A picture containing graphical user interface

Description automatically generated

**CYBV 480 – Cyber Warfare**

The University of Arizona

College of Applied Science & Technology (CAST)

Summer 2022 (7W2)

**Instructor:** Paul Wagner

Email: [paulewagner@arizona.edu](mailto:paulewagner@arizona.edu)

Cell Phone: 513-255-0435

Office: Remote/Online

Office Hours: Office hours are by appointment.

Course Delivery Method: Online

Location & Time: Live lectures will be held on Thursdays from 2-5 PM AZ via Zoom.

See your D2L page for the link and additional details.

# COURSE DESCRIPTION:

CYBV 480 will provide students with an introduction to cyber warfare along with its policy, doctrine, and operational constraints. A broad survey of cyber tools, techniques and procedures will be presented, and students will use hands-on labs to practice and implement attack methodologies. CYBV 480 conforms to the National Security Agency (NSA) Center of Academic Excellence in Cyber Operations (CAE-CO) academic requirements for Offensive Cyber Operations.

***Prerequisites:*** *CYBV385 or Consent of the Instructor*

# REQUIRED TEXTS:

* Kim, P. (2018). *The Hacker Playbook 3: Practical Guide to Penetration Testing.* Secure Planet LLC. ISBN 13: 978-1980901754.
* Easttom, C. (2018). *Penetration Testing Fundamentals: A Hands-On Guide to Reliable Security Audits.* Pearson Education Inc., Indianapolis, IN. ISBN 13: 978-0789759375.
* Supplemental readings and other resources as assigned on D2L throughout the semester.

# STUDENT LEARNING OUTCOMES:

Upon completion of this course students will be able to:

* Understand the phases of offensive cyber operations, what each phase entails, who has authorities to conduct each phase, and how operations are assessed after completion.
* Apply the legal, ethical and policy issues associated with Cyber Operations.
* Describe and demonstrate how to plan, conduct, and defend against automated and web-based reconnaissance.
* Explain and demonstrate how to extract metadata from files and how to defend against metadata reconnaissance.
* Identify and describe network scanning methodology, including the types of network scans and practical scanning considerations.
* Describe and demonstrate how to perform vulnerability scanning
* Identify and describe the Metasploit framework including its Interfaces, Modules, and Exploit Creation tools
* Describe and demonstrate how to gain and leverage shell access to identify and obtain important data from the victim machine
* Identify and describe the different types of password attacks, their strengths and weaknesses and when each is most effective
* Identify & discuss the similarities and differences between reflected and stored XSS attacks
* Describe the characteristics and operation of a command injection attack
* Demonstrate how a command injection attack is used to gain shell access on a victim machine
* Identify & describe the different types of SQL injection attacks

# COURSE OBJECTIVES

During this course students will:

* + Use hands-on exercises to demonstrate they have mastered the basics of cyber reconnaissance
  + Implement a scanning methodology to determine what targets exist as well as the configuration of those targets
  + Determine system vulnerabilities and deliver the proper exploitation to gain remote access to target machines
  + Use organic system capabilities to search and capture data from an exploited target system
  + Recon and exploit a compromised network to regain control of the CyberApolis Water Company systems
  + Develop a Final Report outlining the penetration testing methodologies used in the water company scenario

# EXPECTED COURSE WORKLOAD

Students should expect a minimum of 3 hours of lecture and an additional 15 hours of homework/exercises each week for this course. Live synchronous lectures will be held each week. If a student cannot attend the lecture, the lectures are recorded and can be viewed by the student asynchronously.

# REQUIREMENTS:

Requirements for the course are: five (5) Exercises; two (2) Quizzes; and the Water Company Scenario Report. Students will be expected to draw on course lectures and assigned readings to complete all course assignments and Exercises. *No late work will be accepted so please ensure you allot enough time to complete and turn in your work on time.*

# GRADING:

The final grade in the course will be based upon:

|  |
| --- |
| **Exercises 50% See Course Schedule/D2L** |
| (5 Exercises - 70 points each) |
|  |
| **Quizzes 20% See Course Schedule/D2L** |
| (2 Quizzes – 70 points) |
|  |
| **Final Assessment – Regain Network Access 30% See Course Schedule/D2L** |
| (Water Company Scenario – 210 points) |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| GRADING SCALE | |  | DISTRIBUTION | |
| A | 90 to 100 % |  | 900 – 1000 Points | A |
| B | 80 to 89% |  | 800 – 899 Points | B |
| C | 70 to 79% |  | 700 – 799 Points | C |
| D | 60 to 69% |  | 600 - 699 Points | D |
| E | Below 60% |  | 0 – 599 Points | E |

