

STUDENT WARNING: This course syllabus is from a previous semester archive and serves only as a preparatory reference. Please use this syllabus as a reference only until the professor opens the classroom and you have access to the updated course syllabus. Please do NOT purchase any books or start any work based on this syllabus; this syllabus may NOT be the one that your individual instructor uses for a course that has not yet started. If you need to verify course textbooks, please refer to the online course description through your student portal. This syllabus is proprietary material of APUS.

American Public University System

The Ultimate Advantage is an Educated Mind

School of Science and Technology
Department of Information Technology
ISSC461: IT Security: Countermeasures
3 Credit Hours
Length of Course: 8 weeks
Prerequisite(s): None

Table of Contents

Instructor Information	Evaluation Procedures
Course Description	Grading Scale
Course Scope	Course Outline
Course Objectives	Policies
Course Delivery Method	Academic Services
Resources	Selected Bibliography

Instructor Information

Instructor:
Email:
Phone:
Office Hours:

[Table of Contents](#)

Course Description (Catalog)

This course is a study of Network Security attacks and countermeasures. This course examines various security technologies, such as: intrusion detection, authentication, session hijacking, sniffing, spoofing, denial of service, buffer overflow attack, port scanning, encryption, IPSec, DES encryption, triple DES encryption, message digest 5 algorithm, point-to-point tunneling protocol (PPTP), layer 2 tunneling protocol (L2TP), Kerberos, RSA Pretty Good Privacy(PGP), Secure Shell (SSH), Secure Sockets Layer (SSL), Stateful Packet Inspection (SPI), Network Address Translation (NAT), proxies, content filters, public/private keys, Public Key Infrastructure (PKI), Virtual Private Networks (VPN), security policies, security tokens, digital certificates, viruses, worms, Trojan horses, virus scanners, virus protection, vulnerability assessment, and vulnerability scanners.

[Table of Contents](#)

Course Scope

This course is one in a series of courses on IT security; it examines the threat from computer hackers and the countermeasures to protect against such attacks. These countermeasures include security policies, security hardware and software technologies, vulnerability analysis, security assessments, penetration testing, and vulnerability scanners. The course will cover introduction to Network Security, types of

STUDENT WARNING: This course syllabus is from a previous semester archive and serves only as a preparatory reference. Please use this syllabus as a reference only until the professor opens the classroom and you have access to the updated course syllabus. Please do NOT purchase any books or start any work based on this syllabus; this syllabus may NOT be the one that your individual instructor uses for a course that has not yet started. If you need to verify course textbooks, please refer to the online course description through your student portal. This syllabus is proprietary material of APUS.

Attacks, fundamentals of Firewalls, Firewall Practical Applications, Intrusion Detection Systems, Encryption, Virtual Private Networks, Operating System Hardening, Defending against Virus Attacks, Trojan Horses and Spyware, Security Policies, Assessing a System, Security Standards, Computer-based Espionage and Terrorism.

[Table of Contents](#)

Course Objectives

The successful student will fulfill the following learning objectives:

1. Evaluate the various types of security attacks and exploits; also examine the process used by hackers to launch an attack.
2. Profile the various types of security policies; also appraise the domain, objective, and scope of each type of policy.
3. Appraise various security technologies, such as: packet filtering, Stateful Packet Inspection (SPI), proxy technology, Network Address Translation (NAT), Public Key Infrastructure (PKI) authentication, and encryption.
4. Analyze the concept and the functionality of firewall and routers; and illustrate how they implement network security.
5. Evaluate the goals, benefits, and strategies of VPNs; also appraise the scope, advantages, and limitations of the different types of VPNs.
6. Assess the benefits, risks, and layered-defense architecture associated with wireless LANs.
7. Evaluate the functionality, the features, and the limitations of Intrusion Detection Systems (IDS)
8. Discuss the role of security assessments, penetration testing, and security plans in establishing network security.

[Table of Contents](#)

Course Delivery Method

This **IT Security: Countermeasures** course delivered via distance learning will enable students to complete academic work in a flexible manner completely online. Resources and access to an online learning management system will be made available to each student. **Online assignments are due by the last day of each week** and include Forum questions (accomplished in groups through a threaded Forum), examinations and quizzes (graded electronically), and individual assignments (submitted for review by the Faculty Member). Assigned faculty will support the students throughout this eight-week course.

