



UNIVERSITAS NEGERI MANADO
FAKULTAS TEKNIK
PROGRAM STUDI TEKNIK INFORMATIKA

RENCANA PEMBELAJARAN SEMESTER (RPS)

Nama Mata Kuliah	Kode	Rumpun MK	Bobot		Semester	Tahun Ajaran
Ethical Hacking	5642765	Praktik Profesional	T = 2	P = 1		Ganjil 2025/2026
Otorisasi/Pengesahan	Pengembang RPS		Koordinator MK		Koordinator Prodi	
	Tim Pengembang RPS Prodi TI		 Dr. Quido C. Kainde, ST, MM, MT		 Kristofel Santa, S.ST, M.MT	
Capaian Pembelajaran Mata Kuliah	Capaian Pembelajaran Lulusan Program Studi (CPL Prodi) yang Dibebankan pada Mata Kuliah					
	CPL-1	Mampu menerapkan prinsip etika profesional dalam bidang teknologi informasi.				
	CPL-2	Menguasai konsep dasar keamanan jaringan dan sistem informasi.				
	CPL-3	Mampu mengidentifikasi dan menganalisis kerentanan pada sistem dan jaringan.				
	CPL-4	Mampu menggunakan tools ethical hacking secara profesional dan bertanggung jawab.				
	CPL-5	Mampu bekerja sama dalam tim dan menyampaikan hasil secara efektif.				
	Capaian Pembelajaran Mata Kuliah (CPMK)					
	CPMK-1	Memahami konsep dasar ethical hacking dan ruang lingkupnya.				
	CPMK-2	Menjelaskan metodologi dan tahapan ethical hacking.				
	CPMK-3	Melakukan scanning, enumeration, dan eksploitasi kerentanan pada sistem dengan tools legal.				
	CPMK-4	Mengevaluasi hasil uji penetrasi dan menyusun laporan secara profesional.				
	CPMK-5	Menunjukkan sikap profesional dan etika dalam seluruh aktivitas ethical hacking.				
	Kemampuan Akhir Tiap Tahapan Belajar (Sub-CPMK)					
	Sub-CPMK-1	Menjelaskan konsep dasar ethical hacking dan legalitasnya.				

	Sub-CPMK-2	Menjelaskan langkah-langkah dalam metodologi ethical hacking.					
	Sub-CPMK-3	Mengoperasikan tools scanning dan enumeration.					
	Sub-CPMK-4	Melakukan eksploitasi terhadap kerentanan yang ditemukan.					
	Sub-CPMK-5	Menganalisis dan melaporkan hasil penetration testing.					
	Sub-CPMK-6	Menerapkan etika dan hukum dalam praktik ethical hacking.					
	Korelasi CPMK terhadap Sub-CPMK						
		Sub-CPMK-1	Sub-CPMK-2	Sub-CPMK-3	Sub-CPMK-4	Sub-CPMK-5	Sub-CPMK-6
	CPMK-1	√	√				
	CPMK-2		√	√	√		
	CPMK-3			√	√	√	
	CPMK-4				√	√	√
	CPMK-5					√	√
Deskripsi Singkat Mata Kuliah	Mata kuliah ini membahas konsep dasar ethical hacking, metode dan teknik untuk menguji keamanan sistem informasi serta pendekatan praktis dalam mengidentifikasi kerentanan dan melakukan penetration testing secara legal dan etis. Mahasiswa akan mempelajari tools populer seperti Nmap, Metasploit, Wireshark, dan Burp Suite serta menerapkan dalam studi kasus aktual dengan mempertimbangkan tanggung jawab etis.						
Bahan Kajian Materi Pembelajaran	Pengantar Ethical Hacking, Etika, Hukum						
	Jenis Hacker, Teknik Dasar Keamanan Jaringan						
	Metodologi: Reconnaissance hingga Reporting						
	Passive & Active Reconnaissance						
	Nmap, Zenmap						
	SNMP, SMB, LDAP Enumeration						
	Vulnerability Assessment						
	Tools: Metasploit, SQLMap						
	Payloads, Meterpreter						
	John the Ripper, Hydra						
	Wireshark, TCPDump						
	Penyusunan Laporan Penetration Test						
	Etika dan Tanggung Jawab Hacker						
	Simulasi Uji Penetrasi end-to-end						

