CSST 2374- Threats and Defense

Sul Ross State University

Instructor: Thea Glenn

Office Location: ACR 109-B **Office Phone**: 432-837- 8490

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

Email: tglenn2@sulross.edu **Office Hours:** TBA

Class*: TBA*

Required Materials:

Textbook: Textbook, labs, and workbooks will be provided the instructor.

References:

DShield

This Web site collects current port-based trends in network probes and attacks, and provides daily diaries about current security topics.
http://www.dshield.org/indexd.html

Insecure.org

Insecure.org provides information on Nmap, a very popular port scanning utility. This Web site also provides a large list of hacking and security utilities and applications.
http://insecure.org/

The Internet Systems Consortium (ISC)

ISC is a non-profit public benefit organization that supports the infrastructure of the Internet by providing open source software (such as BIND and DHCP) and protocols.
http://www.isc.org/

United States Computer Emergency Readiness Team (US-CERT)

strives to be a trusted global leader in cybersecurity—collaborative, agile, and responsive in a dynamic and complex environment. (US-CERT)https://www.us-cert.gov/ncas

Videos:

Defcon 21 - Social Engineering: The Gentleman Thief
https://www.youtube.com/watch?v=1kkOKvPrdZ4

Professional Social Engineer & Scammer
https://www.youtube.com/watch?v=7mBN33gt9OM

Computer Science Program Learning Objectives

1. Describe the fundamental concepts of computer science including algorithms and data structures.
2. Describe modern computer systems, databases, and networking.
3. Demonstrate ability to implement current programming methodologies.
4. Demonstrate proficiency with system design based on object-oriented programming.
5. Work as a team in workgroup environments.

Course Objectives:

This course provides students with an understanding of the roles of an operating system, its basic functions, the services provided by the operating system, the skill to perform basic operations involved in system administration by utilizing virtualization technologies. It includes installation and secure configuration of a system, password policies, updates and patches, backups, and port security.

- Explain the history and current state of hacking and penetration testing, including ethical and legal implications.
- Identify fundamental TCP/IP concepts and technologies related to networking.
- Describe cryptology.
- Identify basic equipment controls, physical area controls, and facility controls.
- Identify common information gathering tools and techniques.
- Analyze how hackers use port scanning and fingerprinting.
- Analyze how enumeration is used in conjunction with system hacking.
- Analyze wireless network vulnerabilities exploited by hackers.
- Perform web and database attacks.
- Identify and remove common types of malware from infected systems.
- Identify Trojans, backdoors, and covert communication methods.

- Perform network traffic analysis and sniffing by using appropriate tools.
- Analyze systems using Linux tools.
- Perform incident handling by using appropriate methods.
- Compare and contrast defensive technologies.

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
Quizzes and assignments must be submitted on time. I have set up rules in BlackBoard so that assignments cannot be submitted after the due date.

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.

Grading
Letter grades will be determined using a standard percentage point evaluation as outlined below. Please note that this is a tentative schedule and can change. Any changes that happen will be updated in Blackboard. Due Dates for assignments will also be posted in Blackboard.

Below is the list of weighted grades on each category.

Group Project	40%
Labs	25%
Assignments	25%
Discussion	5%
Quiz	5%

Your final grade will be determined by calculating points based on the following weights:

A	90 - 100 points
B	80 - 89 points
C	70 – 79 points
D	60 – 69 points
F	below 60 points

The table following is a tentative schedule of the planned assignments. The legend for assignments is below the table:

	Activity	Possible Points
Lesson 1: Hacking: The Next Generation		
Required Readings Lab #1	• Chapter 1, "Hacking: The Next Generation" • Assessing and Securing Systems on a Wide Area Network (WAN)	100
Lesson 2: TCP/IP Review		
Required Readings	• Chapter 2, "TCP/IP Review"	

Assignment	• Developments in Hacking, Cybercrime, and Malware	100
Lesson 3: Cryptographic Concepts		
Required Readings Lab #2 Assignment Project	• Chapter 3, "Cryptographic Concepts" • Applying Encryption and Hashing Algorithms for Secure Communications • Cryptography • Project Part 1: Current Security Threats	 100 100 100
Lesson 4: Physical Security		
Required Readings Assignment Quiz	• Chapter 4, "Physical Security" • Vulnerability of a Cryptosystem	100 100
Lesson 5: Footprinting Tools and Techniques		
Required Readings Lab #3	• Chapter 5, "Footprinting Tools and Techniques" • Data Gathering and Footprinting on a Targeted Web Site	 100
Lesson 6: Port Scanning		
Required Readings Lab #4 Assignment	• Chapter 6, "Port Scanning" • Using Ethical Hacking Techniques to Exploit a Vulnerable Workstation • Information Gathering Plan	 100 100
Lesson 7: Enumeration and Computer System Hacking		
Required Readings Assignment	• Chapter 7, "Enumeration and Computer System Hacking" • Top Ports and Rising Ports Review	 100
Lesson 8: Wireless Vulnerabilities		
Required Readings Group Project Part 2	• Chapter 8, "Wireless Vulnerabilities" • Project Part 2: Vulnerability in Information Technology (IT) Security	100
Lesson 9: Web and Database Attacks		

Required Readings Discussion Lab #5 Assignment	• Chapter 9, “Web and Database Attacks” • Web Server Vulnerability Analysis • Attacking a Vulnerable Web Application and Database • Wireless Exploit Research	 100 100
Lesson 10: Malware		
Required Readings Lab #6 Assignment	• Chapter 10, “Malware” • Identifying and Removing Malware on a Windows System • Web Application Attacks Prevention	 100 100
Lesson 11: Sniffers, Session Hijacking, and Denial of Service Attacks		
Required Readings Lab #7 Assignment Group Project Part 3	• Chapter 11, “Sniffers, Session Hijacking, and Denial of Service Attacks” • Analyzing Network Traffic to Create a Baseline Definition • Malware Lifecycle • Investigative Findings on Malware	100 100 100
Lesson 12: Linux and Penetration Testing		
Required Readings Lab #8 Assignment Group Project Part 4	• Chapter 12, “Linux and Penetration Testing” • Auditing a Wireless Network and Planning for a Secure WLAN Implementation • Basic Linux Commands • SQL Injection	 100 100 100
Lesson 13: Social Engineering		
Required Readings Assignment	• Chapter 13, “Social Engineering” • Network Analysis	 100
Lesson 14: Incident Response		
Required Readings Lab #9 Group Project Part 5	• Chapter 14, “Incident Response” • Investigating and Responding to Security Incidents • Analysis of Intrusion Detection System (IDS) Traffic with	 100 100

	Inbound Attacks	
Lesson 15: Defensive Technologies		
Required Readings Lab #10 Assignment Assignment Group Project Part 6	• Chapter 15, "Defensive Technologies" • Securing the Network with an Intrusion Detection System (IDS) • Gaps in Incident Response • Controls • Defense Plan to Prevent Attacks	 100 100 100 100