Spring 2018

About the Instructor:

Andrew Szajlai (andrew.szajlai@temple.edu)
http://community.mis.temple.edu/mis5170sec001sec701sp2018/
Office hours: (by appointment)

Class Location and Time:

Alter 607 5:30 pm – 8:00 pm, Thursday

Course Description:

This course introduces students' to operating system security and tools to secure and audit it's operating systems. Methods of securing operating systems will be explored in theory and in hands on exercises. The course will require simple programming using operating system specific and Open Source scripting languages. For that reason some knowledge of and experience with computer programming is required. General operating system usability with Microsoft Windows and/or Linux is required.

Course Objectives:

In this course, you will gain an understanding of the processes and tools used to secure operating systems and audit their security.

The Key subject areas that are covered in the course are:

1. General overview of operating systems
2. How to secure operating systems
3. Open Source tools used to secure operating systems
4. Commercial alternatives to Open Source tools

In this course, we will focus on securing operating systems. The first part of the course will focus on processes used to secure the MS Windows operating system. The second part of

the course will apply those same techniques to the Linux[1] operating system. The course will discuss techniques and tools used to help reduce weaknesses in default installations/configurations of different operating systems.

Required Text and Readings:

The materials for this course are drawn from multiple sources. There is no required textbook for this course.

There are assigned readings throughout the course. These are available for free on the web. Each week there are assigned reading for the following weeks class, review and post questions to the class blog if there are issues with the any links or the topics. If required updates will be posted as needed if any errors are discovered.

Evaluation and Grading

Item	Weight
Participation (in class and online)	20%
Assignments (4)	30%
Tests (2)	50%

Scale			
94 – 100	A	73 – 76	C
90 – 93	A-	70 – 72	C-
87 – 89	B+	67 – 69	D+
83 – 86	B	63 – 66	D
80 – 82	B-	60 – 62	D-
77 – 79	C+	Below 60	F

Participation

Much of your learning will occur as you prepare for and participate in discussions about the course material. Much of securing operating systems is keeping current with news topics, findings of security researchers, and vendor bulletins to their products. The assignments, analysis, and readings have been carefully chosen to bring the real world into class discussion while also illustrating fundamental concepts.

To encourage participation, 20% of the course grade is earned through preparation before class, and participation during and between classes. Evaluation is based on a consistent demonstrated engagement with the process of learning. Assessments are based on what you contribute, not simply what you know.

1) **Participation between classes** – To facilitate learning the course material, we will also discuss course material on the class blog in between classes. Each week, I will post a

[1] Linux will be used in this text; however, will general apply to all Unix/Linus operating systems. Specific command and command syntax will vary based on the version of Unix/Linux installed on the computer.

discussion question or two on the class blog for the following week's topic. The question will relate to the assigned readings, a topic to be discussed in class, or a relevant current event. Reading and commenting on these analyses will contribute to the quality of our in-class discussions.

Every student is expected to contribute to the online class discussion at least four times each week. Online contributions will be graded on both the quality of your submissions and the overall quantity. Four substantive posts a week will be considered a B.

2) **Participation during class** – We will typically start each discussion with "opening" questions about the assigned readings and analysis. I may ask for volunteers, or I may call on you. Students called on to answer should be able to summarize the key issues, opportunities, and challenges in the case study. All students should be prepared to answer these questions.

   Another important aspect of in-class participation is completion of in-class assignments and contribution to break-out group activities.

   The criteria for class participation includes attendance, punctuality, level of preparation, professionalism, answering questions, discussing readings, discussing case studies, contributing to group activities, and contributing to a positive learning environment.

Assignments

You will officially prepare four assignment reports that are assigned during the semester. For each assignment students are to break into groups and work together to prepare a one to two-page report and a presentation of no more than four slides for presentation in the following class. Your analysis should not exceed one single-spaced page using 11 point Times New Roman font with one-inch margins. Do not prepare a separate cover page, instead put your name, the class section number (MIS5170.001), and the analysis in the top-left corner of the header.

The report should include what you did to secure the OS in clear steps. The reason is to be able to provide those steps to a helpdesk or other organizations to document the risk or mitigation.

