CSST 4372 Intrustion Detection/Prevention Systems

Sul Ross State University

Instructor: Thea Glenn

Office Location: MAB 109-B

Office Phone: 432-837- 8490

Text: 931-237-3324 (No text after 11pm or before 10am)

Email: tglenn2@sulross.edu

Office Hours:

Mon & Wed 8:00-9:00 1:00-2:30 pm

Class*: Online*

Computer Science SLOs

- Understand modern computer systems, databases, and networking.

Required Materials:

- Oriyano, Sean-Philip. *Hacker Techniques, Tools, and Incident Handling*, Third Edition, Burlington, MA: Jones & Bartlett, 2020
- Virtual Security Cloud Labs*
- Student Lab Manual (available within the virtual lab environment)*

* These resources are available if your educational institution purchased the Jones & Bartlett Learning lab manuals along with the courseware.

Recommended Resources

The following series of tables provide sources of supplementary information to augment your learning in digital forensics. You may consult as many resources as you wish.

Web References: Links to Web references in this document and related materials are subject to change without prior notice. These links were last verified on July 1, 2018.

Books

Title	Author(s)	Year	ISBN
Advanced Penetration Testing: Hacking the World's Most Secure Networks	Wil Allsopp	2017	978-1119367680
Hacking Exposed 7: Network Security Secrets & Solutions (Hacking Exposed: Network Security Secrets & Solutions)	Stuart McClure, et al.	2012	978-0071780285
The Hacker Playbook: Practical Guide To Penetration Testing	Peter Kim	2018	978-1980901754
Rtfm: Red Team Field Manual	Ben Clark	2014	978-1494295509

Certification Bodies and Certifications

Organization/Certification(s)	URL
EC-Council Certified Ethical Hacker (CEH), Licensed Penetration Tester (LPT), more	https://www.eccouncil.org/programs/
SANS Institute Global Information Assurance Certification (GIAC) GIAC Penetration Tester (GPEN),GIAC Certified Incident Handler (GCIH), more	https://www.giac.org/certifications/categories

Virtual Labs

Student Lab Manual (may be available in hard copy or within the virtual lab environment**)**

Recommended Resources

Use the following author's names, book/article titles, Web sites, and/or keywords to search for supplementary information to augment your learning in this subject.

Journals/Magazines

Title	URL
Hakin9: IT Security Magazine	http://hakin9.org/
2600 Magazine	https://www.2600.com/

Other References

Organization	URL
Black Hat	https://www.blackhat.com/
HackerOne	https://www.hackerone.com/

Organization	URL
Insecure.org	http://insecure.org/
SANS Internet Storm Center	http://isc.sans.edu/index.html
Security Intelligence	https://securityintelligence.com

Course Description

This course is an introduction to hacking tools, techniques, and incident handling. Areas of instruction include an evolution of hacking and penetration testing; the basics of cryptology for information security; footprinting; vulnerability scanning and exploit; wireless, web, and database attacks; malware and system exploit; traffic analysis; incident response; and defensive technologies and controls. In this course, students will learn how to discover vulnerabilities, how to attack and defend systems, how to respond to attacks, and how to identify and design controls to prevent future attacks.

Major Instructional Areas

1. Evolution of computer hacking
2. The role of information security professionals
3. Hacking tools and techniques
4. Vulnerabilities exploited by hackers
5. Incident response
6. Defensive technologies

Course Objectives

1. Explain the history and current state of hacking and penetration testing, including ethical and legal implications.
2. Identify basic equipment controls, physical area controls, and facility controls.
3. Identify common information-gathering tools and techniques.
4. Analyze how hackers use port scanning and fingerprinting.
5. Analyze how enumeration is used in conjunction with system hacking.
6. Analyze wireless network vulnerabilities exploited by hackers.
7. Perform Web and database attacks.
8. Identify and remove common types of malware from infected systems.
9. Identify Trojans, backdoors, and covert communication methods.
10. Perform network traffic analysis and sniffing by using appropriate tools.
11. Perform incident handling by using appropriate methods.

12. Compare and contrast defensive technologies.
13. Identify methods that attackers use to obtain unauthorized access.
14. Describe methods that attackers use to alter systems and cover their tracks.

Attendance:
Attendance Policy: Students are expected to attend every class. If class must be missed, the student is expected to get the notes from a classmate, and to check with me or on Blackboard for announcements and updated assignments.

Students are expected to arrive to class on time. If a student is perpetually late, they will be asked to not attend class unless they can arrive on time. If tardiness becomes a problem for the class as a whole, people who arrive late will not be permitted to enter the class. If this stricter policy becomes necessary, there will be an announcement made in class.

It is policy of the university to drop a student with a grade of \F" if 9 hours or more of class are missed. For this course that would be 9 or more class sessions missed. For online courses student must log into blackboard with in 3 weeks or will be withdrawn from the course with the grade of an "F"

Need for Assistance
Qualified students with disabilities needing academic or other accommodations to ensure full participation in the programs, services and activities at Sul Ross State University should contact the Disabilities Services Coordinator, in Counseling and Prevention Services, Ferguson Hall 112, Box C-117, Alpine, Texas 79832. Please notify me before the third day of classes.

