Advanced Network & Systems Security

CSF434/534 - Spring 2015
Online Syllabus

General Course Information .................................................................2
   Course Overview ..................................................................................2
   Course Web Site ..................................................................................2
   Getting Help in this Course ..............................................................3
   Grading Information .............................................................................3

Course Assignments and Student Responsibilities .........................4
   Weekly Assignments and Course Organization ..................................4
   Reading Assignments (not graded) ....................................................4
   Video Lectures and Flash Interactives (not graded) .........................4
   Online Help and Assistant Discussion Forums (not graded) .............5
   Homework Exercises (graded) ..........................................................5
   Exams (graded) ..................................................................................5
   Lab Projects and Worksheets (graded) ..............................................6
   Discussion Requirements for Undergraduate Credit [CSF434] .........7
   Additional Course Requirements for Graduate Credit [CSF534] ......8
   Additional Course Requirements for Graduate Credit [CSF534] ......9
   Additional Course Requirements for Graduate Credit [CSF534] .....10

Preliminary Assignment Syllabus .......................................................13
   Lab Assignment Key ...........................................................................14

Academic Integrity ..................................................................................15
GENERAL COURSE INFORMATION

Time & Location: **Online!**

Instructor Information:

- **Instructor:** Timothy Henry, Ph.D., PMP
- **Email:** thenry@cs.uri.edu
- **Phone:** 401-874-2701
- **Office Hrs:** By Appointment

Textbook: *This course has no textbook.*

Software: VMWare Workstation, VMWare Fusion, Jones & Bartlett VSCL

Webpage: URI Sakai Portal - CSF434/534-15S

Course Overview

This course provides a survey of several advanced aspects of security including intrusion detection, penetration testing, incident response, malware analysis, and risk management. It does this with relevant readings and exercises as well hands-on practice of skills and techniques that are essential to any professional in the security field.

Upon successful completion of this course, students should be able to:

- Design and implement a secure network.
- Detect new and advanced attacks before they compromise the network.
- Identify the vulnerable points in an organization’s network.
- Perform basic forensic investigation to find indication of an attack.
- Analyze, defend and detect malware on systems and minimize its impact on a network.
- Manage, control and mitigate risk to critical assets.

This course is required for both the graduate certificate in Cyber Security and the minor in Cyber Security. It provides a foundation for much of the material in both of these programs and is therefore prerequisite for most of the other courses in these programs. The course can also be used as an elective in the CSC undergraduate major or in the Applications category of courses offered for the CSC master’s degree or doctorate programs.

Course Web Site

Because this is an ONLINE course; significant responsibility falls on you, the student, to keep up with the work and not fall behind!

As you can expect, we will use the course web site for all aspects of this course. Students are expected to check the web site regularly for:

- General Course Announcements & Assignment Updates
- Videos, Readings and other Reference Materials
- Quizzes, Assignment Submission and Grades
- Discussion Forums

Any updates to the assignment syllabus will be posted on the course web site. Therefore, if there is a difference between the assignment syllabus and the course web site, information from the course web site should be used. To ensure you receive the maximum credit for your work, follow any templates or guidelines that are provided.
Getting Help in this Course

Questions concerning the content of the course or labs should, as a rule, be directed to the appropriate course discussion forum. This allows your question to be answered by whoever is monitoring the discussion forum, and the answer can benefit all board readers. Please do not send email directly to the TA (teaching assistant) or Dr. Henry with technical questions.

We (the TA and Dr. Henry) are happy to answer questions on the discussion forum. However, email is not intended as a replacement for the discussion forums. Due to our own work schedules, we are not online 24x7 so we may not respond to electronic questions instantly, but we will always reply with 24 hours. If you cannot make it to scheduled office hours, feel free to make an appointment by e-mail or after class.

Grading Information

Material in any course is not learned or mastered simply by reading the material or watching videos. The student needs to spend the time doing the readings, discussing the issues with fellow students, and doing activities based on the course concepts.

