Syllabus

Advanced Ethical Hacking

1191-FIU01-EEL-5807-SECRXDA_mscnsol-14993

General Information | Important Information | Course Detail | Course Calendar

General Information

Professor Information

Instructor:
Alexander Perez-Pons
Phone:
(305) 348-7253
Office:
EC 3145
Office Hours:
By Appointment
E-mail:
apons@fiu.edu

Course Description And Purpose

No matter what field you work in, you cannot help but notice the impact that the Internet has had on society. It has opened up opportunities and markets that people only dreamed of before. As with any technology, there is always a positive and negative aspect. The positive side is tremendous business opportunities; the business world relies increasingly upon data communications, and modern data networks are based mainly on the Internet. The negative side is the huge security risk that is now posed to so many companies, yet few companies are truly aware of the potential danger.

Information is the asset that must be protected. Without adequate protection or network security, many individuals, businesses, and governments are at risk of losing that asset. It is imperative that all networks be protected from threats and vulnerabilities so that a business can achieve its fullest potential. Security risks cannot be eliminated or prevented

completely; however, effective risk management and assessment can significantly minimize the existing security risks.

This course is intended to provide a practical survey of network security applications and standards. The emphasis is on applications that are widely used on the Internet for corporate networks, and on standards that have been widely deployed. It also provides students with the knowledge and skills to begin supporting network security and best practices for implementing security.

The course is comprised of 17 modules. Module availability is open for six days each as listed in the course calendar below. Students will be assessed using a variety of methods: lab assignments, discussion posts and responses, quizzes, one group project, and one final exam.

Topics Covered

- Ethics of Hacking and Cracking
- Reconnaissance
- Scanning Tools
- Sniffers
- TCP/IP Vulnerabilities
- Encryption and Password Cracking
- Spoofing
- Session Hijacking
- Hacking Network Devices
- Trojan Horses
- Denial-of-Service Attacks
- Buffer Overflows
- Programming Exploits
- Mail Vulnerabilities
- Web Application Vulnerabilities

Course Objectives

Students will be able to:

16. Evaluate the tools and techniques to use during reconnaissance, scanning, vulnerability identification, exploitation, and maintaining control and privilege escalation.
17. Assess the security issues in telecommunications and networks.
18. Analyze the design aspects of security including threat identification and risk assessment.
19. Employ best practices and guidelines for developing and verifying effective security policies and procedures, security goals, threats and vulnerabilities,

standards and security policy development, forensics, privacy implications, and ethics.

20. Analyze the different ways of securing Communication and the various threat agents.
21. Assess the differences between ethical and unethical Hacking.
22. Inspect different vulnerabilities and measure how these vulnerabilities are exploited by hackers to gain entry into networks as well as to perform privilege escalation.
23. Synthesize and evaluate intrusion Detection, Policy Creation, Social Engineering, DDoS Attacks, Buffer Overflows and Virus Creation.
24. Analyze and evaluate the severity levels and possible fixes to remediate the uncovered issues and be able to provide comprehensive solutions.

Major & Curriculum Objectives Targeted

In this course, the student will have to show:

25. An ability to apply knowledge of mathematics, science, and engineering,
26. An ability to design and conduct experiments, as well as to analyze and interpret data,
27. An ability to design a system, component, or process to meet desired needs within realistic constraints such as economic, environmental, social, political, ethical, health and safety, manufacturability, and sustainability,
28. An ability to identify, formulate, and solve engineering problems (homework),
29. The broad education necessary to understand the impact of engineering solutions in a global, economic, environmental, and societal context
30. An ability to communicate effectively (through teamwork),
31. An ability to use the techniques, skills, and modern engineering tools necessary for engineering practice,
32. A knowledge of contemporary issues,
33. A knowledge of advanced mathematics.

Teaching Methodology

This is a fully online course in which all of the instructional materials and activities are delivered through Canvas, and/or other internet-based media. Some exams may require the use of an approved proctoring center. Should you have any questions, please contact the professor.

