A. RENCANA PEMBELAJARAN SEMESTER (RPS) BERDASARKAN PERMENRISTEKDIKTI NO. 44/2015 SNPT PASAL 12

RENCANA PEMBELAJARAN SEMESTER

MATA KULIAH : NETWORK SECURITY
SKS : 3
KODE : 1565059
PROGRAM STUDI : TEKNIK INFORMATIKA
SEMESTER : 3
NAMA DOSEN PENGAMPU : Johan Ericka W.P, M.Kom
COURSE LEARNING OUTCOMES (Capaian Pembelajaran Mata Kuliah) : 1. Students are able to explain the concept of network security.

Minggu Ke-	Kemampuan yang Diharapkan pada Setiap Pertemuan	Bahan Kajian	Metode Pembelajaran	Waktu Belajar (Menit)	Pengalaman Belajar Mahasiswa (Deskripsi Tugas)	Kriteria, Indikator dan Bobot Penilaian	Daftar Referensi yang digunakan
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
Ke-1	Mahasiswa mampu memahami tentang topologi jaringan komputer secara fisik	Computer network topology : - BUS - Ring - Star - Tree - Mesh	Diskusi di kelas	3 x 50 menit	1. Mahasiswa memahami kelebihan & kekurangan masing – masing topologi jaringan komputer	6.25 %	
Ke-2	Mahasiswa mampu memahami tentang OSI Layer & TCP/IP layer	OSI vs TCP/IP Layer : - Layer 1 - Layer 2 - Layer 3 - Layer 4 - Layer 7	Diskusi di kelas	3 x 50 menit	1. Mahasiswa memahami proses yang terjadi di masing – masing layer	6.25 %	
Ke-3	Mahasiswa mampu memahami tentang Protokol umum di jaringan komputer	Protokol umum jaringan komputer - TCP - UDP - ICMP - FTP - SSH - HTTP - HTTPS	Diskusi di kelas	3 x 50 menit	1. Mahasiswa memahami konsep dan implementasi protocol – protocol tersebut di dunia nyata	6.25 %	
Ke-4	Mahasiswa mampu memahami tentang kelemahan dari sisi	Kelemahan di sisi user : - Personal (social engineering)	Diskusi di kelas	3 x 50 menit	1. Mahasiswa memahami tentang social engineering,	6.25 %	

Minggu Ke-	Kemampuan yang Diharapkan pada Setiap Pertemuan	Bahan Kajian	Metode Pembelajaran	Waktu Belajar (Menit)	Pengalaman Belajar Mahasiswa (Deskripsi Tugas)	Kriteria, Indikator dan Bobot Penilaian	Daftar Referensi yang digunakan
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
	pengguna / user	- Perangkat (crack, backdoor) - Aplikasi (backdoor)			backdoor pada sistem operasi dan aplikasi		
Ke-5	Mahasiswa mampu memahami tentang kelemahan dari sisi jaringan komputer	Kelemahan di sisi jaringan kabel : - Switch vs Hub - Tap port Kelemahan di sisi jaringan nirkabel : - How wireless network works - Packet Sniffing - MITM Attack	Diskusi di kelas	3 x 50 menit	1. Mahasiswa memahami tentang celah kelemahan di jaringan komputer kabel & nirkabel	6.25 %	
Ke-6	Mahasiswa mampu memahami tentang kelemahan dari sisi server	Kelemahan di sisi server : - Fisik - Sistem operasi - Aplikasi	Diskusi di kelas	3 x 50 menit	1. Mahasiswa memahami tentang celah kelemahan di server	6.25 %	
Ke-7	Mahasiswa mampu memahami tentang eksploitasi kelemahan yang ada pada pengguna	Eksploitasi kelemahan pada pengguna : - Social engineering - Password bruteforce - Phising - Virus / malware	Diskusi di kelas	3 x 50 menit	1. Mahasiswa memahami teknik melakukan serangan terhadap pengguna	6.25 %	
Ke-8	UJIAN TENGAH SEMESTER						
Ke-9	Mahasiswa mampu memahami tentang eksploitasi kelemahan yang ada pada jaringan komputer	Eksploitasi kelemahan pada jaringan komputer - ARP Poison - DNS Cache poisoning - MITM attack - DHCP Rogue	Diskusi di kelas	3 x 50 menit	1. Mahasiswa memahami teknik melakukan serangan terhadap server	6.25 %	
Ke-10	Mahasiswa mampu memahami tentang eksploitasi kelemahan yang ada pada server	Eksploitasi kelemahan pada server - Port scanning - OS weakness	Diskusi di kelas	3 x 50 menit	Mahasiswa memahami teknik melakukan serangan terhadap server	6.25 %	

Minggu Ke-	Kemampuan yang Diharapkan pada Setiap Pertemuan	Bahan Kajian	Metode Pembelajaran	Waktu Belajar (Menit)	Pengalaman Belajar Mahasiswa (Deskripsi Tugas)	Kriteria, Indikator dan Bobot Penilaian	Daftar Referensi yang digunakan
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
		- DDoS - SQL injection - XSS					
Ke-11	Mahasiswa mampu memahami tentang mitigasi resiko keamanan pada sisi pengguna	Mitigasi resiko kelemahan pada pengguna : - Social engineering - Password bruteforce - Phising - Virus / malware - Backup procedures	Diskusi di kelas	3 x 50 menit	1. Mahasiswa memahami teknik melakukan mitigasi resiko kelemahan pada sisi pengguna	6.25 %	
Ke-12	Mahasiswa mampu memahami tentang mitigasi resiko keamanan pada sisi jaringan komputer	Mitigasi resiko kelemahan pada jaringan komputer - Network firewall - NIDS / NIPS - VLAN	Diskusi di kelas	3 x 50 menit	Mahasiswa memahami teknik melakukan mitigasi resiko kelemahan pada sisi jaringan komputer	6.25 %	
Ke-13	Mahasiswa mampu memahami tentang mitigasi resiko keamanan pada sisi server	Mitigasi resiko kelemahan pada server - UFW - Packet Filtering - Log Auditing - Server monitoring	Diskusi di kelas	3 x 50 menit	Mahasiswa memahami teknik melakukan mitigasi resiko kelemahan pada sisi server	6.25 %	
Ke-14	Mahasiswa mampu memahami tentang aturan seputar keamanan jaringan komputer	Network security policy : - UU ITE - ISO 27001-27002 - SOP	Diskusi di kelas	3 x 50 menit	Mahasiswa memahami aturan – aturan yang ada seputar keamanan jaringan komputer	6.25 %	
Ke-15	Mahasiswa mampu mengimplementasikan ilmu yang dipelajari	Proof of Concept	Diskusi di kelas	3 x 50 menit	Mahasiswa memahami implementasi dari ilmu yang telah dipelajari	6.25 %	
Ke-16	UJIAN AKHIR SEMESTER						

Daftar referensi :

1. **Prakasa, Johan E.W (2019), Konsep Dasar Jaringan Komputer. Penerbit : UIN Press**
2. **Regalado, Daniel et. al (2015), Gray Hat Hacking The Ethical Hacker's Handbook 4th edition. Penerbit : McGraw Hill**
3. **Canavan, John E (2001), Fundamentals of Network Security. Penerbit : Artech House telecommunications library**

Malang, 21 januari 2019
Dosen Pengampu Mata Kuliah

Johan Ericka W.P, M.Kom