The final grade will be based on individual grades received on lab assignments, homework exercises, participation in the discussion forums and the final exam. Point values for assignments are based on the level of effort and knowledge required to complete each. The approximate weighting for each area is as follows:

**Undergraduate Students (CSF434)**
- 15% -- Class and Discussion Participation
- 40% -- Lab Assignments
- 25% -- Homework Assignments
- 20% -- Final Project

**Graduate Students (CSF534)**
- 20% -- Class and Discussion Participation
- 35% -- Lab Assignments
- 25% -- Homework Assignments
- 20% -- Final Projects

Assignments that are submitted:

- on time are eligible for full credit based on the rubric for the assignment
- within a week of the due date will be penalized 25%
- more than a week late receive a 50% penalty (DON’T BE LATE!)
Weekly Assignments and Course Organization

Each assignment week begins on a Sunday and ends on the following Sunday. In general, assignments are due each Sunday (at midnight). Here is a brief summary of the assignments we will have each week:

- **Video Lectures and Interactives** - approximately 60 minutes of video lectures based on the readings. Interactive Flash animations are provided for some of the concepts and labs.
- **Lab Assignments** - *multiple* labs using VMware or the VSCL are given each week.
- **Online Discussions** - the two principle discussion forums for this course are the *Course & Lab Help Forum* and the *Helpful Online Resources* forum.

Reading Assignments *(not graded)*

Reading assignments should be completed as early in the week as possible. Reading the assigned articles or reviewing material on the recommended web sites gives you an idea of the concepts that are the focus for the week. Other assignments during the week help to explain the concepts in greater depth and give you experience applying them to actual problems. Therefore, since the readings are fundamental to activities for the week, they should be completed first.

For this course to be successful, you must engage in the material by doing the readings ahead of time, and then complete the labs and participate in online discussions. You are expected to actively participate by asking questions, joining in our discussions, etc. Note that a portion of your grade is attributed to class participation.

In addition to the readings, there will occasionally be notes or slides that outline or expand on key concepts for the week. Reading or reviewing these can help you to understand and organize the material better.

Video Lectures and Flash Interactives *(not graded)*

The video lectures for this course present the material in addition to that in the readings so that you can better understand the concepts in each section. These emphasize important concepts and give examples similar to what you would see in a classroom lecture. Some labs have walkthrough videos to guide you through more difficult procedures.

Many of the VSCL labs also have interactive Flash animations that give background information that can help guide you through the lab or give rational as to the rational behind some of the procedures.
Online Help and Assistant Discussion Forums (not graded)

Helpful Online Resource Forum
As you know from experience, technology is a rapidly advancing field. Many of the cutting edge concepts and tools of just a few years ago have been made non-relevant by newer technologies and platforms. Excellent research skills are critical to staying abreast of the latest trends in security. This requires more than just entering a few words into the search engine of your choice.

Each lab in this course has a worksheet that must be completed that delves into the commands, tools and applications used in the lab. Most of the information needed to complete the worksheets is not presented in the textbook nor the video lectures. It is the responsibility of the student to find an in-depth answer from the Internet, a manual or even the library. Critically review what the search engine returns and apply it to the specific instances present in the labs. And be sure to cite your references!

If you have found a resource that is especially helpful, relevant, recent articles and references, please post a link to them on the Helpful Online Resources forum. You post should contain a link to the reference if it is a web site or a bibliographic reference if it is a book or printed article. The post should also have a short paragraph summarizing why the reference is useful.

Please - do not cut and past from web sites and no plagiarism!

Course and Lab Help Forums
The help forum in this course can be a valuable resource. As a computer science or information security professional, there are many times that discussion forums can give you information or insight to quickly solve problems you have run into (and ways to avoid problems in the future).

When you are stuck on an assignment or consistently run into the same problem, first check the forum to see if someone else had the same problem. If not, post your comment or problem description there. Use descriptive titles for your posts so that other students know what the post is about. Titles such as “I have a problem” are not acceptable. If you have solved a problem that you see someone else struggling with, feel free to post advice on how to work through the problem! This is part of the community building aspect of this course.

Homework Exercises (graded)
The purpose of homework is to reinforce the conceptual material from the readings and labs. Many questions are of a variety that could also appear on exams. You have “unlimited” time on these to submit them, but similar to other assignments, they are due each Sunday evening. The homework can be found under the Labs & Exercises navigation link on the course web site.