34. Student learning will be enabled by textbook reading, PowerPoint Slides, Case Studies, Individual and group assignments, hands-on exercises and quizzes. For each chapter, there will be assignments including quizzes, and practical exercises. These assignments are due each week.
35. Learning will be self-directed and participative. Evaluation of learning will be based on the quantity and quality of student (self-directed) study reflected by

completing all assignments, and examinations. The participation part of the grade will be determined by the assignments, and how well students actively participate in extra exercises (if any) to be announced throughout the semester. We will engage in this type of learning activity through the Discussion Forum part of Canvas.

36. Students are expected to (electronically) complete the assigned readings and learning exercises during the week the assignment is due.
37. Students are expected to play an active role in different learning activities including posting and answering class related questions on the discussion forum. Active participation is encouraged and expected

Important Information

Policies

Please review the FIU's Policies webpage. The policies webpage contains essential information regarding guidelines relevant to all courses at FIU, as well as additional information about acceptable netiquette for online courses.

As a member of the FIU community you are expected to be knowledgeable about the behavioral expectations set forth in the FIU Student Code of Conduct.

Technical Requirements and Skills

One of the greatest barriers to taking an online course is a lack of basic computer literacy. By computer literacy we mean being able to manage and organize computer files efficiently, and learning to use your computer's operating system and software quickly and easily. Keep in mind that this is not a computer literacy course; but students enrolled in online courses are expected to have moderate proficiency using a computer. Please go to the "What's Required" webpage to find out more information on this subject.

This course utilizes the following tools:

38. Virtual Computing Lab
39. Kali Linux or Back Track Security Distros (Linux Distros)
40. Vmware Workstation or Virtual Box

Please visit our Technical Requirements webpage for additional information.

Accessibility and Accommodation

The Disability Resource Center collaborates with students, faculty, staff, and community members to create diverse learning environments that are usable, equitable, inclusive and sustainable. The DRC provides FIU students with disabilities the necessary support to

successfully complete their education and participate in activities available to all students. If you have a diagnosed disability and plan to utilize academic accommodations, please contact the Center at 305-348-3532 or visit them at the Graham Center GC 190.

Please visit our ADA Compliance webpage for information about accessibility involving the tools used in this course.

Please visit the LMS Accessibility webpage for more information:

- Canvas

For additional assistance please contact FIU's Disability Resource Center.

Academic Misconduct Statement

Florida International University is a community dedicated to generating and imparting knowledge through excellent teaching and research, the rigorous and respectful exchange of ideas and community service. All students should respect the right of others to have an equitable opportunity to learn and honestly to demonstrate the quality of their learning. Therefore, all students are expected to adhere to a standard of academic conduct, which demonstrates respect for themselves, their fellow students, and the educational mission of the University. All students are deemed by the University to understand that if they are found responsible for academic misconduct, they will be subject to the Academic Misconduct procedures and sanctions, as outlined in the Student Handbook.

Academic Misconduct includes: **Cheating** – The unauthorized use of books, notes, aids, electronic sources; or assistance from another person with respect to examinations, course assignments, field service reports, class recitations; or the unauthorized possession of examination papers or course materials, whether originally authorized or not. **Plagiarism** – The use and appropriation of another's work without any indication of the source and the representation of such work as the student's own. Any student who fails to give credit for ideas, expressions or materials taken from another source, including internet sources, is responsible for plagiarism.

Learn more about the academic integrity policies and procedures as well as student resources that can help you prepare for a successful semester.

Panthers Care & Counseling and Psychological Services (CAPS)

If you are looking for help for yourself or a fellow classmate, Panthers Care encourages you to express any concerns you may come across as it relates to any personal behavior concerns or worries you have, for the classmate's well-being or yours; you are encouraged to share your concerns with FIU's Panthers Care website.

