CTC 452: Network Security & Hacking Prevention

Instructor: Adam Kaplan, Ph.D. E-Mail: akaplan@csudh.edu WWW (Blackboard Site): http://toro.csudh.edu
Office: NSM E-109 Office-hours: Saturday, 3:00pm – 5:00pm (except 1/22/2011) Class Meetings: Saturday, 12:00pm - 2:45pm in SAC 2102

Final Exam: Saturday, May 14th, 12:00pm-2:00pm in SAC 2102 All exams except final will be taken in class during regular meeting time.

Prerequisites: CSC 428 Operating System Security or consent of instructor. Students should also be familiar with computer networking, specifically the TCP and IP protocols, but this material will be reviewed as part of this course.

Text/References


http://www.justice.gov/criminal/cybercrime/cclaws.html US Department of Justice


http://www.htcia.org/ Hi Tech Crime Investigation Association

https://forms.us-cert.gov/report/ Reporting an Incident to US Cert

Catalog Description
This course takes an in-depth look at network defense concepts and techniques. It examines theoretical concepts that make the world of networking unique. This course also adopts a practical hands-on approach when examining network defense techniques and different strategies.

Course Goals & Objectives
This course will adopt a practical hands-on approach to network security, with an exploration of various network defense techniques. Along with examining different strategies to administer secure networks, detect intruders, and manage firewalls, this course will explore the analysis and interpretation of network traffic. ADD: Student will receive guidance on how to report incident and preparing intrusion documentation evidence
Learning Outcomes

Upon completion of this course, students will be able to:

- Describe common attack threats
- Describe the network security components that make up a layered defense configuration
- List the essential activities that need to be performed in order to protect a network
- Decide how to minimize risk in a network
- Explain what makes an effective security policy
- Explain the “what, why, and how” of virtual private networks (VPNs)
- Demonstrate understanding of the tunneling protocols that enable secure VPN connections
- Describe the encryption schemes used by VPNs
- Know how to adjust packet filtering rules for VPNs
- Explain the benefits of the Common Vulnerabilities and Exposures (CVE) standard
- Describe intrusion detection system components
- Follow the intrusion detection process step-by-step
- Understand options for configuring intrusion detection systems
- Know the issues involved in choosing an intrusion detection system
- Integrate an intrusion detection system (IDS) into a network security configuration
- Demonstrate understanding of why logging network traffic is an integral part of intrusion detection
- Analyze intrusion signatures to block unauthorized access to resources
- Identify suspicious events when they are captured by an intrusion detection device
- ADD: Reporting incident to US CERT /Documenting for turnover to LAW Enforcement
- Develop filters that take a proactive approach to intrusion detection
- Design common firewall configurations
- Establish a set of application rules and restrictions for a firewall
- Describe the difference between stateless and stateful packet filtering
- Create different packet filter rules for real-world situations
- Decide when to use user, session, or client authentication
- Demonstrate understanding of how to work with a proxy server to supplement a firewall with a proxy server
- Describe the most important issues to be faced when managing a firewall

Attendance

The student is responsible for materials missed during an absence, whether excused or not. Classes will start at the prescribed time and will end at the prescribed time. Instructor will be available during the posted office hours and you may make an appointment for times not posted.

Academic Honor Code

Programming assignments must be done individually. Failure to do so will result in a violation of the CSUDH Academic Honor Code. The following cases will be considered as violations: identical code, and extremely similar code. Violations will be reported to the Office of Vice President of Academic Affairs.

Attendance Policy

Excessive absences will result in lowered grades. Excessive absenteeism, whether excused or unexcused, may result in a student’s course grade being reduced or in assignment of a grade of “F”. Absences are
accumulated beginning with the first day of class.

**Student Academic Appeals Process**
Authority and responsibility for assigning grades to students rests with the faculty. However, in those instances where students believe that miscommunication, error, or unfairness of any kind may have adversely affected the instructor’s assessment of their academic performance, the student has a right to appeal by the procedure listed in the Undergraduate Catalog and by doing so within thirty days of receiving the grade or experiencing any other problematic academic event that prompted the complaint.

**ADA Statement**
Students with disabilities, who believe they may need an academic adjustment in this class, are encouraged to contact me as soon as possible to better ensure receipt of timely adjustments.

**Definition Of Cheating and Plagiarism**
CSUDH is dedicated to a high standard of academic integrity among its faculty and students. In becoming part of the California State University academic community, students are responsible for honesty and independent effort. Disciplinary action will be taken against any student who alone or with others engages in any act of academic fraud or deceit. (Read University Regulations in University Catalog)

**Grading**
- Homework Assignments (10%)
  - 2 in CTC452, 3 in CSC495
- Projects (20%)
  - Either 4 or 5 projects will be assigned to both CTC452 and CSC495
  - The exact number of projects TBA
- Midterm Exam (30%)
  - 1 midterm during 7th week
- Final Exam (40%)
  - 1 final exam during finals week

**Grading Scale**

96-100 = A 90-95 = A87-89 = B+ 83-86 = B 80-82=B77-79=C+ 73-76=C 70-72=C67-69=D+ 63-66=D below 60 = F
<table>
<thead>
<tr>
<th>Week</th>
<th>Topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 (1/22)</td>
<td>Network Defense Fundamentals (Chapter 1) and introduction to references provided</td>
</tr>
<tr>
<td>2 (1/29)</td>
<td>Network Defense Fundamentals (Chapter 1, cont) + Encryption + Digital Signatures + Certificates</td>
</tr>
<tr>
<td>3 (2/5)</td>
<td>Security Policy Design &amp; Risk Analysis (Chapter 2)</td>
</tr>
<tr>
<td>4 (2/12)</td>
<td>Security Policy Implementation (Chapter 3)</td>
</tr>
<tr>
<td>5 (2/19)</td>
<td>Network Traffic Signatures – Common Traffic (Chapter 4)</td>
</tr>
<tr>
<td>6 (2/26)</td>
<td>Network Traffic Signatures Suspicious Traffic (Chapter 4, cont) + CVE Standard + Midterm Review</td>
</tr>
<tr>
<td>7 (3/5)</td>
<td>Midterm Exam</td>
</tr>
<tr>
<td>8 (3/12)</td>
<td>VPN Design &amp; Configuration (Chapter 6)</td>
</tr>
<tr>
<td>9 (3/19)</td>
<td>VPN Design &amp; Configuration (Chapter 6, cont)</td>
</tr>
<tr>
<td>10 (3/26)</td>
<td>Intrusion Detection System Concepts (Chapter 7)</td>
</tr>
<tr>
<td>SPRING RECESS</td>
<td>No class on April 2nd !!!</td>
</tr>
<tr>
<td>11 (4/9)</td>
<td>Intrusion Detection: Incident Response (Chapter 8)</td>
</tr>
<tr>
<td>12 (4/16)</td>
<td>Intrusion Detection: Incident Response (Chapter 8, cont) and reporting an incident and documenting for possible turnover to Law Enforcement</td>
</tr>
<tr>
<td>13 (4/23)</td>
<td>Choosing &amp; Designing Firewalls (Chapter 9)</td>
</tr>
<tr>
<td>14 (4/30)</td>
<td>Firewall Topology (Chapter 10)</td>
</tr>
<tr>
<td>15 (5/7)</td>
<td>Strengthening &amp; Managing Firewalls (Chapter 11) + Preparation for Final Exam</td>
</tr>
<tr>
<td>16 (5/14)</td>
<td>Final Exam</td>
</tr>
</tbody>
</table>

All **projects** are due no later than the last week of the semester.