To submit your analysis, you must post it on the class blog no later than **Wednesday at 8:00 AM** of the week it is due. Please copy your analysis in clear text onto the blog.

Late submissions for this deadline will result in no credit earned for this assignment.

There is no one particular style for a good documentation. But, there are some common elements to excellent submissions (additional, grade-specific criteria are provided at the end of this syllabus):

- The opening of the document makes it immediately clear which assignment and what question is being addressed.
- You have specific details regarding what you are correcting or doing to complete the assignment. Specific facts from the assignment instead of general observations about information technology that apply to any vulnerability. Specific details about what settings were before and after completing the steps will help the reader to validate that your findings apply to the problem.
- Based on your steps or your learning from the assignment how can you improve the overall process.
- Based on your findings, is there other mitigations that could protect the operating system? For example, are there other tools that could be deployed to protect the computer while the problem is solved?

Exams

There will be two tests for this course. Both tests will be comprised of short-answer and/or longer open-ended questions. Check the schedule for dates.

A missed test can only be made up in the case of documented and verifiable extreme emergency situations.

Group Project Report and Presentation

The individual and group projects are related. Your individual project will contribute to your team project effort. Therefore, coordination is required in choosing topics for both projects. A detailed description of the assignment will be posted to the class website.

Students may choose their own groups of about three members each. Because group work requires close coordination, I strongly recommend considering compatibility in availability (e.g., work and class schedules, work and home locations, and other constraints) before finalizing group membership.

Refer to the schedule for project deliverable dates.

Weekly Cycle

At outlined above in the **Participation** section, much of your learning will occur as you prepare for and participate in discussions about the course content. To facilitate learning the course material, we will discuss course material on the class blog in between classes. Each week this discussion will follow this cycle:

You: Read, view, etc. content for week (see course blog's Schedule menu)
Me: Post Questions (Friday am)
You: Respond to questions and read & respond to other's answers (thru Wednesday 11:59 pm). Note: Four substantive posts a week will be considered a B
Us: Class (Thursday)
Me: Post summary note (if any) (Wednesday)

Late Assignment Policy

An assignment is considered late if it is turned in after the assignment deadlines stated above. No late assignments will be accepted without penalty.

- The project management simulation and individual report will be assessed **a 20% penalty** each day they are late. No credit is given for assignments turned in over five calendar days past the due date.
- Case analyses cannot be submitted late under any circumstances. If you miss the deadline, you'll need to choose another case study to submit.
- You must submit all assignments, even if no credit is given. **If you skip an assignment, an additional 10 points will be subtracted from your final grade in the course.**
- Weekly write-ups cannot be turned in late. If you miss the deadline you will receive no credit for it, although the additional 10 point grade penalty does not apply here.
- Plan ahead and backup your work. ***Equipment failure is not an acceptable reason for turning in an assignment late.***

Classroom Etiquette

The environment you and your fellow students create in class directly impacts the value that is gained from the course. To that end, the following are my expectation of your conduct in this class:

- Arrive on time and stay until the end of class.
- Turn off cell phones, pagers and alarms while in class.
- Limit the use of electronic devices (e.g., laptop, tablet computer) to class-related usage such as taking notes. Restrict the use of an Internet connection (e.g., checking email, Internet browsing, sending instant messages) to before class, during class breaks, or after class.

- During class time speak to the entire class (or breakout group) and let each person "take their turn."
- Be fully present and remain present for the entirety of each class meeting.

Citation Guidelines

If you use text, figures, and data in reports that was created by others you must identify the source and clearly differentiate your work from the material that you are referencing. If you fail to do so you are plagiarizing. There are many different acceptable formats that you can use to cite the work of others (see some of the resources below). The formats are not as important as the intent. You must clearly show the reader what is your work and what is a reference to someone else's work.

