CYBR 545: BUSINESS CYBERCRIME MANAGEMENT

COURSE SYLLABUS Spring 2024

COURSE INTRODCTION

Course number and name: CYBR 545, Business Cybercrime Management

CRN: 15891, 3 credits.

Class meets : Asynchronous

Class duration: 1/8/2023 – 3/1/2024

Prerequisite Courses: CYBR 530 and PR or CONC: CYBR 535

Instructor: Mohammad (MJ) Ahmad, Ph.D.

Course Materials: All material is posted on eCampus (https://ecampus.wvu.edu).

Course Introduction: This course will provide students with advanced knowledge on offensive security and penetration testing topics from both a technical and management perspective. This is a highly technical course that is designed to provide students with hands-on knowledge of a multitude of common penetration testing techniques and tools, as well as broad knowledge about offensive security from a business and an information security management perspective. The online modules are designed to learn the managerial skills to protect, defend, and audit the security of information systems by ensuring confidentiality, integrity, authentications, availability, and non-repudiation through liability assessments, statistical analysis, and risk-based decision making. Upon completion of the course, students should be able to ensure that appropriate business security controls are in place to safeguard digital files and critical electronic infrastructure. Labs, Exams, Kali Linux exercises, and a research project will be stressed in the student evaluation process. Additionally, optional modules discussions on eCampus will be available for students to interact with peers and the instructor.

INSTRUCTOR INFORMATION

Office location: 2109 Reynolds Hall. **Tel:** +1(304)293-7939

Office hours: Online (and optional on-campus) office hours are Monday And Wednesday @12:30PM-2:20PM, Tuesday 1:30PM-4:00PM EST, please use the Schedule Appointment link to schedule an appointment.

Email: mohammad.ahmad@mail.wvu.edu (Emails sent to @mix.wvu.edu account will be ignored). The best and preferred method of communication is via Email.

Additional and optional channel of communication: Zoom if needed.

INSTRUCTIONAL MATERIALS

Course Required Textbook:

- Walker, M. (2021). *CEH Certified Ethical Hacker All-in-One Exam 5th Edition*. McGraw Hill. https://learning.oreilly.com/library/view/ceh-certified-ethical/9781264269952/

- Weidman, G. (2014). *Penetration Testing: A Hands-On Introduction to Hacking*. No Starch Press, Inc. https://learning.oreilly.com/library/view/penetration-testing/9781457185342/

- NDG Ethical Hacking Labs v2 (about $50.00) https://portal.netdevgroup.com/learn/94pcg4/enroll/
- Computer capable of supporting Oracle VirtualBox with Kali Linux Virtual Machine (VM)
    - https://www.virtualbox.org/ - Virtual Box (Free)
    - https://www.kali.org/downloads/ - Kali Linux 64-bit Installer (Free)

ADDITIONAL BENEFITS OF CLASS: After completion of this course, the student should be able to do additional study and sit for the Certified Ethical Hacker (CEH) v10 Certification Exam. Taking or passing the CEHv10 is in no way a requirement of this class. For students who already have a strong background in offensive security and penetration testing, this course also in part prepares students for the very advanced and practical Offensive Security Certified Professional (OCSP) exam.

COURSE LEARNING OUTCOMES

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

1. Demonstrate via testing, an understanding of advanced offensive security topics on malicious hacking, ethical hacking, and penetration testing.
2. Demonstrate via testing, an understanding of basic operations within the Kali Linux operating system and numerous ethical hacking/penetration testing software
3. Solve advanced problems in a variety of operating systems and software environments and be able to explain solutions through a formal lab-write up.
4. Conduct research on an offensive security topic

COURSE DESIGN AND ORGANIZATION

This course is divided into seven content modules plus an eighth final exam and presentation module. Each is released at the beginning of each week (Monday @12:00AM), and each is intended to take one week to complete. Since we are operating on a compressed schedule, it is critical that you stay on top of the course workload. Stay on top of the wave, don't get swamped by it! If you have any questions along the way, please do not hesitate to e-mail me.