# COURSE SCHEDULE:

## Week 1 – Overview of Cyber Operations and the Cyber Kill Chain

* **Week 1 Learning Objectives** – Upon completion students will be able to**:**
  + Identify and describe the fundamentals of Offensive and Defensive Cyber

Operations and the Cyberspace Domain. Describe and evaluate the Cyber Kill Chain

* + - Reconnaissance
    - Weaponization
    - Delivery
    - Exploitation
    - Installation
    - Command and Control
    - Actions on Objectives
  + Explain how the Cyber Kill Chain can be used to describe and evaluate offensive Cyber Operations
  + Identify and evaluate the problems related to using the Cyber Kill Chain model when designing and implementing a cyber defense plan
    - Perimeter-defense focus
    - Malware-prevention focus

## Week 1 Assignments

* + Week 1 Lecture & Presentation
  + Read JP 3-12(R) Cyberspace Operations Section II
  + Read FM 3-12 Cyberspace and Electronic Warfare Operations
  + Chapter 1 sections 1-1 thru 1-23
  + Read Gaining the Advantage – Lockheed Martin Cyber Kill Chain
  + Read: The Hacker Playbook 3 Chapter 1
  + Read: Penetration Testing Fundamentals Chapter 1
  + Complete Cyber Operations Overview Quiz

## Week 2 – Cyber Operations Mission Planning, Execution, and Evaluation

* **Week 2 Learning Objectives** – Upon completion students will be able to**:**
  + Identify and describe the phases of offensive cyber operations, what each phase entails, and how operations are assessed after completion.
    - Military Decision Making Process (MDMP)
    - Target Identification
    - Cyber Reconnaissance
    - Fingerprinting/Target Enumeration
    - Development of Operational Plans
    - Mission Execution
    - Mission Assessment
  + Describe the decision authorities & authorizations associated with Cyber Operations
* Constitutional Authorities
* President of the United States & Secretary of Defense
* Executive Orders & Operations Orders
* Titles 6, 10, 18, 32, 40, 44, 47, 50
* Executive Order 12333

## Week 2 Assignments

## Week 2 Lecture & Presentation

* + Read FM 3-12 Cyberspace and Electronic Warfare Operations
    - Chapter 1 sections 1-16 thru 1-23, 1-37 thru 1-38, 1-87 thru 1-100
    - Chapter 2 sections 2-5 thru 2-10 and 2-17
    - Chapter 3 sections 3-37 thru 3-80
  + Complete Cyber Operations Mission Planning Quiz

## Week 3 – Cyber Reconnaissance

* **Week 3 Learning Objectives** – Upon completion students will be able to:
  + Identify and demonstrate Cyber Reconnaissance techniques:
    - Online Anonymity & Attribution
    - Documenting Reconnaissance Findings
    - Whois Searches
    - People Searches
    - Credentials Searches
    - Social Media Searches
    - Social Media Monitoring
    - Web Scraping
    - Social Media Monitoring
    - Job Postings Searches
    - Automated Reconnaissance Tools
    - Metadata & Metadata Search Tools
    - Search Engine Searches & Search Diggity Tools
    - Google Cache & Wayback

## Week 3 Assignments

* + Week 3 Lecture & Presentation
  + Read: The Hacker Playbook 3 Chapter 2
  + Read: Penetration Testing Fundamentals Chapter 4
  + Complete Reconnaissance Lab

## Week 4 – Network Scanning

* **Week 4 Learning Objectives** – Upon completion students will be able to:
  + Identify and demonstrate a scanning methodology including the types of network scans and practical scanning considerations.
  + Describe and demonstrate how to sniff and analyze network traffic with tcpdump.
  + Describe and demonstrate how to perform network sweeps & tracing, port scanning, Operating System (OS) fingerprinting and software version scanning with NMAP and Netcat.
  + Describe defenses against network sniffing and scanning.
  + Describe and demonstrate how to perform vulnerability scanning with Nessus and NSE.
  + Describe how to recognize and defend against vulnerability scanning attempts.