Bahan Pustaka	1. Kim, D., & Solomon, M. G. (2022). Fundamentals of Information Systems Security. Jones & Bartlett Learning. 2. EC-Council. (2021). CEH: Certified Ethical Hacker v11 Official Courseware. 3. Grimes, R. A. (2021). Hacking the Hacker. Wiley. 4. Engebretson, P. (2013). The Basics of Hacking and Penetration Testing. Syngress. 5. Official Kali Linux Documentation (https://www.kali.org/docs) 6. Offensive Security (https://www.offensive-security.com)
Dosen Pengampu	QUIDO C KAINDE, ST.,MM.,MT
Mata Kuliah Prasyarat	

Mg ke-	Kemampuan Akhir Tiap Tahapan Belajar (Sub-CPMK)	Penilaian		Bentuk Pembelajaran; Metode Pembelajaran; Penugasan Mahasiswa; Estimasi Waktu		Materi Pembelajaran	Bobot Penilaian (%)
		Indikator	Bentuk Penilaian	Luring	Daring		
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
1	Menjelaskan konsep ethical hacking dan legalitas	Mahasiswa mampu menyebutkan definisi, ruang lingkup EH	Kuis online, Diskusi forum (min. 70% partisipasi)	Forum diskusi via LMS	Ceramah dan tanya jawab	Buku 1, Buku 2	5%
2	Menjelaskan jenis hacker dan teknik dasar keamanan jaringan	Mahasiswa mampu membedakan black hat & white hat hacker	Tugas ringkasan dan penilaian partisipasi diskusi	Tugas upload PDF, diskusi via LMS	Ceramah dan klasifikasi di kelas	Buku 1, Buku 3	5%
3	Menjelaskan tahapan dalam penetration testing	Mahasiswa menyebut dan jelaskan fase PT secara lengkap	Soal uraian dan latihan menyusun flow	Materi video dan kuis online	Latihan kasus PT	Buku 2, Buku 4	5%

4	Melakukan reconnaissance	Mahasiswa mengidentifikasi informasi target	Laporan hasil reconnaissance menggunakan tools	Penggunaan tools dijelaskan via video	Praktikum tools (Whois, nslookup)	Buku 4, Kali Linux Docs	5%
5	Melakukan scanning	Mahasiswa menunjukkan hasil scanning Nmap/Zemap	Laporan hasil scanning, evaluasi penggunaan tools	Panduan video dan quiz	Praktikum scanning	Buku 4, Buku 5	5%
6	Melakukan enumeration informasi	Mahasiswa dapat menunjukkan hasil enumerasi	Laporan teknik dan tools yang digunakan	Studi kasus enumeration	Praktikum menggunakan Netcat, Enum4linux	Buku 3, Offensive Security	5%
7	Mengidentifikasi kerentanan	Mahasiswa menunjukkan hasil identifikasi dengan Nessus	Analisis hasil tools vulnerability scanner	Panduan penggunaan Nessus via LMS	Praktikum eksplorasi tools	Buku 4, Buku 5	5%
8	UTS						
9	Melakukan eksploitasi kerentanan	Mahasiswa mempraktikkan eksploitasi menggunakan exploit	Laporan eksploitasi (Metasploit)	Video eksploitasi dan refleksi	Praktikum eksploitasi	Buku 4, Metasploit Docs	5%
10	Menganalisis payload dan reverse shell	Mahasiswa menjelaskan struktur payload reverse shell	Diskusi, studi kasus, dan kuis teknis	Forum diskusi teknis	Praktikum payload di Metasploit	Buku 4, Buku 5	5%
11	Melakukan password cracking	Mahasiswa mempraktikkan tools cracking dengan wordlist	Laporan hasil praktik dengan John the Ripper / Hydra	Tutorial via LMS	Praktikum brute force tools	Buku 3, Buku 4	5%
12	Melakukan sniffing traffic jaringan	Mahasiswa menganalisis hasil capture Wireshark	Laporan dengan analisis paket sniffing	Pengantar teori sniffing via video	Praktikum dengan Wireshark, TCPDump	Buku 4, Buku 5	5%

13	Menyusun laporan uji penetrasi	Mahasiswa menyusun laporan sesuai standar PT	Draft laporan diuji struktur dan kelengkapan	Template laporan dan contoh via LMS	Workshop simulasi laporan	Buku 2, Buku 4	15%
14	Menunjukkan sikap etis dalam aktivitas hacking	Mahasiswa menyelesaikan studi kasus etika hacking	Diskusi kasus, observasi sikap, post-test	Forum refleksi dan penugasan etika	Diskusi kasus nyata	Buku 1, Buku 3	15%
15	Simulasi studi kasus uji penetrasi	Mahasiswa menyajikan hasil ujian secara berkelompok	Presentasi kelompok, penilaian antar mahasiswa	Penyerahan laporan via LMS	Presentasi langsung di kelas	Buku 4, Referensi Praktikum	15%
16	UAS						

