Syllabus 2024

1. Course Number and Name
CYB 101: Introduction to Information Security

2. Credits and Contact Hours

- three credit hours
- Office Hours: Email or Slack me to schedule an appointment.

3. Instructor Name

- Jason Langston
- Email: Jlangston@sbu.edu

4. Textbook

- Title: *Fundamentals of Information Systems Security*
- Authors: Kim & Solomon
- Edition: 4th Edition
- ISBN: 1284220737
- Publisher: Jones & Bartlett Learning

5. Course Description
This course introduces two primary domains of Information Security and Information Assurance, as the CompTIA Security+ certification exam covers. By the end of the course, students will have demonstrated proficiency in critical areas through various assessments, including written assignments, objective tests, case studies, classroom discussions, and hands-on labs. The objectives include:

- Defining information security and understanding its significance.
- Identifying types of attackers, analyzing vulnerabilities, and suggesting appropriate defenses.
- Exploring various software security applications and vulnerability scanning tools.
- Understanding logical and physical access controls, authentication, authorization, and accounting.
- Defining and explaining risk management and penetration testing.

This course is crucial as security incidents continue to rise. It aims to equip students with the necessary skills to protect both personal and organizational data while raising awareness of the evolving social and technical factors that drive the need for these protective measures. In today's digital age, the importance of information security cannot be overstated, making this course more relevant than ever.

Required for: Cybersecurity major

6. Course Outcomes
Upon completion of this course, students will be able to:

- Navigate Bash and PowerShell command-line environments.
- Create simple Bash and PowerShell scripts.
- Understand laws and regulations guiding cybersecurity across various industries and countries.
- Develop a general understanding of attacks and defenses.
- Grasp the components and standards of the CIA triad.

7. Topics Covered
The course will cover the following topics:

- Threats and Adversaries (e.g., threat actors, malware, natural phenomena)

- Common Attacks
- Basic Risk Assessment
- Security Life-Cycle
- Security Mechanisms (e.g., Identification/Authentication, Audit)
- Separation of Domains and Duties
- Isolation
- Layering (Defense in Depth)
- Least Privilege
- Endpoint Protection
- Social Engineering and People Security
- Cyber Defense Partnerships (Federal, State, Local, Industry)
- Insider Threats
- Threat Information Sources
- Security Program Goals and Objectives
- Security Policies

8. Grading

Your grade will be determined based on the following:

Item	Percent of Final Grade	Number of Assignments
Weekly Quizzes	42% (420 points)	14 (30 points each)
Labs	48% (480 points)	9
Final Project	10% (100 points)	1
Total Points	**1000**	

Grading Scale:

Grade	Percentage
A+	95% and above
A	90% to 94%
B+	85% to 89%
B	80% to 84%
C+	75% to 79%
C	70% to 74%
D	65% to 69%
F	0% to 64%

Weekly Quizzes
A weekly open-book quiz will be administered in person to assess comprehension of the material. The quiz will primarily focus on textbook content but may include additional concepts covered during lectures. Quizzes are generally scheduled for Fridays, though this may vary.

9. Additional Information

Program Goals:
Detailed learning goals for the Cybersecurity program can be found in the SBU Cybersecurity BS Catalog.

Academic Dishonesty Policy:
Cheating or plagiarism will result in a zero for the assignment, with the potential to fail the course depending on the severity. Refer to the University Policy on Academic Honesty for more information.

Students with Disabilities:
Students requiring accommodations should contact the Disability Support Services Office, Doyle, room 26, at 375-2065 as soon as possible. More details are available at SBU Disability Services.

Labs
Labs will emphasize the importance of command-line environments in cybersecurity. The focus will be on mastering Windows and Linux command-line syntax and related tools.

Attendance & Participation
Regular attendance is expected and will be recorded at the start of each class. Attendance and participation will influence your mid-term and final grades. Excused absences, discussed in advance, will be considered case-by-case.

Final Project

The final project will involve comprehensive analysis and documentation of files, IPs, and domains suspected to be involved in malicious activities. The project will include the following sections:

1. **Executive Summary**
   Provide a concise overview of the analysis process, highlighting key findings.
2. **File Analysis**
   Analyze files of interest and document details such as file names, hashes, MIME types, file sizes, and relevant screenshots.
3. **IP Analysis**
   Evaluate suspicious IP addresses and their associations, including GeoIP location and registration details.
4. **Domain Analysis**
   Investigate domains involved in potential threats, documenting associated IPs and registrar information.
5. **Malware Analysis**
   Use file hashes to search online services and summarize the results, noting any commonalities among reported malware.
6. **Sandbox Analysis**
   Utilize AnyRun for sandbox analysis of suspicious files and interpret the results.
7. **Research and Reporting**
   Conduct in-depth research on selected malware samples and report on their purpose, distribution, and persistence mechanisms.

Format and Submission
The final report must be organized and concise and submitted via Moodle by the end of the course's scheduled final exam time.

Schedule

The course schedule is subject to change based on class needs, with prior notice provided. Due to holidays or breaks, content may be carried over from the previous week.

Labs Overview
The labs will cover topics such as:

1. Windows Command Line: Navigation, redirection, and pipelining.
2. Linux Command Line: Navigation, interpreters, and other command-line basics.
3. Advanced Windows Command Line: Command help, variables, copying, and moving files.
4. Advanced Linux Command Line: Hashing and environment context introduction.

5. PowerShell: Looping, variables, and object manipulation.
6. Bash Scripting: Looping and variables.
7. PowerShell Objects: Working with objects and file hashing.
8. PowerShell File Hashing: Looping, hashing, and object manipulation.
9. Bash File Hashing: Looping and hashing basics.