|  |  |  |  |
| --- | --- | --- | --- |
|  | Departemen | : | Teknologi Informasi |
| Kode Mata Kuliah | : | IT – 504 |
| Bobot SKS | : | 3 |
| Status Revisi | : | 0 |
| Tanggal Efektif | : |  |

RENCANA

PEMBELAJARAN

(Course Plan)

NAMA MATA KULIAH

|  |
| --- |
| TEKNOLOGI KEAMANAN SISTEM INFORMASI |

|  |  |  |
| --- | --- | --- |
| Disiapkan oleh | Diperiksa oleh | Disetujui oleh |
|  |  |  |
| Ventje Jeremias Lewi Engel, M.T. | Dr. Herry I. Sitepu | Dr. Ir. Roland Y.H. Silitonga, M.T. |
| Dosen/Dosen Pengampu | Ketua Program Studi | Direktur Akademik |

**INSTITUT TEKNOLOGI HARAPAN BANGSA**

**2018**

**2018/2019**

**Course Plan**

**IT - 504**

**Teknologi Keamanan Sistem Informasi**

Ventje Jeremias Lewi Engel, M.T.

**DEPARTEMEN TEKNOLOGI INFORMASI**

**INSTITUT TEKNOLOGI HARAPAN BANGSA**

**2018**

SEMESTER GANJIL 2018/2019

***(IT-504) Teknologi Keamanan Sistem Informasi***

**KONTEKS MATA KULIAH DALAM *GRADUATE PROFILE***

Matakuliah ini bertujuan untuk mengembangkan:

1. **Kompetensi**: pengetahuan dan kemampuan untuk menguji, menganalisis dan memperbaiki celah keamanan dalam sistem operasi, jaringan komputer, dan aplikasi web.
2. **Karakter**: sikap yang berorientasi pada tujuan, serta kemampuan bekerjasama.
3. **Komitmen**: kesadaran dan komitmen untuk melakukan hal-hal yang menambah nilai (*value creating*) di manapun mahasiswa kelak berkarir.

**SASARAN KULIAH (*LEARNING OUTCOMES*)**

Setelah mengikuti mata kuliah ini mahasiswa diharapkan untuk mampu:

1. Mahasiswa mampu menjelaskan aspek-aspek keamanan internet dan metodologi analisisnya
2. Mahasiswa mampu menguji keamanan sistem operasi komputer, menganalisis dan memperbaiki celah keamanannya
3. Mahasiswa mampu menguji keamanan jaringan komputer, menganalisis dan memperbaiki celah keamanannya
4. Mahasiswa mampu menguji keamanan web, menganalisis dan memperbaiki celah keamanannya

**CAPAIAN PEMBELAJARAN LULUSAN (*CPL*) PROGDI**

1. Mampu merencanakan, mengimplementasikan, dan mengoptimalisasikan pengembangan perangkat lunak, jaringan komputer, telekomunikasi, dan otomasi, sesuai dengan spesifikasi yang dibutuhkan.
2. Menguasai keilmuan di bidang konstruksi perangkat lunak, jaringan komputer, telekomunikasi, dan otomasi.
3. Mampu menguji, mengukur, dan menganalisis kinerja sistem komputer, perangkat lunak, jaringan komputer, telekomunikasi, dan otomasi untuk menyajikan solusi terhadap permasalahan.
4. Bertanggung jawab pada pekerjaan sendiri dan dapat diberi tanggung jawab atas pencapaian hasil kerja organisasi.
5. Menguasai konsep dan teknik terkait dengan fungsi bisnis (kebijakan dan strategi bisnis, organisasi, SDM, sistem informasi, akuntansi, dan keuangan, pemasaran, operasi bisnis), prinsip kepemimpinan dan kewirausahaan dalam bidang teknologi informasi serta mampu mengevaluasi peluang di bidang teknologi informasi dan merealisasikannya menjadi bisnis teknologi informasi.
6. Mampu bekerja secara efektif dalam tim dan mampu berkomunikasi secara lisan dan tulisan dengan efektif menggunakan bahasa Indonesia dan Inggris.
7. Memiliki kesadaran, kemauan dan kemampuan untuk belajar secara mandiri dan berkelanjutan guna meningkatkan kapasitas dan kemampuan untuk menghadapi situasi/ tantangan hidup yang dinamis.
8. Memiliki sertifikasi profesional dalam bidang jaringan serta pemrograman komputer dari lembaga sertifikasi profesi internasional.

