RENCANA PEMBELAJARAN SEMESTER

JUDUL RPS
ETIKA PERETASAN (ETICHAL HACKING)

Oleh:

ATTHARIQ

PROGRAM STUDI
TEKNOLOGI REKAYASA KOMPUTER JARINGAN
JURUSAN TEKNOLOGI INFORMASI DAN KOMPUTER
POLITEKNIK NEGERI LHOKSEUMAWE
AGUSTUS 2025

	POLITEKNIK NEGERI LHOKSEUMAWE **JURUSAN TEKNOLOGI INFORMASI DAN KOMPUTER** **PROGRAM STUDI TEKNOLOGI REKAYASA KOMPUTER JARINGAN**	**Kode Dokumen** RPS-TIK-TRKJ/2025

RENCANA PEMBELAJARAN SEMESTER

MATA KULIAH (MK)	KODE MK	RUMPUN MATA KULIAH (KBK)	BOBOT (sks)		SEMESTER	Tgl Penyusunan
Etika Peretasan (Etichal Hacking)	TRKJ-6314	-	**T=1**	**P=2**	3	20 Agustus 2025
OTORISASI **Ketua Jurusan; Prodi TRKJ;P4M**	**Pengembang RPS** Atthariq, S.ST., MT	**Ketua KBK** -			**Ketua PRODI** **Nanda Saputri, S.S.T., M.T.**	

Capaian Pembelajaran (CP)	**CPL-PRODI yang dibebankan pada MK**	
	ST-8	Menunjukkan sikap bertanggungjawab atas pekerjaan di bidang keahliannya secara mandiri
	ST-9	Menginternalisasi nilai, norma dan etika akademik
	KU	Kemampuan untuk memiliki perspektif kritis dan kreatif dalam mengidentifikasi dan memecahkan masalah dengan menggunakan pemikiran komputasi
	KK	Mengidentifikasi ancaman keamanan komputer baik internal maupun eksternal untuk merencanakan pencegahannya
	PP	Menguasai pengetahuan faktual tentang isu mutakhir di bidang sains komputasi dan rekayasa
	Capaian Pembelajaran Mata Kuliah (CPMK)	
	CPMK1	Mengidentifikasi akar masalah secara komprehensif, serta mengambil keputusan yang tepat berdasarkan analisis informasi dan data (APTIKOM)
	CPMK2	Bekerjasama dengan individu yang memiliki latar belakang sosial dan budaya yang beragam (APTIKOM)
	Kemampuan akhir tiap tahapan belajar (Sub-CPMK)	
	Sub-CPMK1	Mahasiswa dapat menjelaskan pengenalan mengenai *ethical hacking*
	Sub-CPMK2	Mahasiswa dapat menjelaskan konsep *reconnaissance* dan *footprinting*
	Sub-CPMK3	Mahasiswa dapat menjelaskan konsep *scanning* dan enumeration
	Sub-CPMK4	Mahasiswa dapat menjelaskan sistem *hacking*
	Sub-CPMK5	Mahasiswa dapat menjelaskan macam-macam *malware threats*
	Sub-CPMK6	Mahasiswa dapat menjelaskan konsep *sniffing*
	Sub-CPMK7	Mahasiswa dapat menjelaskan *denial of services*
	Sub-CPMK8	Mahasiswa dapat menjelaskan konsep *social engineering*
	Sub-CPMK9	Mahasiswa dapat menjelaskan konsep *session hijacking*

	Sub-CPMK10	Mahasiswa dapat menjelaskan *hacking web*
	Sub-CPMK11	Mahasiswa dapat menjelaskan konsep SQL Injection
	Sub-CPMK12	Mahasiswa dapat menjelaskan konsep Kriptografi
Deskripsi Singkat MK	Mata kuliah Ethical hacking memberikan pemahaman mengenai konsep ethical hacking, teknik-teknik sistem hacking, macam-macam malware threats, SQL injection dan konsep kriptografi dalam ethical hacking	
Bahan Kajian: Materi Pembelajaran	1. Pengenalan ethical hacking 2. Konsep reconnaissance dan footprinting 3. Proses scanning dan enumeration 4. Teknik-teknik sistem Hacking 5. Macam-macam malware threats 6. Konsep sniffing 7. Konsep denial of service 8. Konsep social engineering 9. Konsep session hijacking 10. Konsep hacking web 11. Konsep SQL Injection 12. Konsep Kriptografi	
Pustaka	**Utama :**	
	Kimberly Graves. CEH Certified Ethical Hacker Study Guide. Wiley Publishing, Inc.	
	Pendukung :	
	1. Rafay Baloch. Ethical Hacking and Penetration Testing Guide. CRC Press 2. Patrick Engebretson., The Basics of Hacking Hacking and Penetration Testing. Syngress 3. Karina Astudillo B. Ethical Hacking 101.	
Dosen Pengampu	Atthariq, S.ST., MT	
Matakuliah syarat	1. Dasar-dasar Jaringan 2. Dasar-dasar Keamanan Siber	

