Cyber Breach Investigations

ITP 446x (3 Units)

USC Viterbi School of Engineering

Fall 2014

Objective

Upon completing this course, students will:

- Be able to acquire a live system, physically and through a network cable
- Be able to analyze Windows and Linux Servers
- Be able to analyze Web, SQL, Mail, and Application servers
- Be able to triage a network and isolate rogue, compromised systems

Concepts

This course is designed as an advanced course in computer forensics focusing on investigating computer and network breaches. The course assumes that students have either satisfied the prerequisite of ITP 375 – Digital Forensics, or instructor approval. Students will engage in forensic acquisition and analysis, focusing on large servers and enterprise systems. Investigations and cases will cover Windows & Linux servers, network devices, live and network-based acquisitions, and application server analysis. The course will also focus on large database server analysis for forensics. The course will also address network traces to identify source of breaches.

Prerequisites

ITP 375 or Department Approval
Recommended Preparation: ITP 357

Instructor	TBA
Contacting the Instructor	TBA
Office Hours	Listed on Blackboard under Contacts
Lab Assistants	Listed on Blackboard under Contacts
Lecture/Lab	3 hours/week, TBA

Required Textbooks

Mastering Windows Network Forensics and Investigations. Anson, Bunting. April 2007
ISBN: 0470097620

SQL Server Forensic Analysis. Fowler. December 2008
ISBN: 0321544366

Optional Textbooks

None

Website

All course material will be on Blackboard (http://blackboard.usc.edu).

Grading

The following percentage breakdown will be used in determining the grade for the course.

Lab Assignments	60%
Midterm	15%
Final	25%
Total	100%

Grading Scale

The following shows the grading scale to be used to determine the letter grade.

93% and above	A
90% - 92%	A-
87% - 89%	B+
83% - 86%	B
80% - 82%	B-
77% - 79%	C+
73% - 76%	C
70% - 72%	C-
67% - 69%	D+
64% - 66%	D
63% and below	F

Policies

No make-up exams (except for documented medical or family emergencies) will be offered nor will there be any changes made to the Final Exam schedule.

The labs will be posted on Blackboard under the "Assignments" section. Each lab will include instructions, a due date, and a link for electronic submission. Labs must be submitted using this link.

It is your responsibility to submit your assignments on or before the due date. Assignments turned in one day late will have 20% of the total points deducted from the graded score. Assignments turned in two days late will have 50% of the total points deducted from the graded score. After two days, submissions will not be accepted and you will receive a 0.

All assignments will be digitally submitted through Blackboard except where specified. Do not email them to the lecturer or lab assistant.

Incomplete and Missing Grades

Excerpts for this section have been taken from the University Grading Handbook, located at http://www.usc.edu/dept/ARR/grades/gradinghandbook/index.html. Please see the link for more details on this and any other grading concerns.

A grade of Missing Grade (MG) "should only be assigned in unique or unusual situations… for those cases in which a student does not complete work for the course before the semester ends. All missing grades must be resolved by the instructor through the Correction of Grade Process. One calendar year is allowed to resolve a MG. If an MG is not resolved [within] one year the grade is changed to [Unofficial Withdrawal] UW and will be calculated into the grade point average a zero grade points.

A grade of Incomplete (IN) "is assigned when work is no completed because of documented illness or other 'emergency' **occurring after the twelfth week** of the semester (or 12th week equivalency for any course scheduled for less than 15 weeks)."

Academic Integrity

USC seeks to maintain an optimal learning environment. General principles of academic honesty include the concept of respect for the intellectual property of others, the expectation that individual work will be submitted unless otherwise allowed by an instructor, and the obligations both to protect one's own academic work from misuse by others as well as to avoid using another's work as one's own. All students are expected to understand and abide by these principles. *Scampus,* the Student Guidebook, contains the Student Conduct Code in Section 11.00, while the recommended sanctions are located in Appendix A: http://www.usc.edu/dept/publications/SCAMPUS/gov/. Students will be referred to the Office of Student Judicial Affairs and Community Standards for further review, should there be any suspicion of academic dishonesty. The Review process can be found at: http://www.usc.edu/student-affairs/SJACS/.

