Student Syllabus
CS 332
Ethical Hacking
Spring 2017

Instructor: Vince Skinner, CISSP, CISM, CISA, MCSE
Class Meeting Time: 4:30PM-7:15 PM and 7:30PM-10:15 PM every Wednesday
Class Location: City Center Plaza Rm 260
Contact Info: vinceskinner@gmail.com, vincentskinner@boisestate.edu
Phone #: 208-830-4492

Course Description:

CS 332 covers the study of the fundamental hacking techniques. Topics include information gathering, target enumeration, network sniffing, vulnerability assessment, remote exploitation, social engineering, and web hacking.

Course objectives CS 332:

Upon successful completion of this course, the student will be able to:

- Understand Ethical Hacking for today's organizations.
- Explain the mythologies of Ethical Hacking
- Understand the importance of programming and networks to ethical hacking
- Understand the differences between white hat, grey hat, and black hat hackers.
- Understand the tools and processes to have an affective ethical hacking practice

Prerequisites:

CS 331, or ITM 225 and ITM 455.

Student Textbook

Primary Text
Hands-On Ethical Hacking and Network Defense 2nd Edition
ISBN-13: 978-1435486096
ISBN-10: 1435486099

Instructor Notes:

- Be prepared for lab and class. (paper, pen, book, etc)
- If you miss a class, get the homework from a classmate or instructor.
- 80% of life (school) is showing up.
- The Midterm & Final Exams will be based upon: in-class discussion, textbook reading, textbook questions and other materials.
- **Late Work Policy**: Late work will be accepted but with severe penalties, unless prior notification is given prior to absence.
    - The ultimate success of a student depends upon his/her timely completion of course work as well as the resulting feedback.
    - Students are responsible for their course work.
    - Course work turned in late detracts from the learning environment because every class session builds upon a previous session.
    - Course work not completed on time impacts student preparation for the next set of objectives.
- Create Backup copies of your homework.
- Send homework to your instructor via email in this format "Class.Week.Lab/homework.doc"
    - Example – CS332.week1.lab.doc or CS332.week1.homework.doc
- No excuses, I'm training you for the workplace.
- First Assignment is to send the instructor an email stating:

- Subject: BSU Student Info - <Student Name>
- Your Name:
- Class Number/Name
- Email Address:
- Acknowledgment and Understanding of this Syllabus
- My Primary phone# is:

Category Weights:

Final Grades will be calculated from the percentages earned in class as follows:

Participation	**10%**
Homework Assignments	**10%**
Labs	**25%**
Project–Client-Side	**15%**
Project–Server-Side	**15%**
Final Exam	**25%**

A	90-100%	4.0
B+	85-89%	3.5
B	80-84%	3.0
C+	75-79%	2.5
C	70-74%	2.0
D+	65-69%	1.5
D	60-64%	1.0
F	<59%	0.0

No.	Date	Read / Topic – This schedule is subject to change.
1	1/11	**Introduction to Ethical Hacking** **Read Chapter 1 – Ethical Hacking Overview** **Research Assignment** – Technical Research Paper on Ethical Hacking(Whitehat hacking, Penetration Testing, etc) services. Describe the breadth and their specialties. **Lab** – Learn to update/utilize Kali, Metasploit, SET, etc. Download and install Nessus personal. **Project Overviews** Create a paper outlining the methods of penetration testing and Present the findings at the end of the semester. Server Side Client Side Physical and/or combo of server/client side
2	1/18	**Research Assignment** – Technical Research Paper on the most utilized and effective ethical/penetration attacks today. **Lab** – Demonstrate simple serverside, clientside and physical attacks.
3	1/25	**Read Chapter 2 – TCP/IP Concepts Review** **Research Assignment** – Technical Research Paper on how TCP/IP can be utilized by **a penetration tester** to help them be more affective. **Lab** – Utilize zenmap/nmap to scan a network utilizing CIDR notation. Utilize the various flags/switches to scan/output different information.
4	2/1	**Read Chapter 3 – Network and Computer Attacks** **Research Assignment** – Building on Week 2's assignment, write a technical research paper on the specifics of the various payloads and attacks that are perpetrated by malicious actors. **Lab** – Overview of malicious payloads and other persistent methods. Overview of DDOS conditions and Physical Security Attacks
5	2/8	**Read Chapter 4 – Footprinting and Social Engineering** **Research Assignment** – Technical paper on the processes and tools that you would employ to conduct recon and socially engineer an organization. **Lab** – Find and document the online tools to build a profile of an organization.

