**Intro to Cybersecurity: CPS493-01 / CPS593-06**

**Monday & Thursday – 5:00 PM – 6:15 PM – van den Berg Hall 104**

**Paul Chauvet, MBA, CISSP**

# **Course Description**

This course is meant as a survey course in cybersecurity, covering a wide array of topics. The course will be heavy in lab work with both in-class and at-home exercises. Students will be introduced into core concepts including the threat landscape, social engineering and the psychology of cybersecurity, as well as major vulnerability categories including software security, network and system security, and cryptography. Students will work on exploiting vulnerabilities using the lab exercises using a virtual lab environment, and the Metasploit framework. Real world examples of major data breaches will be discovered – with a discussion of how these attacks could have been prevented, or if not prevented, detected sooner.  
  
Students will be exposed to offensive security techniques for the purposes of avoiding such mistakes in their own code, for analyzing or auditing other code to identify such vulnerabilities, or for the purposes of penetration testing on authorized targets.

The course will not only deal with the technical aspects of attack and defense, but will get students to think about, analyze, and discuss the targets of hackers. In some scenarios, students will put themselves in the place of an information security analyst or manager at a large corporation.

# **Instructor Information**

**Paul Chauvet**

Office: Haggerty Administration Building 49 – Phone: 845-257-3828 – Email: [chauvetp@newpaltz.edu](mailto:chauvetp@newpaltz.edu)  
Office Hours: By appointment – please email to setup an appointment. If I’m in my office otherwise, you’re welcome to stop by though depending on my other work at the college I may have to schedule an alternate time.

# **Required resources**

**Textbook:** *Computer Security: A Hands-On Approach,* by Dr. Wenliang Du, 2019, 2nd edition (ISBN: 978-1733003902). The course will use the SEED (Security Education) Labs associated with the text – which requires the free VirtualBox virtualization software to be installed on your laptops. Printed – not electronic versions – of the text is recommended (due to the exams being open book).  
**Laptops**: A laptop (Windows, Linux, Mac) is required for the course. You’ll use it for lab exercises in class.  
**VirtualBox**: An open source virtualization software package which you will run on your own laptop, available at virtualbox.org.

# **Other Readings and Resources**

SEED Labs: <http://www.cis.syr.edu/~wedu/seed/Labs_16.04/>

CIS/SANS Critical Security Controls: <https://www.cisecurity.org/controls/>

SANS Reading Room: <https://www.sans.org/reading-room>

Threat Modeling: Designing for Security (2014, Adam Shostack – available to view online via library catalog)

Other readings as listed in the schedule

# **Attendance and Evaluation**

This class will heavily focus on the in-class lab exercises. This means that attendance is required. Failure to attend when lab exercises are done will require performing the lab environments at home. Excessive unexcused absences will impact the final grade.

**Weight Criteria**

10% Class-participation

30% Lab assignments

30% Case studies, research review, and other written assignments (non-coding/lab assignments)

15% Midterm exam

15% Final exam

Class participation includes contributions during in-class discussions, as well as in-class lab participation. When assigned, readings should be done before class to be properly prepared for the class discussions. Non-test assignments will be graded upon several factors including, but not limited to:

* Thoroughness of analysis/discussion – don’t just repeat what articles/sources are saying. Find additional resources to back-up points you are making.
* Accuracy of code
  + Note: If code isn’t working – detail any troubleshooting steps you’ve taken, analysis of why it may not be working, etc.
* Code comments – Someone should be able to understand what you’re doing by reading the comments if they have familiarity with the language

Note: Exams are open book/notes. Any non-electronic material can be brought in – but no computers/tablets/phones can be used in the exams.

**100-93 = A, 93-87 = A-, 87-80 = B+, 80 – 75 = B, 75-70 = B-, 70-65 = C+, 65-60 = C, 60-55 = C-, 55=50 = D, 50=0 = F**

# **Assignments**

All assignments should be sent via Blackboard. For writing assignments, please use Microsoft Word (.docx) or Open Document Format files. For code assignments, just send any code as the raw source file. If you have multiple files for a single assignment, you may want to put them in an archive (zip or tar). Code assignments should be commented (comments should include citations if you obtained code segments from sources other than the text/class).

For non-code assignments, especially when doing threat modeling or discussing data breaches, you should find and cite external resources (peer reviewed journal articles and in-depth analysis of past data breaches is especially valuable).

Late assignments provided without a documented medical/family emergency will have letter grades deducted (one letter grade per week).

Early in the semester, each student will pick a real Fortune 500 (or similar size) company. During the semester, various assignments will be given related to your specific company where you will have to work on an assignment as if you were part of the security team within that company. Note: Company should *not* be a dedicated cybersecurity company, nor one of the following big tech companies: Apple, Amazon, Facebook, Google/Alphabet, IBM, or Microsoft. Each company can only be chosen by one student - so the first student to make a selection gets to use that company.

# **Policies Regarding Students with Disabilities**

Students with documented physical, learning, psychological and other disabilities are entitled to receive reasonable accommodations. If you need classroom or testing accommodations, please contact the Disability Resource Center (Student Union Building, Room 205, 257-3020, drc@newpaltz.edu). The DRC will provide forms verifying the need for accommodation. As soon as the instructor receives the form, you will be provided with the appropriate accommodations. Students are encouraged to request accommodations as close to the beginning of the semester as possible. See ADA policy at <http://www.newpaltz.edu/drc/manual_procedures.html>.

