RENCANA PEMBELAJARAN SEMESTER (RPS)
MATA KULIAH : KEAMANAN JARINGAN
PROGRAM STUDI TEKNOLOGI INFORMASI
FAKULTAS SAINS DAN TEKNOLOGI UIN AR-RANIRY BANDA ACEH

A IDENTITAS

1	Prodi	Teknologi Informasi
2	Kode Mata kuliah	2032TI026
3	Nama Mata kuliah	Keamanan Jaringan
4	Semester/SKS	4 / 3 sks
5	Jenis Mata Kuliah	MK KEAHLIAN DAN KETRAMPILAN (MKK)
6	Koordinator Mata Kuliah	1321028801 | Baihaqi, M.T.
7	Dosen Pengampu	Baihaqi, M.T. | Ghufran Ibnu Yasa, M.T| Aulia Syarif Azis., M.Sc.

B CAPAIAN PEMBELAJARAN LULUSAN (CPL-Prodi)

1 Sikap
- a Taat hukum dan disiplin dalam kehidupan bermasyarakat dan bernegara (S6)
- b Memiliki wawasan, pengetahuan lingkungan dan kebencanaan (S10)

2 Pengetahuan
- a Menguasai konsep dan teori struktur diskrit sehingga mampu memodelkan dan menganalisis sistem komputasi (P8)
- b Menguasai bidang bidang yang berfokus pada keilmuan teknologi informasi serta mampu beradaptasi dengan perkembangan ilmu pengetahuan dan teknologi terkini (P12)

3 Keterampilan Umum
- a Mampu mendokumentasikan, menyimpan, mengamankan, dan menemukan kembali data untuk menjamin kesahihan dan bebas dari segala bentuk plagiasi (KU12)
- b Mampu menerapkan pemikiran logis, kritis, sistematis, dan inovatif dalam konteks pengembangan ilmu pengetahuan dan teknologi yang memperhatikan dan menerapkan nilai humaniora yang sesuai dengan bidang keahlian Teknologi Informasi (KU18)

4 Keterampilan Khusus
- a Mampu menganalisis, mengevaluasi, mengembangkan mempertahankan profesi yang berkelanjutan dalam bidang teknologi informasi (KK8)
- b Mampu untuk membuat perencanaan, perancangan, penerapan, pengujian hingga pemeliharaan sistem jaringan komputer dan sistem keamanan jaringan (KK18)
- c Mampu untuk membuat perencanaan, perancangan, penerapan, pengujian hingga pemeliharaan sistem web dan komputasi sistem bergerak (KK20)

C CAPAIAN PEMBELAJARAN MATA KULIAH (CPMK)

1 Mampu memahami konsep keamanan komputer dari sisi fisikal, teknikal, dan prosedural atau administratif

2 Mampu memahami konsep dan penerapan keamanan web browser dan menganalisis kelemahan sebuah web system.

3 Mampu memahami permasalahan dan trend keamanan komputer ke depan

4 Mata Kuliah ini memberikan pengetahuan kepada mahasiswa tentang pengertian sekuriti dan privacy serta hubungan yang terjadi, masalah-masalah yang dapat menghambat pengoperasian sekuriti, pertimbanganpertimbangan dalam sistem sekuriti dan rencana-rencana pengimplementasiannya. Implementasi yang digunakan adalah Ethical Hacking. Ethical hacking melibatkan praktik metode untuk mengidentifikasi, mengevaluasi, menguji, dan melaporkan kerentanan dalam suatu organisasi. Dapat mengevaluasi hampir semua aplikasi atau infrastruktur dengan mengidentifikasi potensi kerentanan dan memberikan rekomendasi tentang bagaimana kerentanan tersebut dapat diperbaiki.

5 Mampu memahami konsep dasar keamanan komputer meliputi aset Sistem komputer, properti keamanan komputer, vulnerability, threat, dan kontrol.

