American Public University System
American Military University | American Public University

ISSC262

Course Summary

Course : ISSC262 **Title :** Red and Blue Team Security
Length of Course : 8
Prerequisites : N/A **Credit Hours :** 3

Description

Course Description:

This course examines the techniques and technologies for penetration of networks, detection of attacks, and prevention of attacks. This course addresses the techniques, the technologies, and the methodologies used by cyber intruders (hackers) to select a target and launch an attack. Students will gain insight into the motives and desired goals of hackers as well as effective tools and techniques used as countermeasures ensuring data assets remain secure. This course focuses on techniques and technologies to detect such attacks even while the attack is in progress; early detection enables the administrator to track the movements of the hacker and to discover the intent and goals of the hacker. This course assesses the various countermeasures to keep the system out of the “sights” of the hacker and to keep the hacker out of the perimeter of the target network. This course also explores the laws and the legal considerations in prosecuting computer crime.

Course Scope:

This course will allow students to see how attacks target networks and the methodology they follow. Students will also learn how to respond to hacking attacks and how to fend them off. With the help of the experts in the Information Systems Security and Assurance Series, the book will provide examples of information security concepts and procedures are presented throughout the course.

Objectives

After successfully completing this course, you will be able to:

1. Show how attackers map organizations
2. Describe common port scanning techniques
3. Identify some of the tools used to perform enumeration
4. Explain the significance of wireless security
5. List the issues facing Web servers
6. Describe the characteristics of malware
7. List the ways of detecting Trojans
8. Describe the process of DoS attacks
9. Describe the benefits of automated assessment tools
10. List the components of incident response
11. List the detective methods of IDS

Outline

Week 1: Course Overview Getting Started Introduction to Ethical Hacking

Activities

Reading: Chapters 1, 2, 3 and 4

PPT Review: Lessons 1, 2 and 3 (Physical Security)

Week 1 Discussion

Lab

Week 2: Footprinting, Port Scanning and Enumeration

Activities

Reading: Chapters 5, 6, and 7

PPT Review: Lessons 3 (Footprinting) and 4

Week 2 Discussion

Lab

Week 3: Web and Database Attacks

Activities

Reading: Chapter 9

PPT Review: Lesson 6

Week 3 Discussion

Lab

Week 4: Malware, Worms, Viruses, Trojans and Backdoors

Activities

Reading: Chapters 10 and 11

PPT Review: Lesson 7

Week 4 Discussion

Lab

Week 5: Network Traffic Analysis

Activities

Reading: Chapters 12 and 13

PPT Review: Lesson 8

Week 5 Discussion

Midterm

Lab

Week 6: Wireless Vulnerabilities

Activities

Reading: Chapter 8

PPT Review: Lesson 5

Week 6 Discussion

Lab

Week 7: Incident Response

Activities

Reading: Chapter 14

PPT Review: Lesson 9 (Incident Response)

Week 7 Discussion

Week 7 Research Paper Due

Lab

Week 8: Defensive Technologies

Activities

Reading: Chapter 15

PPT Review: Lesson 9 (Defense Technologies)

Week 8 Discussion

Final Exam

Lab

Evaluation

Grading will be based on weekly assignments: discussions labs, quizzes, an individual project paper (topic selection, outline and paper) and a case study.

- There will be **eight discussions** (3.13% each) counting a total of 25% of the final grade. Answers should restate the question with supporting sentences using the terms, concepts, and theories from the required readings. The key requirement is to express your idea and then support your position to demonstrate that you understand the material.

In addition, you are to **respond** to at least **two** of your classmates' postings by critiquing, supporting or supplementing the other students' answers. All responses should be courteous with sound supporting sentences. You may respond multiple times within a continuous discussion with points and counter points. Duplicate responses **will not** receive credit.

- There will be **eight labs** (2.5% for each) counting a total of 25% of the final grade. You can access labs by selection on **Online Labs**. Step-by-Step instructions for each lab are available, and you can access these files within **Lessons**. Submit deliverables through the **Assignments** link within your course.
- There will be **one final exam** (25 questions worth 4 points per question) and **one Midterm exam** (25 questions worth 4 points per question) accounting for a total of 25% of the final grade. Each exam will consist of 25 multiple choice questions pulled from chapters covered from week 1 through 5 for the Midterm and Weeks 1 through 8 for the Final exam.
- There will be **three exercises** during this term counting a total of 25% of the final grade, completed as follows:

a. Week 2 Topic Selection – selection of topic for the Week 7 Research Paper.
b. Week 4 Outline – outline of topics and subtopics for the Week 7 Research Paper.
c. Week 7 Research Paper – present research paper on your chosen topic.

Below is a list of pre-approved topics for the Week 7 Research Paper:

- Protecting IT: A Roadmap for Securing the Enterprise
- Best Practices for Network Security
- Firewalls: Great Network Security Devices, but Not a "Silver Bullet" Solution
- Modern Day Attacks Against Firewalls and VPNs
- VPN Security Vulnerabilities Exposed

The key to the research assignment is to demonstrate your understanding of the topics, not to re-word the text or reference material.

The paper will follow a conventional report format (introduction, body, conclusion, references). The paper is to follow the APA style guide, Sixth Edition (available via bookstores). Also refer to APA's online resources: and the APUS web site:

Note: Review **Announcements** and **Lessons** for additional instructions and course materials.

- Each week you will also have chapter readings assigned, and PowerPoint presentations to review.

All assignments, labs, discussion questions and quizzes are required by 11:59 PM Eastern Standard Time of the Sunday of the week assigned.

