

Syllabus – CS340 Cyber Security

Spring 2008

Time: MW 2-3:15 pm

Location: GH 206A

Instructor: Dr. Sarita Bassil

Contact: (304) 696-5444 or by email bassil@marshall.edu

Office Hours: Mon/Wed 3:30pm – 5pm, Tue 2pm – 5pm

Office Location: GH 207E (across from the elevator)

Course Description:

This course is designed to provide the technical and analytical skills to implement computer security in a typical medium to small-sized enterprise. The course focuses on introducing students to the elements of computer security: technology, people, and policies. Students should have a basic understanding of how networks and operating systems function. At the completion of the course, students will be able to take the CompTIA Security+ certification exam. Pre-requisite: CS320 (Internetworking), or permission of the instructor.

Textbooks:

- Principles of Computer Security *Security+ and Beyond*, Conklin, White, Cothren, Williams, and Davis
- Computer Security Lab Manual, Nestler, Conklin, White, and Hirsch

Course Objectives:

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

- Describe common attack methodology
- Define and use basic commands and tools for network probing
- Define basic security terminology
- Describe the security needs common to all organizations
- Identify poor security practices
- Describe the role of cryptography in security
- Define authentication
- Describe potential holes in a network architecture that impacts security
- Define the points of weakness in an infrastructure that intruders target
- Describe weaknesses in remote access
- List best-practices in wireless network implementation
- Describe how Intrusion detection systems work
- Describe common attacks used for unauthorized intrusions
- Define current malware risks
- Define best practices in disaster recovery
- Define the steps in incident response
- Identify common computer forensics tools
- Identify Internet sites for security information

Course Format:

The methods of instruction will use class lecture, on-line discussions, and computer lab exercises. The class will use Vista as the course delivery tool and also for some online work (e.g., quizzes, discussions). Students are required to have an MU account in order to access the materials. Lectures and labs will alternate each week. Labs start on “Week 3” of the course. Students must complete their lab exercise during the week assigned. The computer lab will not have the available software or configuration necessary to complete assignments outside of the class times. Some exercises may be done on the student’s own computer.

Disability Statement:

Any student with a documented disability needing academic adjustments is requested to notify the instructor as early as possible in the semester. Verification from MU disabled Student Support Services is required. All discussions will remain confidential.

Assignments:

Reading – Reading will be from the textbook, lab book, selected material (available for download from Vista), and web sites (URLs).

Slides – The PowerPoint slides are to be used for review and to cover additional material not found in the reading. The slide sets will be available in Vista.

Lab/Computer Assignments – There will be 8 lab assignments that involve an exercise and a write-up. These will be worth 25 points each. Some lab exercises will be done in the class lab while others you will do outside of class. All lab assignments are team assignments with a single write up. Lab write-ups are to be delivered to the Vista dropbox by midnight on the due date.

Discussion – The on-line discussion component allows us to extend our in-class discussion. The instructor will provide students with an introduction to using Vista during the first week of class. The course requirement is to post a response to each thread (discussion topic) at least 2 times during the week of the posted discussion topic. A single discussion runs from Monday to Sunday. There will be 8 discussion topics. On-line discussions will be graded according to the following rubric: Each discussion is graded on number of posts and quality of the posts. No participation earns a zero and full participation earns 10 pts with partial contributions earning between 1 and 10 pts depending on the number of posts. The quality of your contributions will be graded on whether your discussions includes analysis of the question, extends the topic’s discussion, includes references to the textbook reading for reinforcement of your viewpoint and includes outside sources. A series of quality posts that exceed the minimum number (2) for each discussion can earn up to 15 pts with fewer posts and lesser contributions earning between 1 and 15 pts. No posts will earn a zero. Simple responses are not discouraged but they do not count for the quality component of the grade. Each discussion will be worth 25 pts. The rubric below will be used to assign quality points.

High
Your contributions to each Topic indicate your mastery of the materials assigned. Your responses might integrate multiple views and/or show value as a seed for reflection for other participants' responses to the thread. You provide evidence that you are reading the assigned materials and other student postings and are responding accordingly, bringing out interesting interpretations. You know the facts and are able to analyze them and handle conceptual ideas.
Medium
Your responses build on the ideas of another participant (or more) and dig deeper into assignment questions or issues. When you make intelligent posts during the week, including some good critique of the course material, then you have demonstrated you have an understanding of the material, are reading posts of your colleagues, and are contributing to the class. Your posts demonstrate confidence with the materials, but may be just a bit off target in one area or another.
Low
You have meaningful interaction with other participants' postings. Posts that state "I agree" or "I disagree" include an explanation of what is disagreed or agreed upon and why, or introduce an argument that adds to the discussion. However, you may have rambling, lengthy posts that show no sign of having been re-read and refined before posting, and your writing suffers lack of clarity and comprehension.
Unsatisfactory
You will receive little credit in the week's discussion by just showing up and making trivial comments, without adding any new thought to the discussion. At the low end of the spectrum, no participation gets a "0." If you are not in the discussion, you do not earn any points.

