Course Syllabus

Instructor: Eric Rettke
Phone: 818 364-7775
email: rettkeeg@lamission.edu (36 hour response)

Fall 2016
Computer Science 411 - Principles of Cyber Security 1

Please keep a copy of the syllabus handy for the duration of the class. It contains key dates and will help you to know exactly what to do each week.

Texts:

1. Inside Out Windows Server 2012 R2 Services, Security and Infrastructure.
   ISBN 978-0-7356-8255-9 (Links to an external site.)
2. The Basics of Hacking and Penetration Testing.
   ISBN 978-0-12-411644-3 (Links to an external site.)

Required Computer System:

You will need a modern Intel i5 processor with 16 GB of RAM and at least 100 GB of free space and a high speed internet connection. You will get legal fully functional software versions of Windows Server 2012 R2, Windows 7 & 10 Enterprise Workstations. Most importantly you will get Kali Linux, the most advanced penetration testing platform available today.

Course Major Topics:

1. Be familiar with what hackers do on the attacking side of the Cyber game, the tools used to carry out attacks, and the underlying protocols used in order to do so.
2. Penetrate a built in layered defense architecture
3. Circumvent intrusion detection systems and firewalls
4. Gain access and dominate your target (lower case "t") system.
5. Case Study: Target (upper case "T") Stores recent data breach of 40 million credit cards and 70 million personal records.
   http://www.tripwire.com/state-of-security/vulnerability-management/targets-point-sale-system-compromised/ (Links to an external site.)

Course Description:

An introduction to the theory and practice of information security. The topics covered include Windows basics, Windows networking, accounts basics, threats, vulnerabilities, and

exploits, domain name servers (DNS), workgroups, domains, servers, access control, authentication and basic cryptography and design of system defensive strategies.

Student Learning Outcomes:

1. You will identify well known Window Services and demonstrate how to disable and/or enable them.
2. Use Microsoft Internet Explorer (IE) built-in security tools to lock down IE

Learning Components used in this course include:

1. Hands on practical labs to create your own virtual cyber range and launch attacks.
2. Discussion Forums - Each week begins with icebreaker discussions in which no ideas are too wild. Don't be afraid to comment. Expect posts that are both silly and truly inspired.
3. Quizzes - To nail down crucial terminology and basic security principles
4. Short research topic papers - to internalize the learning and understand the broader contexts.
5. Online weekly live CCConfer (like a Webex conference) Thursdays from 7-9 pm. in which you can ask your questions and get personal feedback that will be archived for reference throughout the course.

Grading:

- Lecture, textbook, and module quizzes (each week) 15%
- Discussion Forums 15%
- Assessments: Midterm and Final 45%
- Lab Assignments (each week) 25%

Letter Grade Assigned:

(A) 100-90% = Awesome
(B) 89-90% = Better
(C) 79-70% = "C"atisfactory
(D) 69-60% = Dunno
(F) 59 or less = For god's sake where were you?

Course Modules by Week:

Week 1: Introduction (Aug 28 - Sep 3)

1. Ethical Hacking within a security compliance program.
2. Your Virtual Box Cyber Range

3. Stick to your Cyber Range. Hacking is illegal
4. Hacking and Penetration Testing Methodology Made Easy
5. Online Assessment Exam

Week 2: Windows basics and features of Information Security (Sep 4 - 10)

1. Using Remote Desktop Management
2. Operating systems attacks
3. Exploiting specific network protocol implementations
4. Attacking built in authentication systems
5. Breaking file system security
6. Cracking passwords and weak encryption implementations

Week 3: Windows Networking infrastructure attacks (Sep 11 - Sep 17)

1. Networking with TCP/IP
2. Managing TCP/IP Networking
3. Connecting to a network through an unsecured wireless router attached behind a firewall
4. Exploiting weakness with too many requests, creating a denial of service (DoS) for legitimate requests.
5. Installing a network analyzer on a network and capturing every packet that travels across it, revealing confidential information in clear text.

