MIST 400
Advanced Information Security
Mohammad (MJ) Ahmad, Ph.D.
West Virginia University
CRN 13328
Spring 2024
MWF, 11:30AM to 12:20PM – Reynolds Hall 4006

Instructor: Mohammad (MJ) Ahmad Ph.D
Teaching Assistant Professor of Cybersecurity and MIS
Department of Management Information Systems
2109 Reynolds Hall
+1(304)-293-7939
Mohammad.ahmad@mail.wvu.edu

Office: 2109 Reynolds Hall
Office Hours: Online (and optional on-campus)
Monday/Wednesday @12:30PM-2:20PM, Tuesday 1:30:00PM-4:00PM EST
please use the Schedule Appointment link to schedule an appointment.

Required Materials: Santos, O., and Taylor, R. *CompTIA Pentest+ PT0-002 Cert Guide. Pearson.* ISBN-13:9780135226186.
https://learning.oreilly.com/library/view/comptia-pentest-pt0-002/9780137566204/

Weidman, G. Penetration Testing: A Hands-On Introduction to Hacking. No Starch Press. ISBN-13:9781593275648
https://learning.oreilly.com/library/view/penetration-testing/9781457185342/

(Can be viewed online for free using WVU's O'Reilly Books Subscription – Link on eCampus)

NDG Ethical Hacking Labs v2 $50.00 USD.
Join the MIST 400 on the NDG portal by accessing the enrollment link (https://portal.netdevgroup.com/learn/4n9twe/enroll/). Please read the description of these labs before enrollment.

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)

COURSE INFORMATION

EXECUTIVE SUMMARY: This course focuses on advanced managerial and technical topics in information security for the modern-day business enterprise. Specifically, this course examines cybersecurity topics through the lens of offensive security management, covering topics such as penetration testing, digital forensics, OSINT, and social engineering. Students will learn to examine organizational security from an adversarial and proactive security prospective, and will learn to employ appropriate methods to discover, analyze, and remediate cybersecurity threats in modern information systems. Upon completion of the course, students should be able to ensure that appropriate business security controls are in place to safeguard organizational data, assets, and critical electronic infrastructure.

COURSE DESCRIPTION & LEARNING OUTCOMES: 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. By the end of the course, the student should:

1. Demonstrate via testing, that the student has a good understanding of offensive security topics and concepts as well as knowledge of advanced technical topics such as digital forensics, social engineering, network scanning and enumeration.
2. Demonstrate via testing, the business need for penetration testing and information security auditing, as well as the various contractual agreements involved in penetration testing of business enterprise networks.
3. Demonstrate knowledge of techniques, skills and offensive security tools necessary for offensive security practice in modern business enterprise networks and information systems through formal lab report write-ups.
4. Read and interpret a formal penetration testing report.
5. Demonstrate in essay writing an understanding of key concepts of current challenges and issues in offensive security.

ADDITIONAL BENEFITS OF CLASS: After completion of this course, the student should be able to do additional study and sit for the CompTIA Pentest+ Certification or the Certified Ethical Hacker (CEH) v10 Certification Exam. Taking or passing the Pentest+ or CEHv10 is in no way a requirement of this class.

COURSE PREREQUISITES:

Strongly Recommended: MIST 355 (Data Communications), MIST 356 (Network Security)

COURSE DESIGN: This course focuses on providing students with the fundamentals behind offensive security topics that are covered in the Pentest+ and Certified Ethical Hacker (CEH) exams, and hands-on penetration testing practice using Kali Linux VMs, Capture the Flag (CTF) Challenges and online isolated practice labs which employ a variety of offensive security exercises and tools.

ASSESSMENTS

The in-lab lectures with the online lectures, online class discussions, online labs and online exams are all designed to explore information security assurance topics, risk management, and compliance.

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

- **Semester Tests**: There are three individual tests during the semester as well as a cumulative individual final will be held during the exam period. The tests will be mostly multiple choice, and will test on material covered on both books, and the practice labs, as well as any supplementary learning material on eCampus. Tests will be timed but are open book.

- **NDG Ethical Hacking Labs.**: 15 team-based NDG eCampus Ethical Hacking labs will be assigned throughout this course. To practice and prepare for these labs, you need to create an account on the NDG portal and pay fees ($50 per account). Since this is a team-based assessment, each group needs to have access to the portal using only one account, and only one copy of the lab should be submitted per team on eCampus. That said, it is highly recommended that each student joins the portal and completes these online labs individually. Students who finish at least 80% of these labs online via the NDG portal will gain 10% extra bonus. The team-based lab component is worth 20% of the total grade. Each team member is required to evaluate each team member using the lab peer evaluation tool. You may enroll in MIST 400 section on the NDG portal use the following link https://portal.netdevgroup.com/learn/4n9twe/enroll/ .