## Week 4 Assignments

* + Week 4 Lecture & Presentation
  + Read: The Hacker Playbook 3 Chapter 4
  + Read: Read: Penetration Testing Fundamental Chapter 8
  + Complete Scanning Lab

## Week 5 – Exploitation

* **Week 5 Learning Objectives** – Upon completion students will be able to:
  + Identify and describe the Metasploit framework including its Interfaces, Modules, and Exploit Creation tools.
  + Describe and demonstrate the compromise of a victim machine using the Metasploit framework.
  + Describe and demonstrate the use of the Meterpreter payload on a compromised victim machine.
    - Describe and demonstrate how to gain and leverage shell access on a compromised victim machine.
  + Describe and demonstrate how to identify and obtain important data from the victim machine.
  + Describe how to recognize and defend against data exfiltration attempts.
  + Describe and demonstrate how to use shell access to create persistence mechanisms on a victim machine.
  + Describe how to recognize and defend against persistence mechanisms

## Week 5 Assignments

## Week 5 Lecture & Presentation

* + Read: The Hacker Playbook 3 Chapter 7
  + Complete Exploitation Lab

## Week 6 – Password Attacks & Defenses

* **Week 6 Learning Objectives** – Upon completion students will be able to:
  + Identify and describe the different types of password attacks, their strengths and weaknesses and when each is most effective.
  + Identify and describe the Windows and Linux password representation formats.
  + Describe and demonstrate obtaining password Hashes from Windows and Linux systems.
  + Identify and describe the defenses against weak passwords and password policies.
  + Describe and demonstrate password guessing with THC Hydra
  + Describe and demonstrate password cracking with John the Ripper.
  + Describe how to drive up the computational requirements for password cracking through implementation of strong passwords

## Week 6 Assignments

* + Week 6 Lecture & Presentation
  + Read: The Hacker Playbook 3 Chapter 8
  + Read: Penetration Testing fundamentals Chapter 3, 9, and 10
  + Complete Password Lab
  + **Final Project Available: Due August 19, 2022**

**Week 7 – Web Application Attacks**

* **Week 7 Learning Objectives** – Upon completion students will be able to:
  + Identify & discuss the similarities and differences between XSRF and XSS
  + Describe how to identify and defend against XSRF attacks through proper coding techniques and defensive measures.
  + Identify & discuss the similarities and differences between reflected and stored XSS attacks.
  + Describe reflected and stored XSS attacks
  + Describe how to identify and defend against XSS attacks through proper coding techniques and defensive measures
  + Identify and describe the characteristics and operation of a command injection attack.
  + Describe and demonstrate using a command injection attack to gain shell access on a victim machine.
  + Describe how to identify and defend against command injection attacks through proper coding techniques and defensive measures
  + Identify & describe the different types of SQL injection attacks.
  + Describe how to locate an SQL injection flaw and how to obtain database information with SQL injection attacks.
  + Describe how to identify and defend against SQL attacks through proper coding techniques and defensive measures

## Week 7 Assignments

* + Week 7 Lecture & Presentation
  + Complete Command Injection Lab

## Final Assessment (Water Company Scenario) will be due August 19, 2022.

**University of Arizona Final Examination Policy:** [https://www](http://www.registrar.arizona.edu/courses/final-examination-schedule-fall-).re[gistra](http://www.registrar.arizona.edu/courses/final-examination-schedule-fall-)r.ari[zona.edu/courses/final-examination-schedule-fall-](http://www.registrar.arizona.edu/courses/final-examination-schedule-fall-) 2020?audience=students&cat1=10&cat2=31 and Final Exam Schedule <http://www.registrar.arizona.edu/schedules/finals.htm>

## Grading Policy:

University policy regarding grades and grading systems is available at: <http://catalog.arizona.edu/policy/grades-and-grading-system>

Requests for incompletes (I) and withdrawal (W) must be made in accordance with university policies which are available at <http://catalog.arizona.edu/policy/grades-and-> grading-system#incomplete and <http://catalog.arizona.edu/policy/grades-and-grading-> system#Withdrawal respectively.

