CpE-568: Computer Network Forensics: Fall 2014

Instructor: Dr. John Moody  
Phone: 304 692 9991  
Email: moodywv@gmail.com or jmoody2@wvu.edu

Office Hours: As needed prior to and after class, others by appointment

Class Time: Tuesday 6:00-9:00 PM

Class Location:  
3102 Prete Building, 3040 University Ave, Morgantown, WV

Prerequisite Background:  
Student should be knowledgeable in a high level language as well as assembly language, have computer architecture or computer organization background, and knowledge of TCP/IP such as from CS-453.

Corequisites: none

Course Materials:  

Description: This course is an introduction to threat assessment in modern networked computer systems; and the techniques, methodologies and technologies for preventing intrusions, detecting intrusions, recovering from intrusions, and finally techniques for collecting evidence of intrusions.

Objectives: The objective of this course is to provide students with a comprehensive view of the threats for networked computer systems, the various tools and technologies for protecting the network, techniques for emergency response, and, finally, methods to gather evidence.

Course Objectives: This course is to serve as an overview course of network forensics.

Outcomes:  
- Understand computing network architecture, components and their functions  
- Understand network protocols, their uses, and vulnerabilities  
- Understand and apply protection measures against various network protocol attacks and other malicious code.  
- Be able to plan, implement and assess security protection mechanisms in generic computer and communication systems.  
- Understand the various alternatives for firewalls, intrusion detection, trace-back and evidence gathering systems.  
- Familiarity with a number of tools used in network forensics.  
- Ability to investigate the occurrence, identification and source of break-ins by examining computer logs and other traces left in compromised computers.
RULES OF OPERATION:

Attendance:
Students are not required to attend lectures but are responsible for all materials covered in lectures, homework, labs, and tests.

Communication:
E-mail addresses will be collected during the first day of class to set up an email distribution list. This will be used to make class announcements, so check your email regularly.

Homework and Programming Assignment:
Homework and programming assignments will be due at the beginning of class. The due dates for these assignments will be announced during class. Homework that is turned in later than the beginning of that class is defined as late. Unexcused late assignments will be marked down 10% per day. Assignments submitted in the evening will be accepted on the next working day. Assignments that are more than seven days late will not be accepted and the student will receive a zero (0) for that assignment. Homework should be typed using a standard word processor.

Exams/Work:
Two tests will be administered during the semester. Tests, unless otherwise noted, will be closed book/closed notes, no calculators/computers/cell phones allowed to be used during the exam. A paper will also be due covering a selected topic on which the student will present a short lecture. Labs will be conducted periodically during the same time as the normal class period.

Course Grade:
The two tests, the paper/lecture, homework and labs will count toward the final grade according to the following general breakdown Test 1: 30%, Test 2: 30%, Paper/Lecture: 25%, Homework/Labs: 15%. Grades will be based on: A = 90-100%, B = 80-89%, C = 70-79%, D = 60-69%, F < 60%.

Academic Honesty:
Students are expected to exhibit the same level of professionalism and integrity that will distinguish them in the future careers. Your signature on assignments attests to your completion of the work in an ethical and professional manner. Penalties outlined in the WVU Student Handbook for academic dishonesty will be enforced.

Other Policies:
During class periods, cell phones/pagers should not be heard ringing and should not be answered in class. Utilization of the Internet during class periods should be limited to activities related to the course.

From time to time, we may discuss vulnerabilities in widely deployed computer systems. This is not intended as an invitation to go exploit those vulnerabilities. It is important that we be able to discuss real-world experience candidly; students are expected to behave responsibly. WVU’s policy on this is clear: you may not break into machines that are not your own; you may not attempt to attack or subvert system security. Breaking into other people’s systems is inappropriate; and the existence of a security hole is no excuse.
Homework: Students are encouraged to discuss homework assignments but must submit their own individually prepared assignments. Jointly prepared and/or copied assignments will be severely penalized.

Reading and Research Joint work is prohibited. No discussion with anyone until after work is turned in. Jointly prepared and/or copied assignments will be severely penalized

Other notes on academic dishonesty in addition to the above 3 and 4:
- I consider it academic dishonesty if you share final assignments, work, solutions, etc. with other students.
- Changing variable names and/or output messages does not make it original work!
- If ANYTHING, including code, is “reused,” you must site the source (code source can be cited in the comments for that code or routine. This includes your own previous work!)
- Allowing others to view your work by leaving permissions set incorrectly or leaving files on hard drives or other disks accessible by others will be considered academic dishonesty and will result in an F in the course.
- If a student does discuss and share work with another, thinking that the person who is receiving that information will not copy it, both people will be held responsible for academic dishonesty if identical work is submitted and both claim that it is original.
- Work is submitted and both claim that it is original.\footnote{Roy S. Nutter, 2014.}

West Virginia University is committed to social justice. I concur with that commitment and expect to maintain a positive learning environment based upon open communication, mutual respect, and non-discrimination. Our University does not discriminate on the basis of race, sex, age, disability, veteran status, religion, sexual orientation, color or national origin. Any suggestions as to how to further such a positive and open environment in this class will be appreciated and given serious consideration.