Counseling and Psychological Services (CAPS) offers free and confidential help for anxiety, depression, stress, and other concerns that life brings. Professional counselors are available for same-day appointments. Don't wait to call 305-348-2277 to set up a time to talk or visit the online self-help portal.

Course Prerequisites

This course has a prerequisite. Review the Course Catalog webpage for detailed information.

- MAP 3302

Proctored Exam Policy

Please note that the information contained in this section applies only if your course requires a proctored exam.

Through a careful examination of this syllabus, it is the student's responsibility to determine whether this online course requires proctored exams. Please visit our Student Proctored Exam Instructions webpage for important information concerning proctored exams, proctoring centers, and important forms.

Textbook

Computer Security and Penetration Testing
Alfred Basta, Nadine Basta, Mary Brown, PhD, CISSP, CISA
Cengage Learning, 2013
ISBN-10: 0840020937
ISBN-13: 9780840020932
You may purchase your textbook online at the FIU Bookstore.

Expectations of this Course

This is an online course, which means most (if not all) of the course work will be conducted online. Expectations for performance in an online course are the same for a traditional course. In fact, online courses require a degree of self-motivation, self-

discipline, and technology skills which can make these courses more demanding for some students.

Students are expected to:

- Review the how to get started information located in the course content
- Introduce yourself to the class during the first week by posting a self introduction in the appropriate discussion forum
- Take the practice quiz to ensure that your computer is compatible with Canvas
- Interact online with instructor/s and peers
- Review and follow the course calendar
- Log in to the course 5 times per week
- Respond to discussion boards, blogs and journal postings within 2 days
- Respond to email within 2 days
- Submit assignments by the corresponding deadline

The instructor will:

- Log in to the course 5 times per week
- Respond to discussion boards, blogs and journal postings within 3 days
- Respond to emails within 2 days
- Grade assignments within 7 days of the assignment deadline

Course Detail

Course Communication

Communication in this course will take place via **Email**.

The Email feature is an external communication tool that allows users to send emails to users enrolled within the course. Emails are sent to the students' FIU email on record. The Email tool is located on the Course Menu, on the left side of the course webpage.

Visit our Writing Resources webpage for more information on professional writing and technical communication skills.

Discussion Forums

Keep in mind that your discussion forum postings will likely be seen by other members of the course. Care should be taken when determining what to post.

Discussion Forum Expectations:

Introduce Yourself Forum

- Please introduce yourself during the first week of class.
- Please follow the guidelines in the forum.

Lab Assignment Discussion Forum

- The professor will use this forum to post lab assignments and instruction on how to conduct each.
- This forum is for you to interact with your peers by posting and responding to general conversations/questions report assignments.
- You are encouraged, but not required to participate.
- Posts will not be graded.

Report Discussion Forum

- This forum is for you to interact with your peers by posting and responding to general conversations/questions report assignments.
- You are encouraged, but not required to participate.
- Posts will not be graded.

Chapter Discussion Forums

- There will be two discussion topics posted by the professor every week except for exam weeks.
- Forums will be available from Monday - Thursday.
- The professor will review student discussion posts and participate in the discussion at least twice a day for five days from Monday-Sunday.
- Student discussion board posts will be worth 15% of the student grade.
- Students can earn 10 discussion points per week - 5 points for an original post and 5 points for responding to a peer's post. Students must do each to earn full credit.
- Please follow the guidelines listed in the Discussion Participation Rubric.
- The expected turn-around time for feedback or grades is 7 days.

Web Links Discussion Forum

- Students will be assigned TASKs in each module.
- Each TASK requires the student to search for online material relevant to module material.
- A prompt for each TASK is provided in the course.
- Posts will be evaluated according to the TASK Assignment Grading Rubric.

Assessments

In order to mitigate any issues with your computer and online assessments, it is very important that you take the "Practice Quiz" from each computer you will be using to take your graded quizzes and exams. It is your responsibility to make sure your computer meets the minimum hardware requirements.