**SASARAN KULIAH (*LEARNING OUTCOMES*)**

| **CPL MK** | **CPL PRODI** |
| --- | --- |
| **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** |
| Mahasiswa mampu menjelaskan aspek-aspek keamanan internet dan metodologi analisisnya. |  | **✔** |  |  |  |  |  |  |
| Mahasiswa mampu menguji keamanan sistem operasi komputer, menganalisis dan memperbaiki celah keamanannya. |  |  | **✔** |  |  |  |  |  |
| Mahasiswa mampu menguji keamanan jaringan komputer, menganalisis dan memperbaiki celah keamanannya. |  |  | **✔** |  |  |  |  |  |
| Mahasiswa mampu menguji keamanan web, menganalisis dan memperbaiki celah keamanannya. |  |  | **✔** |  |  |  |  |  |

**MATERI KULIAH**

Keamanan informasi; keamanan fisik; keamanan sistem operasi; autentikasi; akses kendali; proses & memori; jaringan komputer; reconnaissance; scanning; firewall; teknologi web; serangan traversing; SQL Injection; cross site scripting (XSS); reflected XSS; stored XSS; keamanan session; session hijacking

**DAFTAR PUSTAKA**

1. Easttom, C. 2016*. Computer Security Fundamentals*. 3rd Edition. Pearson Education, Inc.
2. Gibson, D. 2011. *CompTIA Security+ Get Certified Get Ahead*. CreateSpace
3. Gutierrez, G. 2016. *Kali Linux Web Penetration Testing Cookbook*. Packt Publishing Ltd.

**EVALUASI DAN PENILAIAN**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ***Learning Outcomes*** | **Tugas****(25%)** | **Sikap dan Keaktifan****(10%)** | **Kuis****(10%)** | **UTS****(20%)** | **UAS****(35%)** |
| Mahasiswa mampu menjelaskan aspek-aspek keamanan internet dan metodologi analisisnya | **✔** |  |  | **✔** |  |
| Mahasiswa mampu menguji keamanan sistem operasi komputer, menganalisis dan memperbaiki celah keamanannya | **✔** |  | **✔** | **✔** |  |
| Mahasiswa mampu menguji keamanan jaringan komputer, menganalisis dan memperbaiki celah keamanannya | **✔** |  | **✔** | **✔** | **✔** |
| Mahasiswa mampu menguji keamanan web, menganalisis dan memperbaiki celah keamanannya | **✔** |  | **✔** |  | **✔** |

**KEHADIRAN**

Minimal 80% sebagai syarat diprosesnya nilai.

**TATA TERTIB & DISIPLIN KELAS**

1. Peserta wajib membaca bacaan persiapan sebelum masuk kelas.
2. Peserta diwajibkan aktif dalam diskusi kelas.
3. Keterlambatan masuk kelas maksimum 15 menit.
4. Plagiasi tugas atau kuis diberikan sanksi nilai 0. Khusus plagiasi ujian nilai mata kuliah otomatis E.
5. Keterlambatan pengumpulan tugas diberikan penalti -10 poin per jam.

**KUIS**

Direncanakan akan dilaksanakan 2-3 kali selama 1 semester dengan menggunakan bahan yang sudah dipelajari. Kuis akan dilaksanakan sewaktu-waktu, bisa dengan atau tanpa pemberitahuan terlebih dahulu. Bagi mahasiswa yang tidak hadir ketika pelaksanaan kuis, tidak akan ada kuis susulan.

**UAS**

UAS dilaksanakan pada minggu terakhir perkuliahan. UAS akan diselenggarakan dalam bentuk ujian praktek.

**PRAKTIKUM**

Mata kuliah ini disertai dengan kegiatan praktikum di laboratorium. Pelaksanaan praktikum diatur terpisah.