[Table of Contents](#)

Resources

Pleeger, Charles (2012). Analyzing Computer Security: A Threat / Vulnerability / Countermeasure Approach. ISBN: 978-0-13-278946-2. Prentice Hall-Pearson Publication

[Table of Contents](#)

Evaluation Procedures

Evaluation Criteria

Course Requirements: Your final grade will be based on the following course requirements and percentages:

<i>Course Requirement</i>	<i>Percent</i>
8 Forums (4 Percent Each)	32
Research Paper – Topic	1
1-Page Outline of Research Paper	4
Attack Project Presentation	15

STUDENT WARNING: This course syllabus is from a previous semester archive and serves only as a preparatory reference. Please use this syllabus as a reference only until the professor opens the classroom and you have access to the updated course syllabus. Please do NOT purchase any books or start any work based on this syllabus; this syllabus may NOT be the one that your individual instructor uses for a course that has not yet started. If you need to verify course textbooks, please refer to the online course description through your student portal. This syllabus is proprietary material of APUS.

Research Paper – Rough Draft	8
Research Paper – Final Copy	20
Attack Project Paper	20
Total	100

Assignment Requirements

This course has a strong writing component. The goal is to organize, synthesize, and demonstrate your comprehension of core concepts investigated during this course by applying a combination of the terms, concepts, and details you have learned in a systematic way. As important as "the details" that you analyze and arrange in your writing, however, are the conclusions you draw from those details, and your predictions, responses to, and ultimate interpretation of those details.

FORUM POSTINGS:

Each week a Forum question will be provided for a discussion of the week's readings. A specific assignment for posting on the Forum will be announced each week. The assignments may involve discussion or debate. The number of postings required each week will vary and will be announced in the assignment for the week. In most cases, you will be required to post at least one original post and two follow-ups to your classmates' posts.

Your first post each week must be posted by Wednesday at midnight EST. Please try not to be late with this post because your classmates will be relying on you to post on time to give them a post to respond to later in the week. All follow-up posts must be posted by Sunday at midnight EST.

RESEARCH PAPER:

You will be required to write one research paper this semester. The specifications are as follows:

1. 8-10 pages (double-spaced) Times New Roman 12 pt font.
2. Choose any topic related to the course and write about the latest developments and issues.
3. Use at least five references outside of your textbook (you may use your textbook too, but are not required to).
4. In addition to the required number of pages for the assignment, you must also include a reference page (bibliography), written in **APA style** and a title page. Be sure to give all of your papers a descriptive title!
5. You must get your topic approved by the end of Week 2.
6. You must provide a 1-page outline of your paper by the end of Week 3. Your outline must include citations to three references (other than your textbook) and a brief summary of at least three references that you will use in your paper.
7. You must submit a rough draft at the end of Week 5. This is to be a **complete** paper, meeting the page requirements – not a partially completed paper. Points will be deducted for short or incomplete papers. Your rough draft will not be graded by the rubric, but helpful feedback will be provided to indicate where you are falling short. You may correct any deficiencies before resubmitting your final draft at the end of Week 7.
8. Typewritten in double-spaced format with a readable style and font and submitted inside the electronic classroom (unless classroom access is not possible and other arrangements have been approved by the professor).
9. Page margins Top, Bottom, Left Side and Right Side = 1 inch, with reasonable accommodation being made for special situations
10. Your paper must be in your own words, representing original work. Paraphrases of others' work must include attributions to the authors. **Limit quotations to an average of no more than 3-5 lines, and use quotations sparingly!** It is always better to paraphrase than to directly quote.

Attack Project Paper Vulnerability and Attack Analysis Plan

STUDENT WARNING: This course syllabus is from a previous semester archive and serves only as a preparatory reference. Please use this syllabus as a reference only until the professor opens the classroom and you have access to the updated course syllabus. Please do NOT purchase any books or start any work based on this syllabus; this syllabus may NOT be the one that your individual instructor uses for a course that has not yet started. If you need to verify course textbooks, please refer to the online course description through your student portal. This syllabus is proprietary material of APUS.