Mg Ke-	**Kemampuan akhir tiap tahapan belajar (Sub-CPMK)**	**Penilaian**		**Bantuk Pembelajaran, Metode Pembelajaran, Penugasan Mahasiswa, [Estimasi Waktu]**		**Materi Pembelajaran [Pustaka]**	**Bobot Penilaian (%)**
		Indikator	**Kriteria & Bentuk**	**Luring (*offline*)**	**Daring (*online*)**		

(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
1	• Mahasiswa dapat memahami struktur perkuliahan, aturan pengerjaan tugas, UTS, dan UAS. • Mahasiswa mampu memahami kewajiban dan hak mahasiswa selama perkuliahan.	Ketuntasan menjelaskan kemampuan yang diperoleh dan mengetahui aktifitas yang harus dilakukan mahasiswa selama menjalani proses perkuliahan	Menunjukkan tahapan aktifitas untuk mencapai CPMK (non tes)	Bentuk: Kuliah Metode: Ceramah Tatap Muka (TM) Waktu: [1x(2x50")]	Bentuk: Kuliah F-LMS App Metode: Ceramah Belajar Mandiri (BM): Waktu: [1x(2x50")]	Kontrak kuliah, RPS, CPMK, Dokumen KKNI, Peraturan Akademik PNL.	
2	Mahasiswa dapat menjelaskan pengenalan mengenai ethical hacking	1.Ketepatan menjelaskan definisi ethical hacking 2.Ketepatan menjelaskan tujuan ethical hacking 3.Ketepatan menjelaskan terminologi ethical hacking 4.Ketepatan menjelaskan tahapan dalam ethical hacking	Ketepatan menjelaskan pengenalan dan konsep dasar ethical hacking Bentuk non-test : Tugas Individu	Bentuk: Kuliah Metode: Ceramah, SDL TM [1x(2x50")]	Bentuk: Kuliah F-LMS App Metode: SDL BM [1x(2x50")]	1. Definisi ethical hacking 2. Tujuan ethical hacking 3. Terminologi ethical hacking 4. Tahapan dalam ethical hacking [1] Hal. 1 - 23 [4] Hal. 10 - 15	5
3	Mahasiswa dapat menjelaskan konsep reconnaissance dan footprinting	1. Ketepatan menjelaskan konsep reconnaissance 2. Ketepatan menjelaskan metodologi pengumpulan informasi	Ketepatan menjelaskan konsep reconnaissance dan footprinting Bentuk non-test : Tugas Individu	Bentuk: Kuliah Metode: Ceramah, SDL TM [1x(2x50")]	Bentuk: Kuliah F-LMS App Metode: SDL BM [1x(2x50")]	1. Konsep reconnaissance 2. Metodologi pengumpulan informasi 3. Konsep footprinting [1] Hal. 31 – 48	5

		3. Ketepatan menjelaskan konsep *footprinting*					
4	Mahasiswa dapat menjelaskan konsep scanning dan enumeration	1. Ketepatan menjelaskan konsep dasar dan metodologi scanning 2. Ketepatan menjelaskan Teknik-teknik scanning 3. Ketepatan menjelaskan konsep enumeration	Ketepatan menjelaskan konsep scanning dan enumeration Bentuk non-test : Tugas Individu	Bentuk: Kuliah Metode: Ceramah, CoL TM [1x(2x50")]	Bentuk: Kuliah F-LMS App Metode: SDL BM [1x(2x50")]	1. Konsep dan metodologi scanning 2. Teknik-teknik scanning 3. Konsep enumeration [1] Hal. 63 - 85 [3] Hal. 86 -114 [4] Hal 51 - 95	
5	Mahasiswa dapat menjelaskan teknik- teknik sistem hacking	1. Ketepatan menjelaskan Teknik password-cracking 2. Ketepatan menjelaskan tipe-tipe password 3. Ketepatan mengidentifikasi jenis jenis tools password-cracking	Ketepatan dalam menjelaskan teknikteknik sistem hacking Bentuk non-test : Tugas Individu	Bentuk: Kuliah Metode: Ceramah, CoL TM [1x(2x50")]	Bentuk: Kuliah F-LMS App Metode: SDL BM [1x(2x50")]	1. Teknik password-cracking 2. Tipe-tipe password 3. Jenis-jenis tools password-cracking [1] Hal. 95 - 114 [3] Hal. 138 -150	
6	Mahasiswa dapat menjelaskan macam-macam malware threats	1. Ketepatan menjelaskan trojan 2. Ketepatan menjelaskan backdoors 3. Ketepatan menjelaskan virus	Ketepatan dalam menjelaskan macam-macam malware threats	Bentuk: Kuliah Metode: Ceramah, CoL TM [1x(2x50")]	Bentuk: Kuliah F-LMS App Metode: SDL BM [1x(2x50")]	1. Trojan 2. Backdoors 3. Virus 4. Worm [1] Hal. 125 - 145	

