95-856 Hacking Exposed
Master of Information System Management
Carnegie Mellon University
Fall 2007 (6 units)

Instructor Info:

Rohyt Belani
Cell: 646.244.4698
rohyt.belani@intrepidusgroup.com

Earl Crane
Cell: 949.637.8330
earlcrane@gmail.com

Abstract:

In the 1980’s, and 1990’s, “hacking” was as a fun and intellectually stimulating activity for the curious teenage prankster. Today, hacking has transformed into a mainstay of organized crime; financial gains are the primary objective of computer attacks. Thus, commercial and government entities are taking information security very seriously.

This course will expose students to the practical applications of information security concepts, thus preparing them for a career in the field. Students will conduct hands-on security assessments (hacking exercises) of wired and wireless networks, and web applications. The instructors will also highlight countermeasures that could have been applied to prevent the successful execution of such activities. In addition, real world attacks that the instructors have responded to will be presented as case-studies to put the knowledge in perspective.

The course is hands-on in all respects. Classroom and homework practical labs allow all students to perform the hands-on steps. The instructors will provide current assessment utilities. Bring Your Own Laptop (BYOL)

Goals:

• Provide a strong base in practical information security concepts
• Learn to apply fundamental security principles to real world applications
• Gain hands-on experience in the methodologies and techniques currently used to assess the security of wired and wireless networks, and web applications.
• Learn how to validate security implementations
• Learn unique critical thinking skills

Requirements:

• Intellectual curiosity
• Laptop with Windows XP, 2000 (Macs/Linux acceptable if students feel comfortable in the command line environment – no support will be provided) and the latest Java Runtime Environment (JRE)
• Laptops with Vista are not fully supported and not recommended.
• Ethernet connectivity with BOTH Ethernet Cable and 802.11b/g wireless capability.

The course website is available through your blackboard homepage.

Evaluation:
Grades will be based on homework assignments (25%), a final project (50%), and class participation/in-class exercises (25%).

Due to the compressed nature of this course, attendance is mandatory at all sessions. Students that miss classes will not be given credit for the course. Be on time for all classes!

The assignment is a practical review of the material presented in class. Students will conduct a security assessment of a live web application (created for training purposes).

Class participation is based on timely attendance and completion of daily in class assignments.

The final group project summarizes the learning objectives of the course. Students will create a tool to automate or enhance some portion of the assessment process, or produce a research paper on an approved topic. Results will be presented to the class during the final session.

Grades:
A = 90-100%
B = 80-90%
C = 70-80%
F = below 70%

Course Schedule: (Hamburg Hall, 1000)
September 22-23
October 6-7
October 20-21

Session 1 (Network Security)
10:00 AM – 3:00 PM (Five Hours)
Overview of Course
Review of Basic Security Principles
Introduction to Network Assessments
Network Assessment Methodology
Publicly available information
Network Discovery
  - WHOIS, ARIN
  - DNS server information
Host Discovery
Service Discovery
Host enumeration
Service enumeration
Multi-protocol network mapping

Session 2 (Network Security)
10:00 AM – 3:00 PM (Five Hours)
Access Path Enumeration
- ICMP, UDP, TCP scans
- Using TTLs
- Interpreting firewall response
Vulnerability Scanning
- Vulnerability Identification
- Exploiting Vulnerabilities
- Establishing back channels
- Remote access techniques and network sniffing

Session 3 (Web Application Security)
10:00 AM – 3:00 PM (Five Hours)
Introduction to Web Application Security
Tools of the Trade
Application Assessment Methodology
Web Server Assessment
Application Discovery
OWASP Top Ten
SQL Injection
Cross Site Scripting

Session 4 (Web Application Security)
10:00 AM – 3:00 PM (Five Hours)
Session Management
Cookie Manipulation
Parameter Tampering
Cross Site Request Forgery
Introduction to Wireless Technologies
Detecting Wireless Networks
- Cloaked v/s Broadcasting
Wireless Network Enumeration
Detecting Rogue Access Points

Session 5 (Wireless Security)
10:00 AM – 3:00 PM (Five Hours)
Mapping Wireless Networks
Cracking WEP
Wireless Man-In-The-Middle Attack
Sniffing Wireless Traffic
Real World Attacks
- Browser Attacks
- Zero Day Exploits
- Wireless Attacks
Session 6
10:00 AM – 3:00 PM (Final Presentations)
Students will present the results of their final project to the class.

Textbook:
There is no textbook for this course.

Reference Text:
Hacking Exposed: Web Applications 2 by Joel Scambray, Mike Shema, Caleb Sima