On-line – Access Vista at <http://vista.marshall.edu/>. Your computer must be able to display the Vista content and there is an exercise on the Vista web site that can be used to check for the proper settings to enable the student to use Vista. Disabling popups will interfere with the content! Assignments can be turned in via the class drop-box in Vista. The course gradebook (to track your progress) will be available in Vista. Students should check online for announcements daily. Lecture slides can also be downloaded from Vista. All materials will be available in Vista. All assignments have a midnight due date and late submissions will be penalized at the discretion of the instructor. For problems with Vista, please call the MU help desk for assistance.

Quizzes – There will be a quiz every two weeks for a total of 8 quizzes. The instructor will specify whether the quiz is available in Vista or to be taken in class. Quizzes will cover content from the reading, lecture, and online discussions. Each quiz will be worth 25 pts. If available in Vista, a quiz is accessible for only one week and expires.

Grading:

Please note that the grading scale is **not** traditional. Excellent work must be superior in quality and content and the student must be an active classroom, on-line and team participant to earn an "A" grade. An "incomplete" will not be given unless a documented emergency exists at the end of the semester that prevents the completion of the class. An

“incomplete” will be given only when all assignments have been turned in and the assignments received a passing grade up to the point of the request for the “incomplete”. The work not completed must have an agreed-upon due date for completion. By the end of the course, if all work has been submitted (on-time and a passing grade) and the student takes and passes the CompTIA Security+ exam, the student will receive an “A” grade in the course.

Grade	Per Cent Earned
A	90 - 100
B	82 - 89
C	75 - 81
D	65 - 74
E	< 64

Activities	Points
Discussion	200
Assignments	200
Quizzes	200
Total	600

Course Policies:

Teams

Students can form into teams of two students each for lab assignments. Each team is responsible for learning the material and performing the required lab work. The work should be divided between the students and reflect a joint effort. If a team member stops contributing, it is an obligation to inform the instructor. Lab exercises are to be completed by a team and receive a “team” grade.

Plagiarism Policy

All work submitted under your name is assumed to be done by you. If it is discovered that the work submitted by you or your team was written by another or if material is copied without proper attribution, the instructor will record an E grade for the course. **Cutting and pasting from web sites is considered plagiarism unless attribution is given.** Entire pages of content cannot be attributed to someone else and you still receive credit for doing original work. Be aware that cutting and pasting is detectable forensically.

Schedule of Events:

The schedule is organized by units, every unit equals to approximately two week intervals.

Unit	Week/Date	Reading	Topics	Quiz?	Lab	On-line discussion?
1	1 1/14 – 1/16	Chapters 1, 4, and 24	- Introduction to the course, using Vista, ethics agreements in security, lab rules - Incidents, threats, trends, attack methods, legal restrictions			
	2 1/21 (no class) – 1/23	Chapters 2 and 3 Lab1: hand-outs	- Security controls, models, and policies - Physical security - Social Engineering	✓		✓
2	3 1/28 – 1/30	Lab2: Lab manual (Chap. 1)	- Computer network, configuration and connectivity: ipconfig, ping, arp, local hosts, nslookup, tracert		Lab1 due Lab2	
	4 2/4 – 2/6	Chapters 7, 8, and 9	- Standards, protocols, physical security, networks	✓		✓
3	5 2/11 – 2/13	Lab3: Lab manual (Chap. 2 and 3)	- TCP/UDP, network applications: FTP, HTTP, netstat, Telnet		Lab3	
	6 2/18 – 2/20	Chapters 10, 11, and 12	- Infrastructure, remote access, wireless, IM	✓		✓
4	7 2/25 – 2/27	Lab4: Lab manual (Chap. 4, 5, and 6)	- Compromising networks: Nmap, SMBSie, Netbus, Keylogger		Lab4	
	8 3/3 – 3/5 (mid-semester)	Chapters 5 and 6 Lab5: hand-outs	- Cryptography: Hashing, symmetric/asymmetric encryption - PKI	✓		✓

5	9 3/10 – 3/12	Chapters 13, 14, 15, and 16	- Intrusion detection - Security baselines - Attacks & malware - E-mail		Lab5 due	
	10 3/17 – 3/19	Lab6: Lab manual (Chap. 7 and 8)	- Preventing harm to networks: hardening, securing network	✓	Lab6	✓
6	11 3/24 – 3/30	Spring break				
	12 3/31 – 4/2	Chapters 17 and 18	- Web components - Software development: SE process, good practices	✓		✓
7	13 4/7 – 4/9	Lab7: Lab manual (Chap. 9 and 10)	- Detecting attacks - Responding to attacks (forensics)		Lab7	
	14 4/14 – 4/16	Chapters 19, 20, 21, and 22	- Disaster recovery (DR), business continuity, organizational policies - Risk management (RM) - Change management (CM) - Privilege management (RM)	✓		✓
8	15 4/21 – 4/23	Lab8: hand- outs	- Forensic tool kits		Lab8	
	16 Dead week 4/28 – 4/30	Review		✓		✓