Exams (graded)
There will be one examinations given in this course: a final exam. Students are to submit their own work on the exam. If you need help or clarification on a problem or exercise, you are to make a post on the discussion forum or contact the TA or instructor.

• You are not permitted to get help from other students when completing exams.
• Late exams will be penalized the same as late homework assignments.
• The material in this course is cumulative, and so the final exam will be cumulative.
Lab Projects and Worksheets (graded)

Each week there will be multiple practical labs that must be completed. Each lab is designed to take about an hour and you are encouraged to walk-through each lab at least twice so that you become comfortable with the commands, tools and applications used in the lab.

Virtual Security Cloud Lab (VSCL)

Many of the labs for this course use the Jones & Bartlett Virtual Security Cloud Lab (VSCL) infrastructure. The directions for these labs are in the VSCL lab workbook. Here are some guidelines for working on these labs:

• You need to have Flash, Javascript and Java enable on you browser to run these labs.

• If you stop working on a lab before you have completed it, your work on the virtual machine is not saved. For many labs, this is not important and you can restart the lab where you stopped. Several labs require you to restart the lab from the beginning if you do not finish it. We will try to let you know ahead of time which labs these are.

• These labs require you to make screen captures to document your progress through the exercise. It is best if you make the screen capture from the host machine. If you perform the screen capture on the virtual machine, you’ll need to transfer the file to the host machine for submission for ending the lab.

• The worksheets for these labs are PDF forms that must be completed and submitted with the screen captures at the end of the lab. The VSCL worksheets can be found under the Lab Worksheet navigation link on the course web site.

VMWare Virtual Machine Linux Labs

These labs use a virtual machine you create during Week #1 of the course using VMWare Workstation (Microsoft Windows) or VMWare Fusion (Apple Mac OS X). You can download a free copy of VMWare through the DFCSC by following the VMWare Download navigation link on the course web site. Here are some guidelines for working on these labs:

• Your work on these labs is saved by VMware. If you stop a lab before finishing, you can restart where you left off.

• It is recommended that before you complete each of the Linux Security labs, you take a snapshot of the virtual machine so that you can revert to it if you make a mistake on the lab. This gives you the ability a restart point for the lab similar to a save point or checkpoint in a game.

• The worksheets for these labs are online forms similar to Sakai tests and quizzes. You have “unlimited” time on these to submit them, but similar to other assignments, they are due each Sunday evening. The VMWare lab worksheets can be found under the Labs & Exercises navigation link on the course web site.
Discussion Requirements for Undergraduate Credit [CSF434]

Weekly Discussion Participation Requirement (UGrad Students Only):

By class time Sunday, each undergraduate student is expected to make at least two discussion posts in the Topic A discussion forum for the week, with the first post in each made by midnight Wednesday.

Guidelines for Participation in Weekly Mandatory Discussion:

Starting on Sunday of Week #3, each week there is one mandatory graded discussion forum (Topic A) led by graduate students in which you must participate. Online discussion participation is graded based on frequency and quality of your posts.

Frequency:

Posts made during each week must meet the following frequency or participation requirements:

- At least one post must be made in each discussion by midnight Wednesday.
- At least two posts must be made before class the following Sunday in each of the two discussion forums.
- Additional posts in each forum are acceptable, but only two posts count towards your grade.

Meeting the minimum course participation requirements earns you four points for the week’s discussion grade.

Mandatory forums close on 11:59 PM, Sunday of each week. No late posts are accepted once a discussion has been closed.

