Subject Description Form

Subject Code	EIE4118 (for 42480 and 42470)
Subject Title	Intrusion Detection and Penetration Test
Credit Value	3
Level	4
Pre-requisite	For 42480: EIE3120 Network Technologies and Security For 42470: EIE4106 Network Management and Security
Co-requisite/ Exclusion	Nil
Objectives	1. To provide a solid foundation to the students in network security with a focus on intrusion detection and penetration test; 2. To enable the students to master the knowledge about intrusion detection and penetration test in the context of real-life applications; 3. To prepare the students for understanding, evaluating critically, and assimilating new knowledge and emerging technology in network security.
Intended Subject Learning Outcomes	**Upon completion of the subject, students will be able to:** Category A: Professional/academic knowledge and skills 1. Understand the physical location, the operational characteristics and the various functions performed by the intrusion detection/prevention system 2. Describe how components in different layers inter-operate in the intrusion detection/prevention system 3. Understand the current network security vulnerabilities and effective procedures of penetration test 4. Learn new techniques and to align new security technologies to existing network infrastructure Category B: Attributes for all-roundedness 5. Present ideas and findings effectively 6. Learn independently
Subject Synopsis/ Indicative Syllabus	**Syllabus:** 1. Vulnerabilities and Security Threats to Computer Networks Sources of vulnerabilities, types of attacks, attacks against various security objectives, countermeasures of attacks. 2. Penetration Test Methodologies and Procedures White-box / grey-box testing, security surfaces for evaluation, automated tools for vulnerability scan and penetration test. 3. Intrusion Detection and Prevention Technologies Host-based intrusion detection system (IDS) / intrusion prevention system (IPS), network-based IDS/IPS. Intrusion detection techniques, misuse detection: pattern matching, policy-based and state-based; anomaly detection: statistical based, honeypots-based; hybrid detection. 4. IDS and IPS Architecture Tiered architectures, single-tiered, multi-tiered, peer-to-peer. Sensor: sensor functions, sensor deployment and security. Agents: agent functions, agent deployment and security. Alert management: alert types, alert manager deployment and security. Information flow in IDS and IPS, defending IDS/IPS.

5. Network Security Monitoring
   Network traffic collection and storage, detection mechanisms and indicators of compromise, packet analysis, friendly and threat intelligence.

6. Deployment of IDS/IPS
   Case study on commercial and open-source IDS.

Possible Laboratory Experiments:

1. Vulnerability scan and penetration test
2. Protocol and traffic analysis
   Intrusion detection using Snort

Teaching/Learning Methodology

Teaching and Learning Method	**Intended Subject Learning Outcome**	**Remarks**
Lectures	1, 2, 3, 4	Fundamental principles and key concepts of the subject are delivered to students.
Tutorials	1, 2, 3, 4, 5, 6	Supplementary to lectures and are conducted with smaller class size; Students will be able to clarify concepts and to have a deeper understanding of the lecture material; Problems and application examples are given and discussed.
Laboratory sessions	3, 5, 6	Students will conduct practical exercises in intrusion detection and prevention to reinforce concepts and techniques learned.

Assessment Methods in Alignment with Intended Subject Learning Outcomes

Specific Assessment Methods/ Tasks	**% Weighting**	**Intended Subject Learning Outcomes to be Assessed (Please tick as appropriate)**					
		1	**2**	**3**	**4**	**5**	**6**
1. Continuous Assessment	70%						
• Quiz	15%	✓	✓	✓		✓	
• Project	30%	✓	✓	✓	✓	✓	✓
• Laboratory demonstration and reports	25%	✓	✓	✓		✓	
2. Examination	30%						
• Practical Test	30%	✓	✓	✓		✓	
Total	100%						

<table>
<tr><td></td><td colspan="2">Explanation of the appropriateness of the assessment methods in assessing the intended learning outcomes:

<table>
<tr><th>Specific Assessment Methods/Tasks</th><th>Remark</th></tr>
<tr><td>Project</td><td>Students need to think critically and creatively in order to come with a solution for a practical problem.</td></tr>
<tr><td>Quiz</td><td>Mainly objective quizzes conducted to measure the students' understanding of the theories and concepts as well as their comprehension of subject materials.</td></tr>
<tr><td>Examination (Practical Test)</td><td>Hands-on type problems emulate real-life penetration test and intrusion detection scenarios, which are used to evaluate students' ability in applying concepts and skills learnt in the classroom.</td></tr>
<tr><td>Laboratory sessions</td><td>Each student is required to produce a real-life demo and/or a written report to evaluate his/her technical knowledge and communication skills.</td></tr>
</table></td></tr>
<tr><td rowspan="6">Student Study Effort Expected</td><td>Class contact (time-tabled):</td><td></td></tr>
<tr><td>1. Lecture</td><td>27 Hours</td></tr>
<tr><td>2. Tutorial/Laboratory/Practice Classes</td><td>12 Hours</td></tr>
<tr><td>Other student study effort:</td><td></td></tr>
<tr><td>3. Lecture: preview/review of notes; homework/assignment; preparation for test/examination</td><td>24 Hours</td></tr>
<tr><td>4. Tutorial/Laboratory/Practice Classes: preview of materials, revision and/or reports writing</td><td>42 Hours</td></tr>
<tr><td>Total student study effort:</td><td>105 Hours</td></tr>
<tr><td>Reading List and References</td><td colspan="2">Reference Books:

1. C. Endorf, E. Schultz and J. Mellander, Intrusion Detection & Prevention, McGraw-Hill/Osborne, 2004.
2. Ali A. Ghorbani, Network intrusion detection and prevention concepts and techniques, Springer, 2010.
3. J. M. Kizza, Computer Network Security, Springer, 2005.
4. D. Jacobson, Introduction to Network Security, CRC Press, 2009.
5. Chris Sanders and Jason Smith, Applied Network Security Monitoring: Collection, Detection, and Analysis, Syngress, 2013.
6. Richard Bejtlich, The Practice of Network Security Monitoring: Understanding Incident Detection and Response, No Starch Press, 2013.
7. Peter Kim, The Hacker Playbook 3: Practical Guide To Penetration Testing, May 2018.</td></tr>
<tr><td>Last Updated</td><td colspan="2">November 2021</td></tr>
<tr><td>Prepared by</td><td colspan="2">Dr H. Hu</td></tr>
</table>