CSC 422 – Network and Web Security

1. CSC 422 – Network and Web Security

2. credit units 4  contact hours 6

3. Course Coordinator: Bruce DeBruhl

4. Textbook (or other required material): None

5. a. Course Description:
   Introduction to network and web security, including denial of service, botnets, access control, routing attacks, transport layer attacks, tunneling mechanisms, VPNs, IDS, firewalls, penetration testing, key distribution, browser security, social network security, email security, jamming, and wireless security. 3 lectures, 1 laboratory. Crosslisted as CPE/CSC 422.

   b. Prerequisite: CPE 464

   c. Required/Elective/Selective Elective for CPE, CSC, EE, SE

<table>
<thead>
<tr>
<th></th>
<th>CSC</th>
<th>CPE</th>
<th>SE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Required</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Elective</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Selective Elective</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

6. a. Course Learning Objectives
The student will be able to:
   - Discuss common network vulnerabilities and the vectors attackers use to exploit them.
   - Classify historical and current network and web attacks including potential mitigation approaches.
   - Create web applications that are robust against common vulnerabilities including XSS and CSRF.
   - Justify the need for security related mechanisms in networks and web applications to a broad audience.
   - Evaluate the harm of new network and web attacks from listening to security podcasts and reading security literature.
   - Evaluate trade-offs in various network defenses to make reasoned decisions about a network security policy.

b. Level at which Student Outcomes are addressed
   (“B” = Basic level, “I” = Intermediate level, “A” = Advanced level)

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSC</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>N/A</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SE/ CPE</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
</tr>
</tbody>
</table>
7. Major Topics Covered: (number of lecture hours per)

- Network infrastructure attacks (6)
  - DNS, Routing, TCP, DoS, Botnets
- Network defenses (5)
  - VPNs, IDS, Firewalls, Pen testing, Anonymous routing
- Web attacks (3)
  - XSS CSRF, XSSI, Session hijacking, Injection attacks
- Web defenses (3)
  - Browser security, TLS/SSL, Session management, Sanitization
- Wireless security (5)
  - MAC security, Jamming, Wi-Fi Security, Wireless tracking
- Special Topics (3)