Quality:

Each post is worth up to four quality points and is graded on quality according to this rubric:

<table>
<thead>
<tr>
<th>Pts</th>
<th>Description of Post or Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>Contributes to topic and indicates student’s mastery of the materials assigned. Integrates multiple views and/or shows value as a seed for reflection or inspiration for other participants’ responses in the discussion. Provides evidence that student is reading the assigned materials and other student postings and is responding accordingly, bringing out interesting interpretations. Post reflects student’s knowledge of the facts and ability to analyze them and to handle conceptual ideas.</td>
</tr>
<tr>
<td>3</td>
<td>Builds on the ideas of another participant (or more) and digs deeper into assignment questions or issues. Includes a good critique of the course material, demonstrating student has an understanding of the material, is reading posts of other students, and is contributing to the class. Demonstrates confidence with the materials, but may be just a bit off target in one area or another.</td>
</tr>
<tr>
<td>2</td>
<td>Meaningfully interacts with other participants’ postings. Posts that state “I agree” or “I disagree” also include an explanation of what is disagreed or agreed upon and why, or introduce an argument that adds to the discussion. Rambling, lengthy posts that show no sign of having been re-read and refined before posting. Writing suffers lack of clarity and comprehension.</td>
</tr>
<tr>
<td>1</td>
<td>Is of the form “I agree” or “That’s correct” and does not provide additional information to the conversation. Appears to be made only to meet the minimum posting requirements.</td>
</tr>
</tbody>
</table>

The maximum discussion grade for each week is **20 points** — a maximum of four points per post for four posts plus four frequency/participation points.
Additional Course Requirements for Graduate Credit [CSF334]

**WEEKLY DISCUSSION PARTICIPATION REQUIREMENT (GRAD STUDENTS ONLY):**

*By class time Sunday, each graduate student is expected to make at least two discussion posts in each of the two graded discussion forums for the week, with the first post in each made by midnight Wednesday.*

**WEEKLY DISCUSSION LEADERSHIP REQUIREMENT (GRAD STUDENTS ONLY):**

*Starting in Week #3 of the course, each graduate student has the responsibility of leading two weekly mandatory discussions — a network and system security discussion assigned by the instructor and a topic chosen by the graduate student. On any one week, a graduate student only needs to lead one discussion. The second assigned discussion will occur later in the semester. Discussion topics and leadership weeks will be assigned during the first week of classes.*

The following pages have details on the two parts of this course requirement. Following those sections, there is a listing of potential discussion topics to choose from.

Each graduate student needs to email Dr. Henry his or her top three desired discussion topics in order of preference. Topics are assigned based on the order they are received.
GUIDELINES FOR PARTICIPATION IN WEEKLY MANDATORY DISCUSSION:

Starting on Sunday of Week #3, each week there are two mandatory graded discussion forums led by fellow graduate students. Online discussion participation is graded based on frequency and quality of your posts.

Frequency:

Posts made during each week must meet the following frequency or participation requirements:

- At least one post must be made in each discussion by midnight Wednesday.
- At least two posts must be made before class the following Sunday in each of the two discussion forums.
- Additional posts in each forum are acceptable, but only two posts count towards your grade.
- Meeting the minimum course participation requirements earns you four points for the week’s discussion grade.
- Mandatory forums close on 11:59 PM, Sunday of each week. No late posts are accepted once a discussion has been closed.

Quality:

Each post is worth up to four quality points and is graded on quality according to this rubric:

<table>
<thead>
<tr>
<th>Points</th>
<th>Description of Post or Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>Contributes to topic and indicates student’s mastery of the materials assigned. Integrates multiple views and/or shows value as a seed for reflection or inspiration for other participants’ responses in the discussion. Provides evidence that student is reading the assigned materials and other student postings and is responding accordingly, bringing out interesting interpretations. Post reflects student’s knowledge of the facts and ability to analyze them and to handle conceptual ideas.</td>
</tr>
<tr>
<td>3</td>
<td>Builds on the ideas of another participant (or more) and digs deeper into assignment questions or issues. Includes a good critique of the course material, demonstrating student has an understanding of the material, is reading posts of other students, and is contributing to the class. Demonstrates confidence with the materials, but may be just a bit off target in one area or another.</td>
</tr>
<tr>
<td>2</td>
<td>Meaningfully interacts with other participants' postings. Posts that state “I agree” or “I disagree” also include an explanation of what is disagreed or agreed upon and why, or introduce an argument that adds to the discussion. Rambling, lengthy posts that show no sign of having been re-read and refined before posting. Writing suffers lack of clarity and comprehension.</td>
</tr>
<tr>
<td>1</td>
<td>Is of the form “I agree” or “That’s correct” and does not provide additional information to the conversation. Appears to be made only to meet the minimum posting requirements.</td>
</tr>
</tbody>
</table>