Grading:

Name	Grade %
Discussions	25.00 %
Week 1 Discussion	3.13 %
Week 2 Discussion	3.13 %
Week 3 Discussion	3.13 %
Week 4 Discussion	3.13 %
Week 5 Discussion	3.13 %
Week 6 Discussion	3.13 %
Week 7 Discussion	3.13 %
Week 8 Discussion	3.13 %
Labs	25.00 %
Week 1 Lab	3.13 %
Week 2 Lab	3.13 %
Week 3 Lab	3.13 %
Week 4 Lab	3.13 %
Week 5 Lab	3.13 %
Week 6 Lab	3.13 %
Week 7 Lab	3.13 %
Week 8 Lab	3.13 %
Quizzes/Exams	25.00 %
ISSC262 Final Exam	12.50 %
ISSC262 Midterm Exam	12.50 %
Exercises	25.00 %
Week 2 Topic Selection	2.50 %
Week 4 Outline	7.50 %
Week 7 Research Paper	15.00 %

Materials

Book Title: Requires CITRIX CLIENT SOFTWARE INSTALLATION FOR ONLINE VIRTUAL LABS accessibility - instructions provided inside the classroom.

Author: No Author Specified

Publication Info:

ISBN: N/A

Book Title: Hacker Techniques, Tools, And Incident Handling, 2nd ed. - the VitalSource e-book is provided inside the classroom

Author: Oriyano

Publication Info: VS-Jones & Bartlett

ISBN: 9781284031713

Book Title: ISSC262 virtual lab manual provided inside the classroom

Author:

Publication Info: CLASS-Jones & Bartlett

ISBN: 9781284064100

Starting April 2016 this title & edition has moved to VitalSource. The VitalSource e-book is provided via the APUS Bookstore. Please visit for more information.

Software Requirements

1. Microsoft Office (MS Word, MS Excel, MS PowerPoint)
2. Mozilla Firefox (recommended browser)

Course Guidelines

Citation and Reference Style

- Attention Please: Students will follow the APA Format as the sole citation and reference style used in written work submitted as part of coursework to the University. Assignments completed in a narrative essay or composition format must follow the citation style cited in the APA Format.

Tutoring

- Tutor.com offers online homework help and learning resources by connecting students to certified tutors for one-on-one help. AMU and APU students are eligible for 10 free hours* of tutoring provided by APUS. Tutors are available 24/7 unless otherwise noted. Tutor.com also has a SkillCenter Resource Library offering educational resources, worksheets, videos, websites and career help. Accessing these resources does not count against tutoring hours and is also available 24/7. Please visit the APUS Library and search for 'Tutor' to create an account.

Late Assignments

- Students are expected to submit classroom assignments by the posted due date and to complete the course according to the published class schedule. The due date for each assignment is listed under

each Assignment.
- Generally speaking, late work may result in a deduction up to 15% of the grade for each day late, not to exceed 5 days.
- As a working adult I know your time is limited and often out of your control. Faculty may be more flexible if they know ahead of time of any potential late assignments.

Turn It In

- Faculty may require assignments be submitted to Turnitin.com. Turnitin.com will analyze a paper and report instances of potential plagiarism for the student to edit before submitting it for a grade. In some cases professors may require students to use Turnitin.com. This is automatically processed through the Assignments area of the course.

Academic Dishonesty

- Academic Dishonesty incorporates more than plagiarism, which is using the work of others without citation. Academic dishonesty includes any use of content purchased or retrieved from web services such as CourseHero.com. Additionally, allowing your work to be placed on such web services is academic dishonesty, as it is enabling the dishonesty of others. The copy and pasting of content from any web page, without citation as a direct quote, is academic dishonesty. When in doubt, do not copy/paste, and always cite.

Submission Guidelines

- Some assignments may have very specific requirements for formatting (such as font, margins, etc) and submission file type (such as .docx, .pdf, etc) See the assignment instructions for details. In general, standard file types such as those associated with Microsoft Office are preferred, unless otherwise specified.

Disclaimer Statement

- Course content may vary from the outline to meet the needs of this particular group.

Communicating on the Discussion

- Discussions are the heart of the interaction in this course. The more engaged and lively the exchanges, the more interesting and fun the course will be. Only substantive comments will receive credit. Although there is a final posting time after which the instructor will grade comments, it is not sufficient to wait until the last day to contribute your comments/questions on the discussion. The purpose of the discussions is to actively participate in an on-going discussion about the assigned content.
- "Substantive" means comments that contribute something new and hopefully important to the discussion. Thus a message that simply says "I agree" is not substantive. A substantive comment contributes a new idea or perspective, a good follow-up question to a point made, offers a response to a question, provides an example or illustration of a key point, points out an inconsistency in an argument, etc.
- As a class, if we run into conflicting view points, we must respect each individual's own opinion. Hateful and hurtful comments towards other individuals, students, groups, peoples, and/or societies will not be tolerated.

Identity Verification & Live Proctoring

- Faculty may require students to provide proof of identity when submitting assignments or completing assessments in this course. Verification may be in the form of a photograph and/or video of the student's face together with a valid photo ID, depending on the assignment format.
- Faculty may require live proctoring when completing assessments in this course. Proctoring may include identity verification and continuous monitoring of the student by webcam and microphone during testing.

University Policies

Student Handbook

- Drop/Withdrawal policy
- Extension Requests
- Academic Probation
- Appeals
- Disability Accommodations

The mission of American Public University System is to provide high quality higher education with emphasis on educating the nation's military and public service communities by offering respected, relevant, accessible, affordable, and student-focused online programs that prepare students for service and leadership in a diverse, global society.