University of Rhode Island
Department of Computer Science and Statistics

CSF 102 – Fundamentals for Cyber Security
Summer 2015

Instructor: Mark Gadoury
Office: Tyler 101
Phone: 874-2701
Email: csf102.uri@gmail.com

Office Hours: By email appointment
Class Meetings: Online
Web Site: sakai.uri.edu

Prerequisites: none

Course Description: Overview of the technical background required to provide solutions to many cyber security problems. This background includes: binary/hex number systems, operating systems concepts, file systems, OSI model, network topologies and protocols, and wireless standards and implementations. The material will be presented in the context of its necessity for providing cyber security solutions.

Course Goals:

- To introduce students to basic cyber security concepts.
- To provide students with hands-on practice with fundamental cyber security practices.
- To prepare students for more advanced cyber security and digital forensics courses.

- Specific learning outcomes are listed with the course topics below.

Required Readings:

- System Fundamentals For Cyber Security, (free) wikibook available at http://csf102.dfcsc.uri.edu/wiki/
- Other online readings linked in the lessons on the course web site.

Other Equipment Requirements:

- You will be required to have a USB thumb drive, preferably less than 2GB
- You must have access to a computer that meets these requirements:
  - At least 20 GB of free hard drive space
  - At least 1GB of RAM
  - A USB drive
  - Sound card and speakers or headphones for listening to video lectures
  - High speed Internet connection for downloading and/or streaming.

This course is designed for you to do your work on your personal computer, which can be Windows, Macintosh, or Linux (all are supported). You will be instructed to download the VirtualBox virtual environment software to your personal computer and install a Windows XP virtual machine (VM). You will do many of your assignments using the Windows XP VM on your computer.

Lessons: The material in the course is provided as lessons on the Lessons link of the course Sakai web site. Each lesson states the learning outcomes, readings, video lectures, quiz, and assignment. All the lessons will be available from the start of the course, however, each lesson, its quiz, and its assignment will be due on specified dates.

Readings: Reading are assigned in each lesson and should be completed before attempting the quiz or practicum.

Video Lectures: The video lectures for this course present the material in a form different from the readings so that you can better understand the concepts in each section. Each lesson, there will be approximately 60 minutes of video lectures to view. These emphasize important concepts and give examples similar to what you would see in a classroom lecture. Videos in a lesson should be watched with you taking notes before you attempt the quiz or practicum for that lesson.

Practicum: Practicum assignments are meant to allow students to practice some of the skills that are discussed in the readings and video lectures using prominent tools.

Quizzes: The quizzes in this course are designed to assess basic understanding of concepts. The material for the quizzes will be from the readings and the video lectures. The quizzes will typically include multiple choice and true/false questions. There will be a quiz for each lesson through the course web site (Sakai) quiz mechanism and the quizzes will be open-book and open-notes (you may use the material given to you on the sakai website)

Online Discussions: There is a discussion forum on the course web site used for students to post questions about the material or about the assignments. The instructor or other students will post responses to help answer the questions that are posted. Students are not required to use this forum, but is it recommended that they use it for any questions that arise.

Final Grade: Your final grade will be comprised of your Assignments grade and Quizzes grade.

Grading Policy:

Calculation of Grades:	
Assignments	60%
Quizzes	40%

Typical Grading Scale:	
A 94-100	C+ 77-79
A- 90-93	C 73-77
B+ 87-89	C- 70-72
B 83-86	D+ 67-69
B- 80-82	D 60-66
	F <60

Late Penalty for Assignments: Assignments submitted after the due date will receive a 5% late penalty per day. No assignment submissions will be accepted later than 4 days past the due date. In addition, teaching staff will not be available to offer assistance on an assignment past its due date.

Feedback: Feedback on the exercises is available on the course web site after grading has been completed. Students have one week from the posting of a grade to submit any concern about that grade, in email to the instructor. Concerns expressed after one week from posting are not considered.

Confidentiality: All discussion is considered confidential within the course - content posted on the course discussion board is not to be shared with people outside of the course. All class discussion should be on the class discussion board, direct student-to-student contact is not allowed unless approved by the instructor.

Getting Help: There is an online forum on the course web site. There are two kinds of topics in the Forum:

- Questions on Assignment X - there is a topic for each assignment; all questions about that assignment should be posted there. Students can answer other student's questions, and the Professor and TA will answer too.
- General Discussion - this topic is all other things on which you wish to ask questions, or talk about. Students the teaching staff can all participate.

If you have questions about assignments or grades, email your instructor Mark Gadoury at csf102.uri@gmail.com

Tentative Due Date Schedule of Topics and Assignments:

The lesson, its quiz, and its assignment will be due according to the schedule below. This is based on a Wednesday, Sunday schedule however, note that the last two lessons are due on the last day of class, Friday July 25. The learning outcomes for each lesson are listed.