Week 4: Account basics (Sep 18 - Oct 1)

1. Managing users, groups and computers in Active Directory
2. Unsecured files containing sensitive information are scattered throughout workstation and server shares, and database systems contain numerous vulnerabilities that malicious users can exploit.
3. Account permissions and privileges
4. Built in Windows user accounts

Week 5: Threats and Vulnerabilities (Oct 2 - 8)

1. Threats, vulnerabilities and exploits
2. Security risks
3. Hackers and attackers
4. Hacking Techniques

Week 6: Threats, Vulnerabilities and Patching (Oct 9 - 15)

1. Patching (threats, vulnerabilities, and exploits)
2. Unpatched systems
3. Patching methods
4. Microsoft Patch Process
5. Types of anti-virus software
6. Anti-virus update and installation

Week 7: DNS, Routing, Workgroups, and Domains (Oct 16 - 22)

1. Workgroups and Domains
2. Domain Controllers
3. Active Directory and Trusts
4. DNS
5. Basic routes and routing

Week 8: Services, DR and Shadow Copies (Oct 23 - 29)

1. Basic service components
2. Ports and service mappings
3. Services attack vector
4. Windows default services
5. Service checking tools
6. Backup and restore

Week 9: Authentication, Access Controls and Basic Cryptography (Oct 30 - Nov 5)

1. Strong password creation and management
2. Password cracking
3. Cryptography
4. File integrity

Week 10: Servers and File Servers (Nov 6 - 12)

1. Server types and roles
2. Multiple roles and vulnerabilities
3. Service configurations

Week 11: Locking Down Servers with Built-in Utilities and Add-on Utilities (Nov 13 - 19)

1. Networks and server placement
2. IDS/IDSP
3. Techniques for locking down servers

4. Utilities and add-ons for locking down servers

Week 12: Ethical Hacking Methodology (Nov 20 - 26)

Week 13: Hack Networks (Nov 27 - Dec 3)

Week 14: Penetration Testing (Dec 4 - 10)

Week 15: The Penetration Testing Report (Dec 11 - 17)

Week 16: Online Exam Final (Dec 15)

CSIT Lab Office Hours:

Wednesday 3 - 4 p.m.
or by appointment ----- call 818 364-7775
or by email – rettkeeg@lamission.edu
Thursdays 7-9 p.m. Weekly by CCConfer

DATES YOU NEED TO KNOW:

Aug 29	DAY AND EVENING CLASSES BEGIN
Sep 11	Deadline to add online
Sep 11	Drop Classes without Incurring Fees or with a Refund (by Internet only)
Nov 20	***Drop classes with a "W"*** – A letter grade is required after this date forward
Dec 11	Classes end
Dec 12	Final Exams Week
Dec 15	OUR CLASS FINAL

HOLIDAYS (College CLOSED)

Labor Day - September 5
Veteran's Day - November 11
Thanksgiving Day - November 24 and 25

Students with Disabilities:

Disabled Students Programs and Services (DSP&S) at Los Angeles Mission College is a support system that enables students to fully participate in the college's regular programs and activities. DSP&S provides a variety of services from academic and vocational support to assistance with Financial Aid. If you are a disabled student and need a modification, special assistance or accommodation in order to participate in this class, alert the instructor

promptly and contact the DSP&S office at 818 364-7732 or 818 364-7861. Modifications, special assistance or accommodations can only be made with proper documentation and coordination with DSP&S.

Standards of Student Conduct:

Students are expected to maintain a professional level of conduct to facilitate a learning environment. Use of profanity in class in not appropriate and will not be tolerated.

Cheating and Plagiarism:

The instructor reserves the right to determine if cheating or plagiarism has occurred; if it does the student will received a “F” on the assignment or exam, and may receive a “F” for the course. Please review the following document:
https://lamission.edu/library/docs/Plagiarism.pdf