Plagiarism and Academic Dishonesty

Plagiarism and academic dishonesty can take many forms. The most obvious is copying from another student's exam, but the following are also forms of this:

- Copying material directly, word-for-word, from a source (including the Internet)
- Using material from a source without a proper citation
- Turning in an assignment from a previous semester as if it were your own
- Having someone else complete your homework or project and submitting it as if it were your own
- Using material from another student's assignment in your own assignment

Plagiarism and cheating are serious offenses, and behavior like this will not be tolerated in this class. In cases of cheating, both parties will be held equally responsible, i.e. both the student who shares the work and the student who copies the work. Penalties for such actions are given at my discretion, and can range from a failing grade for the individual assignment, to a failing grade for the entire course, to expulsion from the program.

Student and Faculty Academic Rights and Responsibilities

The University has adopted a policy on Student and Faculty Academic Rights and Responsibilities (Policy # 03.70.02) which can be accessed through the following link: http://policies.temple.edu/getdoc.asp?policy_no=03.70.02

Disability Resources and Services

Temple University is committed to the inclusion of students with disabilities and provides accessible instruction, including accessible technology and instructional materials.

The process for requesting access and accommodations for this course is: (1) Advise me of the need to access or accommodations; (2) Contact Disability Resources and Services to request accommodations; (3) DRS will consult with me as needed about essential components of the program; (4) Present me with a DRS accommodation letter.

Grading Criteria

The following are the criteria used for evaluating assignments. You can roughly translate a letter grade as the midpoint in the scale (for example, an A- equates to a 91.5).

Criteria	Grade
The assignment consistently exceeds expectations. It demonstrates originality of thought and creativity throughout. Beyond completing all of the required elements, new concepts and ideas are detailed that transcend general discussions along similar topic areas. There are no mechanical, grammatical, or organization issues that detract from the ideas.	A- or A
The assignment consistently meets expectations. It contains all the information prescribed for the assignment and demonstrates a command of the subject matter. There is sufficient detail to cover the subject completely but not too much as to be distracting. There may be some procedural issues, such as grammar or organizational challenges, but these do not significantly detract from the intended assignment goals.	B-, B, B+
The assignment fails to consistently meet expectations. That is, the assignment is complete but contains problems that detract from the intended goals. These issues may be relating to content detail, be grammatical, or be a general lack of clarity. Other problems might include not fully following assignment directions.	C-, C, C+
The assignment constantly fails to meet expectations. It is incomplete or in some other way consistently fails to demonstrate a firm grasp of the assigned material.	Below C-

Readings

Week	Readings
1	• Hypervisor Installation Fusion: VMWare Fusion, VMWare Workstation, VMWare Player • Networking Overview: Cisco Server Farm Security • Data Center Design: Cisco Enterprise Data Center Topology • Physical Security: https://www.giac.org/paper/gsec/2892/computer-rooms-meet-physical-security-measures/104866 • Physical Security: https://www.sans.org/reading-room/whitepapers/physical/physical-security-important-37120, https://d0.awsstatic.com/whitepapers/aws-security-whitepaper.pdf

2	• PowerShell: Cheat Sheet, Overview Guide, PowerShell On-Line,Video Help with Jeffrey Snover On-LineMust View the Help section about PowerShell. ***Optional Reference Links*** PowerShell for Beginners • Python Tutorial: On-Line, ***Optional Reference book*** at NoStarchPress.com: Python Crash Course, Gray Hat Python, Black Hat Python • Microsoft Pash-the-Hash Mitigation: two-white papers (Mitigating Pass-the-Hash (PtH) Attacks and Other Credential Theft Techniques_English.pdf, Mitigating-Pass-the-Hash-Attacks-and-Other-Credential-Theft-Version-2.pdf) • Limit Services: On-Line • Windows ACLs: On-Line
3	• Windows 2008 Baseline: On-Line • Windows 7 Baseline: On-Line • CIS Windows 2008 Security Baseline: On-Line • CIS Windows 7 Security Baseline: On-Line • CIS security site: On-Line • Configuration Management Best Practices: On-Line Cisco, On-Line Wikipedia • Windows Hardening: On-Line • Windows Group Policy: On-Line • Security Detection: On-Line

4	• WSUS – Read the Get Started Section: On-Line
	• Open VAS Vulnerability Scanner: On-Line
	  ○ How to change the password of admin
	  ▪ openvasmd --user=admin --new-password=<password>
	  ▪ On-Line
	  ▪ Need to use Chrome; Safari does not work
	• Import .ova file into Fusion: On-Line
	• Import .ova file into Workstation: On-Line