		4. Ketepatan menjelaskan worms					
7	Mahasiswa dapat menjelaskan konsep sniffing	1. Ketepatan menjelaskan protocol yang rawan terhadap sniffing 2. Ketepatan menjelaskan sniffing aktif dan pasif 3. Ketepatan menjelaskan ARP Poisoning 4. Ketepatan menjelaskan MAC flooding	Ketepatan dalam menjelaskan konsep sniffing Bentuk non-test : Tugas Individu	Bentuk: Kuliah Metode: Ceramah, CoL TM [1x(2x50")]	Bentuk: Kuliah F-LMS App Metode: SDL BM [1x(2x50")]	1. Protokol rawan terhadap sniffing 2. Sniffing aktif dan pasif 3. ARP Poisoning 4. MAC flooding [1] Hal. 153 -164 [2] Hal. 139 – 160	
8	Evaluasi Tengah Semester / Ujian Tengan Semester						
9	Mahasiswa dapat menjelaskan konsep denial of services	1. Ketepatan menjelaskan tipe tipe DoS attacks 2. Ketepatan menjelaskan cara kerja DDoS attacks 3. Ketepatan menjelaskan cara kerja BOTs/BOTNETs 4. Ketepatan menjelaskan DoS/DDoS countermeasures	Ketepatan dalam menjelaskan konsep denial of services Bentuk non-test : Tugas Individu	Bentuk: Kuliah Metode: Ceramah, CoL TM [1x(2x50")]	Bentuk: Kuliah F-LMS App Metode: SDL BM [1x(2x50")]	1. Tipe – tipe DoS attacks 2. Cara kerja DDoS attacks 3. Cara kerja BOTs/BOTNETs 4. Dos/DDoS countermeasures [1] Hal. 174 - 182	
10	Mahasiswa dapat menjelaskan konsep social engineering	1. Ketepatan menjelaskan	Ketepatan dalam menjelaskan konsep	Bentuk: Kuliah	Bentuk: Kuliah F-LMS App	1. Definisi social engineering	

		definisi social engineering 2. Ketepatan menjelaskan jenis jenis penyerangan 3. Ketepatan menjelaskan social engineering countermeasures	social engineering Bentuk non-test : Tugas Individu	Metode: Ceramah, CoL TM [1x(2x50")]	Metode: SDL BM [1x(2x50")]	2. Jenis-jenis penyerangan 3. Social engineering countermeasures [1] Hal. 50 - 54 [3] Hal. 175 - 189	
11	Mahasiswa dapat menjelaskan konsep session hijacking	1. Ketepatan menjelaskan definisi hijacking 2. Ketepatan menjelaskan jenis-jenis session hijacking 3. Ketepatan menjelaskan tahapan menampilkan session hijacking 4. Ketepatan menjelaskan cara mencegah session hijacking	Kemampuan dalam menjelaskan konsep session hijacking Bentuk non-test : Tugas Individu	Bentuk: Kuliah Metode: Ceramah, CoL TM [1x(2x50")]	Bentuk: Kuliah F-LMS App Metode: SDL BM [1x(2x50")]	1. Definisi hijacking 2. Jenis-jenis session hijacking 3. Tahapan menampilkan session hijacking 4. Cara mencegah session hijacking [1] Hal. 183 - 187	
12	Mahasiswa dapat menjelaskan web hacking	1. Ketepatan menjelaskan tipe tipe web server vulnerabilities 2. Ketepatan menjelaskan tipe-tipe penyerangan ke	Kemampuan dalam menjelaskan konsep web hacking Bentuk non-test : Tugas Individu	Bentuk: Kuliah Metode: Ceramah, CoL TM [1x(2x50")]	Bentuk: Kuliah F-LMS App Metode: SDL BM [1x(2x50")]	1. Tipe-tipe web server vulnerabilities 2. Tipe-tipe penyerangan ke web server 3. Web application scanner	

