Course: CS 361S | Network Security and Privacy  
Syllabus – Fall 2016

Time/Location: Mondays & Wednesdays 2:00 – 3:30pm @ BUR 108
Instructors: Cam Beasley | Charlie Scott | UT Austin Information Security Office

Description:
This course will provide students hands-on experience in how vulnerable systems and applications can be attacked and compromised in a real-world setting. Additionally, this course will provide students with an opportunity to understand practical applied techniques used to setup and defend systems and applications located in dangerous or exposed networks. Members of the UT Information Security Office will instruct this course and mentor students through each project.

Prerequisites:
You are expected to have taken and passed the following courses (or equivalent) with a grade of at least C-: Computer Science 439. If you don't have the prerequisites, be sure to clear it with the CS department or risk being dropped from the class.

You are also expected to have a basic level of knowledge of computer networking (e.g., network segmentation, IP addressing, DNS, etc.) and the Linux operating system (e.g. be able to navigate the file system and execute programs from the command line). These basic topics will not be covered in class, so if you do not know them, you will be required to learn them on your own.

Required Text: None

Supplemental Reading:
- The Elements of Style
- The Chicago Manual of Style Online
- Smashing the Stack for Fun and Profit (Slides, Update for new gcc)
- OWASP Top 10
- Nmap Online Manual
- Metasploit Unleashed
- RTFM
- Cisco Certified Entry Networking Technician Essential Training
- LI Guide to Lockpicking

Topics to be covered will include:
- Security Principles and Ethics
- Intrusion Detection
- Secure Development Practices
- Reconnaissance Techniques
- Penetration Testing of Systems and Applications
- Communicating Findings in an Effective Manner

Objectives:
At the completion of the course, you will be able to:
- Perform reconnaissance to target vulnerabilities
- Identify and exploit vulnerabilities based on reconnaissance
- Successfully perform a focused attack on a vulnerable system
- Successfully perform a focused attack on a vulnerable application
- Effectively communicate your security-related findings

Page 1 of 4
Projects:

- For each Capture-the-Flag (CTF) project, students will work in a randomly selected team of 3, set at the start of the course. Teams can’t be changed except on request with cause.
- Students will be required to identify and exploit various forms of vulnerabilities and then indicate how the vulnerabilities would be most effectively remediated.
- CTF progress will be tracked in real-time via scoreboard.
- A technical paper detailing these findings and remediation actions will be required from each team for every project.
- Each student will be required to submit a confidential peer evaluation, rating each team member’s individual contribution to the overall team, at the conclusion of each project.

Week 1: Introduction
[W 8/24]: Overview, Ethics and Ground Rules
   Cam

Week 2: Ground Rules & Preparing for a Security Assessment
[M 8/29]: Setting up your hacking rig | What is a CTF? | Writing an Actionable Report
   Tools: Kali (network setup)
   Justin

   MiniCTF Walkthrough with Sample Report (Screencast)
   Charlie

   [W 8/31]: Network Scanning & Reconnaissance
   Tools: nc, nmap, zmap, ARIN, DNS, RADB
   James

Week 3: Network Security
[M 9/05]: LABOR DAY
[W 9/07]: Layer 2 & 3 Attacks | Firewall Evasion
   Tools: Wireshark, Ettercap, SSH (proxies)
   Charlie

PROJECT 1: Bacon Pancakes CTF (Starts: W 9/07; Report due: M 9/19)

Week 4: Network & System Security
[M 9/12]: Firewalls | Network Segmentation | 802.1x
   Tools: iptables, Snort, network taps
   Kelly

   [W 9/14]: Scanning for Vulnerabilities
   Tools: nmap (with NSEs), Rapid7 Nexpose (student edition)
   Lindsay

Week 5: System Security
[M 9/19]: Introduction to Metasploit
   Tools: Metasploit
   Charlie or HD

   [W 9/21]: Advanced usage of Metasploit
   Tools: Metasploit (pivoting)
   Charlie or HD
Course: CS 361S | Network Security and Privacy  
Syllabus – Fall 2016

Week 6: System Security
[M 9/26]: Shells | Meterpreter
  Tools: nc, Metasploit, Meterpreter
  Jason R.
[W 9/28]: System Configuration Reconnaissance | Password Attacks
  Tools: JtR, hashcat, Metasploit (mimikatz)
  Jason R.

PROJECT 2: Sysmis CTF (Starts: W 9/28; Report due: M 10/10)

Week 7: System Security
[M 10/03]: Advanced Password Attacks (Rainbow tables, pass the hash, etc.)
  Tools: JtR, hashcat, Metasploit (modules)
  Jason R.
[W 10/05]: Log Analysis & Intrusion Detection
  Cam

Week 8: Web Application Security
[M 10/10]: Introduction to Burp and HTTP proxies
  Tools: Burp
  Justin
[W 10/12]: XSS | CSRF | Direct Object References | Session & Authorization Attacks
  Tools: Burp
  Justin

Week 9: Web Application Security
[M 10/17]: Injection Attacks | SQLi
  Tools: sqlmap, Burp
  Bryan
[W 10/19]: LFI | RFI | Insecure Uploads
  Bryan

PROJECT 3: Parchment CTF (Starts: W 10/10; Report due: M 10/31)

Week 10: Web Application Security
[M 10/24]: Secure Architecture
  Sean
[W 10/26]: Secure Applications
  Sean

Week 11: Application Security
[M 10/31]: GDB & Objdump (RE Malware)
  Daryl
[W 11/02]: GDB & Objdump (RE Malware)
  Daryl

Week 12: Application Security
[M 11/07]: Fuzzing | Finding Privileged Programs
  Ben
  Jgor
Course: CS 361S | Network Security and Privacy
Syllabus – Fall 2016

Week 13: Application Security
[M 11/14]: Binary Exploitation, cont.
   jgor
[W 11/16]: Binary Exploitation, cont.
   jgor

PROJECT 4: Digimodo CTF (Starts: W 11/16; Report due: F 12/05)

Week 14: Application Security
[M 11/21]: Stack Smashing Prevention
   Ben

THANKSGIVING BREAK (11/23 - 11/26)

Week 15: Physical Security
[M 11/28]: Lockpicking
   Bryan
[W 11/30]: Electronic & Biometric Locks
   Bryan

Week 16:
[M 12/05]: Facets of Information Security | CSAW | CCDC
   Cam

LAST DAY OF CLASSES (12/05)

NOTE: Lecture topics may change as course evolves

Grading Criteria:
   Project 1 (20% of final grade; 30% CTF, 50% report, 20% peer evaluation)
   Project 2 (25% of final grade; 30% CTF, 50% report, 20% peer evaluation)
   Project 3 (25% of final grade; 30% CTF, 50% report, 20% peer evaluation)
   Project 4 (30% of final grade; 30% CTF, 50% report, 20% peer evaluation)

Academic Dishonesty:
   • Evidence of working with other teams or cheating will result in a zero for all associated team members