



UNIVERSITAS MATARAM
(University of Mataram)
FAKULTAS TEKNIK
(Faculty of Engineering)
PROGRAM STUDI TEKNIK INFORMATIKA
(Department of Informatics Engineering)

MODULE HANDBOOK DESCRIPTION

Information Technology Security (D18KB304)

| | |
|---|---|
| Module designation | Information Technology Security |
| Semester(s) in which the module is taught | <i>5 / third year</i> |
| Person responsible for the module | <i>Ahmad Zafrullah Mardiansyah, S.T., M.Eng.</i> |
| Language | <i>Indonesian</i> |
| Relation to curriculum | <i>Compulsory</i> |
| Teaching methods | <i>Lectures, Discussions, Project</i> |
| Workload (incl. contact hours, self-study hours) | Contact Hours every week, each week of the 16 weeks/semester including Evaluation <ul style="list-style-type: none"> ● 2 x 50 minutes lecturer/week ● 2 x 60 minutes class exercise/week ● Self Study hours = 120 minutes/week Total workload 340 minutes/week |
| Credit points | <i>2 (~ 3,2 ECTS)</i> |
| Required and recommended prerequisites for joining the module | |

| | |
|---|--|
| <p>Module objectives/intended learning outcomes</p> | <ol style="list-style-type: none"> 1) Introduction <ol style="list-style-type: none"> a. Element of information security b. Trend of information security c. Hacking concept d. Hacking attack vector e. Penetration testing f. Law and regulations 2) Footprinting and Reconnaissance <ol style="list-style-type: none"> a. Footprinting concept b. Search engine and google advance hacking c. Social media footprinting d. Email footprinting e. Whois, DNS, Network footprinting f. Social engineering g. Footprinting tools h. Footprinting for penetration testing 3) Vulnerability Analysis <ol style="list-style-type: none"> a. Type of vulnerability b. Vulnerability Assessment c. Assessment tools d. Assessment reporting 4) Sniffing <ol style="list-style-type: none"> a. Sniffing concept b. MAC and DHCP attack c. ARP and DNS poisoning d. Sniffing tools e. Sniffing for penetration testing 5) Denial of Service <ol style="list-style-type: none"> a. DoS dan DDoS fundamental b. Botnet concept c. DoS tools d. DoS for penetration testing 6) SQL Injection <ol style="list-style-type: none"> a. SQLi concept b. Type of SQLi c. SQLi tools a. SQLi detection tools |
| <p>Content</p> | <p>The Information Technology Security course provides an understanding of security concepts, system understanding, and system security, evaluation of system security, securing information systems, email security, web security, exploitation of system security, cyber law, and wireless system security.</p> |

| | |
|------------------------------------|---|
| Examination forms | <i>Assignments, Quiz, Simulation, Project (Oral Presentation)</i> |
| Study and examination requirements | <i>Assignments 10%, Quiz 25%, Simulation 25%, Project 40%</i> |
| Reading list | 1. Certified Ethical Hacker V10 |