SISTEM PENILAIAN DAN SISTEM EVALUASI

A. Sistem Penilaian

1. Sistem penilaian menggunakan penilaian acuan pokok pada RPS.
2. Komponen, bobot, dan rentang penilaian sebagai berikut:
 - Komponen: nilai kompetensi (CPMK) sebesar 90% dan nilai kehadiran sebesar 10%.
 - Nilai akhir mata kuliah = jumlah nilai CPMK + nilai kehadiran.
 - Bobot masing-masing CPMK dan kehadiran dapat dilihat pada tabel berikut:

No.	Kompetensi dan Kehadiran	Bobot Penilaian						Target Pengukuran	
		Tugas (10%)	Quiz (10%)	UTS (15%)	UAS (15%)	Project (50%)	Kehadiran	Maksimal	Konversi
1.	CPMK-1	2%	2%	3%	3%	10%			A
2.	CPMK-2	2%	2%	3%	3%	10%			A
3.	CPMK-3	2%	2%	3%	3%	10%			A

4.	CPMK-4	2%	2%	3%	3%	10%			B
5.	CPMK-5	2%	2%	3%	3%	10%			B
6.	Kehadiran						0%		A
TOTAL		10%	10%	15%	15%	50%	0%	100%	A

- Rentang penilaian huruf mengikuti tabel berikut.

No .	Rentang Nilai Angka Skala 100	Nilai Angka Skala 4	Nilai Huruf
1.	80,00 – 100,00	4,00	A
2.	68,00 – 79,99	3,00	B
3.	56,00 – 67,99	2,00	C
4.	45,00 – 55,99	1,00	D
5.	00,00 – 44,99	0,00	E

B. Sistem Evaluasi

1. Mahasiswa dinyatakan lulus dalam mata kuliah ini bila nilai minimal D.
2. Nilai kehadiran mahasiswa dalam perkuliahan harus lebih dari 75%, bila kurang dari nilai tersebut maka nilai otomatis E.

	UNIVERSITAS NEGERI MANADO FAKULTAS TEKNIK PROGRAM STUDI TEKNIK INFORMATIKA					
RENCANA PEMBELAJARAN SEMESTER (RPS)						
Nama Mata Kuliah	Kode	Rumpun MK	Bobot		Semester	Tahun Ajaran
Ethical Hacking	5642765		T = 3	P =		Ganjil 2022/2023
Otorisasi/Pengesahan	Pengembang RPS		Koordinator MK		Koordinator Prodi	
	Tim Pengembang RPS Prodi TI				 Vivi P Rantung, S.T, MISD	
Capaian Pembelajaran Mata Kuliah	Capaian Pembelajaran Lulusan Program Studi (CPL Prodi) yang Dibebankan pada Mata Kuliah					
	CPL-1	Mampu menerapkan prinsip etika profesional dalam bidang teknologi informasi.				
	CPL-2	Menguasai konsep dasar keamanan jaringan dan sistem informasi.				
	CPL-3	Mampu mengidentifikasi dan menganalisis kerentanan pada sistem dan jaringan.				
	CPL-4	Mampu menggunakan tools ethical hacking secara profesional dan bertanggung jawab.				
	CPL-5	Mampu bekerja sama dalam tim dan menyampaikan hasil secara efektif.				
	Capaian Pembelajaran Mata Kuliah (CPMK)					
	CPMK-1	Memahami konsep dasar ethical hacking dan ruang lingkupnya.				
	CPMK-2	Menjelaskan metodologi dan tahapan ethical hacking.				
	CPMK-3	Melakukan scanning, enumeration, dan eksploitasi kerentanan pada sistem dengan tools legal.				
	CPMK-4	Mengevaluasi hasil uji penetrasi dan menyusun laporan secara profesional.				
	CPMK-5	Menunjukkan sikap profesional dan etika dalam seluruh aktivitas ethical hacking.				
	Kemampuan Akhir Tiap Tahapan Belajar (Sub-CPMK)					
	Sub-CPMK-1	Menjelaskan konsep dasar ethical hacking dan legalitasnya.				
	Sub-CPMK-2	Menjelaskan langkah-langkah dalam metodologi ethical hacking.				

