

Introduction to Cybersecurity

COS430

George Markowsky
Computer Science Department
University of Maine

GOALS

1. To provide you with a broad view of cybersecurity as information security.
2. To provide you with a general view of security, so that you understand how cybersecurity fits into this more general picture.
3. To help you understand that cybersecurity is as much a problem of people and institutions as it is a technical problem.
4. To help you better understand the nature of the attacks and attackers that you might face.
5. To provide you with some basic tools and techniques for defending yourself from cyberattacks.
6. To help you get acquainted with basic sources that you will need to use to effectively work in cybersecurity.

GENERAL NOTE

This is only the third time I am offering this course, so it is still a work in progress. In particular, it is quite different from last semester because I have changed one of the textbooks and because each student will maintain a server alone. Thus, the syllabus should be considered as a proposed syllabus that might change in significant ways.

PREREQUISITES

COS 230, COS 431 and one semester of programming.

GRADING

This course will have three types of homework: structured written homework, free-form written homework, and system homework and documentation. Structured homework consists of exercises for which there is little or no choice for the correct answer. Free-form homework consists of questions for which there are a wide variety of answers or of problems that are unique to the student. System homework consists of maintaining your system and documenting its performance, for launching attacks against other systems, and for defending yourself against attacks. You will receive separate grades for each type of homework, and the type of homework will be noted when it is assigned.

Cheating has become all too common in contemporary academic settings. I am very much opposed to it because it keeps people from acquiring the skills that are taught in the course. Furthermore, as you will see, cybersecurity depends on trusting individuals to protect cyber-assets. It should be clear that people who cheat in their cybersecurity course are not worthy of passing the course since they

are not developing the skills that they need and are not demonstrating the high level of integrity that is necessary to be effective in this area. Cheating will be dealt with severely in this course.

Your final average will be computed using the harmonic mean of the three types of homework. This averaging method places equal emphasis on the three types of homework. In particular, if you get a very poor grade on any one type of homework it will seriously drag your average down. There will be weekly homework in this class.

1. I will use +/- grading in the class. The grades will be assigned on the basis of your **final class average** based on the following ranges:

A	-- 90 or above	C	-- 70 to 72
A-	-- 85 to 89	C-	-- 65 to 69
B+	-- 83 or 84	D+	-- 63 or 64
B	-- 80 to 82	D	-- 60 to 62
B-	-- 75 to 79	D-	-- 55 to 59
C+	-- 73 or 74	E	-- 54 or below

2. The different homework grades will be computed by using the arithmetical average of all homeworks of a given type.

3. All numbers are rounded and the letter grades are assigned according the scale mentioned in 1.

THE HARMONIC MEAN APPROACH TO GRADING

In this course, all the different types of homework are very important. The arithmetical mean allows a good performance in one area to offset a poor performance in another. Since I want to emphasize good performance on all types of homework, I will use the harmonic mean of the homework grades as your final average.

The exact formula for the harmonic mean of three quantities is

$$G = 3/(1/St + 1/FF + 1/Sys)$$

Here St is the structured homework grade, FF is the free-form homework grade and Sys is your system grade. Your final grade G will be computed by using this formula exactly and rounding off to the nearest whole number. Note that if any of St, FF or Sys are 0, then G is also 0.

The harmonic mean is very sensitive to extremes in performance. In other words, if your homework grades are close to one another, their harmonic mean is essentially the same as the usual arithmetic mean. If they are far apart, the harmonic mean is pulled sharply down toward the lowest grade. Thus, students who copy their structured homework from others cannot use the good grades they obtain in this manner to offset their poor free-form homework grades. For example, if you get 100 for your structured homework, 80 for your free from homework and 40 for your system work your final grade will be 63.