Assessments in this course are not compatible with mobile devices and should not be taken through a mobile phone or a tablet. If you need further assistance please contact FIU Online Support Services.

Self-Assessments:

- Self-Assessments will not be graded and are primarily for students to check comprehension of course material.
- Students will complete assessments based on chapter content.
- Students will have unlimited time to complete the assessment.
- Once started, the assessment must be completed in one sitting.
- Students will be allowed to take assessments ONE time.
- The score and the correct answers will be available to the student upon completion.
- Students should compare their answers to the submitted answers to gauge how well they are comprehending course content.
- Self-Assessment availability is unlimited.
- Late self-assessments will not be accepted.

Quiz Expectations:

- This course consists of 7 quizzes.
- Quizzes will be available Monday at 12:00 AM - Friday at 11:59 PM.
- Students will be given ONE attempt for each quiz.
- Students will be given 30 minutes to complete each quiz
- Students will be able to see their score upon submission.
- Quizzes must be completed by their set deadline.

Exam Expectations:

- This course consists of ONE final exam.
- **The exam will be available 2/22 at 12:00 AM - 2/23 at 11:59 PM.**
- Students will be given one attempt for the exam.
- Students will be given 60 minutes to complete the exam.
- Students will see their score upon submission.

Assignments

- Explicit instructions and grading criteria will be provided for all assignments.
- Unless specified otherwise, all assignments are to be completed by the individual student.
- Each student will submit their own original work. Any evidence of duplication, cheating or plagiarism will result at least a failing grade for the course.
- All work is to be submitted via Canvas. DO NOT send assignments by email.

- **All work submitted should display Panther ID number and should be signed, as the students' own work, and that no unauthorized help was obtained.**
- Assignments are due on the date specified. Assignments submitted late (within 1 week) will receive half credit.
- Students are encouraged to ask questions and to discuss course topics with the instructor and with each other via the Lab Assignment Discussion Forum.
- To get assistance try to see me by an appointment.
- The expected turn-around time for feedback or grades is 7 days.

Group Research Project

- The course includes a group project (15%) requiring the review and the implementation of attacks or defenses of a non-trivial network security issue.
- **The group project becomes available on 2/18 at 12:00 am and is due on 2/24 by 11:59 pm.**
- The groups contain 3 - 4 students working together throughout the semester.
- Groups will be formed during the first week of the semester via the Groups tool in Canvas.
- Students will submit a recorded presentation, including research paper in IEEE format using the IEE template and the presentation PowerPoint slides at the end of the semester.
- Submissions will be evaluated using the Research Paper Grading Rubric and Presentation Grading Rubric.

Chapter Reports

- Chapter Report assignments will be given as practice to prepare for the final exam.
- Reports are optional and will not be graded.
- Students are provided with a Report Discussion Forum for collaboration. Posts will not be graded.
- Chapter Reports will be submitted in the Assignment Dropbox if the student needs feedback from the professor to complete the project.
- Short essay, no more than two pages, please.
- Students who do not require feedback and who do not have questions regarding the project should not submit projects to the Assignment Dropbox.

Grading

Course Requirements	Weight
Quizzes	10%
Lab Assignments	10%
Discussion and Participation (Chapter Discussion Forums and TASKs)	15%
Group Research Project	15%

Course Requirements	Weight
Final Exam	50%
Total	**100%**

Letter	Range (%)	Letter	Range (%)	Letter	Range (%)
A	95- 100	B	82-85	C	70 - 73
A-	90 - 94	B-	78 - 81	D	69 - 60
B+	86 - 89	C+	74 - 77	F	0 - 59

Department Regulations Concerning Incomplete Grades

To qualify for an Incomplete, a student MUST:

117. Contact (e.g., phone, email, etc.) the instructor or secretary before or during missed portion of class.
118. Be passing the course prior to that part of the course that is not completed.
119. Make up the incomplete work through the instructor of the course.
120. See Instructor. All missed work must be finished before last two weeks of the next term.