# **Academic Integrity**

Students are expected to maintain the highest standards of honesty in their college work. Cheating, forgery, and plagiarism are serious offenses, and students found guilty of any form of academic dishonesty are subject to disciplinary action. For definitions of theses offenses, as well as the process that a faculty member may follow if a student is found to be engaging in any form of academic dishonesty, see the section on Academic Integrity in the Advising Handbook, available at <http://www.newpaltz.edu/advising/policies_integrity.html>.

Copying and pasting code from web resources or other classmates is also considered plagiarism. If you use outside resources, cite them in your code. ***Do not share your work with other students. If two students are found to submit the same work – then both will be failed on the assignment (regardless of who copied and who was copied from)***. This includes in-class exams.

# **Ethics & Policy Issues**

During this course, various techniques and tools will be discussed, used, and taught. Many of these tools can be used for both legitimate and illegitimate purposes. These techniques should not be used on systems, networks, or individuals, where there is not explicit authorization to do so (by the system owner, as well as the source and destination network). Students in this course should strive to work towards the betterment of society and the common good by helping to reduce cybersecurity risk.

Many lab exercises will require offensive security techniques. For the purpose of this course, a waiver against the traditional prohibitions on these techniques (outlined in the *Acceptable Uses and Privacy Policy* available at [www.newpaltz.edu/itpolicy](http://www.newpaltz.edu/itpolicy)) is made for authorized course exercises on targets explicitly authorized by the instructor. Any use of these techniques on the college’s general network or systems, or external systems, is still prohibited. If there is any doubt as to the scope of an exercise, please contact the instructor.

Students are responsible for securing their own computers – especially when setting up networking for Metasploitable exercises. New Paltz is not responsible for any systems compromised as a result of incorrectly setup devices or virtual machines. If you have issues – reach out.

# **Evaluation of Instructor**

Near the end of the semester, you will get a chance to provide a “Student Evaluation of Instruction” (SEI). I would encourage you all to both complete this, as well as to feel free to provide feedback to me during the semester.

As stated in class – this is only the second time I’m teaching, though I have worked for years in cybersecurity and information technology. As such, your feedback (positive, negative, or neutral) is especially valuable. If we’re going too quickly, if things are not being explained clearly, never hesitate to either ask me in class, send me an email, etc.

# **Course Schedule Notes**

The course schedule below may be adjusted due to time constraints (for example, if covering a topic takes more time than originally allotted, it will impact future dates.

Special notes:

* Thursday classes are held on Tuesday, March 24th – so we will actually have 3 classes that week.
* My apologies, but there will be no classes held on April 20th and 23rd as I will be out of state at a security conference. Anyone who wants to meet to work on labs can do so during this time. Additionally, the official makeup day (May 7th) will be used for our final class as a pre-final review.

|  |  |  |  |
| --- | --- | --- | --- |
| Week | Date(s) | Topic(s) | Text chapter or reading |
| 1 | Jan 23 | Course overview and Linux/VirtualBox overview  ***Virtual Box – networking assignment given*** |  |
| 2 | Jan 27  Jan 30 | Security controls, defense in depth, Kill Chain model of intrusion  Buffer overflow lecture | Du, Chapter 4 |
| 3 | Feb 3/6 | Buffer overflow lab  ***Buffer overflow lab assignment given*** |  |
| 4 | Feb 10/13 | Vulnerabilities and attack vectors & Threat modeling  ***Threat modelling assignment given*** | Threat Modeling: 12 Available Methods – Nataliya Schevchenko  <https://insights.sei.cmu.edu/sei_blog/2018/12/threat-modeling-12-available-methods.html> |
| 5 | Feb 17/20 | Cryptography (Encryption/Hashing/Digital Signatures)  ***Cryptography assignment given*** | Du, Chapters 15 & 16 |
| 6 | Feb 24/27 | Psychology and Social Engineering | Psychology of Security – Bruce Schneier – parts 1 & 2  <https://www.schneier.com/essays/archives/2008/01/the_psychology_of_se.html> |
| 7 | Mar 2/5 | *Cross-Site Request Forgery (CSRF)*  ***CSRF assignment given*** | Du, Chapter 10 |
| 8 | Mar 9 | Network Security, DNS, DHCP  ***Case study assignment given*** |  |
| 8 | Mar 12 | ***Mid-term exam*** | Includes all topics from weeks 1 through 7. |
| 9 | **Spring Break – no classes March 16th through 20th** | | |
| 10 | Mar 23/24/26 | Case Studies on previous data breaches including class discussion  Continuation of network security topics | Note: Thursday classes are held on Tuesday the 24th this week so there are three classes this week. |
| 11 | Mar 30/Apr 2 | *Cross-Site Scripting Attacks (XSS) & Lab*  ***XSS assignment given*** | Du, Chapter 11 |
| 12 | Apr 6 | SQL Injection Attacks  ***SQL Injection assignment given*** | Du, Chapter 12 |
| 12 | April 9 | **Note: April 9th – no class (Easter/Passover)** | |
| 13 | Apr 13/16 | Kali Linux, network reconnaissance, nmap, and vulnerability scanning  ***Reconnaissance assignment given*** |  |
| 14 | Apr 20/23 | Class will not meet this week – see special note on previous page | |
| 15 | Apr 27/30 | Kali, Metasploit, and Metasploitable  ***Metasploit/Kali assignment given*** |  |
| 16 | May 7th | Makeup date for classes – attendance is not required but recommended as there will be a review before the final exam. | |
| Final | May 11th | ***Final is 5:00-7:00PM – not normal course time.*** |  |