	Sub-CPMK-3	Mengoperasikan tools scanning dan enumeration.					
	Sub-CPMK-4	Melakukan eksploitasi terhadap kerentanan yang ditemukan.					
	Sub-CPMK-5	Menganalisis dan melaporkan hasil penetration testing.					
	Sub-CPMK-6	Menerapkan etika dan hukum dalam praktik ethical hacking.					
	Korelasi CPMK terhadap Sub-CPMK						
		Sub-CPMK-1	Sub-CPMK-2	Sub-CPMK-3	Sub-CPMK-4	Sub-CPMK-5	Sub-CPMK-6
	CPMK-1	√	√				
	CPMK-2		√	√	√		
	CPMK-3			√	√	√	
	CPMK-4				√	√	√
CPMK-5					√	√	
Deskripsi Singkat Mata Kuliah	Mata kuliah ini membahas konsep dasar ethical hacking, metode dan teknik untuk menguji keamanan sistem informasi serta pendekatan praktis dalam mengidentifikasi kerentanan dan melakukan penetration testing secara legal dan etis. Mahasiswa akan mempelajari tools populer seperti Nmap, Metasploit, Wireshark, dan Burp Suite serta menerapkan dalam studi kasus aktual dengan mempertimbangkan tanggung jawab etis.						
Bahan Kajian Materi Pembelajaran	Pengantar Ethical Hacking, Etika, Hukum						
	Jenis Hacker, Teknik Dasar Keamanan Jaringan						
	Metodologi: Reconnaissance hingga Reporting						
	Passive & Active Reconnaissance						
	Nmap, Zenmap						
	SNMP, SMB, LDAP Enumeration						
	Vulnerability Assessment						
	Tools: Metasploit, SQLMap						
	Payloads, Meterpreter						
	John the Ripper, Hydra						
	Wireshark, TCPDump						
	Penyusunan Laporan Penetration Test						
	Etika dan Tanggung Jawab Hacker						
	Simulasi Uji Penetrasi end-to-end						

Bahan Pustaka	1. Kim, D., & Solomon, M. G. (2022). Fundamentals of Information Systems Security. Jones & Bartlett Learning. 2. EC-Council. (2021). CEH: Certified Ethical Hacker v11 Official Courseware. 3. Grimes, R. A. (2021). Hacking the Hacker. Wiley. 4. Engebretson, P. (2013). The Basics of Hacking and Penetration Testing. Syngress. 5. Official Kali Linux Documentation (https://www.kali.org/docs) 6. Offensive Security (https://www.offensive-security.com)
Dosen Pengampu	FERDINAN I SANGKOP
Mata Kuliah Prasyarat	

Mg ke-	Kemampuan Akhir Tiap Tahapan Belajar (Sub-CPMK)	Penilaian		Bentuk Pembelajaran; Metode Pembelajaran; Penugasan Mahasiswa; Estimasi Waktu		Materi Pembelajaran	Bobot Penilaian (%)
		Indikator	Bentuk Penilaian	Luring	Daring		
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
1	Menjelaskan konsep ethical hacking dan legalitas	Mahasiswa mampu menyebutkan definisi, ruang lingkup EH	Kuis online, Diskusi forum (min. 70% partisipasi)	Forum diskusi via LMS	Ceramah dan tanya jawab	Buku 1, Buku 2	5%
2	Menjelaskan jenis hacker dan teknik dasar keamanan jaringan	Mahasiswa mampu membedakan black hat & white hat hacker	Tugas ringkasan dan penilaian partisipasi diskusi	Tugas upload PDF, diskusi via LMS	Ceramah dan klasifikasi di kelas	Buku 1, Buku 3	5%
3	Menjelaskan tahapan dalam penetration testing	Mahasiswa menyebut dan jelaskan fase PT secara lengkap	Soal uraian dan latihan menyusun flow	Materi video dan kuis online	Latihan kasus PT	Buku 2, Buku 4	5%

