Course Title: Intrusion Detection and Response Methods and Systems for Computer Networks
(Advanced Concepts in Computer Networks)

<table>
<thead>
<tr>
<th>Course Type: Advanced Course</th>
<th>Prerequisites: None</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unit Type: Theoretical</td>
<td>Project and Seminar: Yes</td>
</tr>
<tr>
<td>Units: 3</td>
<td>Teaching Hours: 48</td>
</tr>
</tbody>
</table>

Objectives:
This course intends to introduce the student to security treats in the computer networks and security mechanisms devised to improve the security of the network operation. The approach for this course is both theoretical approach and study of the reported works in this area. As required, in each part of the course students will be introduced to the theories related to the subject area and the applied theories in the current reported works. Students will become familiar with the intrusion detection methods their pre and post processes, intrusion prevention and response systems and honeypots. In addition course will introduce the students to the concepts of Security Operation Center (SOC), operation of the related network security organizations and security standards.

Syllabus:
1. Introduction to the problems caused by the security treats and intrusions on the networks and some of their methods.
2. Intrusion detection methods such as signature-based and anomaly-based intrusion detection.
4. Honeypots and Introduction to their duties and applications.
5. An overview on the theories and applicable to the intrusion detection in computer networks (Data mining, Principal Component Analysis (PCA), …).
6. Intrusion prevention and response systems.
7. Introduction to some intrusion detection systems, SOC and CERT centers and their responsibilities.
8. ISO standards related to the security of the network management centers and intrusion detection systems.

Recommended References

1- Current published research works in the area of interest in this course.