- **Capture the Flag (CTF) Challenges:** 5 team-based "Capture the Flag" or "CTF" challenges will be assigned through the course. CTF assignments are interactive puzzles which will require the use of a variety of software tools, problem solving techniques, online research, and ingenuity to find the "flag" (i.e., bits of data) that indicate that you have successfully solved the problem. Students will be required to construct a formal write up of their solution following the completion of the challenge.

- **Applied Offensive Security Projects**. Each team will identify, research, and develop an applied research project on a cybersecurity subject or topic. Projects will go beyond developing a standard research presentation, and will have an applied focus, producing a deliverable that would be useful for solving real-world business cybersecurity problems. Emphasis on creativity, utility, and in-depth research is encouraged.

  Example projects could be:

  - Producing security awareness training materials for a business which focus on the most current social engineering threats and trends
  - An in-depth demonstration and walkthrough of a suite of common information security tools (i.e. Metasploit, SET, aircrack-ng, nmap, nessus, etc)

- Developing a new cybersecurity tool or script in Python
- Write a best-practices manual for conducting Gap Analyses
- Developing a mapping of modern compliance frameworks by industry
- Constructing a database of modern security threats to various parts of Enterprise IT.
- Demonstrating the use of machine learning techniques for malware identification or steganography detection
- Developing a new enterprise security architecture framework

- **Peer evaluations for group assessments:** To maintain transparency, you are expected to evaluate each of your peers when your group submits team-based assessments. There are three evaluation you need to fill out, the instructor will release those throughout the semester and notify students when they are due.

- Performance on graded activities will be recorded in the grade book. Anticipate grades to appear within a week or two following the due date.

- **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 10 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

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

Course Grading:

Assessment	Count	Delivery	% Of total grade
Semester Tests	3	Individual	25
NDG Ethical Hacking Labs	15	team-based	30
Capture the Flag (CTF) Challenges	5	team-based	10
Offensive Security Project	1	team-based	10
Cumulative Final Exam	1	Individual	15
Peer evaluations for group assessments	3	Individual	10
Total			**100%**

CLASS POLICIES

Attendance Policy:
Attendance is mandatory encouraged in this class, students are required to record their attendance within 5 minutes of the beginning of the class, using the attendance sheet on eCampus. Students who miss more than 6 classes without a legitimate reason and without contacting Dr. Ahmad will lose up-to 5% of the total course grade. Students who consistently attend classes can gain up-to 5% bonus if they do not miss more than 6 classes without a legitimate reason. This class will be offered on campus in the room and building stated above. Some bonuses will be handed out during the class, and only those attending can get credit for the bonus assessments. If needed, this class might be streamed online, and students will be notified if any changes take place.

Instructor Access: 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 "MIST400- 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.

Team-based assessments Policy:
In the first week of classes, students will self-select into working groups for the semester. Each group can have up-to 4 group members, please refer to the groups sign-up form on eCampus to create and view groups. Students are expected to collaborate professionally with all group members to submit team-based assessments. For each team-based assessment, each member is required to submit peer evaluations as described above. For groups to function efficiently and fairly, you may like to find a common time to meet regularly physically, or via Zoom by using a website such as Doodle or Calendly. The groups are expected to distribute the work among the group members equally. If there are any issues the arise regarding the groups or group-based assessments, please do reach out to your instructor ASAP.

Assessment Submission Policy:
All assessments are due on the Friday of the week they are due on. Students are responsible for all material covered in the course, keeping track of assignments and examination dates. All materials will be posted on eCampus, and your assessments must be submitted in the expected formats by the given due dates on eCampus, submissions over email are not accepted. Any late work may be rejected without a grade except when a policy indicates otherwise. You should keep secure copies of your work in case of data loss. Assessments submitted after the due date are not encouraged however, if this happens, Late penalties will be applied for late submitted assessments (20% immediate and 20% for each late day). Once grades for an assessment are posted, you have 7 calendar days to contact your instructor if you believe they are incorrect. After that, they are final.

Class Academic Integrity: Academic integrity is very important to us, It's your responsibility to know our policy. Not reading the syllabus is not an excuse. Do you work individually when stated, do not use others' work by any means. If you cheat, you will get caught, and severe penalties will be strictly enforced. Students who violate the academic integrity the first time will get 0 in that assessment and lose 5% of the total, and all bonus points. If a student violates the academic integrity twice, they will get F for the course, even if you had no warning of the first violation.

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.

Computer Hardware and Software: All students must have Internet connectivity. Students must have access to Microsoft Office, and a computer capable of running Oracle VirtualBox w/ Kali Linux VM.

Makeup Assignments: I understand life gets in the way of education at times, however, please try to honor the due dates for each assignment. Should outside commitments cause a problem in meeting a due date, contact the instructor to arrange a resolution to the conflict.

Honors EXCEL Students: Students participating in the Honors Experiential and Community Engaged Learning (EXCEL) program will be required to write and submit a bi-weekly journal which provides a reflection on what the student has learned in the course so far, and how the course content has influenced their EXCEL project. In addition, Honor's EXCEL students will be required to write a short paper (5-10 pages) on their EXCEL project focus, due at the end of the semester.

