Course Information

CNS 418 910 - Host Based Security – Spring 2015
Meeting Time: Monday 5:45 PM – 9:00 PM
Meeting Location: CDM 216

Course Description

Principles of host based security. Review of security methods used to ensure the confidentiality, integrity, and availability of the information stored on a host. The class will cover OS configuration, access control, anti-malware, public facing application security, host-based intrusion detection/prevention, host-based firewalls and audit & compliance. Course includes laboratory work with both the Linux and Windows operating systems.

Instructor Information

Instructor: David Berg
Office: CDM 709
Office Hours: Monday 4:30 – 5:30 in CDM 709
Monday 45 minutes after class in CDM 216.
Other times by appointment.
Telephone: 630-999-3875
Email: dberg2@cdm.depaul.edu

Important Dates

April 10, 2015 – Last day to drop classes with no financial penalty. Last day to select pass/fail option.
May 15, 2015 – Last day to withdraw from Spring 2015 classes with financial penalty.
June 12, 2015 – Last day of the quarter. All assignments due.

Prerequisites

Basic knowledge of operating systems: CSC374 Computer Systems II or TDC311 Computers in Telecommunication Systems

Textbook

There is no required textbook – we will work from the web, Safari books, as well as class notes and presentations.

Course Objectives

At the conclusion of the course, students will be able to

1. Install and configure virtual Windows (desktop and server) and Linux hosts
2. Install, configure, and secure real world services on the aforementioned hosts
3. Configure group policy and delegate appropriate services to users
4. Configure secure access control
5. Implement file permissions, access control lists, and IPtables
6. Install and configure additional protective software
7. Assemble a host-based security policy and standard build documentation
8. Configure advanced security configurations of both hosts and services
9. Use common security tools to analyze real world problems
10. Display a deeper understanding of covered security principles through additional research, laboratory exercises, and HW

Agenda

DATE	TOPIC	ASSIGNMENT DUE
Week 1	Introduction - Syllabus Review Host Based Security General Principles & Security GUI vs CLI Virtualization	
Week 2	Windows & Windows Server	Virtualization Lab Networking HW
Week 3	Windows & Windows Server Cont.	Windows Lab 1 Security Baseline HW
Week 4	Linux	Windows Lab 2 Windows FW HW
Week 5	Linux Cont.	Linux Lab 1 Linux HW 1 Midterm
Week 6	Host Based IPS/IDS/Firewalls	Linux Lab 2 Linux HW 2
Week 7	Malware & Anti-Malware (Guest)	FW and Security Lab
Week 8	Cryptography & Encryption	Host Based Security Policy Exploit Research HW
Week 9	Internet Services, SSL/TLS, IPSec	Standard Build Documentation
Week 10	Security Tools & Penetration Testing	Presentation
Week 11		Security Project Paper

Grading

Grading is based on the manner in which you fulfill the objectives of this course. I will grade all your assignments on a percentage basis, which I will then convert to a letter. I will convert percentages to letters based on the following schedule:

A = 90% -100%,
B = 80% - 89%
C = 70% - 79%
D = 60% - 69%
F = 0% - 59%

The weights of each assignment for contributing to the final average are as follows:

Homework & Labs = 40%
Policies = 10%
Midterm = 10%
Presentation = 10%
Security Project = 20%
Paper = 10%

Homework & labs

Homework & labs will be due on the assigned date at 11:59 PM unless otherwise announced. Late homework will be penalized 10% per day after the due date.

Exploit Research

You will be required to research a current exploit related to the class and provide a one page write-up about the exploit, complete with references. Due date and late penalties are as with homework.

Policies

You will write two policies – one, the standard build documentation, will be a course long assignment that you will develop as you learn the how to build and secure your hosts. The second policy will be a host based security policy. Policies will be due as with homework with the same late penalties.

Presentation

There will be a single technology presentation due near the end of the course. This will be a presentation on a topic of your choosing that must be approved. This will involve researching and understanding outside sources and integrating them to present your topic. The presentation will be due as homework with the same late penalties.

Security Project

All students will use the techniques, tools, and security acumen learned throughout the course to install, configure, and secure services within. There will be no final exam. The Security Project will be due on the last day of the quarter, June 12, 2015, and will not be accepted late.

Paper

There will be a security paper due near the end of the course. This will be a paper on a topic of your choosing, which will involve reading outside sources and integrating them to present your topic. The paper will be due on the last day of the quarter, June 12, 2015, and will not be accepted late.

Attendance

I expect that you will attend every class; it is the single most important action you can take in mastering the course objectives. You are responsible for material covered, assignments delivered or received, and announcements made in class sessions or on D2L.

Class Cancellation

Unless DePaul University closes because of weather, we will have class.

Incompletes

Students must formally request an incomplete by filling out an Incomplete Grade Request Form.

Online Course Evaluation

Evaluations are a way for students to provide valuable feedback regarding their instructor and the course. Detailed feedback will enable the instructor to continuously tailor teaching methods and course content to meet the learning goals of the course and the academic needs of the students. They are a requirement of the course and are key to continue to provide you with the highest quality of teaching. The evaluations are anonymous; the instructor and administration do not track who entered what responses. A program is used to check if the student completed the evaluations, but the evaluation is completely separate from the student's identity. Since 100% participation is our goal, students are sent periodic reminders over three weeks. Students do not receive reminders once they complete the evaluation. Students complete the evaluation online in CampusConnect.

Academic Integrity & Plagiarism

This course will be subject to the university's academic integrity policy. I expect that you have read and understood this policy (http://academicintegrity.depaul.edu/). It is part of this syllabus; follow it.

Academic Policies

All students are required to manage their class schedules each term in accordance with the deadlines for enrolling and withdrawing as indicated in the University Academic Calendar. Information on enrollment, withdrawal, grading and incompletes can be found at http://www.cdm.depaul.edu/Current%20Students/Pages/PoliciesandProcedures.aspx.

Students with Disabilities

Students who feel they may need an accommodation based on the impact of a disability should contact the instructor privately to discuss their specific needs. All discussions will remain confidential.
To ensure that you receive the most appropriate accommodation based on your needs, contact the instructor as early as possible in the quarter (preferably within the first week of class), and make sure that you have contacted the Center for Students with Disabilities (CSD) at:
Lewis Center 1420, 25 East Jackson Blvd.
Phone number: (312)362-8002
Fax: (312)362-6544
TTY: (773)325.7296

Changes to Syllabus

This syllabus is subject to change as necessary to better meet the needs of the students. Significant changes are unlikely, and will be thoroughly addressed in class. Minor changes, especially to the weekly agenda, are possible at any time. If a change occurs, it will be thoroughly addressed during class, posted under Announcements in D2L and sent via email.