6	2/15	**Read Chapter 5 – Port Scanning** **Research Assignment** – Technical Research Paper on the tools and techniques to port scan an external host and what the differences would be when port scanning an internal network. **Lab** – Find a tool/script that would portscan, report-on and give visuals of any websites/portals that are found and then run it against sample hosts.
7	2/22	**Read Chapter 6 - Enumeration** **Research Assignment** – Write a technical research paper on the automated scripts and tools that you would utilize to enumerate an organization. **Lab –** Download, Install and configure and run Nessus against internal targets. Utilize netbios tools to enumerate targets on the internal
8	3/1	**Read Chapter 7 – Programming for Security Professionals** **Research Assignment** – Write a technical research paper on which programming tools that you would utilize most in conducting penetration tests; demonstrate the languages that correspond with the tools. **Lab** – Find ten of the most popular/useful security hacking tools where the sourcecode is freely available.
9	3/8	**Read Chapter 8 – Desktop and Server OS Vulnerabilities** **Research Assignment** – Write a technical research paper on the worst software(operating system and application) vulnerabilities. Give details regarding the exploit and the reason why the vuln is bad(Impact) **Lab** – Overview and examples of some of the worst most impactful vulnerabilities and corresponding exploits.
10	3/15	**Read Chapter 9 – Embedded Operating Systems: The hidden threat** **Research Assignment** – Write a technical research paper on the advantages and disadvantages of Embedded OS's when it comes to security of the device. **Lab** – Analyze the vulnerabilities with an Embedded OS.
11	3/22	Spring Break – No Class
12	3/29	**Read Chapter 10 – Hacking Web Servers** **Research Assignment** – Write a technical research paper on the current most impactful methods that webservers are exploited/breached. **Lab** – Utilize web server hacking tools and test the various exploits and vulnerabilities shown in webservers.

13	4/5	**Read Chapter 11 – Hacking Wireless Networks** **Research Assignment** – Write a technical research paper on the ways that wireless networks are vulnerable and exploited; what is a scenario that could exist to impact an organization. **Lab** – Test the various wireless hacking tools to exploit wireless networks.
14	4/12	**Read Chapter 12 – Cryptography** **Research Assignment** – Write a technical research paper on penetration testers and blackhat hackers utilize encryption to make impacts on organizations. **Lab** – Collaborate and create a process that could be utilized by a hacker to utilize encryption or obfuscation to exfiltrate data.
15	4/19	**Read Chapter 13 – Network Protection Systems** **Research Assignment** – Write a technical research paper on the best methods that a hacker would utilize to bypass today's network and host based protections. **Lab** – Collaborate and create a process and the tools that could be utilized by a hacker to bypass protective/detective/preventative systems.
16	4/26	Presentations and Semester Projects due
17	5/3	Final Exam

Notice of Policy on Scholastic Dishonesty

The following statement is the university's policy on academic honesty. It applies to conduct in this class:

> The university's goal is to foster an intellectual atmosphere that produces educated, literate people. Because cheating and plagiarism are at odds with that goal, they shall not be tolerated in any form. Students are expected to adhere to the rules and regulations as set forth in the Student Code of Conduct. Therefore, all work submitted by a student must represent that student's own ideas and effort; when the work does not, the student has engaged in academic dishonesty.
>
> Plagiarism occurs when a person passes in another person's work as his or her own or borrows directly from another person's work without proper documentation. For example, academic dishonesty occurs whenever a student:
>
> - Buys a paper or other project, then seeks to receive credit for the paper or project
> - Copies from another student's exam, either before, during, or after the exam
> - Uses "crib notes" while taking an exam or uses information stored in a computer or calculator (if prohibited from doing so)
> - Allows another person to take an exam in his or her place or takes an exam for another person
> - Collaborates on take-home exams when such collaboration is forbidden
> - Copies the work of another person and attempts to receive credit for that work
> - Fails to properly document source material in a paper or project
> - Receives editorial assistance that falls outside the scope of acceptable assistance
>
> NOTE: The list above is intended only to provide general guidelines for recognizing and avoiding common types of academic dishonesty. It is in no way an exhaustive or comprehensive list of all the types of academic dishonesty.
>
> Except in cases of major offenses, responding to academic dishonesty is the responsibility of the instructor of the course in which the dishonesty occurs. If a student is responsible of academic dishonesty, the student may be dismissed from the class and may receive a failing grade. Other penalties may include suspension or expulsion from school.

Incidents involving academic dishonesty will be addressed on an individual basis and forwarded with documentation to the appropriate administrative office within the parameters provided through Boise State policy and procedures. Please note that this means a student must clearly distinguish between content that represents their own thought/analysis and written material that is drawn, either completely or paraphrased, from the work of another.