The typical module will involve text readings, a text -based online content lecture on the fundamentals behind offensive security topics that are covered in the Certified Ethical Hacker (CEH) exam, hands-on penetration testing practice using Kali Linux VMs, and online isolated practice labs which employ a variety of offensive security exercises and tools.

There will be five individual module discussions, four Kali Linux exercises, a set of ethical hacking labs on the NDG portal, 15 team-based lab assessments, five individual semester-regular exams, one individual final exam, and one team-based research project on any offensive security or penetration testing topic of the student team's choice. To maintain transparency, you are expected to evaluate each of your peers when your group submits team-based assessments.

CYBR PURPOSE

Offensive Security, Penetration Testing, Information Systems Auditing, Ethical Hacking, Offensive Reconnaissance, Information Security Management, Offensive Security Management, Malicious Software Analysis, Social Engineering, Cryptography, Steganography, Security Tools, Web Security, Software Security, Kali Linux, Information Security Attacks, Client-Side and Server-Side Exploitations, Backdoors, Security Architecture

ASSESSMENTS

The online lectures, online class discussions, online labs and online exams are all designed to explore topics such as offensive security topics such as penetration testing, red team operations, and cybercrime :

- Learning. Students are required to read the assigned texts, practice with penetration testing tools using a Kali Linux VM as suggested in the Weidman text, as well as read the additional educational/supplemental materials available via eCampus.

- Kali Linux Exercises. 4 team-based hands on exercises in Kali Linux will be assigned throughout this course. Each team is expected to complete the assignment and produce a formal report addressing the questions within the exercise.

- NDG Ethical Hacking Labs v2, Series 1: Each student is expected to complete the series 1 of the ethical hacking lab on the NDG portal. You need to enroll and complete those on the NDG's portal online, nothing to be submitted on eCampus. Note that this is a paid subscription, which will cost around $50/ student. Those labs will help your group completing the group based NDG labs posted on eCampus. You may enroll in CYBR 545 section on the NDG portal use the following link https://portal.netdevgroup.com/learn/94pcg4/enroll/ . Students will have to finish at least 50% of those labs by the midterm, 2/8/2024, and 100% by the last day of classes.

- eCampus NDG Labs. 15 team based NDG eCampus Ethical Hacking labs will be assigned throughout this course, those las are like the labs on the NDG portal. Since this is a team-based assessment, each group needs to submit one lab report each eCampus.

- Exams. There are five individual exams during the semester as well as a cumulative final exam held during the exam period. The exams will be multiple choice, and will test on material covered on both books, and the practice labs, as well as any supplementary learning material on eCampus. Exams will be timed but are open book.

- Group Research Projects. Each team will be required to submit group project/ research during Module 8. The group project can be on any offensive security or penetration testing topic. The group project can be a PowerPoint presentation, written paper, or a poster.
  Sample subjects/topics are as follows:
    - Penetration Testing Methodologies
    - Malware
    - Advanced Persistent Threats (APTs)
    - Cryptography
    - Wireless Attacks
    - Penetration Testing Case Studies
    - Advanced Web Attacks and Exploitation (AWAE)

  Note: Since this is a team-based assessment, each student is required to submit a project peer evaluation, this is worth 3% of the total grade.

- Course Discussion Forums: These optional, ungraded discussions will be used to address anything in the class and respond to any questions. Students are encouraged to use these discussions to post their questions, comments, ideas, and responses which could be beneficial to the entire class. Although these are not graded discussions, the instructor may use them to grant up-to 5% bonus to active students who participate in these discussions. To be eligible to each extra credit, students will need to respond to at least 5 different discussion forums on eCampus. The instructor will respond to these discussions when needed. There will be two types of discussions:
    - Course Questions and Discussion Forum: Will relate to any general questions you might have about the class, syllabus, due dates, books, assignments, exams, or anything that others might benefit from seeing the answers to. This is the place to bring them up to share with everybody. Make sure you provided a meaningful title for your discussion. For example, if you want to ask a question regarding homework #2, please provide something like "Homework #2, Question #x question". All students will have the opportunity to view, comment, and respond to your questions and comments. This discussion will be available on the first day of classes.