ADDITIONAL NOTES

1. I want people to work on the homework individually. You can talk to each other and give help, but this help should not take the form of letting other people copy your work. It is important that you understand how to do all the problems on your own. **If you have questions, please ask them in class, send me e-mail, drop by during office hours or come by during some other mutually agreed-upon time.**
2. The homework grading will be strict since the goal is to make you more careful. Errors are the source of much mischief, so it is important to reduce them as much as possible. Even minor arithmetical mistakes will result in points being lost, so do your work carefully.
3. If a problem asks you to write a program, a function or a procedure, always submit a printed listing and output, even if the problem does not explicitly ask for these. **Handwritten code is not acceptable.**
4. If your programs have bugs, I expect you to make a reasonable effort to find the bug on your own. I will be happy to help you find problems in your programs, but you must come with evidence that you have tried to find the problem on your own and the program I see should have evidence of your efforts to debug it.
5. If you run out of time and must turn in a program that doesn't run, submit output showing the crash and the error message as well as a listing.
6. Be sure that your listings include comments that explain what you are doing if it is not completely obvious. It is up to you to explain what you are doing.
7. If you do not understand a problem get a clarification from me. Do not waste a lot of time working on something that you don't understand.
8. I do not accept late homework except in special circumstances. You must get permission in order to turn your homework in late. Such permission is the exception rather than the rule. Homework turned in late without permission will lose points.
9. Since this is a senior level course, I expect very high quality submissions from you. **Points will be deducted for sloppy or disorganized work.**
10. Programs must be integrated into your homework manuscript. In other words, don't just hand in a program listing stapled to the homework. Place it close to the text giving the answer to that particular problem. It must be clearly labeled and relevant parts highlighted. In particular, I don't want little short paragraphs that say "see PROGRAM..." with a pile of printout attached. The pages of the homework should be consecutively numbered.
11. Any program that you submit must include sample output that adequately tests it. This sample run should not be copied from the screen by hand and should not be a screen dump attached

separately. If you want to use a screen dump, put it close to the relevant problem in the homework and give adequate indications of where the output can be found. Alternatively, have the output sent to a file and include the file in your manuscript. You should think carefully about what constitutes an adequate test for each program that you write. You will lose points for inadequate testing.

12. When you write programs, pay attention to the human interface. The requests for data should be reasonable. Ridiculous interfaces will lose points just for being ridiculous.

13 Be sure that you answer the question. If you are asked for an analysis of an algorithm, be sure to supply one. Do not assume that you will receive the bulk of the points simply for coding it. Also, if I ask you to analyze a particular algorithm, analyze the one you are given. Don't analyze some other algorithm. Don't answer questions that are "almost" like the questions you are asked.

14. I expect your algorithms to be reasonably efficient. Just simply whipping something together that gets the job done might not be enough. Also, if you make modifications to algorithms, you will lose points if you make the algorithm perform significantly less efficiently from what was presented.

15. Do not scatter your work all over the place. I will not read through listings to find an analysis of an algorithm. This analysis should be in the text, not in the listing somewhere.

16. Submit all necessary pieces. I don't want to guess what data types you used, etc.

17. You will lose points for submitting poorly organized and unreadable material. **I expect your homework to be stapled together not paper clipped together.**

18. You will lose points for poor programming style. I do not want to see hoards of global variables in your programs. You have been taught how to do things correctly and I want to see you do it.

19. I will post current grades on the web encoded by class ID. This process will be explained in class and you will be able to pick your class ID. You should check this listing regularly to make sure that your grades have been recorded correctly.

20. **I am only interested in grading your original work. I am not interested in grading solutions to the problems that have been posted by other professors on the Web. You can lose many points if you simply copy solutions from other people or other sources.**

OFFICE HOURS

Office : 237 Neville Hall.
Office Hours : 10:45-12:00 Tuesdays, and Thursdays. Check website.
Phone : 581-3940
E-mail : markov@umcs.maine.edu
Web : www.cs.umaine.edu/~markov

Please check <http://www.umcs.maine.edu/~markov/appointments.html> to make sure I will have time to see you. In general, it is best if you make appointments via the website. That way I can notify you in case anything changes. If you are planning to come to office hours from far away please check

with the Computer Science Office (581-3941) to make sure that some event will not prevent me from being at office hours as well as my website. If you have problems with this course and need help come in to see me immediately. Don't fool around until the end of the semester and then try to learn all the material in a week.

TEXTS

The texts for the course are *Hands-On Ethical Hacking and Network Defense* by Michael T. Simpson (Thompson Course Technology, 2006), and *Practical Unix & Internet Security* Third Edition by Simson Garfinkel, Gene Spafford and Alan Schwartz (O'Reilly, 2003). If you are not an experienced Linux system administrator, you might consider the optional recommended book *Beginning Ubuntu Server Administration* by Sander van Vugt (Apress 2008).

TEACHING ASSISTANT

The teaching assistant is Larry Whitsel.

Office : 113 Neville Hall.
Office Hours : 1:00-2:00 Tuesdays, and Thursdays and by appointment
Phone : 299-5951
E-mail : larry.whitsel@umit.maine.edu

COS 498 SYLLABUS AND HOMEWORKS

I plan to cover both books during the semester. On a weekly basis, you will have to write summaries of the assigned reading. This will be part of your free-form homework. These will be primarily graded on the basis of whether it looks like you read the material and successfully summarized it in your own words. Points will be deducted for sloppy work, spelling mistakes, grammatical errors, and similar deficiencies.