Course Polices
Contact your professor if it becomes difficult to keep up in class due to life issues. I will post 2 weeks before the end of class the last day I will accept assignments. The sooner you turn it in the faster I can grade it. If you know you can improve your grade that is up to you to resolve. I do not give extra credit.

Academic Dishonesty: Honesty in completing assignments is essential to the mission of the university and to the development of the personal integrity of the student. Cheating, plagiarism, or other kinds of academic dishonesty will not be tolerated and will result in appropriate sanctions that may include failing an assignment, failing the class, or being suspended or expelled. Suspected cases in this course may be reported to Student Life.

Posting of Grades
As soon as assignments, exams, and quizzes are graded, the grades will be posted in Blackboard.

Learning Materials and References

Information Search

Use the following keywords to search for additional online resources that may be used for supporting your work on the course assignments:

- **Asymmetric encryption**
- **Cryptanalysis**
- **Cryptographic system**
- **Cryptographic technologies**
- **Cryptographic tools**
- **Data-gathering techniques**
- **Encryption**
- **Enumeration**
- **Ethical hacking**
- **Ethical laws and standards for penetration testers**
- **Footprinting**
- **Hacker**
- **Hacking**
- **Hashing**
- **Information gathering**
- **Internet of Things (IoT)**
- **OS fingerprinting**
- **Penetration testing**
- **Social media**
- **Symmetric encryption**
- **Vulnerability scanning**

Course Plan

Course Outline

Course textbook: *Ethical Hacking and Systems Defense*, National CyberWatch Center edition, (Oriyano and O'Brien, 2016)

Note: Assignments in the following table are listed as when they are **due**.

Grading Category	Activity Title
Lesson 1: Hacking: The Next Generation	
Required Readings	Chapter 1: Hacking: The Next Generation
Discussion	Hacker Motives
Lab	Assessing and Securing Systems on a Wide Area Network (WAN)
Lesson 2: TCP/IP Review	
Required Readings	Chapter 2: TCP/IP Review
Discussion	TCP/IP and the OSI Model
Project	Project Part 1: Current Security Threats
Lesson 3: Cryptographic Concepts	
Required Readings	Chapter 3: Cryptographic Concepts
Discussion	Encryption Technologies
Lab	Applying Encryption and Hashing Algorithms for Secure Communications
Lesson 4: Physical Security	
Required Readings	Chapter 4: Physical Security
Discussion	Biometric Controls
Assignment	Datacenter Controls
Lesson 5: Footprinting Tools and Techniques	
Required Readings	Chapter 5: Footprinting Tools and Techniques
Discussion	Information Exposure Countermeasures
Lab	Data Gathering and Footprinting on a Targeted Web Site
Lesson 6: Port Scanning	

Grading Category	Activity Title
Required Readings	Chapter 6: Port Scanning
Discussion	Port Scanning Countermeasures
Lab	Using Ethical Hacking Techniques to Exploit a Vulnerable Workstation
Lesson 7: Enumeration and Computer System Hacking	
Required Readings	Chapter 7: Enumeration and Computer System Hacking
Discussion	Enumeration and Security Policy
Project	Project Part 2: Vulnerabilities in IT Security
Required Readings	Chapter 8: Wireless Vulnerabilities
Discussion	Security Features of Wireless Technologies
Lab	Auditing a Wireless Network and Planning for a Secure WLAN Implementation
Lesson 9: Web and Database Attacks	
Required Readings	Chapter 9: Web and Database Attacks
Discussion	Secure Web Applications
Lab	Attacking a Vulnerable Web Application and Database
Lesson 10: Malware	
Required Readings	Chapter 10: Malware
Discussion	Scareware versus Ransomware
Lab	Identifying and Removing Malware on a Windows System
Lesson 11: Sniffers, Session Hijacking, and Denial of Service Attacks	
Required Readings	Chapter 11: Sniffers, Session Hijacking, and Denial of Service Attacks
Discussion	Network Sniffing: Ethics and Other Issues
Assignment	Network Traffic and Exploit Identification
Lesson 12: Linux and Penetration Testing	
Required Readings	Chapter 12: Linux and Penetration Testing
Discussion	Linux Tools
Lab	Analyzing Network Traffic to Create a Baseline

Grading Category	Activity Title
	Definition
Lesson 13: Social Engineering	
Required Readings	Chapter 13: Social Engineering
Discussion	Passwords and Social Networking
Project	Project Part 3: SQL Injection Response
Lesson 14: Incident Response	
Required Readings	Chapter 14: Incident Response
Discussion	Incident Response Process

Evaluation and Grading

Evaluation Criteria

The graded assignments will be evaluated using the following weighted categories:

Category	Weight
Lab	40%
Exam	20%
Projects	40%
TOTAL	**100%**

Grade Conversion

The final grades will be calculated from the percentages earned in the course, as follows:

Grade	Percentage
A	90–100%
B+	85–89%
B	80–84%
C+	75–79%
C	70–74%
D+	65–69%
D	60–64%
F	<60%