The maximum discussion grade for each week is **20 points** — a maximum of four points per post for four posts plus four frequency/participation points.
GUIDELINES FOR LEADING WEEKLY MANDATORY DISCUSSIONS

Starting in Week #3 of the course, each graduate student has the responsibility of leading two weekly mandatory discussions — a network and system security discussion assigned by the instructor and a topic chosen by the graduate student. On any one week, a graduate student only needs to lead one discussion. The second assigned discussion will occur later in the semester. Discussion topics and leadership weeks will be assigned during the first week of classes.

The discussion leader can earn up to 50 points for each of the discussions:

- **15 points**  Quality of primary discussion questions
- **25 points**  Demonstrates knowledge and understanding of subject
- **10 points**  Frequency of posts – engages students and does not stifle discussion

PRIOR TO THE DISCUSSION WEEK:

- Research the discussion topic using the textbook, Internet and other resources you have available.

- Develop at least four questions to provoke thought and discussion. The questions should be neither too open-ended nor too limiting. Simple yes/no questions do not inspire deep conversations. Questions can pose a somewhat controversial statement and ask student to prove or disprove it, agree or disagree with it, but always challenge the student to explain or defend his or her perspective.

DURING THE DISCUSSION WEEK:

- **By 6:00 PM on Sunday** post the first question and links to any additional readings that could help students prepare for the discussion.

- Review the discussion posts daily throughout the week. The discussion leader is considered the expert on the discussion topic and should answer any questions other students have on the material and clarify any misunderstandings. Comment on student posts and use the “Socratic Method” when possible:
  - **Respond** — A valid, friendly, personal response to a question or answer above it.
  - **Extend** — Some follow up analysis, discussion, redirection of the prior responses, and moving “forward” in the discussion.
  - **Probe** — At least one (or more) follow-up questions to get the students moving even deeper into the material.

- Use the additional prepared questions to keep the discussion moving. Be sure that students have questions available and themes to explore.

- To actively lead a discussion, discussion leaders should expect to make one post to every five to eight student posts. Too many posts can stifle the discussion and too few can give the impression the leader is not involved in the discussion.
Potential Weekly Discussion Topics

1. **Risk Management**: What is the best value that should be assessed when evaluating the worth of an information asset to the organization—replacement cost or lost income while repairing or replacing? What is the likelihood value of a vulnerability that no longer must be considered? In what instances is baselining or benchmarking superior to cost benefit analysis? How can we find out what the organization’s risk appetite is? Why is this important?

2. **Privacy**: Discuss how the definition of privacy that is commonly used (freedom from observation) may differ from the definition of privacy from the information security perspective (freedom from unsanctioned intrusion).

3. The decision to escalate incidents to law enforcement is an area fraught with conflict. Lead a class discussion on the pros and cons of law enforcement involvement.

4. Incident classification is based on the judgment of the information security professionals involved. Discuss with the class how one can determine if any given circumstance is business as usual, an incident, or a disaster.

5. The many authors believe that all information security begins with solid policy. Have the class brainstorm a list of reasons why this is so. Also, keeping policy current is critical. Have the class discuss how policy needs to be updated to accommodate current events.

6. **Technology**: Which architecture for deploying a firewall is most commonly used in businesses today? Why? What are the reasons that VPN technology has become the dominant method for remote workers to connect to the organizational network?

7. **Cryptography**: What are challenges and solutions for businesses in the use of cryptography for data storage and communications? What about law enforcement? Will biometrics involve encryption? How are biometric technologies dependent on the use of cryptography? Consider PKI (as discussed in the textbook) What is the future of PKI? Acceptance of PKI solutions—and product sales—has fallen short of early estimates. What would the “killer app” for PKI sales look like?

8. “*If someone really wants to get at the information, it is not difficult if they can gain physical access to the computer or hard drive.*” Is this statement categorically true or just true in most cases? Why? What are some recent incidents, such as the break-in at the VUDU offices that support or refute this statement?