Course Calendar

Weekly Schedule

Note: The instructor reserves right to change course materials or dates as necessary.

WEEK/DATES	TOPICS/TASKS
	Module 1 – Ethics of Hacking and Cracking
	Supports Course Learning Objective(s):
	6. Assess the differences between ethical and unethical Hacking
Week 1	**Module Learning Objectives:**
1/07 - 1/13	○ Explain the roles of hackers and their motivation. ○ Identify the issues associated with pirated software and protection of Intellectual property.
	Tasks:
	123. Read Chapter 1 - Ethics of Hacking and Cracking

WEEK/DATES	TOPICS/TASKS

124. View Chapter 1 Presentation
125. Post in Chapter 1 Discussion Forum
126. Complete Chapter 1 Report (optional)
127. Complete Chapter 1 Self-Assessment (optional)
128. View Additional Resources (optional)

Module 2 - Reconnaissance

Supports Course Learning Objective(s):

7. Inspect different vulnerabilities and measure how these vulnerabilities are exploited by hackers to gain entry into networks as well as to perform privilege escalation.

8. Synthesize and evaluate intrusion Detection, Policy Creation, Social Engineering, DDoS Attacks, Buffer Overflows and Virus Creation.

Module Learning Objectives:

- Identify techniques for performing reconnaissance and their legality.
- Describe the methods used in social engineering leading to physical intrusion.
- Explain how to crawl web to collect useful information (Google dorks, Malego, etc).

Tasks:

132. Read Chapter 2 - Reconnaissance
133. View Chapter 2 Presentation
134. Watch posted videos
135. Post in Chapter 2 Discussion Forum
136. Post for Discussion 1 - TASKs 1-1 and 1-2
137. Complete Chapter 2 Report (optional)
138. Complete Lab Assignment 1
139. Complete Chapter 2 Self-Assessment (optional)
140. Submit Quiz 1
141. Form Research Project Group
142. View Additional Resources (optional)

Module 3 - Scanning Tools

Week 2

1/14 - 1/20

Supports Course Learning Objective(s):

1. Evaluate the tools and techniques to use during reconnaissance, scanning,

WEEK/DATES	TOPICS/TASKS

vulnerability identification, exploitation, and maintaining control and privilege escalation.

2. Assess the security issues in telecommunications and networks.

3. Analyze the design aspects of security including threat identification and risk assessment.

7. Inspect different vulnerabilities and measure how these vulnerabilities are exploited by hackers to gain entry into networks as well as to perform privilege escalation.

Module Learning Objectives:

- Identify popular scanning tools.
- Explain how scanners work.

Tasks:

145. Read Chapter 3 - Scanning Tools
146. View Chapter 3 Presentation
147. Post in Chapter 3 Discussion Forum
148. Complete Chapter 3 Report (optional)
149. Complete Chapter 3 Self-Assessment (optional)
150. View Additional Resources (optional)

Module 4 - Sniffers

Supports Course Learning Objective(s):

1. Evaluate the tools and techniques to use during reconnaissance, scanning, vulnerability identification, exploitation, and maintaining control and privilege escalation.

2. Assess the security issues in telecommunication and networks.

3. Analyze the design aspects of security including threat identification and risk assessment.

7. Inspect different vulnerabilities and measure how these vulnerabilities are exploited by hackers to gain entry into networks as well as to perform privilege escalation.

Module Learning Objectives:

WEEK/DATES **TOPICS/TASKS**

- Describe where to place sniffers to obtain specific data.
- Describe the parts associated with sniffers.
- Identify popular sniffier programs/tools.

