Course Information

CNS 418 710 - Host Based Security – Autumn 2018
Meeting Time: Monday 5:45 PM – 9:00 PM
Meeting Location: CDM 226

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 342 or Class - Other times by appointment
Office Hours: Monday 5– 5:40 in CDM 342
Monday 50 minutes after class in assigned classroom or text but I will be in the building.
Cell: 630-999-3875 – Call or Text
Email: dberg2@depaul.edu

Important Dates

September 11, 2018 – Last day to add (or swap) classes to AQ2018 schedule (11:59pm Deadline)
September 18, 2018 – Last day to drop with no penalty
September 18, 2018 – Last day to select pass/fail option
September 19, 2018 – Grades of "W" assigned for AQ2018 classes dropped on or after this day
September 25, 2018 – Last day to select auditor status
October 1, 2018 – DEADLINE: Application for November 2018 degree conferral
October 11, 2018 – Begin December Quarter/Graduate Intercession and Winter Quarter 2019 Registration
October 23, 2018 – Last day to withdraw from AQ 2018 classes
November 13, 2018 – End AQ2018 Day & Evening classes
November 14, 2018 – Begin AQ2018 Day & Evening Final Exams
November 19, 2018 – TUITION DUE: December Quarter/Graduate Intersession 2018
November 20, 2018 – End AQ2018 Day & Evening Final Exams and END AUTUMN QUARTER 2018
November 20 thru 25, 2018 – Thanksgiving Holiday - University officially closed
November 29, 2018 – AUTUMN 2018 GRADES DUE

Prerequisites

Basic knowledge of operating systems: CSC 374: Computer Systems II or TDC 311: Computers in Telecommunication Systems or IT 373: System Concepts

Textbook

There is no required textbook – we will work from free resources on 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 & WL1	Academic Integrity Pledge Networking HW
Week 3	Windows & Windows Server Cont. & WL2	Windows Lab 1
Week 4	Linux	Windows Lab 2
Week 5	Linux Cont. & LL1	Linux Lab 1
Week 6	Host Based Firewalls & FWL1	Midterm
Week 7	Flex Week	
Week 8	Host Based IPS/IDS	FW and Security Lab
Week 9	Malware & Anti-Malware (Guest?) Cryptography & Encryption	Exploit Research Presentation
Week 10	Security Tools & Penetration Testing	378/418 Policy HW 418 Policy HW 2
Week 11		Paper & Final Lab (November 20)

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. The only exception to that is that the final lab score which will have an additional effect on your overall class score by applying a coefficient to the overall grade. The better you do on the final lab the more the coefficient works to improve your overall class score, vice versa, if you perform poorly or do not do the final lab, it will have an additional negative effect on your overall class grade.

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 & Procedures = 10%
Midterm = 10%
Presentation = 10%
Research Paper = 10%
Final = 20%

Homework & labs

Homework & labs will be due on the assigned date at the start of class unless otherwise announced. Late homework and labs will not be accepted. Prepare accordingly. If D2L is down, assignments can be emailed to me before the due date and time.

Policies & Procedures

You will write two policies – The first will be a workstation patch management policy. The second policy will be a server patch management policy. Late submissions will not be accepted.

Midterm

The midterm format will be a multiple choice, short answer, fill-in-the-blank, and matching and will be given either during midterm week or the week after. There will be no makeup exams.

Exploit Research Presentation

You will be required to research an exploit or vulnerability related to the class and present a 5-minute presentation to the class. Additionally, you will submit a written review of 5 presentations from other students. Late submissions will not be accepted.

Research Paper

There will be a security research 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 and will not be accepted late.

Final Lab

All students will use the techniques, tools, and security acumen learned throughout the course to install, configure, and secure services within their lab environment. There will be no final exam. The Final Lab will be due on the last day of the quarter 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.