CS 4740 – Security Vulnerabilities and Attack Prevention

Instructor: Leon Trappett

Phone: (801) 695-7575

Email: ltrappett@bankofutah.com

Office Hours: Times available by appointment


ISBN: 978-0071832380

Course Objectives: A treatment of security issues related to computers and computer networking. This course is designed for advanced users, system administrators and network administrators. The course covers TCP/IP security issues, security policies, packet filtering, Internet firewall architecture and theory, detecting and monitoring unauthorized activity, password authentication, intrusion detection and prevention and other security issues involving Linux, UNIX and Microsoft Windows operating systems. A team project is included.

Prerequisite: MATH 1040 or MATH 1220 or MATH 3410, ENGL 3100 or NTM 3250, CS 3100 and CS 3705.

Students with Disabilities: Students who have special needs or disabilities that may affect their ability to access information and/or material presented in this course are encouraged to contact Lee Ellen Stevens, Director of Disability Support Services (DSS), immediately, on campus at 957-4529 for additional disability-related educational accommodations. You are not required to disclose these disabilities to your instructor, but the instructor can only accommodate accommodation requests that officially come through the DSS.

Allocated Time: You should anticipate spending two to three hours of study per week for each credit hour of a university course. Computer and programming classes typically require time in the upper range.

Grading:

Projects and/or Assignments 60%

Midterm Exam / CTF 15%

Final Exam / CTF 15%

Participation / Attendance 10%
**In-Class Projects / Homework:** In-Class Projects and Homework assignments will generally be assigned on Mondays, and will be due the following Monday. These in-class projects / homework will require the use of software to run virtual machines. In class we will be utilizing VMWare. To accomplish the projects and homework at least 2 virtual machines should be able to run in parallel including your host operating system.

**Letter Grades:**

A  94 <= Total
A- 90 <= Total < 94%
B+ 87 <= Total < 90%
B 84 <= Total < 87%
B- 80 <= Total < 84%
C+ 77 <= Total < 80%
C 74 <= Total < 77%
C- 70 <= Total < 74%
D+ 67 <= Total < 70%
D 64 <= Total < 67%
D- 60 <= Total < 64%
F Total < 60%

**Projects and/or Assignments (tentative list):**

Install / Setup / Configure VMPlayer verify Images (Week 1 - January 12)

Introduction to Kali Linux  (Week 1 - January 12)

No School - Martin Luther King Jr. Day (January 19)

Metasploit and Metasploitable (Week 2 - January 21)

Programming Survival Skills (Chapter 2 - Week 3 - January 26)
Fuzzing (Chapter 5 - Week 3 - January 26)

Shellcode Strategies / Writing Linux Shellcode (Chapter 6,7 - Week 4 - February 2)

Basic Linux Exploits (Chapter 10 - Week 4 - February 2)

Windows Exploits (Chapter 12 - Week 5 - February 9)

No School (Week 6 - February 16)

Mid-Term (February 18)

Introduction and Use of Volatility (Week 7 - February 23)

Exploiting the Windows Access Control Model (Chapter 14 - Week 8 - March 2)

SPRING BREAK March 9 and March 11

Exploiting Web Applications (Chapter 15 - Week 10 - March 16)

Exploiting IE - Smashing the Heap / Use-after-Free Technique (Chapter 16,17 - Week 11 - March 23)

Social Engineering - (Week 12 - March 30)

Client-Side Attacks and Vulnerabilities (Week 12 - March 30)

Volatility and Malware Analysis - (Week 13 - April 6)

Log Analysis for Intrusion Detection - (Week 14 - April 13)

Penetration Test / Lab - (Week 15 - April 20)

April 27 - Final Exam