Tasks:

154. Read Chapter 4
155. View Chapter 4 Presentation
156. Post in Chapter 4 Discussion Forum
157. Complete Chapter 4 Report (optional)
158. Complete Chapter 4 Self-Assessment (optional)
159. Review Additional Resources (optional)

Module 5 - TCP/IP Vulnerabilities

Supports Course Learning Objective(s):

1. Evaluate the tools and techniques to use during reconnaissance, scanning, vulnerability identification, exploitation, and maintaining control and privilege escalation.

2. Assess the security issues in telecommunication and networks.

3. Analyze the design aspects of security including threat identification and risk assessment.

7. Inspect different vulnerabilities and measure how these vulnerabilities are exploited by hackers to gain entry into networks as well as to perform privilege escalation.

Module Learning Objectives:

- Define TCP/IP, flags, addresses, ports, etc.
- Describe the steps of setting-up a TCP/IP communication.
- Describe ways to exploit TCP/IP, including spoofing attacks.

Tasks:

163. Read Chapter 5 - TCP/IP Vulnerabilities
164. View Chapter 5 Presentation
165. Watch posted videos
166. Post in Chapter 5 Discussion Forum
167. Post for Discussion 2 - TASKs 2-1 and 2-2
168. Complete Lab Assignment 2
169. Complete Chapter 5 Self-Assessment (optional)

WEEK/DATES	TOPICS/TASKS

170. Submit Quiz 2
171. Complete Chapter 5 Report (optional)
172. View Additional Resources (optional)

Module 6 - Encryption and Password Cracking

Supports Course Learning Objective(s):

1. Evaluate the tools and techniques to use during reconnaissance, scanning, vulnerability identification, exploitation, and maintaining control and privilege escalation.

2. Assess the security issues in telecommunications and networks.

3. Analyze the design aspects of security including threat identification and risk assessment.

7. Inspect different vulnerabilities and measure how these vulnerabilities are exploited by hackers to gain entry into networks as well as to perform privilege escalation.

Module Learning Objectives:

Week 3

1/21 - 1/27

- Evaluate the effectiveness of password hashing.
- Identify key encryption associated with different security levels.

Tasks:

175. Read Chapter 6
176. View Chapter 6 Presentation
177. Post in Chapter 6 Discussion Forum
178. Complete Chapter 6 Self-Assessment (optional)
179. Complete Chapter 6 Report (optional)
180. View Additional Resources (optional)

Module 7 - Spoofing

Supports Course Learning Objective(s):

3. Analyze the design aspects of security including threat identification and risk assessment.
4. Employ best practices and guidelines for developing and verifying effective security policies and procedures, security goals, threats and vulnerabilities, standards and security policy development,

WEEK/DATES	TOPICS/TASKS
	forensics, privacy implications, and ethics. 5. Determine the different ways of securing Communication and the various threat agents. **Module Learning Objectives:** o Explain the mechanics of spoofing a trusted relationship. o Define various types of spoofing, include DNS spoofing. **Tasks:** 183. Read Chapter 7 - Spoofing 184. View Chapter 7 Presentation 185. View posted videos 186. Post in Chapter 7 Discussion Forum 187. Post for Discussion 3 - TASKs 3-1 through 3-3 188. Complete Lab Assignment 3 189. Complete Chapter 7 Self-Assessment (optional) 190. Submit Quiz 3 191. Complete Chapter 7 Report (optional) 192. Submit Group Research Project Proposal 193. View Additional Resources (optional) **Module 8 - Session Hijacking** **Supports Course Learning Objective(s):** 3. Analyze the design aspects of security including threat identification and risk assessment. 4. Employ best practices and guidelines for developing and verifying effective security policies and procedures, security goals, threats and vulnerabilities, standards and security policy development, forensics, privacy implications, and ethics. 5. Determine the different ways of securing Communication and the various threat agents. **Module Learning Objectives:** o Define the causes of an ACK storm. o Describe some ways that route tables are affected by hackers. **Tasks:** 196. Read Chapter 8 - Session Hijacking
Week 4 **1/28 - 2/3**	

