Network Security

Course Title: Network Security					
Course Code: CIT61019	**Student Workload:** 8.50 Hours / Weeks	**Credits:** 3 Credits (4.50 ECTS)	**Semester:** 5th Semester	**Frequency:** Odd Semester	**Duration:** 16 Weeks/ Semester (*Lecture*: 14 weeks; *Midterm assessment*: 1 week; *Final assessment*: 1 week)

1	**Types of Courses:** Specific skills	**Contact Hours:** *Lecturing*: 2.50 Hours/ Week; *Practical Work*: 0.00 Hours/ Week	**Independent Study:** *Self-study:* 3.00 Hours/ Week; *Structured Assignment*: 3.00 Hours/ Week	**Class Size:** 40 Students

2 **Prerequisites for Participation** (If Applicable)**:**
-

3 **Learning Outcomes:**

1. M1: Understand the basic concepts of network security.
2. M2: Understand the concept of physical security.
3. M3: Able to define potential security breach.
4. M4: Able to explain security at the physical layer.
5. M5: Able to explain security on wireless networks.
6. M6: Able to explain security at the data link layer.
7. M7: Able to explain security at Network Layer.
8. M8: Able to explain security at Transport Layer.
9. M9: Able to explain security at the application layer.
10. M10: Able to explain the types of attacks on the HTTP protocol.

4 **Subject aims/Content:**

At the end of the course, students are expected:

1. L1: Able to define network security concepts.
2. L2: Able to define threats and be able to explain the sources of threats.
3. L3: Able to define vulnerabilities in computer networks.
4. L4: Able to explain general defense techniques.
5. L5: Able to define security policy.
6. L6: Able to define security audit function and network vulnerability testing.
7. L7: Able to define physical destruction of material as a security threat.
8. L8: Able to explain how to handle security breaches on physical material.
9. L9: Able to define and explain social engineering as a potential security breach.
10. L10: Able to define and explain port scanning mechanisms.
11. L11: Able to define and explain network mapping mechanism.
12. L12: Able to define the types of physical network media and their supporting components.
13. L13: Able to define risk on the physical network.
14. L14: Able to explain security techniques for physical layer.
15. L15: Able to define attack tracking at the physical layer.
16. L16: Able to explain the implementation of physical security on LAN by area.
17. L17: Able to explain Firewall mechanism and its implementation.
18. L18: Able to explain the working principle of wireless networks.
19. L19: Able to explain security protocols on wireless networks.
20. L20: Able to explain security risks in wireless networks.
21. L21: Able to explain security methods on wireless networks.

	22. L22: Able to define data flow at the data link layer. 23. L23: Able to define security protocols that work at the data link layer. 24. L24: Able to define uncommon usage at the data link layer. 25. L25: Able to define security techniques at the data link layer. 26. L26: Able to explain the working principle of routers and routing protocols. 27. L27: Able to define risk in routing activity. 28. L28: Able to define risk in addressing scheme. 29. L29: Able to define risk in fragmentation. 30. L30: Able to define security measures at the Network layer. 31. L31: Able to define risk in ICMP protocol. 32. L32: Able to define common protocols at the transport layer. 33. L33: Be able to define the main functions of the transport layer. 34. L34: Able to define security risks at the transport layer. 35. L35: Able to define risks on TCP and UDP. 36. L36: Able to describe Attacks aimed at TCP connection sessions. 37. L37: Able to describe Attacks aimed at UDP connection sessions. 38. L38: Able to define session risk and explain session attack. 39. L39: Able to explain general security techniques for application layer. 40. L40: Able to explain the working mechanism of VPN technology. 41. L41: Able to explain SSL implementation. 42. L42: Be able to explain the SSH mechanism. 43. L43: Able to explain the supporting components of the HTTP protocol. 44. L44: Able to explain URL exploitation attacks. 45. L45: Able to explain security risks in HTTP protocol. 46. L46: Able to explain security methods on HTTP protocol.
5	**Teaching Methods:** Lecturing, Group Discussion, Case-Based Learning
6	**Assessment Methods:** Essay, multiple-choice, product assessment, anecdotal record/logbook
7	**This Course is Used in The Following Study Programme/s as Well:** -
8	**Responsibility for Course:** Dany Primanita Kartikasari, S.T., M.Kom
9	**Other Information :** Bibliography: 1 Stallings, Wiliam, Cryptography and Network Security, 5th edition, Prentice Hall, 2011 2 Harrington, Jan, Network Security A Practical Approach, Morgan Kaufmann, 2005 3 Vacca, John. Network and System Security, Syngress, 2010 4 Douligeris, Christos, Network Security: Current Status and Future Direction, IEEE Press, 2007