Date	Lesson (Conceptual Quiz & Practicum Assignment)
MON 5/25	Introduction • Define *cyber security*, and *digital forensics* • Define the principals of Information Assurance: *Confidentiality, Integrity, Availability, Authenticity, Non-Repudiation, Accountability.* • Describe types of digital evidence and how they can be used • Describe an example cyber security incident such as a hack in a casino
MON 5/25	Virtual Machines • Define what a *virtual machine* is, including its relationship to a physical machine. • Describe important uses of virtual machines. • Install and use a virtual machine on a personal computer.
MON 6/1	Digital Data • Explain the digital representation of text, numbers, images and other data types • Convert among numeric systems (binary, decimal, and hexadecimal) • Identify file headers in prominent file types • Explain compression and its effect on file sizes and the quality of the content of the file • Use the Winhex hex editor to examine the bytes of a file
MON 6/8	Computer Hardware • List and identify major computer components • Describe the functions of major computer components • Describe in general what firmware does as well as several typical functions of firmware • Use a Windows virtual machine to identify characteristics such as RAM and page file on the VM
MON 6/15	Disks and other Storage Media • Define *Logical Block Addressing* (LBA) • Define *disk partitioning* and *volume formatting* • Define the logical areas of a disk • Define *RAID* and describe how it is used • Define *Solid State Drives* (SSD) and how they differ from typical magnetic drives • Identify types of storage media • Define disk geometry terms *cluster, block, sector, cylinder* • Explain the advantages and disadvantages of allocation of disk space using cluster/block and sectors • Use Windows Disk Management to determine properties of the physical disks of the computer, delete partitions, and create partitions
MON 6/22	Operating Systems • Describe the three main functions of an operating system • Define what an operating system *driver* is • Describe the purpose of *virtual memory* • Define *multi-tasking* and *time sharing* • Describe what an operating system *process* is • Describe what a *file* is and what each of the main file attributes are • Define what a *file system* is and what its primary purposes are

	• Define what the *Windows Registry* is and name some of the types of information that it records • Describe how *file permissions* are used • Describe the differences among Windows, Mac OSX, and Linux important directories • Use the command line on a live Linux system • Use Windows Control Panels to find out information about the system • Use AccessData's Registry Viewer to find out information about the system from the Windows registry (e.g. the timezone that the computer is set to). • Use basic Linux commands such as cd and ls
MON 6/29	Networking • Name the seven layers of the *OSI model,*describe their purpose, name prominent protocols in each layer • Define what an *IP address* is • Define *Domain Name Service* • Describe the functions of various network devices such as *routers* and *switches* • Identify and describe the parts of a URL • Define *subnet* and *mask* as used with IP addresses • Describe what the *DHCP protocol* does • Define what a *network artifact* is as used in forensics and name examples of common network artifacts • Describe how an email header can have forensic significance • Do a WHOIS lookup to determine information about a registered domain • Find the network settings on a personal computer • Trace an email using its originating IP address • Use a hosting service to install a simple web site • Use a tool like tracert to trace the route that data takes in a simple Internet interaction
MON 6/29	Malware • Define the prominent types of malware and what harm they cause
MON 7/6	Digital Forensics • Describe how digital evidence is acquired in a way that is acceptable for legal proceedings. • Describe how digital evidence is analyzed in a way that is acceptable for legal proceedings. • Name and explain the basic legal considerations in performing digital forensics. • Use a tool like FTK imager to create an image of a disk • Use Windows searching to find evidence on a disk
MON 7/13	Authentication • Define authentication in the context of cyber security. • List and describe the three factors of authentication. • Name several methods for authentication. • Describe various password cracking techniques. • Define Public Key Infrastructure. • Use a password cracking tool to crack a password on a Word document
MON 7/20	Information Assurance • List and describe the three corners of the *CIA Triad.* • Define *encryption, steganography, digital signatures, virtual private network* • Perform steganography with a free tool • Perform MD5 hash digital signatures using a simple tool • Encrypt and decode a simple message using a *Caesar cipher*. • Perform encryption of a file using an encryption tool • List the properties of a good *hash function.*

*FRI 7/24	Cyber Threats and Defenses • Describe some of the major categories of technical attacks (*man-in-the-middle, denial of service, buffer overflow, zero day attack)* • Identify common vulnerabilities in web applications (*cross-site scripting, SQL injection)* • Define *social engineering.* • Identify common methods of social engineering: *phishing attack, shoulder surfing, dumpster diving, wardriving* • Define *insider threat* and provide an example of it. • Define a *rogue wireless access point.* • Identify common network defense technologies (*firewalls, ids, proxies)* • Define *penetration testing* for cyber security. • Define *incident response* for cyber security • Configure a Windows firewall and describe its functions Analyze vulnerabilities using Windows tools