USEFUL LINKS

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

Organization of Course Material:

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.
All assessments are due on the Friday of the week they are due on.

Module	Topic	Text Chapters	Deliverables and Notes
Week 1 (1/8- 1/12)	**Course Introduction, Syllabus Overview, NDG Labs, CTF Challenges** **Introduction to Ethical Hacking and Penetration Testing for Businesses**	Chapter 1, Santos	Group Sign-Up Sign up for NDG Labs Note: January 12 - Last Day to Register, Add New Courses, Make Section Changes, Change Pass/Fail and Audit
Week 2 (1/15 - 1/19)	**Planning and Scoping a Penetration Testing Environment** • Importance of planning and preparation • Legal concepts • Scoping a testing engagement • Compliance-based assessments	Chapter 2, Santos Weidman Readings on eCampus	NO CLASS (1/15) – Dr. Martin Luther King Jr. Holiday NDG Labs 1 & 2
Week 3 (1/22 - 1/26)	**Information Gathering and Vulnerability Identification, Part I** • Information gathering • Active reconnaissance	Chapter 3, Santos Weidman Readings on eCampus	NDG Labs 3 & 4 CTF 1
Week 4 (1/29 - 2/2)	**Information Gathering and Vulnerability Identification, Part II**	Chapter 3, Santos	NDG Lab 5

	• Passive reconnaissance • OSINT gathering • Vulnerability scans		
Week 5 (2/5 - 2/9)	**Social Engineering Attacks** • Phishing and pharming • Mavertising • Elicitation, interrogation, and impersonation • Social engineering motivation techniques • Shoulder surfing USB key drop	Chapter 4, Santos Weidman Readings on eCampus	Exam 1 (Chapters 1 – 3)
Week 6 (2/12 - 2/16)	**Exploiting Wired and Wireless Networks, Part I** • Exploiting network-based vulnerabilities	Chapter 5, Santos Weidman Readings on eCampus	NDG Labs 6 & 7 CTF 2
Week 7 (2/19- 2/23)	**Exploiting Wired and Wireless Networks, Part II** • Exploiting wireless and RF-based attacks and vulnerabilities	Chapter 5, Santos Weidman Readings on eCampus	NDG Lab 8
Week 8 (2/26 – 3/1)	**Exploiting Application-Based Vulnerabilities, Part I** • Web applications • Building a web application lab • Injection-based vulnerabilities • Authentication-based vulnerabilities • Cross-site scripting vulnerabilities	Chapter 6, Santos Weidman Readings on eCampus	Exam 2 (Chapters 4 & 5)

Week 9 (3/4 - 3/8)	**Exploiting Application-Based Vulnerabilities, Part II** • Cross-site request forgery • Clickjacking • Exploiting security misconfiguration • File inclusion vulnerabilities • Insecure code practices	Chapter 6, Santos Weidman Readings on eCampus	NDG Labs 9 & 10 CTF 3
Week 10 (3/11 – 3/15)	**Spring Recess (3/9 – 3/17) – NO CLASS**		
Week 11 (3/18 - 3/22)	**Cloud, Mobile, and IoT Security** • Researching Attack Vectors • Account Takeover • Metadata Service Attacks • Resource Exhaustion • Side-Channel Attacks • IoT Vulns • Data Storage System Vulns	Chapter 7, Santos Weidman Readings on eCampus	NDG Labs 11 & 12
Week 12 (3/25 – 3/29)	**Performing Post-Exploitation Techniques** • Network vulnerability scanning • C2 Utilities • Custom Daemons, process, and Backdoors, Post-Exploitation Scanning	Chapter 8, Santos Weidman Readings on eCampus	NDG Labs 13 & 14 Note: March 29 - Spring Holiday (University Closed) CTF 4

Week 13 (4/1 - 4/5)	**Reporting and Communication** • Note Taking • Report Contents • Communication Triggers • Goal Reprioritization • Presentation of findings	Chapter 9, Santos	Exam 3 (Chapters 6 – 8)
Week 14 (4/8 – 4/12)	**Tools and Code Analysis** • Logical Constructs • Data Structures • Python, Bash, Powershell	Chapter 10, Santos Weidman Readings on eCampus	NDG Lab 15
Week 15 (4/15 – 4/19)	**Tools and Code Analysis** • Perl, Java • Pentesting Linux Distros • Use Cases of Pentesting Tools	Chapter 10, Santos	Work on Projects CTF 5
Week 16 (4/22 – 4/26)	**Finalizing a Penetration Test** • Post-engagement activities • Report writing best practices Report handling and communication best practices	Chapter 11, Santos	Project Note: April 26 - Last Day of Classes
4/29- 5/3	**Finals Week** **Cumulative Final Exam (Chapters 1 – 10)**	Review Chapters 1- 11	Taking and Passing the CompTIA Pentest+ or Certified Ethical Hacker (CEH v10) will count as an automatic 100% on the Final Exam. Final exam due on 5/2/2024 @ 11:00AM