9. Life safety must be of paramount concern in almost all settings (except perhaps a few national security areas). What guidelines are needed when life safety is not the paramount physical security concern?

10. What actions can each person take to minimize the risk of identity theft? Take a few minutes to discuss and generate a list of concrete actions each student can take to control this risk.

11. The placement of the security function is a broad topic. Discuss the placement of security in that organization.

12. Maintenance is an essential task that is often considered to be dull. In information security, penetration testing may be wrongly perceived as being a “hacker-like” activity. In fact, when
done correctly, ethical hacking is an important part of risk management. Penetration analysts work under very restrictive rules of engagement when testing systems. Brainstorm ways that penetration analysts limit the risk they pose to internal systems.

13. Privacy goes hand in hand with security, but many of the activities of information security analysts seem to be an invasion of privacy. Discuss how employers can justify the use of tools, such as Encase by Guidance Software.

14. Outsourcing is an interesting discussion topic. Lead a discussion about various elements of the outsourcing process—RFP, evaluation, contract award, and exit strategies. How does this relate to security?

15. The theories of change management (based on the Lewin model) add insight to how users deal with change. What are the change management issues that arise when implementing an information security plan?

**GENERAL TOPIC AREAS**

If you choose one of these areas, you must provide a specific sub-topic you wish to address since these are very broad.

16. Information Security Planning and Governance

17. Information Security Education, Training and Awareness Programs

18. Intrusion Detection and Prevention Systems: Strengths, weaknesses, strategies

19. Issues in physical security of information

20. Should certification be required for information security professionals?

21. Strategies and issues in the ongoing maintenance of information security

22. Digital Forensics (select a specific area)
The topics, readings and labs below are subject to change based on the actual pace of the course. Please check the course web site for the most up-to-date information.

## Advanced Topics in Network and Systems Security

<table>
<thead>
<tr>
<th>Date</th>
<th>Week</th>
<th>Topic</th>
<th>Labs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jan 18</td>
<td>Week #1</td>
<td>Introductory Topics and Administration</td>
<td></td>
</tr>
<tr>
<td>Jan 25</td>
<td>Week #2</td>
<td>System Forensics Methods</td>
<td>IIR #1</td>
</tr>
<tr>
<td>Feb 1</td>
<td>Week #3</td>
<td>Collecting, Seizing and Protecting Evidence</td>
<td>IIR #3, IIR #4</td>
</tr>
<tr>
<td>Feb 8</td>
<td>Week #4</td>
<td>Hiding, Scrambling and Recovering Data</td>
<td>IIR #6, IIR #8</td>
</tr>
<tr>
<td>Feb 15</td>
<td>Week #5</td>
<td>Basic Windows Forensics</td>
<td>IIR #5</td>
</tr>
<tr>
<td>Feb 22</td>
<td>Week #6</td>
<td>Basic Linux Forensics</td>
<td>IIR #9</td>
</tr>
<tr>
<td>Mar 1</td>
<td>Week #7</td>
<td>Performing Network Analysis</td>
<td>IIR #7,</td>
</tr>
<tr>
<td>Mar 8</td>
<td>Week #8</td>
<td>Incident and Intrusion Response</td>
<td>IIR #10</td>
</tr>
<tr>
<td>Mar 15</td>
<td></td>
<td>Spring Break Week</td>
<td></td>
</tr>
<tr>
<td>Mar 22</td>
<td>Week #9</td>
<td>Ethical Hacking, Pen Testing &amp; White Hats</td>
<td>HTT #1, HTT #2</td>
</tr>
<tr>
<td>Mar 29</td>
<td>Week #10</td>
<td>Footprinting and Social Engineering</td>
<td>HTT #3</td>
</tr>
<tr>
<td>Apr 5</td>
<td>Week #11</td>
<td>Port Scanning and Enumeration</td>
<td>HTT #4, HTT #7</td>
</tr>
<tr>
<td>Apr 12</td>
<td>Week #12</td>
<td>Wireless Vulnerabilities</td>
<td>HTT #8,</td>
</tr>
<tr>
<td>Apr 19</td>
<td>Week #13</td>
<td>Web and Database Attacks</td>
<td>HTT #5, HTT #6</td>
</tr>
<tr>
<td>Apr 26</td>
<td>Week #14</td>
<td>Physical Security, Defensive Technologies, and Incident Response</td>
<td>HTT #9, HTT #10</td>
</tr>
<tr>
<td>May 3</td>
<td></td>
<td>Final Exam Week</td>
<td></td>
</tr>
</tbody>
</table>
Lab Assignment Key