Students with Disabilities

Any student requesting academic accommodations based on a disability is required to register with Disability Services and Programs (DSP) each semester. A letter of verification for approved accommodations can be obtained from DSP. Please be sure the letter is delivered to your course instructor (or TA) as early in the semester as possible. DSP is located in STU 301 and is open from 8:30am to 5:00pm, Monday through Friday. Website and contact information for DSP http://sait.usc.edu/academicsupport/centerprograms/dsp/home_index.html (213) 740-0776 (Phone), (213) 740-6948 (TDD only), (213) 740-8216 (FAX) ability@usc.edu

Emergency Preparedness/Course Continuity in a Crisis

In case of emergency, when travel to campus is difficult, if not impossible, USC executive leadership will announce a digital way for instructors to teach students in their residence halls or homes using a combination of the Blackboard LMS (Learning Management System), teleconferencing, and other technologies. Instructors should be prepared to assign students a "Plan B" project that can be completed 'at a distance.' For additional information about maintaining your classes in an emergency, please access: http://cst.usc.edu/services/emergencyprep.html

Course Title

ITP 446 (3 Units)

Course Outline

Note: Schedule subject to change

Week 1 – Digital Forensics Review

- Investigative process
- Analysis methodologies
- Tools and techniques
- File Systems

Reading

Mastering Windows Network Forensics and Investigations (MWNFI) Chapters 1 & 7

Week 2 – Networking Overview

- Introduction to networks & networking
- Introduction to network investigations
- Windows networks
- Users and groups

Reading

MWNFI Chapters 2, 5

Week 3 – Windows Servers

- Server roles
- Server analysis
- Windows registry
- Event Logs

Reading

MWNFI Chapters 9, 11, 12

Assignment/Lab

Windows Server Analysis

Week 4 – Understanding Windows Breaches

- Anatomy of a breach
- Common points of compromise
- Identifying compromised server systems
- Compromised Active Directory
- Windows Rootkits

Reading

Instructor Handouts

Assignment/Lab

Compromised Windows Server Analysis

Week 5 – IIS & Microsoft Exchange Server

- IIS server
- Exchange (mail) Server

Reading

MWNFI Chapters 13, 14, 15

Assignment/Lab

Compromised IIS Server

Week 6 – Introduction to SQL Server & Databases

- Introduction to databases
- Microsoft SQL server
- SQL server permissions and encryption

Reading

SQL Server Forensic Analysis(SSFA) Chapters 1, 2, 5

Assignment/Lab

Microsoft SQL Server Setup

Week 7 – Live SQL Server Acquisitions

- SQL server forensics vs. traditional windows forensics
- SQL server artifacts
- Resident vs. non-resident artifacts
- Remote SQL server acquisitions
- Logical collection of SQL databases

Reading

SSFA Chapters 3, 4, 6, 7

Assignment/Lab

SQL Server Acquisition

Week 8 – SQL Server Forensic Analysis

- Analysis database
- Importing evidence
- Activity reconstruction
- Data recovery
- SQL Server Rootkits

Reading

SSFA Chapters 8, 9, 10

Assignment/Lab

SQL Server Analysis

Week 9 – Midterm

Week 10 – Linux Forensics I

- Review of Linux file systems
- Review of Linux file structure
- Common Linux Server configurations
- Linux Artifacts

Reading

Instructor Handouts

Assignment/Lab

Linux Server Analysis

Week 11 – Linux Forensics II

- Apache server forensics
- LAMP forensics
- SMB and Linux file shares
- Syslog analysis

Reading

Instructor Handouts

Assignment/Lab

Syslog and other Linux log analysis

Week 12 – Network Forensics and Network Traffic Analysis

- Network addressing
- OSI review
- DNS poisoning
- ARP table analysis
- DHCP analysis
- Wireshark analysis

Reading

Instructor Handouts

Assignment/Lab

Wireshark analysis

Week 13 – Network Device Forensics I

- Introduction to managed switches and routers
- Network administrators and mindsets
- Diagraming physical networks
- Securing and isolating physical devices

Reading

Instructor Handouts

Week 14 – Network Device Forensics II

- Collecting volatile evidence from a router
- Collecting non-volatile evidence from a router

Reading

Instructor Handouts

Assignment/Lab

Cisco router forensics

Week 15 – Network Device Forensics III

- Collecting volatile evidence from a managed switch
- Collecting non-volatile evidence from a managed switch
- Intrusion detection (IDS) and intrusion prevention system (IPS) forensic analysis

Assignment/Lab

IDS analysis

Final Exam

To be held according to the final exam schedule on the Schedule of Classes