6 Mampu memahami konsep keamanan komputer dari sisi fisikal, teknikal, dan prosedural atau administratif.

7 Mampu memahami SOP dan audit sistem keamanan komputer.

D DESKRIPSI MATA KULIAH

Mata Kuliah ini memberikan pengetahuan kepada mahasiswa tentang pengertian sekuriti dan privacy serta hubungan yang terjadi, masalah-masalah yang dapat menghambat pengoperasian sekuriti, pertimbanganpertimbangan dalam sistem sekuriti dan rencana-rencana pengimplementasiannya. Implementasi yang digunakan adalah Ethical Hacking. Ethical hacking melibatkan praktik metode untuk mengidentifikasi, mengevaluasi, menguji, dan melaporkan kerentanan dalam suatu organisasi. Dapat mengevaluasi hampir semua aplikasi atau infrastruktur dengan mengidentifikasi potensi kerentanan dan memberikan rekomendasi tentang bagaimana kerentanan tersebut dapat diperbaiki.

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	3 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	• 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, 2
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	3 x 50 Menit	• Mahasiswa mampu menjawab soal • Mahasiswa dapat mempraktikkan footprinting	• 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, 2, 3

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	3 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, 2, & 3
4	• Memelajari 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	X	X	Ceramah, Diskusi, Praktik	3 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, 2, 3

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	X	X	Ceramah, Diskusi, Praktik	3 x 50 Menit	Mahasiswa dapat menjawab pertanyaan : • Malware Threats • Sniffing	• 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, 2
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	X	X	Ceramah, Diskusi, Praktik	3 x 50 Menit	Mahasiswa dapat menjawab pertanyaan : • Social engineering • Denial of Service (DoS)	• 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%	3

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					
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	X	X	Ceramah, Diskusi, Praktik	3 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 & 2
8	Mahasiswa mampu menjawab soal-soal tes terhadap materi yang sudah diajarkan minimal 85 %	UTS dari materi ajar dari pertemuan 1-7	X			Ujian tertulis	3 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	• Bentuk penilaian tes tulis • Kriteria dan indikator penilaian adalah ketepatan dan pengu-asaan • Ketepatan menjelaskan pengertian materi yang ditanyakan • Mampu menguasai materi yang dipelajari minimal 80%	1

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					
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	X	X	Ceramah, Diskusi, Praktik	3 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
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	X	X	Ceramah, Diskusi, Praktik	3 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

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					
11	• Mempelajari tentang enkripsi nirkabel, metodologi dan alat peretasan nirkabel, dan alat keamanan Wi-Fi.	• Hacking Wireless Networks	X	X	X	Ceramah, Diskusi, Praktik	3 x 50 Menit	Mahasiswa dapat menjawab pertanyaan : • Hacking Wireless Networks	• 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
12	• Mempelajari tentang vektor serangan platform seluler, eksploitasi kerentanan Android, serta pedoman dan alat keamanan seluler.	• Hacking Mobile Platforms	X	X	X	Ceramah, Diskusi, Praktik	3 x 50 Menit	Mahasiswa dapat menjawab pertanyaan : • Hacking Mobile Platforms	• 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

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	X	X	Ceramah, Diskusi, Praktik	3 x 50 Menit	Mahasiswa dapat menjawab pertanyaan : • Hacking IoT (internet of things) and OT (Operational Technology)	• 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
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	X	X	Ceramah, Diskusi, Praktik	3 x 50 Menit	Mahasiswa dapat menjawab pertanyaan : • Cloud Computing	• 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

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					
15	• Mempelajari tentang kriptografi dan penyandian, infrastruktur kunci publik,	• Kriptographi	X	X	X	Ceramah, Diskusi, Praktik	3 x 50 Menit	Mahasiswa dapat menjawab pertanyaan : • Kriptographi	• 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%	3
16	Mahasiswa mampu menjawab soal-soal tes terhadap materi yang sudah diajarkan dari pertemuan 1-15 minimal 80 %	Materi ajar yang telah dipelajari dari pertemuan 1-15	X			Ujian tertulis	3 x 50 Menit	Mahasiswa menjawab soal-soal yang diujikan dengan baik dan benar	• Bentuk penilaian tes tulis • Kriteria dan indikator penilaian adalah ketepatan dan pengu-asaan • Ketepatan menjelaskan pengertian materi yang ditanyakan • Mampu menguasai materi yang dipelajari minimal 80%	1
17										
18										
19										
20										