(VSCL) Incident Investigation and Response
IIR #1: Perform a Byte-Level Computer Audit
IIR #2: Apply the Daubert Standard on the Workstation Domain
IIR #3: Create a Forensic System Case File for Analyzing Forensic Evidence
IIR #4: Uncover New Digital Evidence Using Bootable Utilities
IIR #5: Automate Digital Evidence Discovery Using Paraben’s P2 Commander
IIR #6: Apply Steganography to Uncover Modifications to an Image File
IIR #7: Decode an FTP Protocol Session and Perform Forensic Analysis
IIR #8: Automate Image Evaluations and Identify Suspicious or Modified Files
IIR #9: Craft an Evidentiary Report for a Digital Forensics Case
IIR #10: Perform an Incident Report Investigation for a Suspicious Logon

(VSCL) Hacker Tools and Techniques
HTT #1: Develop an Attack & Penetration Test Plan
HTT #2: Implement Hashing and Encryption for Secure Communications
HTT #3: Perform Data Gathering and Footprinting on a Targeted Website
HTT #4: Compromise and Exploit a Vulnerable Microsoft Workstation
HTT #5: Perform a Website and Database Attack by Exploiting Identified Vulnerabilities
HTT #6: Identify & Mitigate Malware & Malicious Software on a Windows Server
HTT #7: Conduct a Network Traffic Analysis & Baseline Definition
HTT #8: Audit and Implement a Secure WLAN Solution
HTT #9: Perform Incident Response for an Infected Microsoft Windows Workstation
HTT #10: Design and Implement SNORT as an Intrusion Detection System (IDS)

(VMWare) Ubuntu Security
UBT #1: Install a Minimal Ubuntu Server
UBT #2: Configure Basic Security Controls on a Ubuntu Linux Server
UBT #3: Install a Secure FTP Server and Harden su
UBT #4: Apply Hardened User Account Management and Security Controls
UBT #5: Apply Hardened Linux File System Security Controls
UBT #6: Apply Hardened Security for Linux Services and Applications
UBT #7: Apply Hardened Security for Controlling Access
UBT #8: Apply Hardened Security for the Linux Kernel
UBT #9: Implement Best Practices for Secure Software Management
UBT #10: Implement Best Practices for Security Logging and Monitoring
UBT #11: Define Linux OS and Application Backup and Recovery Procedures
Academic Integrity

All work is to be the result of your own individual efforts unless explicitly stated otherwise. Plagiarism, unauthorized cooperation or any form of cheating will be brought to the attention of the Dean for disciplinary action. If you have any uncertainties in this area, see the appropriate sections (8.27) of the University Manual.

You may discuss homework in a general way with other students, but you may not consult any one else's written work. Sharing of code on individual programming assignments is a form of academic dishonesty. Any similarity in form or notation between submissions with different authors will be regarded as evidence of academic dishonesty -- so protect your work.

Software piracy will be dealt with exactly like stealing of university or departmental property. Any abuse of computer or software equipment will subject to disciplinary action.

You should use your own solutions to any of the programming assignments. If you use excerpts of code from the textbook or an Open Source project, always cite your source and check the license or copyright agreement to ensure how you use the code is acceptable. In most cases, you can freely use Open Source software as long as the appropriate copyright notice is maintained in your derivative work.

**Remember - cite the source of your material if it was not your creation!**

Another common area of plagiarism is in homework assignments. In this internet age, it is quick and easy to do a web search on the text of a homework question and find web pages where students and even instructors, have posted solutions. To copy and paste these solutions into your assignment is plagiarism. As a warning, this type of plagiarism is very easy to discover because I can easily perform the same web search.