For this course you will assess an organization, collect information, pinpoint vulnerabilities and come up with an attack plan that should work in theory. This project is not meant to be carried out but is meant to build a plan that will be used without actually taking the steps to perform the attack.

This project will be performed in two phases, the first will be an outline of the plan with a summary of tasks to be completed. The second is a group paper that will reveal all of the details of the attack.

The Outline of the Attack Plan

Develop an attack plan that covers these criteria:

1. Choose a company/organization for analysis/attack.
2. Give summary information about the organization. Remember, you have to think like an intruder – what information do you think would be relevant?
3. Find tools on the web that could help you find information about systems/networks, etc.. that could be used to find vulnerable points. Remember, you have to find this info, use tools to look for more information and vulnerabilities that you could exploit. Name these tools and what they can do to help.
4. Is social engineering an option here? What methods could you use to gather sensitive information? What questions might you ask? What kind of messages could you send? What are some physical security flaws (if any) do you think would be an option or not relevant?
5. This outline can be presented in a Power Point presentation, complete with illustrations, and references. For illustrations, screenshots can be used to display various techniques you might employ.
6. This presentation should be at least 12-15 slides, any style you wish and must have references to information you use. Keep in mind, this is not meant to be very detailed, this is just an outline of the plan. The details will go in the paper.

The Paper

The Attack Project Paper will be like a report of the analysis and attack strategy.

1. First you will report the information you gathered on the organization.
2. Then you will list the tools, give a details description of each and give a description of how you used it.
3. What sort of attacks would work in this case? Give some examples and how you would carry them out.
4. What social engineering and physical security aspects were discovered/devised? Give a detailed explanation.
5. With all of these methods for finding information, using it to gain access to the organizations systems; what methods could you employ to help secure these vulnerabilities? What suggestions would you make to the organization if you were a penetration tester?

This paper is not a traditional paper since it will look more like a report. However, make sure you format the paper in this way:

1. Title page with the name of the course, name of the project, students name, date and any other relevant information.

STUDENT WARNING: This course syllabus is from a previous semester archive and serves only as a preparatory reference. Please use this syllabus as a reference only until the professor opens the classroom and you have access to the updated course syllabus. Please do NOT purchase any books or start any work based on this syllabus; this syllabus may NOT be the one that your individual instructor uses for a course that has not yet started. If you need to verify course textbooks, please refer to the online course description through your student portal. This syllabus is proprietary material of APUS.

2. Give a summary of what we are about to read (this is like an abstract)
3. Make sure to include a table of contents.
4. Label the criteria in sections to break it up and organize the paper.
5. Make sure to have a reference page.

Grading Scale

Please see the [student handbook](#) to reference the [University's grading scale](#). [Table of Contents](#)

Course Outline

<u>Week</u>	<u>Topic(s)</u>	<u>Learning Objective(s)</u>	<u>Reading(s)</u>	<u>Assignment(s)</u>
1	Introduction to security & Authentication Edit	CO-1	Ch. 1 & 2	Forum Posting Research Paper Topic Due
2	Application Security & Malicious Code	CO-2	Ch. 3 & 4	Forum Posting By now you should have started working on your Attack Plan
3	Access Control & Physical Protection	CO-3	Ch. 5 & 7	Forum Posting Research Paper Annotated Bibliography Due
4	Buffer Overflow & Rootkits	CO-4	Ch. 6 & 8	Forum Posting Attack Project Presentation is Due by the end of Week 4
5	Network Security & Intrusion	CO-5	Ch. 9 & 12	Forum Posting Research Paper Rough Draft Due
6	WiFi, VPNs & Encryption	CO-6	Ch. 10,11 & 16	Forum Posting
7	Web Security Issues & DoS	CO-7	Ch. 13,14 & 15	Forum Posting Research Paper Final Draft Due
8	File Sharing & Social Media Security	CO-8	Ch. 17 & 18	Forum Posting Attack Project Paper Due by end of Week 8

[Table of Contents](#)

Policies

Please see the [student handbook](#) to reference all University policies. Quick links to frequently asked question about policies are listed below.