F REFERENSI

1 Wajib

a EC-Council Academia, Ethical Hacking and Countermeasures version 11 Complete, EC-Council Academia, 2021

b Charles P. Pfleeger dan Shari P. Pfleeger , Security in Computing 2nd Edition, Prentice Hall, 2003

2 Pendukung

a Matt Bishop, Computer Security Art and Science, Addison-Wesley, 2003

b Bruce Schneier, Applied Cryptography Protocols, Algorithms and Source Code in C, John Wiley & Sons, 1996

c Simson Garfinkel dan Gene Spafford, Practical UNIX and Internet Security, O'Reilly & Associates, 1996

d Rahmat Rafiudin, Menguasai Security UNIX, Elex Media Komputindo, 2002

e Gede Artha ZP, Hacker Sisi Lain Legenda Komputer, Adigna, 1999

Mengetahui:
Ketua Prodi Teknologi Informasi

Ima Dwitawati, M.B.A.
NIDN : 0113108204

Banda Aceh, 18 Januari 2024
Koordinator/Dosen Mata Kuliah

Baihaqi, M.T.
NIDN : 1321028801

TUGAS KEGIATAN TERSTRUKTUR (TKT)

Nama Mata Kuliah	Keamanan Jaringan
Kode mata Kuliah	2032TI026
Semester/SKS	4/3 sks

1 Tujuan Tugas

2 Uraian Tugas

- a Obyek garapan
- b Yang harus dikerjakan dan batasan-batasan
- c Metode/cara pengerjaan, acuan yang digunakan
- d Deskripsi luaran tugas yang dihasilkan/dikerjakan

3 Kriteria Penilaian

- a Ketepatan penyerahan tugas
- b Kesempurnaan substansi/isi tugas
- c Desain tugas

Mengetahui:
Ketua Prodi Teknologi Informasi

Ima Dwitawati, M.B.A.
NIDN : 0113108204

Banda Aceh, 18 Januari 2024
Koordinator/Dosen Mata Kuliah

Baihaqi, M.T.
NIDN : 1321028801

TUGAS KEGIATAN MANDIRI (TKM)

Nama Mata Kuliah	Keamanan Jaringan
Kode mata Kuliah	2032TI026
Semester/SKS	4/3 sks

Capaian Pembelajaran Mata Kuliah (CPMK)

1 Mampu memahami konsep keamanan komputer dari sisi fisikal, teknikal, dan prosedural atau administratif

2 Mampu memahami konsep dan penerapan keamanan web browser dan menganalisis kelemahan sebuah web system.

3 Mampu memahami permasalahan dan trend keamanan komputer ke depan

4 Mata Kuliah ini memberikan pengetahuan kepada mahasiswa tentang pengertian sekuriti dan privacy serta hubungan yang terjadi, masalah-masalah yang dapat menghambat pengoperasian sekuriti, pertimbanganpertimbangan dalam sistem sekuriti dan rencana-rencana pengimplementasiannya. Implementasi yang digunakan adalah Ethical Hacking. Ethical hacking melibatkan praktik metode untuk mengidentifikasi, mengevaluasi, menguji, dan melaporkan kerentanan dalam suatu organisasi. Dapat mengevaluasi hampir semua aplikasi atau infrastruktur dengan mengidentifikasi potensi kerentanan dan memberikan rekomendasi tentang bagaimana kerentanan tersebut dapat diperbaiki.

5 Mampu memahami konsep dasar keamanan komputer meliputi aset Sistem komputer, properti keamanan komputer, vulnerability, threat, dan kontrol.

6 Mampu memahami konsep keamanan komputer dari sisi fisikal, teknikal, dan prosedural atau administratif.

7 Mampu memahami SOP dan audit sistem keamanan komputer.

Jenis Tugas :

Mengetahui:
Ketua Prodi Teknologi Informasi

Ima Dwitawati, M.B.A.
NIDN : 0113108204

Banda Aceh, 18 Januari 2024
Koordinator/Dosen Mata Kuliah

Baihaqi, M.T.
NIDN : 1321028801

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 Teknologi Informasi

Ima Dwitawati, M.B.A.
NIDN : 0113108204

Banda Aceh, 18 Januari 2024
Koordinator/Dosen Mata Kuliah

Baihaqi, M.T.
NIDN : 1321028801