WEEK/DATES	TOPICS/TASKS

197. View Chapter 8 Presentation
198. Post in Chapter 8 Discussion Forum
199. Complete Chapter 8 Self-Assessment (optional)
200. Complete Chapter 8 Report (optional)
201. View Additional Resources (optional)

Module 9 - Hacking Network Devices

Supports Course Learning Objective(s):

3. Analyze the design aspects of security including threat identification and risk assessment.
4. Employ best practices and guidelines for developing and verifying effective security policies and procedures, security goals, threats and vulnerabilities, standards and security policy development, forensics, privacy implications, and ethics.
5. Determine the different ways of securing Communication and the various threat agents.

Module Learning Objectives:

- Identify the differences among firewalls and their vulnerabilities.
- Identify the vulnerabilities of virtual private networks (VPNs).

Tasks:

204. Read Chapter 9 - Hacking Network Devices
205. View Chapter 9 Presentation
206. Watch posted videos
207. Post in Chapter 9 Discussion Forum
208. Complete Chapter 9 Report (optional)
209. Post for Discussion 4 - TASKs 4-1 through 4-3
210. Complete Lab Assignment 4
211. Complete Chapter 9 Self-Assessment (optional)
212. Submit Quiz 4
213. Review Additional Resources (optional)

Module 10 - Trojan Horses

Week 5

2/4 - 2/10

Supports Course Learning Objective(s):

7. Inspect different vulnerabilities and measure how these vulnerabilities are exploited by hackers to gain entry into networks as well as to perform privilege escalation.

WEEK/DATES **TOPICS/TASKS**

8. Synthesize and evaluate Intrusion Detection, Policy Creation, Social Engineering, DDoS Attacks, Buffer Overflows and Virus Creation.
9. Analyze and evaluate severity levels and possible fixes to remediate the uncovered issues and be able to provide comprehensive solutions.

Module Learning Objectives:

- Describe the main characteristics used by recent Trojan horse attacks.
- List ways in which Trojan horses are deployed.

Tasks:

216. Read Chapter 10 - Trojan Horses
217. View Chapter 10 Presentation
218. Post in Chapter 10 Discussion Forum
219. Complete Chapter 10 Report (optional)
220. Complete Chapter 10 Self-Assessment (optional)
221. View Additional Resources (optional)

Module 11 - Denial-of-Service Attacks

Supports Course Learning Objective(s):

7. Inspect different vulnerabilities and measure how these vulnerabilities are exploited by hackers to gain entry into networks as well as to perform privilege escalation.
8. Synthesize and evaluate Intrusion Detection, Policy Creation, Social Engineering, DDoS Attacks, Buffer Overflows and Virus Creation.
9. Analyze and evaluate severity levels and possible fixes to remediate the uncovered issues and be able to provide comprehensive solutions.

Module Learning Objectives:

- Explain what a denial-of-service (DoS) attack is and what it accomplishes.
- Describe several varieties of DoS attacks.

Tasks:

224. Read Chapter 11 - Denial-of-Service Attacks
225. View Chapter 11 Presentation
226. Post in Chapter 11 Discussion Forum