5	• Paloalto Network: AppliPedia, Palo Alto Resources • WireShark Overview: You Tube Training • NetMon Download: On-Line • Microsoft Message Analyzer Operating Guide: On-Line • Microsoft Message Analyzer Download: On-Line • Microsoft Malicious Software Removal Tool: On-Line
6	• Microsoft Netsh commands for Windows Firewall: On-Line • Windows Firewall: On-Line • IPSec Primer: On-Line • IPSec Microsoft site: On-Line
7	• Event log: Windows Event Log, List of event ids • Regex: Web-Site Debugger, CheatSheet • Splunk: Splunk Documents On-Line
8	• Linux Security HOWTO: http://www.tldp.org/HOWTO/Security-HOWTO/index.html • Ubuntu Docs: On-Line Docs • Basic Unix basics: Basic Commands

9	Spring Break
10	
11	
12	
13	

Schedule

Week	Topic	Assignments
1 – Jan 18th	• Overview of Course • Computer Hardware Overview • Operating System Overview • Hypervisor Overview • Networking Overview • Physical Security Overview • Operating Systems Security Overview	Reading Week 1
2 – Jan 25th	• Hypervisors • Network Fundamentals • IPSec • TCP/IP and Network Architecture and its impact on Operating System Security • Assignment 1 Overview	Reading Week 2 Assignment 1 Start

3 – Feb 1st	• Scripting
	  • PowerShell
	  • Python
	• Appropriate permissions
	  • Access Control
	• Limit services
	• Shares
	  • Windows file shares / ACL
		Reading Week 3
		Quiz 1
		
		Assignment 1 Due Feb 8th

4 – Feb 8th	• Configuration management practices
	• System hardening
	• Windows Group Policies
	• Baselines
	  • Enabling Logging
	  • Baseline Standards
	• Intrusion detection
	  • Host based
	  • Network based
	• Intrusion prevention
	  • Host based
	  • Network based
	• Assignment 2 Overview
		Reading Week 4
		Start Assignment 2
		Quiz 2

5 – Feb 15th	• Patching	Reading Week 5

	• Native patching tools • Third-Party • Vulnerability scanning and remediation	Quiz 3 Assignment 2 Due Feb 22
6 – Feb 22nd	• Malware/Spyware • Detection tools • Native • Third-Party • Antivirus • Microsoft • Third-Party • Sniffers • NetMon • WireShark • Assignment 3 Overview	Reading Week 6 Start Assignment 3 Quiz 4
7 – Mar 1st	• Firewalls • Host based • IPSec • Network based • Review for 1st Test	Reading Week 7 Test 1 Assignment 3 Due Mar 8th
8 – Mar 8th	Spring Break	Have Fun
9 – Mar 15th	• Logging • Using Windows EventLog • Paid Products • Splunk • SEIM(s)	Reading Week 8 Assignment 3 Due Mar 9th
10 – Mar 22nd	• Unix/Linux basics • Scripting • bash basics • Python • Appropriate permissions • Access Control • Sudo & PAM • Limit services • Shares • NFS • Assignment 4 Overview	Reading Week 10 Start Assignment 4 Quiz 5
11 – Mar 29th	• Configuration management practices • Unix/Linux System hardening • Baselines • Enabling logging • /var/log/messages or /var/log/syslog • Baseline Standards	Reading Week 11 Assignment 4 Due Apr 5th Quiz 6

12 – Apr 5th	• Patching
	  • Native patching tools
	  • Third-party
	• Vulnerability scanning and remediation
		Reading Week 12

13 – Apr 12th	• Sniffers
	  • Snoop/tcpdump
	• Firewalls
	  • Host based
	  • iptables
	  • Network based
		Reading Week 13
		Quiz 7

14 – Apr 19th	• Network controls • Review findings from Pen-Testing Class	Quiz 8
15 – Apr 26th	• Review for 2nd Test • Questions	Test 2

Acknowledgements

This syllabus represents the collaborative efforts of MIS Department Professors Schuff, Weinberg, Yoo, Johnson and Mackey.