		web server Ketepatan menjelaskan web application scanner				[1] Hal. 195 – 213 [2] Hal. 313 - 319	
13	Mahasiswa dapat menjelaskan konsep SQL Injection	1. Ketepatan menjelaskan definisi SQL injection 2. Ketepatan menjelaskan tahapan tahapan pada SQL injection 3. Ketepatan menjelaskan SQL server vulnerabilities 4. Ketepatan menjelaskan SQL Injection countermeasures	Kemampuan dalam menjelaskan konsep SQL Injection Bentuk non-test : Tugas Individu	Bentuk: Kuliah Metode: Ceramah, CoL TM [1x(2x50")]	Bentuk: Kuliah F-LMS App Metode: SDL BM [1x(2x50")]	1. Definisi SQL injection 2. Tahapan pada SQL Injection 3. SQL server vulnerabilities 4. SQL injection countermeasures [1] Hal. 222 – 231 [2] Hal. 344 - 369	
14	Mahasiswa dapat menjelaskan konsep Kriptografi	1. Ketepatan menjelaksan definisi dan Teknik kriptografi 2. Ketepatan menjelaskan public dan private key 3. Ketepatan menjelaskan algoritma kriptografi	Kemampuan dalam menjelaskan konsep Kriptografi Bentuk non-test : Tugas Individu	Bentuk: Kuliah Metode: Ceramah, CoL TM [1x(2x50")]	Bentuk: Kuliah F-LMS App Metode: SDL BM [1x(2x50")]	1. Definisi dan Teknik kriptografi 2. Public dan private key 3. Algoritma kriptografi [1] Hal. 323 - 337	
15	Evaluasi Akhir Semester / Ujian Akhir Semester						

Silabus Singkat MK

	POLITEKNIK NEGERI LHOKSEUMAWE **JURUSAN TEKNOLOGI INFORMASI DAN KOMPUTER** **PRODI TEKNIK INFORMATIKA**

SILABUS		
MATA KULIAH	Nama	Etika Perentasan
	Kode	TRKJ-6314
	Kredit	3 sks
	Semester	3

DESKRIPSI MATA KULIAH

Mata kuliah Ethical hacking memberikan pemahaman mengenai konsep ethical hacking, teknik-teknik sistem hacking, macam-macam malware threats, SQL injection dan konsep kriptografi dalam ethical hacking

CAPAIAN PEMBELAJARAN MATA KULIAH

No	CPL-MK
1	Mengidentifikasi akar masalah secara komprehensif, serta mengambil keputusan yang tepat berdasarkan analisis informasi dan data
2	Bekerjasama dengan individu yang memiliki latar belakang sosial dan budaya yang beragam

SUB CAPAIAN PEMBELAJARAN MATA KULIAH

No	Sub-CP-MK
1	Mahasiswa dapat menjelaskan pengenalan mengenai *ethical hacking*
2	Mahasiswa dapat menjelaskan konsep *reconnaissance* dan *footp*
3	Mahasiswa dapat menjelaskan konsep *scanning* dan enumeration
4	Mahasiswa dapat menjelaskan sistem *hacking*
5	Mahasiswa dapat menjelaskan macam-macam *malware threats*
6	Mahasiswa dapat menjelaskan konsep *sniffing*
7	Mahasiswa dapat menjelaskan *denial of services*
8	Mahasiswa dapat menjelaskan konsep *social engineering*
9	Mahasiswa dapat menjelaskan konsep *session hijacking*
10	Mahasiswa dapat menjelaskan *hacking web server dan web application*
11	Mahasiswa dapat menjelaskan konsep SQL Injection
12	Mahasiswa dapat menjelaskan konsep Kriptografi

POKOK BAHASAN

1 Pengenalan *ethical hacking*
2 Konsep *reconnaissance* dan *footprinting*
3 Proses *scanning* dan *enumeration*
4 Teknik-teknik sistem hacking
5 Macam-macam *malware threats*
6 Konsep *sniffing*
7 Konsep *denial of services*
8 Konsep *social engineering*
9. Konsep *session hijacking*
10. Konsep *hacking web server* dan *web application*
11. Konsep SQL Injection
12 Konsep Kriptografi.

PUSTAKA

No	**PUSTAKA UTAMA**

1	Kimberly Graves. CEH Certified Ethical Hacker Study Guide. Wiley Publishing, Inc.
2	
	PUSTAKA PENDUKUNG
	1. Rafay Baloch. Ethical Hacking and Penetration Testing Guide. CRC Press 2. Patrick Engebretson., The Basics of Hacking Hacking and Penetration Testing. Syngress 3. Karina Astudillo B. Ethical Hacking 101.