WEEK/DATES	TOPICS/TASKS
	227. Complete Chapter 11 Report (optional) 228. Post for Discussion 5 - TASKs 5-1 through 5-4 229. Complete Chapter 11 Self-Assessment (optional) 230. Submit Quiz 5 231. View Additional Resources (optional)
	Module 12 - Buffer Overflow **Supports Course Learning Objective(s):** 7. Inspect different vulnerabilities and measure how these vulnerabilities are exploited by hackers to gain entry into networks as well as to perform privilege escalation. 8. Synthesize and evaluate Intrusion Detection, Policy Creation, Social Engineering, DDoS Attacks, Buffer Overflows and Virus Creation. 9. Analyze and evaluate severity levels and possible fixes to remediate the uncovered issues and be able to provide comprehensive solutions. **Module Learning Objectives:** o Define what a buffer overflow attack is. o Identify a few C functions that are susceptible to buffer over attacks. o Identify the techniques used to avoid buffer overflows.
Week 6 **2/11 - 2/17**	**Tasks:** 235. Read Chapter 12 - Buffer Overflows 236. View Chapter 12 Presentation 237. Post in Chapter 12 Discussion Forum 238. Complete Chapter 12 Report (optional) 239. Complete Chapter 12 Self-Assessment (optional) 240. View Additional Resources (optional)
	Module 13 - Programming Exploits **Supports Course Learning Objective(s):** 7. Inspect different vulnerabilities and measure how these vulnerabilities are exploited by hackers to gain entry into networks as well as to perform privilege escalation. 8. Synthesize and evaluate Intrusion Detection, Policy Creation, Social Engineering, DDoS Attacks, Buffer Overflows and Virus Creation.

WEEK/DATES	TOPICS/TASKS
	9. Analyze and evaluate severity levels and possible fixes to remediate the uncovered issues and be able to provide comprehensive solutions. **Module Learning Objectives:** Module Learning Objectives: o Recognize vulnerabilities associated with ActiveX components. o Recognize vulnerabilities in scripting languages like VBscript. **Tasks:** 243. Read Chapter 13 - Programming Exploits 244. View Chapter 13 Presentation 245. Read Smash the Stack for Fun and Profit document 246. Watch posted video 247. Post in Chapter 13 Discussion Forum 248. Complete Chapter 13 Report (optional) 249. Post for Discussion 6 - TASKs 6-1 and 6-2 250. Complete Lab Assignment 5 251. Complete Chapter 13 Self-Assessment (optional) 252. Submit Quiz 6 253. View Additional Resources (optional) **Module 14 - Mail Vulnerabilities** **Supports Course Learning Objective(s):** 7. Inspect different vulnerabilities and measure how these vulnerabilities are exploited by hackers to gain entry into networks as well as to perform privilege escalation. 9. Analyze and evaluate severity levels and possible fixes to remediate the uncovered issues and be able to provide comprehensive solutions.
Week 7 **2/18 - 2/24**	**Module Learning Objectives:** o Define SMTP vulnerabilities. o Outline Microsoft Exchange server vulnerabilities (POP and IMAP). **Tasks:** 256. Read Chapter 14 - Mail Vulnerabilities 257. View Chapter 14 Presentation 258. Complete Chapter 14 Report (optional)

WEEK/DATES **TOPICS/TASKS**

259. Complete Chapter 14 Self-Assessment (optional)
260. View Additional Resources (optional)

Module 15 - Web Application Vulnerabilities

Supports Course Learning Objective(s):

7. Inspect different vulnerabilities and measure how these vulnerabilities are exploited by hackers to gain entry into networks as well as to perform privilege escalation.
9. Analyze and evaluate severity levels and possible fixes to remediate the uncovered issues and be able to provide comprehensive solutions.

Module Learning Objectives:

- Recognize the factors that impact Web server vulnerabilities.
- Discuss ways and tools used to exploit Web servers vulnerabilities.

Tasks:

263. Read Chapter 15 - Web Application Vulnerabilities
264. View Chapter 15 Presentation
265. Watch posted videos
266. Post in Chapter 15 Discussion Forum
267. Complete Chapter 15 Report (optional)
268. Post for Discussion 7 - TASKs 7-1 and 7-2
269. Begin Lab Assignment 6
270. Complete Chapter 15 Self-Assessment (optional)
271. Submit Quiz 7
272. View Additional Resources (optional)
273. Complete Final Exam (Available 2/22, 12:00 am - Due 2/23, 11:59 pm)
274. Submit Group Research / Project Final Paper (Available 2/18, 12:00 am - Due 2/24, 11:59 pm)
275. Submit Group Research / Project Presentation (Available 2/18, 12:00 am - Due 2/24, 11:59 pm)