If you are a person with a disability and anticipate needing any type of accommodation in order to participate in this class, please advise me and make appropriate arrangements with Disability Services (293-6700).

“WVU recognizes the diversity of its students and the needs of those who wish to be absent from class to participate in Days of Special Concern, which are listed in the Schedule of Courses. Students should notify their instructors by the end of the second week of classes or prior to the first Day of Special Concern, whichever is earlier, regarding Day of Special Concern observances that will affect their attendance. Further, students must abide by the attendance policy of their instructors as stated on their syllabi. Faculty will make reasonable accommodation for tests or field trips that a student misses as a result of observing a Day of Special Concern.”
This Computer Forensics class requires that all students in the class acknowledge that they have been informed about the Program’s drug policy. This policy supports a drug-free lifestyle and recognizes that internship sites and prospective law enforcement agencies and companies wishing to employ our graduates may require drug testing and polygraph assessment as a condition of internship or employment. Each student must recognize this possibility as they enter the forensics field. We, therefore, require each student to read and sign the following statement acknowledging that this information has been presented to him or her.

**Computer Forensics PROGRAM DRUG POLICY**

The Computer Forensics program encourages all students to maintain a **totally** drug-free lifestyle to insure they will not be denied access to internship sites or employment especially with various security and law enforcement agencies as the result of any past or present use of illegal drugs.

A number of security and law enforcement agencies will require prospective employees from our program to sign a statement affirming that they have never used these substances and will require them to take a polygraph related to their statements. Some agencies providing internships will also require our Computer Forensic students to take a polygraph related to their drug history. Students must recognize they can be denied access to some internship sites and employment at security and law enforcement agencies if they fail any of the checks or the polygraph questions related to the use of illegal drugs.

I agree that I have been informed of the above.

_______________________________
Signature of Student

_______________________________
Date

_______________________________
Signature representative of the
WVU Computer Forensics Program
<table>
<thead>
<tr>
<th>Date</th>
<th>Lecture</th>
<th>Subject/Notes</th>
<th>Lab</th>
</tr>
</thead>
<tbody>
<tr>
<td>26-Aug</td>
<td>Introduction, Ch 1: Foundation, Ch 2: Technical Fundamentals</td>
<td>Ch 1-2 Text</td>
<td></td>
</tr>
<tr>
<td>2-Sep</td>
<td>Ch 3: Evidence Acq, Ch 4: Packet Analysis</td>
<td>Ch 3-4 Text</td>
<td></td>
</tr>
<tr>
<td>9-Sep</td>
<td>Ch 4: Packet Analysis, Ch 5: Statistical Flow Analysis</td>
<td>Ch 4-5 Text</td>
<td></td>
</tr>
<tr>
<td>16-Sep</td>
<td>Ch. 5 Statistical Flow Analysis</td>
<td>Ch 5 Text, Lab: Port Scanners, Packet Sniffers</td>
<td>X</td>
</tr>
<tr>
<td>23-Sep</td>
<td>Ch 6: Wireless Network Forensic, Ch 7 Network Intrusion Detection</td>
<td>Ch 6-7 Text</td>
<td></td>
</tr>
<tr>
<td>30-Sep</td>
<td>Ch 7: Network Intrusion Detection</td>
<td>Ch 7 Text</td>
<td></td>
</tr>
<tr>
<td>7-Oct</td>
<td>Test 1, Lab</td>
<td>Test 1, Lab IDS</td>
<td>X</td>
</tr>
<tr>
<td>14-Oct</td>
<td>Fall Break Recess</td>
<td></td>
<td></td>
</tr>
<tr>
<td>21-Oct</td>
<td>Hack Anatomy, Buffer Overflow, Ch 8: Event Log Aggregation, Correlation, Analysis</td>
<td>Supplied materials, Ch 8 Text</td>
<td></td>
</tr>
<tr>
<td>28-Oct</td>
<td>Ch 9: Switches, Router Firewalls, Ch 10: Web Proxies</td>
<td>Ch 9-10 Text, Paper Topic Selection Due</td>
<td></td>
</tr>
<tr>
<td>4-Nov</td>
<td>General Election Day</td>
<td></td>
<td></td>
</tr>
<tr>
<td>11-Nov</td>
<td>Ch 10: Web Proxies, Ch 11: Network Tunneling</td>
<td>Ch 9-10 Text</td>
<td>Lab, Time permitting</td>
</tr>
<tr>
<td>18-Nov</td>
<td>Ch 12: Malware Forensics, Test 2</td>
<td>Ch 12 Text, Test 2</td>
<td></td>
</tr>
<tr>
<td>25-Nov</td>
<td>Thanksgiving Recess</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2-Dec</td>
<td>Presentations</td>
<td>6 Presentations (20 minutes each)</td>
<td></td>
</tr>
<tr>
<td>9-Dec</td>
<td>Presentations/ Review of Class</td>
<td>4 Presentations (20 minutes each), Paper Due</td>
<td></td>
</tr>
</tbody>
</table>