**JADWAL PERKULIAHAN**

| **MINGGU KE-** | **TOPIK** | **TUJUAN** | **PERSIAPAN***(bahan yang harus dibaca mahasiswa sebelum kuliah)* | **PENGUKURAN** |
| --- | --- | --- | --- | --- |
| 1 | **Pengantar Keamanan Informasi*** 1. Definisi Keamanan Informasi
	2. Prinsip-Prinsip Keamanan Informasi
	3. Ruang Lingkup TKSI
	4. Celah Keamanan dan *Penetration Testing*
 | * Menerangkan prinsip-prinsip keamanan informasi
* Mencontohkan prinsip-prinsip keamanan informasi dalam praktek
* Menerangkan ruang lingkup teknologi keamanan sistem informasi
* Mendapatkan gambaran langkah-langkah penetration testing untuk analisis celah keamanan
* Menyatakan dan mengingat etika dalam melakukan *pentest*
 | Ref. 1 Ch. 1Ref. 2 Ch. 1 | * Tanya-jawab lisan
* Tugas 1
 |
| 2 | **Keamanan Sistem Operasi I*** 1. Pengamanan Komputer
	2. *Authentication vs. Authorization*
	3. Kendali Akses di Windows dan Linux
 | * Mencontohkan cara pengamanan komputer secara fisik
* Membedakan proses autentikasi dan *authorization* dalam pengamanan akses komputer
* Menerangkan dan mencontohkan jenis autentikasi
* Membandingkan mekanisme autentikasi *single-factor* dengan *two-factor*
* Menggunakan fitur pengamanan kendali akses untuk *authorization* di Windows & Linux
 | Ref. 1 Ch. 1Ref. 2 Ch. 2 | * Tanya-jawab lisan
* Tugas 2
 |
| 3 | **Keamanan Sistem Operasi II*** 1. Hubungan Proses dan Memori dalam OS
	2. Peran Alokasi Memori
	3. Akses dan Manipulasi Memori
 | * Menyimpulkan pentingnya keamanan pada memori dalam OS
* Mengidentifikasi dan menerangkan peran alokasi memori: *heap*, *stack*, *static*
* Mengakses dan memanipulasi memori kerja pada Windows
* Mengakses dan memanipulasi memori kerja pada Linux
 | Ref. 1 Ch. 1 | * Tanya-jawab lisan
* Tugas 3
 |
| 4 | **Dasar Keamanan Jaringan*** 1. Akses Sumber Daya
	2. Autentikasi dan Akses Kendali
	3. Enkripsi dalam Jaringan
 | * Mengakses dan mengidentifikasi sumber daya dalam jaringan
* Menerangkan proses autentikasi dan akses kontrol dalam jaringan
* Menggambarkan mekanisme autentikasi dengan pihak ketiga
* Menerangkan kebutuhan enkripsi untuk keamanan data dalam jaringan
* Mencontohkan beberapa metode enskripsi dan karakteristik penggunaannya
 | Ref. 1 Ch. 2Ref. 2 Ch. 3 | * Tanya-jawab lisan
* Tugas 4
 |
| 5 | ***Recon*, *Scan*, dan *Exploit***1. *Reconnaissance*
2. *Scanning*
3. *Exploit*
 | * Menyimpulkan pentingnya melakukan pengumpulan informasi untuk analisis celah keamanan dalam jaringan
* Mengidentifikasi informasi sumber daya yang akan dikumpulkan: infrastruktur, topologi, IP dan subnet
* Membedakan metode pengumpulan informasi *recon* dengan *scanning*: Kali Linux
* Menggunakan berbagai *tools* untuk *recon* dan *scanning* jaringan
* Menggunakan hasil *recon* dan *scanning* untuk eksploitasi: menaikkan level akses
 | Ref. 1 Ch. 11Ref. 2 Ch. 4 | * Tanya-jawab lisan
* Tugas 5
 |
| 6 | **Firewall dan Nmap**1. Firewall: Pengamanan
2. Nmap: Celah Keamanan
 | * Menjelaskan mekanisme *firewall* dalam jaringan
* Membedakan metode *firewall* secara *hardware* maupun *software*
* Memetakan fungsi *firewall* dengan kebutuhan sistem dan bisnis
* Mengkonfigurasi *firewall* sesuai dengan kebutuhan bisnis
* Mengidentifikasi celah keamanan jaringan dengan Nmap
* Mengkonfigurasi *firewall* sesuai dengan hasil Nmap
