber security) dan langkah-langkah penanganannya

2 Uraian Tugas

a	Obyek garapan	Materi pengayaan perkuliahan yang terdapat dalam RPS
b	Yang harus dikerjakan dan batasan-batasan	Menyelesaikan solusi dari studi kasus dan latihan
c	Metode/cara pengerjaan, acuan yang digunakan	Memberikan solusi berbasis security terhadap keterkaitan materi ajar yang dipelajari
d	Deskripsi luaran tugas yang dihasilkan/dikerjakan	laporan tertulis dan project tentang keamanan sistem

3 Kriteria Penilaian

a	Ketepatan penyerahan tugas	10%
b	Kesempurnaan substansi/isi tugas	80%
c	Desain tugas	10%

Mengetahui:
Ketua Prodi Pendidikan Teknologi Informasi

Mira Maisura, M.Sc.
NIDN : 2027058602

Banda Aceh, 06 Februari 2024
Koordinator/Dosen Mata Kuliah

Aulia Syarif Aziz, S.Kom., M.Sc.
NIDN : 1321059301

TUGAS KEGIATAN MANDIRI (TKM)

Nama Mata Kuliah	Cybersecurity
Kode mata Kuliah	223PTI025
Semester/SKS	5/2 sks

Capaian Pembelajaran Mata Kuliah (CPMK)

1. Membangun dan mengevaluasi sistem cyber security dalam berbagai area, termasuk yang berkaitan dengan ragam ancaman dan kerentanan, aset dan resiko, teknologi keamanan data, teknologi keamanan jaringan, atau tata kelola cyber security
2. Menguasai teori dan konsep yang mendasari ilmu komputer.khususnya cyber security
3. Menentukan pendekatan sistem cyber security yang sesuai dengan problem yang dihadapi, memilih representasi pengetahuan dan mekanisme penalarannya

Jenis Tugas :

Mengetahui:
Ketua Prodi Pendidikan Teknologi Informasi

Mira Maisura, M.Sc.
NIDN : 2027058602

Banda Aceh, 06 Februari 2024
Koordinator/Dosen Mata Kuliah

Aulia Syarif Aziz, S.Kom., M.Sc.
NIDN : 1321059301

PENILAIAN SIKAP, PENGETAHUAN DAN KETERAMPILAN

A. PENILAIAN SIKAP (RUBRIK)

Prediket	Skor Angka	Deskripsi Perilaku

Keterangan :

Prediket :
Diisi dengan deskripsi tingkatan nilai, dengan jumlah tingkat yang kerinciannya sesuai dengan yang dikehendaki (sangat baik, baik, cukup, kurang, gagal).

Skor Angka :
Diisi dengan rentang angka yang sesuai dengan tingkat nilai pada kolom jenjang.

B. KRITERIA PENILAIAN PENGETAHUAN DAN KETERAMPILAN

Nilai Huruf (NH)	Nilai Bobot (NB)	Nilai Angka (NA)	Predikat
A	4.00	90-100	Sangat Baik Sekali
A-	3.67	85-89	Sangat Baik
B+	3.33	78-84	Baik
B	3.00	72-77	Agak Baik
B-	2.67	68-71	Cukup
C+	2.33	65-67	Agak Kurang Baik
C	2.00	60-64	Kurang Baik
D	1.00	50-59	Sangat Kurang Baik
E	0	0-49	Gagal

Mengetahui:
Ketua Prodi Pendidikan Teknologi Informasi

Mira Maisura, M.Sc.
NIDN : 2027058602

Banda Aceh, 06 Februari 2024
Koordinator/Dosen Mata Kuliah

Aulia Syarif Aziz, S.Kom., M.Sc.
NIDN : 1321059301