Motivation & Objectives:

The use of the Internet and web technologies increased significantly; also mobile devices and their wireless/cellular connectivity providing easy access to online information and resources. However, the openness and anonymity in the Internet and it underlying technology being abused by hackers and criminals for fraud, identity theft and such activities are increasing with the rising popularity of online businesses and other use of the cyberspace in the society. Hackers are increasingly launching sophisticated attacks to exploit the systems than ever before.

The course covers both the principles and practice of Internet and Network security. This is an advanced level course that provides hands-on experience in security-related tools and technologies for better understanding of new threats and vulnerabilities, and how to adopt various security measures. One of the important components of the course is a term project that will allow students to do extensive study/research on current topics in network and Internet security.

PREREQUISITES: COMP 7120 / COMP 6410 and COMP 6310 or permission of the instructor.

Course Syllabus (The following topics will be covered through teaching, selected reading and project activities subject to availability of time):

- **Quick Review** of Cryptography, Networking, Virus & Worms, basic security issues and countermeasures; **Communication Security**: IP Concepts, Protocols (IPv4, v6), Mobile IP, Covert Channels and DNS.
- **Defense in Depth techniques & tools:**
  - Authentication, Authorization, Access Control, Password Management and user Attribution, etc.
  - Intrusion Detection and Prevention Systems, Monitoring & Response
  - Virtualization and Cloud Security, Moving Target Defense, Vulnerability Analysis
  - Firewall, Filtering and Proxying Tools, Virtual Private networks (VPN)
  - Security Management and Improvement: Vulnerability analysis tools
- **Various Internet Security topics:** OSN analysis, Wireless Security, Honeypots, TEMPEST Security, Botnet, Reverse Engineering, Advanced Persistent Threats (APTs), Insider Threats
- Security Policy, Risk Analysis, Security Metrics, Incident Response, Security visualization
- **Computational Intelligence (CI) Techniques in Cyber Security**– AI Methods, Neural Networks, Genetic Algorithms, Data Mining, Agent-Based, Immunity-Based, Statistical, etc.

Suggested Textbook:
6. Selected Reading

References:
Instructor: Dr. Dipankar Dasgupta
Email: dasgupta@memphis.edu
Office Hours: - Room No. DH 333 (Wednesday: 12:00Noon - 1:30PM, and other times by appointment or through email).
Class Schedule: Wednesday: 4:00PM - 7:00PM
Room: FIT 324

Evaluation:

Students are expected to participate in class discussions as the part of active learning (continuous two-sided feedback) process, which (a) allow students to assess themselves on their progress in learning the material/understanding the security issues; and (b) allows the instructor to assess how well he is fostering the communication process with and among students. Good evaluations will thus reflect not only your grasp of the material, but also how well you take advantage of class time and how well you end up communicating with other people (class participants) about the course material. The evaluation process will include paper presentations, assignments, software testing, tests (or quizzes), and a term project to make sure that you have integrated the material into your general practice of secure computing. Students registered for COMP 8327 will have to do some additional work.

Your final grade for the course will be based on the grades in the following course-related activities (given in percentages):

Grading:

<table>
<thead>
<tr>
<th>Activity</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Class performance</td>
<td>10%</td>
</tr>
<tr>
<td>Paper presentation</td>
<td>10%</td>
</tr>
<tr>
<td>Tests/quizzes/Exams</td>
<td>30%</td>
</tr>
<tr>
<td>Experiments/Assignments</td>
<td>25%</td>
</tr>
<tr>
<td>Final project + proposal</td>
<td>25%</td>
</tr>
</tbody>
</table>

Grading Scale:

<table>
<thead>
<tr>
<th>Grade</th>
<th>Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>A+</td>
<td>95.1-100</td>
</tr>
<tr>
<td>A</td>
<td>90.1-95</td>
</tr>
<tr>
<td>A-</td>
<td>88.1-90</td>
</tr>
<tr>
<td>B+</td>
<td>85.1-88</td>
</tr>
<tr>
<td>B</td>
<td>82.1-85</td>
</tr>
<tr>
<td>B-</td>
<td>79.1-82</td>
</tr>
<tr>
<td>C+</td>
<td>76.1-79</td>
</tr>
<tr>
<td>C</td>
<td>70.1-76</td>
</tr>
<tr>
<td>C-</td>
<td>66.1-70</td>
</tr>
<tr>
<td>D+</td>
<td>60.1-66</td>
</tr>
<tr>
<td>D</td>
<td>50-60</td>
</tr>
<tr>
<td>F</td>
<td>&lt; 50</td>
</tr>
</tbody>
</table>

Term Project:

The project (on cyber security) is one of the important components of the course. The topic/problem needs to be approved by the instructor. This individual project needs to be completed into three phases:

Phase 1: Submission of the project proposal:

A one-page proposal (identifying techniques/software/methods to solve the given security problem, provides references) of worth 5% (of the project's grade) must be submitted to the instructor for approval. There will be one student for each project.

Due date: (2/17/2015).
Phase 2:
Project Progress Presentation (on Implementation of the project): March 23rd

Phase 3:
Final Demo and report of the project:

Your final project report should be 6 to 8 pages long. You have to implement the approved project. You need to search on the web for the references and for further resources. Also, feel free to think and propose others (new ideas) that may better solve the problem.

Due date: Project presentation/demo on the last day of class (4/27/16) and Submission of the project report (5/1/2016). It will be extremely difficult to get any extensions, so plan on finishing by the due date.