4	Melakukan reconnaissance	Mahasiswa mengidentifikasi informasi target	Laporan hasil reconnaissance menggunakan tools	Penggunaan tools dijelaskan via video	Praktikum tools (Whois, nslookup)	Buku 4, Kali Linux Docs	5%
5	Melakukan scanning	Mahasiswa menunjukkan hasil scanning Nmap/Zemap	Laporan hasil scanning, evaluasi penggunaan tools	Panduan video dan quiz	Praktikum scanning	Buku 4, Buku 5	5%
6	Melakukan enumeration informasi	Mahasiswa dapat menunjukkan hasil enumerasi	Laporan teknik dan tools yang digunakan	Studi kasus enumeration	Praktikum menggunakan Netcat, Enum4linux	Buku 3, Offensive Security	5%
7	Mengidentifikasi kerentanan	Mahasiswa menunjukkan hasil identifikasi dengan Nessus	Analisis hasil tools vulnerability scanner	Panduan penggunaan Nessus via LMS	Praktikum eksplorasi tools	Buku 4, Buku 5	5%
8	UTS						
9	Melakukan eksploitasi kerentanan	Mahasiswa mempraktikkan eksploitasi menggunakan exploit	Laporan eksploitasi (Metasploit)	Video eksploitasi dan refleksi	Praktikum eksploitasi	Buku 4, Metasploit Docs	5%
10	Menganalisis payload dan reverse shell	Mahasiswa menjelaskan struktur payload reverse shell	Diskusi, studi kasus, dan kuis teknis	Forum diskusi teknis	Praktikum payload di Metasploit	Buku 4, Buku 5	5%
11	Melakukan password cracking	Mahasiswa mempraktikkan tools cracking dengan wordlist	Laporan hasil praktik dengan John the Ripper / Hydra	Tutorial via LMS	Praktikum brute force tools	Buku 3, Buku 4	5%
12	Melakukan sniffing traffic jaringan	Mahasiswa menganalisis hasil capture Wireshark	Laporan dengan analisis paket sniffing	Pengantar teori sniffing via video	Praktikum dengan Wireshark, TCPDump	Buku 4, Buku 5	5%

13	Menyusun laporan uji penetrasi	Mahasiswa menyusun laporan sesuai standar PT	Draft laporan diuji struktur dan kelengkapan	Template laporan dan contoh via LMS	Workshop simulasi laporan	Buku 2, Buku 4	5%
14	Menunjukkan sikap etis dalam aktivitas hacking	Mahasiswa menyelesaikan studi kasus etika hacking	Diskusi kasus, observasi sikap, post-test	Forum refleksi dan penugasan etika	Diskusi kasus nyata	Buku 1, Buku 3	5%
15	Simulasi studi kasus uji penetrasi	Mahasiswa menyajikan hasil ujian secara berkelompok	Presentasi kelompok, penilaian antar mahasiswa	Penyerahan laporan via LMS	Presentasi langsung di kelas	Buku 4, Referensi Praktikum	5%
16	UAS						

SISTEM PENILAIAN DAN SISTEM EVALUASI

A. Sistem Penilaian

1. Sistem penilaian menggunakan penilaian acuan pokok pada RPS.
2. Komponen, bobot, dan rentang penilaian sebagai berikut:
 - Komponen: nilai kompetensi (CPMK) sebesar 90% dan nilai kehadiran sebesar 10%.
 - Nilai akhir mata kuliah = jumlah nilai CPMK + nilai kehadiran.
 - Bobot masing-masing CPMK dan kehadiran dapat dilihat pada tabel berikut:

No.	Kompetensi dan Kehadiran	Bobot Penilaian						Target Pengukuran	
		Tugas (10%)	Quiz (10%)	UTS (15%)	UAS (15%)	Project (50%)	Kehadiran	Maksimal	Konversi
1.	CPMK-1	2%	2%	3%	3%	10%			A
2.	CPMK-2	2%	2%	3%	3%	10%			A
3.	CPMK-3	2%	2%	3%	3%	10%			A

4.	CPMK-4	2%	2%	3%	3%	10%			B
5.	CPMK-5	2%	2%	3%	3%	10%			B
6.	Kehadiran						0%		A
TOTAL		10%	10%	15%	15%	50%	0%	100%	A

- Rentang penilaian huruf mengikuti tabel berikut.

No	Rentang Nilai Angka Skala 100	Nilai Angka Skala 4	Nilai Huruf
1.	80,00 – 100,00	4,00	A
2.	68,00 – 79,99	3,00	B
3.	56,00 – 67,99	2,00	C
4.	45,00 – 55,99	1,00	D
5.	00,00 – 44,99	0,00	E

B. Sistem Evaluasi

1. Mahasiswa dinyatakan lulus dalam mata kuliah ini bila nilai minimal D.
2. Nilai kehadiran mahasiswa dalam perkuliahan harus lebih dari 75%, bila kurang dari nilai tersebut maka nilai otomatis E.