Module designation	CE641 Computer Network Security
Semester(s) in which the module is taught	5
Person responsible for the module	Samuel Hutagalung
Language	Indonesian
Relation to curriculum	Compulsory
Teaching methods	Lecture, Interactive Multimedia, Independent Learning
Workload (incl. contact hours, self-study hours)	Total workload: 90.72 hours - 23.34 Synchronous lecture. - 56.04 Self-study and assignments in the form of essays. - 2x5.67 related to exam project and self study
Credit points	2 / 3.36 ECTS
Required and recommended prerequisites for joining the module	CE449 Computer Network
Module objectives/intended learning outcomes	Module objectives: Able to analyze the basic principles of singular computer system and network security problems with their solutions. ELO (Performance Indicator) : H1 - Understand the concept of communications between computer systems, operating systems, and computer security.
Content	This course discusses definitions and understandings on computer security, particularly the networks security, operating system security, and web security. The course starts with basic principles of computer security, the problems, and lastly the solutions for preventing and detecting security attacks.
Examination forms	Written Test
Study and examination requirements	The total weighted average for the assignments (30%), midterm (30%), and final (40%) exams must be >= 55.
Reading list	1. Stallings, William, 2013, Cryptography and Network Security: Principles and Practice (6th Edition), Prentice Hall. 2. Reflections on Trusting Trust, Ken Thompson

	3. Measuring Pay-per-Install: The Commoditization of Malware Distribution, by J. Caballero, C. Grier, C. Kreibich, V. Paxson. 4. Buffer Overflows: Attacks and Defenses for the Vulnerability of the Decade, Crispin Cowan, et al. 5. Basic Integer Overflows, blexim 6. Bypassing Browser Memory Protections, A. Sotirov 7. SetUID Demystified, Chen, Dean, and Wagner, 2002. 8. Operating Systems Security, T. Jaegeri, 2008. Chapter 4, Security in Ordinary Operating Systems. 9. The BREACH attack: encryption and compression don't mix, by Gluck, Harris, and Prado 10. The case for prefetching and prevalidating TLS server certificates, by E. Stark, L.S. Huang, et al. 11. Securing Browser Frame Communication. Adam Barth, Collin Jackson, and John C. Mitchell 12. The Security Architecture of the Chromium Browser. Adam Barth, Collin Jackson, Charles Reis, and the Google Chrome Team 13. Exposing private information by timing web applications. A. Bortz, D. Boneh, and P. Nandy 14. Cross site scripting explained, Amit Klein 15. SQL Injection attacks, Chris Anley 16. Robust Defenses for Cross-Site Request Forgery. Adam Barth, Collin Jackson, and John C. Mitchell 17. Secure Session Management With Cookies for Web Applications. Chris Palmer 18. Origin Cookies: Session Integrity for Web Applications. by Bortz et al. 19. ForceHTTPS: protecting high-security web sites from network attacks, by A. Barth and C. Jackson 20. The case for short-lived certificates. by Topalovic et al. 21. A look back at Security Problems in the TCP/IP Protocol Suite, S. Bellovin, ACSAC 2004. 22. BGP Security in Partial Deployment, Lychev, Goldberg, Schapira, 2013. 23. DNS cache poisoning, Steve Friedl 24. A Security Evaluation of DNSSEC with NSEC3, J. Bau and J.C. Mitchell 25. Distributed Firewalls, S. Bellovin 26. Bro: A System for Detecting Network Intruders in Real-Time, V. Paxon 27. Details of a recent large-scale DDoS event (2013) 28. Practical network support for IP Traceback, S. Savage, et al. 29. A DoS-Limiting Network Architecture, Yang, Wetherall, and Anderson 30. All your iFrames point to us, N. Provos et al. 31. Hunting for metamorphic, P. Szor 32. Is finding security holes a good idea, E. Rescorla

	33. Know Your Enemy: Fast-Flux Service Networks, Honeynet 34. CEH Certified Ethical Hacker Study Guide v.6, Kimberly Graves