Course Policies:

Students are expected to attend all scheduled classes and submit assignments/reports on time. If you miss a class, it is your responsibility to obtain the notes for the missed class from another student and catch up on the course content. There will be no makeup test for this course.

Ethical behavior/Plagiarism/Cheating Policy:

Ethical behavior is an important part of this course. Since some of the methods, codes and tools that will be discussed and experimented in the course can be very harmful, if abused, it is expected that students will behave in a responsible fashion. In particular, always ask your local site administrator for permission before experimenting with security-related tools. In-class discussions of techniques for exploiting potential security threats and risks do not imply to use them! You will be sole responsible for any such violation.

Plagiarism or cheating behavior in any form is unethical and detrimental to proper education and will not be tolerated. All work submitted by a student (projects, programming assignments, lab assignments, quizzes, tests, etc.) is expected to be a student’s own work. The plagiarism is incurred when any part of anybody else’s work is passed as your own (no proper credit is listed to the sources in your own work) so the reader is led to believe it is therefore your own effort. Students are allowed and encouraged to discuss with each other and look up resources in the literature (including the internet) on their assignments, but appropriate references must be included for the materials consulted, and appropriate citations made when the material is taken verbatim.

If plagiarism or cheating occurs, the student will receive a failing grade on the assignment and (at the instructor’s discretion) a failing grade in the course. The course instructor may also decide to forward the incident to the University Judicial Affairs Office for further disciplinary action. For further information on U of M code of student conduct and academic discipline procedures, please refer to http://www.memphis.edu/studentconduct/pdfs/csrr.pdf and the student handbook and planner.

“Your written work may be submitted to Turnitin.com, or a similar electronic detection method, for an evaluation of the originality of your ideas and proper use and attribution of sources. As part of this process, you may be required to submit electronic as well as hard copies of your written work, or be given other instructions to follow. By taking this course, you agree that all assignments may undergo this review process and that the assignment may be included as a source document in Turnitin.com’s restricted access database solely for the purpose of detecting plagiarism in such documents. Any assignment not submitted according to the procedures given by the instructor may be penalized or may not be accepted at all.” (Office of Legal Counsel, October 17, 2005)
SPRING 2016  TENTATIVE SCHEDULE  COMP 7/8327

Week 1 (1/20): Course Aims & Agenda, Pre-requisite topics: review of basic security issues, cyber threads, Selected reading (from COMP 6410): Cryptography overview-DES, AES, MD5, Digital Signature, etc.

Week 2 (1/27): - Networking & security issues - Review IP concepts, network protocols, Mobile IP, DNS; Vulnerability-CVSS, CVE, etc.

First Assignment

Week 3 (2/3): Intrusion Detection Systems (IDS): Host-based, Network-based and Application-based, Attack Taxonomy, Traffic analysis, security monitoring tools, etc. CI technique

Week 4 (2/10): Authentication and Access control, Password and Attack methods, Protocol security issues, CI technique

Paper Presentation starts / Second Assignment

Week 5 (2/17): Scanning and sniffing tools, Security Policy, threat model and risk analysis, NMAP Experiments

Submission of the project proposal

Week 6 (2/24): Malware, bugs, Virus and Worm, Antivirus tools, scanning and sniffing tools, Integrity checker: tripwire, etc.

Week 7 (3/2): Firewalls, Experimenting Security tools and software (demo)

Third Assignment/Lab Exercise

Week 8 (3/9): (Spring Break- March 7-13)

Week 9 (3/16): Virtualization security, Cloud Security, APTs


Reporting Project Progress


Week 12 (4/6): Moving Target Defense, Experimenting Security tools and software (demo)

Fourth Assignment / Survey of Project Topics

Week 13 (4/13): Secure Software, Mobile code, reverse engineering, Govt. standards e.g. AR 25-2, INFOSEC 1-99, COMSEC Policy, ITSEC


NOTE 1: Paper presentation will start from February 10th and each student will present 2 papers on different dates. Each paper presentation will be of 15 minutes long (plus 5 minutes for question & answer). Discussants need to ask questions to get 5% presentation credit.

NOTE 2: We plan to have some Lab exercises and demo with various tool and Techniques. However, for any technical reason if the Lab session needs to be cancelled, we will have lecture session or an alternative arrangement will be made.

NOTE 3: Tests/Quizzes/Exams will be scheduled in every one or two weeks, but students should come prepared (on previous lectures and topics covered) for Quiz in each class.

NOTE 4: All course-related information will be available from elearn.memphis.edu. Check the course Web page at http://elearn.memphis.edu for class notes and updated information.

NOTE 5: If I need to communicate with the class as a group, I'll be using elearn email. You may need to check your email regularly.

Important Web links:

- Internet Storm Center (SANS)
- Current Internet Threat Level (ISS)
- United States Computer Emergency Response Team (US-CERT)
- Stay Safe Online.Org (National Cyber Security Alliance)
- McAfee Threat Center
- http://sectools.org/
- National Vulnerability Database (NVD)
- DCN-Network Security
- NIST Publications

Suggested Project Topics:

- Cloud Security
- Moving Target Defense
- Malware Detection
- Mobile device security
- Social Networks security & Privacy issues
- Insider Threat detection
- Targeted Attacks
- Authentication mechanism-Active Multi-Factor Auth
- Wireless/Sensor Network Security
- Advanced Persistent Threats
- Smart Grid Security