The schedule below refers to the two textbooks using the abbreviation EH for *Ethical Hacking* and PS for *Practical Unix & Internet Security*. Numbers following the abbreviations are chapter numbers.

A key component of this course is extensive hands-on experience and the in-class cyberwars. This semester, you will each get a computer and be expected to set up a Linux server and monitor it on the Internet. After some experience on the Internet, the cyberwars will begin. I hope to have two complete wars, each lasting about a month. During the first war, each person will try to attack the computers belonging to other people and try to compromise them. Of course, you will need to defend your computer against attack as well. After the first cyberwar, we will have a review of events and have a second cyberwar. During the second cyberwar, we will divide the class into 3 or 4 teams of servers, and the goal will be for the teams to attack each other and also to defend all the servers on the team.

Below is the tentative syllabus for the course. Pay special attention to the reading assignments. HW assignments will be distributed by e-mail once everyone submits an e-mail address and class ID on my website.

DATE	EVENT
1/13	Intro to the course, Intro to Unix/Linux; PS(1-3), EH(1,9,A)
1/15	Policies, Guidelines, Legal Issues; PS(1-3), EH(1,9,A)
1/20	Servers Released; TCP/IP; Unix; PS(4-5), EH(2)
1/22	TCP/IP; Unix; PS(4-5), EH(2)
1/27	Network and Computer Attacks; File Systems, Cryptography; PS(6-7),EH(3)
1/29	Network and Computer Attacks; Files Systems, Cryptography; PS(6-7),EH(3)
2/03	Servers Due for placement on Internet; Footprinting and Social Engineering; Physical & Personnel Security; PS(8-9), EH(4)
2/06	Footprinting and Social Engineering; Physical & Personnel Security; PS(8-9), EH(4)
2/10	Port Scanning; Dial-Up Security, TCP/IP; PS(10-11), EH(5)
2/12	Port Scanning; Dial-Up Security, TCP/IP; PS(10-11), EH(5)
2/17	Servers returned for reconfiguration and preparation for Cyberwar I; Enumeration; Securing TCP/UDP; PS(12), EH(6)
2/19	Enumeration; Securing TCP/UDP; PS(12), EH(6)
2/24	Servers returned for placement on PirateNet[©]; Cyberwar I; Programming for security Professionals; Sun RPC, Authentication; PS(13-14), EH(7)
2/26	Programming for security Professionals; Sun RPC, Authentication; PS(13-14), EH(7)
3/03	SPRING BREAK
3/05	SPRING BREAK
3/10	SPRING BREAK
3/12	SPRING BREAK
3/17	Microsoft OS Vulnerabilities; Filesystems, Programming; PS(15-16), EH(8)
3/19	Microsoft OS Vulnerabilities; Filesystems, Programming; PS(15-16), EH(8)
3/24	Linux OS Vulnerabilities; Backups, Defense; PS(17-19); EH(9)
3/26	Linux OS Vulnerabilities; Backups, Defense; PS(17-19); EH(9)
3/31	Servers returned to teams, review of Cyberwar I; Hacking Web Servers; Integrity, Auditing, Forensics; PS(20-21); EH(10,B)
4/02	Hacking Web Servers; Integrity, Auditing, Forensics; PS(20-21); EH(10,B)
4/07	Servers returned for placement on PirateNet[©]; Cyberwar II; Hacking Wireless Networks; Intruders, Defense; PS(22-23); EH(11)
4/09	Hacking Wireless Networks; Intruders, Defense; PS(22-23); EH(11)
4/14	Cryptography; DoS, Crime, Trust; PS(24-26), EH(12)
4/16	Cryptography; DoS, Crime, Trust; PS(24-26), EH(12)
4/21	Protecting Networks with Security Devices; Misc.; PS(A-E), EH(13)
4/23	Protecting Networks with Security Devices; Misc.; PS(A-E), EH(13)
4/28	Penetration Testing; EH(C)
4/30	Penetration Testing; EH(C)
5/04-5/08	Wrap-up of Cyberwar II; Cleaning up computers; Final Reports

I reserve the right to modify the syllabus as we go along.

I occasionally have to travel during the semester. If this happens, I will either have a guest lecturer, deliver the class via video or reschedule any missed classes to a mutually convenient time.

I am hoping to bring in one or more speakers to talk on the subject of cybersecurity this semester. There will be more information on this subject during the semester.

There are no prelims or final in this course. However, you must finish up Cyberwar II and submit your final report during final exam week, which is the week of May 4-8.