    - Individual Module Discussion Forum: Each module will have one discussion with a set questions/ topics/ ideas/ thoughts to consider while studying the module. Students are encouraged to view these discussions and respond when appropriate. The instructor will release each of these discussions when each module is released.

GRADES

Performance on graded assessments will be recorded in the eCampus grade book. Anticipate grades to appear within a week following the due date. If the count of any assessment changes, the total percentage of that assessment type will remain the same.

Grading Scale: >90% A; 80-89.9% B; 70-79.9% C; 60-69.9% D; <60% F

Course Grading:

Assessment	Delivery	Count	% Of total grade
Kali Linux Exercises	Team	4	20
eCampus NDG Ethical Hacking Labs	Team	15	20
Portal NDG Labs, v2	Individual	Series 1(18 labs)	15
Semester-regular Exams	Individual	5	20
Research project	Team	1	10
Peers' evaluations	Individual	2	5
Final Exam	Individual	1	10
Total			100

CLASS POLICIES

Attendance Policy:

There is no residency associated with this course. The course is designed for asynchronous learning. If needed, there will be periodic opportunities to meet online for supplementary presentations via Zoom, which all WVU students have access to through their Mix accounts.

Class Meetings and Virtual Meetings:

The presentation of this course will occur through asynchronous delivery of course material in the form of eCampus content, annotated slide lectures, activities, and optional videos. The course has been divided into 8 modules. Each lesson has an opening and a closing date, functioning as a window in which all lesson material must be completed. The instructor will respond to all student emails during the class session period within 24 hours M-F.

Team-based assessments Policy:

In the initial week of the semester, students are required to form working groups, with each group comprising up to four members. Enrollment in groups is facilitated through the sign-up form available on eCampus. Teamwork is essential, as students will collaborate on team-based assignments. It's recommended to use scheduling tools like Doodle or Calendly for arranging regular Zoom meetings.

Equitable distribution of workload within each group is crucial. Should any issues arise regarding group dynamics or assignments, students should promptly contact their instructor. Additionally, each group member is responsible for evaluating their peers by submitting two group evaluations during the semester, one around the midterm and the other during the final's week, to gauge each member's contribution to the group tasks.

Assessment Submission Policy:
All assessments are due on the Sunday of the week they are released. Students are responsible for staying informed about all course materials, tracking assignment deadlines, and exam dates. Course materials will be available on eCampus, where assessments should be submitted in the specified formats by the stated deadlines. Please note, submissions via email will not be accepted. Late submissions risk being rejected without a grade, except in circumstances outlined by specific policies. It is advisable to maintain secure backups of your work to safeguard against data loss.

Makeup Assignments: Should outside commitments cause a problem in meeting a due date, contact the instructor in advance to arrange a resolution to the conflict.

General Comments: The instructor reserves the right to change this syllabus as time and circumstances dictate.

RELATED STATEMENTS

Institutional Policies: Students are responsible for reviewing policies (https://tlcommons.wvu.edu/qualitymatters/syllabus-policies-and-statements) on inclusivity, academic integrity, incompletes, sale of course materials, sexual misconduct, adverse weather, as well as student evaluation of instruction, and days of special concern/religious holiday statements.

Student Evaluation of Instruction: Effective teaching is a primary mission of West Virginia University. Student evaluation of instruction provides the university and the instructor with feedback about your experiences in the course for review and course improvement. Your participation in the evaluation of course instruction is both strongly encouraged and highly valued. Results are strictly confidential, anonymous, and not available to the instructor until after final grades are released by Admissions and Records. Information about how you can complete this evaluation will be provided later. I faithfully read my evaluations and incorporate improvements to our future classes based on useful criticism from your SEI's, so please be sure to complete these forms.