## Classroom Behavior Policy:

To foster a positive learning environment, students and instructors have a shared responsibility. We want a safe, welcoming, and inclusive environment where all of us feel comfortable with each other and where we can challenge ourselves to succeed. To that end, our focus is on the tasks at hand and not on extraneous activities (e.g., texting, chatting, reading a newspaper, making phone calls, web surfing, etc.).

## Threatening Behavior Policy:

The UA Threatening Behavior by Students Policy prohibits threats of physical harm to any member of the University community, including to oneself. See: <http://policy.arizona.edu/education-and-student-affairs/threatening-behavior-students>

## Accessibility and Accommodations:

At the University of Arizona we strive to make learning experiences as accessible as possible. If you anticipate or experience physical or academic barriers based on disability or pregnancy, you are welcome to let me know so that we can discuss options. You are also encouraged to contact Disability Resources (520-621-3268 or **https://drc.arizona.edu**) to explore reasonable accommodation.

If our class meets at a campus location: Please be aware that the accessible table and chairs in this room should remain available for students who find that standard classroom seating is not useable.

## Code of Academic Integrity as described in the UA General Catalog:

Students are encouraged to share intellectual views and discuss freely the principles and applications of course materials. However, graded work/exercises must be the product of independent effort unless otherwise instructed. Students are expected to adhere to the UA Code of Academic Integrity as described in the UA General Catalog. See: https://deanofstudents.arizona.edu/policies/code-academic-integrity

The University Libraries have some excellent tips for avoiding plagiarism available at: <http://new.library.arizona.edu/research/citing/plagiarism>

All written work is submitted to *Turnitin*, an anti-plagiarism application that compares submitted assignments to a comprehensive database that includes all published and internet sources as well of hundreds of thousands of student papers. You will be able to see for yourself what percentage of your written work is considered “non-original” once you have submitted it to the appropriate Dropbox in D2L. My position on plagiarism is non-negotiable—any written work that is plagiarized will result in a failure for that assignment and possibly the course. Please familiarize yourself with the rules regarding plagiarism.

## UA Nondiscrimination and Anti-Harassment Policy:

The University is committed to creating and maintaining an environment free of discrimination; see <http://policy.arizona.edu/human-resources/nondiscrimination-and-> anti-harassment-policy. Our classroom is a place where everyone is encouraged to express well-formed opinions and their reasons for those opinions. We also want to create a tolerant and open environment where such opinions can be expressed without resorting to bullying or discrimination of others.

## Absence and Class Participation Policy:

The UA’s policy concerning Class Attendance, Participation, and Administrative Drops is available at: <http://catalog.arizona.edu/policy/class-attendance-participation-and-> administrative-drop

The UA policy regarding absences for any sincerely held religious belief, observance or practice will be accommodated where reasonable, <http://policy.arizona.edu/human-> resources/religious-accommodation-policy.

Absences pre-approved by the UA Dean of Students (or Dean Designee) will be honored. See: https://deanofstudents.arizona.edu/absences

**Additional Resources for Students:**

**UA Academic policies and procedures are available at**: <http://catalog.arizona.edu/policies>

## Student Assistance and Advocacy information is available at:

https://deanofstudents.arizona.edu/support/student-assistance

## Academic Advising:

If you have questions about your academic progress this semester, please reach out to your academic advisor (https://advising.arizona.edu/advisors/major). Contact the Advising Resource Center (https://advising.arizona.edu/) for all general advising questions and referral assistance. Call 520-626-8667 or email to advising@.arizona.edu

## Life Challenges:

If you are experiencing unexpected barriers to your success in your courses, please note the Dean of Students Office is a central support resource for all students and may be helpful. The Dean of Students Office can be reached at (520) 621-2057 or DOS- [deanofstudents@email.arizona.edu.](mailto:deanofstudents@email.arizona.edu)

## Physical and Mental-Health Challenges:

If you are facing physical or mental health challenges this semester, please note that Campus Health provides quality medical and mental health care. For medical appointments, call (520) 621-9202. For After Hours care, call (520) 570-7898. For the Counseling & Psych Services (CAPS) 24/7 hotline, call (520) 621-3334.

## Confidentiality of Student Records

<http://www.registrar.arizona.edu/personal-information/family-educational-rights-and-> privacy-act-1974-ferpa?topic=ferpa

## \*Subject to Change Statement

Information contained in the course syllabus, other than the grade and absence policy, may be subject to change with advance notice, as deemed appropriate by the instructor.