 | Ref. 1 Ch. 9Ref. 2 Ch. 5 | * Tanya-jawab lisan
* Tugas 6
 |
| 7 | **UTS** |  |  |  |
| 8 | **Teknologi Web dan Internet*** 1. HTTP
	2. Enkoding HTML & Cookies
	3. *Client-Side* dan *Server-Side*
	4. *Browser*
 | * Menerangkan mekanisme HTTP untuk *world wide web* (WWW)
* Mengakses dan menjelaskan *header* HTTP, HTTP *Request*, dan HTTP *Response*
* Mencontohkan enkoding HTML dan Cookies untuk halaman web
* Membedakan teknologi web yang digunakan untuk *client-side* dengan yang *server-side*
* Menggunakan *browser* *development tools* untuk melihat struktur dan operasi halaman web
 | Ref. 3 Ch. 1Various Ref | * Tanya-jawab lisan
* Tugas 7
 |
| 9 | **Recon & Scanning untuk Web** | * Menyimpulkan pentingnya melakukan pengumpulan informasi untuk analisis celah keamanan web
* Mengidentifikasi informasi sumber daya yang akan dikumpulkan: teknologi, tipe CMS, *database*, IP, domain dan subdomain
* Menggunakan mesin pencari Google untuk melakukan *recon*
* Menggunakan berbagai *tools* untuk melakukan *scanning* web
* Menggunakan hasil *recon* dan *scanning* untuk melakukan eksploitasi: akses *file*
 | Ref. 3 Ch. 2, 3 | * Tanya-jawab lisan
* Tugas 8
 |
| 10 | **Harvesting & Traversing*** 1. Harvesting
	2. Command Injection
	3. File Inclusion & Directory Traversal
 | * Menerangkan definisi serangan ke web yang termasuk dalam *non-programming attack*: *harvesting* dan *traversing*
* Mencontohkan serangan dan mengidentifikasi celah keamanan web terhadap *username harvesting*
* Mencontohkan serangan dan mengidentifikasi celah keamanan terhadap *command injection*
* Mencontohkan serangan dan mengidentifikasi celah keamanan web terhadap *file inclusion - directory traversal*
 | Ref. 3 Ch. 9 | * Tanya-jawab lisan
* Tugas 9
 |
| 11 | **SQL Injection*** 1. Celah Input
	2. SQL Syntax
	3. SQL Injection
 | * Menerangkan definisi serangan SQL *Injection*
* Mengenal dan menggunakan SQL untuk *query* dan operasi tabel
* Mengidentifikasi celah keamanan *input* di web untuk SQL *Injection* Mencontohkan serangan SQL *Injection* langsung di Web
* Mencontohkan serangan SQL *Injection* menggunakan *tools*
 | Ref. 3 Ch. 4, 6 | * Tanya-jawab lisan
* Tugas 10
 |
| 12 | **CrossSite Scripting (XSS)**12.1 Javascript di Web12.2 Reflected XSS12.3 Stored XSS | * Menerangkan definisi serangan *cross site scripting* (XSS)
* Mengidentifikasi jenis serangan yang termasuk ke dalam XSS
* Mencontohkan berbagai kode web yang memiliki kelemahan terhadap XSS
* Membandingkan karakteristik, kelebihan, dan kelemahan 3 tipe XSS: *reflected*, *stored*, dan DOM-*based*
* Menggambarkan mekanisme menutup celah keamanan terhadap XSS
 | Ref. 3 Ch. 4, 6 | * Tanya-jawab lisan
* Tugas 11
 |
| 13 | **Session Security**13.1 Session13.2 Session Hijacking & Fixation13.3 Serangan Session dengan Packet Sniffing | * Menyimpulkan kegunaan *session* dalam menyimpan informasi di web
* Mengakses dan mendapatkan *session* web: URL, HTML, HTML5 WebStorage
* Membedakan karakteristik 2 macam serangan *session*: *session hijacking* dan *session fixation*
* Mencontohkan serangan *session hijacking* melalui XSS
* Mencontohkan serangan *session hijacking* dengan *packet sniffing*
 | Ref. 3 Ch. 4, 6 | * Tanya-jawab lisan
 |
| 14 | **UAS** |  |  |  |