Instructor Access: My office hours are Monday/Wednesday @12:30PM-2:20PM and Tuesday 1:30Pm-4:00PM. please schedule an appointment to meet during office hours. I am always happy to meet with you then, or else any time that is mutually convenient by appointment. It is easy for me to set up a Zoom for a video chat that meets with your convenience. You are always welcome to email me with questions or to arrange a meeting. I will always respond to your emails within 24 hours, Monday through Friday. If you choose to email me, please always include the course number in the title of your email and which assessment/ issue you are reaching out about. For example, if you have a question regarding HW 2, please

use something like this in your email title "CYBR545- HW #2 question". If your email relates to a team-based assessment, please make sure you always include your group number in your email. I enjoy meeting with students during my office hours, am also happy to discuss possible research and collaboration research in any cybersecurity topics, or any issues which are important to you about the class. If you are uncomfortable with any aspect of the course and wish to make a criticism or make a suggestion, but wish to do so anonymously, please leave an unsigned and an anonymous note in this CYBR545 suggestion box, and I will try and accommodate you if possible. Note that you will need to login using your mix account for verification however, your emails will not be collected.

USEFUL LINKS

- 2023-2024 Academic Calendar
- Spring 2024 Final Exams calendar

EXPECTED TIMELINE

The following schedule is an estimate schedule of the topics covered in this class along with the designated week. This might change depending on the progress of students in the class.

Week #	Date (2024)	Text Chapter(s)	Topics	Assessment(s) due
1	1/8 - 1/14	Walker – Chapters 1 & 2 (pp 1 – 82)	**Module # 1:**	Sign-up for Groups
		Weidman – Chapters 1 & 2 (pp 9 – 75)	Course Introduction, Ethical Hacking Basics, Reconnaissance, Introduction to Kali Linux	Set-up Kali Env
2	1/15 - 1-21	Walker – Chapters 3 & 4 (pp 83 – 180)	**Module #2:**	NDG Labs 1, 2
			Scanning and Enumeration, Sniffing and Evasion, Metasploit Framework, Programming	
		Weidman – Chapters 3, 4 & 5 (pp 75 - 113)	Special Topic:	Exam 1
			Trending Cybersecurity Threats to Watch	
3	1/22 - 1/28	Walker - Chapters 5, 6, 7 (pp 183 – 295)	**Module #3:**	Kali Exercise 1
			Attacking a System, Web-Based & Wireless Network Hacking, Finding Vulnerabilities, Packet Capture, Vulnerability Exploitation	NDG Labs 3, 4, 5
		Weidman - Chapters 6, 7, & 8 (pp 133 -197)	Special Topic:	
			Ransomware Attacks	Exam 2
4	1/29 - 2/4	Walker – Chapter 8, 9 (pp 297 - 347)	**Module #4:**	
			Mobile Communications and IoT, Security in Cloud Computing, Client-Side Exploitation, Password Attacks	NDG Labs 6, 7, 8
		Weidman - Chapters 9, 10, 11 (pp 197 - 257)	Special Topic:	Exam 3
			Stuxnet & ICS Attacks	
5	2/5 - 2/11	Walker - Chapter 10, 11 (pp 349- 424)	**Module #5:**	NDG Labs 9, 10, 11
			Trojans/Malware, Cryptography, Bypassing Antivirus Applications, Post Exploitation Processes, Web Application Testing	Kali Exercise 2 Midterm check (50% required of NDG Labs on portal)
			Special Topic:	Exam 4

		Weidman - Chapters 12, 13, 14 (pp 257 - 339)	TBD	
6	2/12 - 2/18	Walker - Chapter 12, 13 (pp 425 - 475)	**Module #6:**	NDG Labs 12, 13
			Social Engineering, Penetration Testing, Exploit Development, Linux & Windows Exploits	
		Weidman - Chapters 15, 16, 17 (pp 339 - 401)	Special Topic:	Exam 5
			TBD	Kali Exercise 3
7	2/19 - 2/25	Weidman - Chapters 18, 19, 20 (pp 379 - 472)	**Module #7:**	NDG Labs 14, 15
			Exception Handling, Fuzzing, Mobile Hacking	
			Special Topic:	Kali Exercise 4
			TBD	
8	2/26 - 3/1	**Module 8**		Final Projects Due
		Research and Final Exam Due this week		Cumulative Final Exam Taking and passing either the OSCP or CEH certification exams will count as an automatic 100% on the Final Exam