- [Drop/Withdrawal Policy](#)
- [Plagiarism Policy](#)
- [Extension Process and Policy](#)

WRITING EXPECTATIONS

STUDENT WARNING: This course syllabus is from a previous semester archive and serves only as a preparatory reference. Please use this syllabus as a reference only until the professor opens the classroom and you have access to the updated course syllabus. Please do NOT purchase any books or start any work based on this syllabus; this syllabus may NOT be the one that your individual instructor uses for a course that has not yet started. If you need to verify course textbooks, please refer to the online course description through your student portal. This syllabus is proprietary material of APUS.

All written submissions should be submitted in a font and page set-up that is readable and neat. It is recommended that students try to adhere to a consistent format, which is described below.

- Typewritten in double-spaced format with a readable style and font and submitted inside the electronic classroom (unless classroom access is not possible and other arrangements have been approved by the professor).
- Arial 11 or 12-point font or Times New Roman styles.
- Page margins Top, Bottom, Left Side and Right Side = 1 inch, with reasonable accommodation being made for special situations and online submission variances.

CITATION AND REFERENCE STYLE

Assignments completed in a narrative essay or composition format must follow APA guidelines. This course will require students to use the citation and reference style established by the American Psychological Association (APA), in which case students should follow the guidelines set forth in *Publication Manual of the American Psychological Association* (6th ed.). (2010). Washington, D.C.: American Psychological Association.

APA Tutorial

Please check out this tutorial on APA Style Guidelines. It is a narrative with examples and has proved to be very helpful. Pay special attention to citing. [CLICK HERE](#)

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. As adults, students, and working professionals I understand you must manage competing demands on your time. Should you need additional time to complete an assignment please contact me before the due date so we can discuss the situation and determine an acceptable resolution. Routine submission of late assignments is unacceptable and may result in points deducted from your final course grade. Assignments submitted late without a prearranged extension will be subject to a 10% late penalty. **No late assignments will be accepted after the last day of the course.**

Academic Services

ONLINE LIBRARY RESEARCH CENTER & LEARNING RESOURCES

The Online Library Resource Center is available to enrolled students and faculty from inside the electronic campus. This is your starting point for access to online books, subscription periodicals, and Web resources that are designed to support your classes and generally not available through search engines on the open Web. In addition, the Center provides access to special learning resources, which the University has contracted to assist with your studies. Questions can be directed to orc@apus.edu.

- **Charles Town Library and Inter Library Loan:** The University maintains a special library with a limited number of supporting volumes, collection of our professors' publication, and services to search and borrow research books and articles from other libraries.
- **Electronic Books:** You can use the online library to uncover and download over 50,000 titles, which have been scanned and made available in electronic format.
- **Electronic Journals:** The University provides access to over 12,000 journals, which are available in electronic form and only through limited subscription services.
- **Turnitin.com:** Turnitin.com is a tool to improve student research skills that also detect plagiarism. Turnitin.com provides resources on developing topics and assignments that encourage and guide students in producing papers that are intellectually honest, original in thought, and clear in expression. This tool helps ensure a culture of adherence to the University's standards for intellectual honesty. Turnitin.com also reviews students' papers for matches with Internet materials and with thousands of student papers in its database, and returns an Originality Report to instructors and/or students.

STUDENT WARNING: This course syllabus is from a previous semester archive and serves only as a preparatory reference. Please use this syllabus as a reference only until the professor opens the classroom and you have access to the updated course syllabus. Please do NOT purchase any books or start any work based on this syllabus; this syllabus may NOT be the one that your individual instructor uses for a course that has not yet started. If you need to verify course textbooks, please refer to the online course description through your student portal. This syllabus is proprietary material of APUS.

- **Smarthinking:** Students have access to 10 free hours of tutoring service per year through [Smarthinking](#). Tutoring is available in the following subjects: math (basic math through advanced calculus), science (biology, chemistry, and physics), **accounting, statistics, economics, Spanish**, writing, grammar, and more. Additional information is located in the Online Research Center. From the ORC home page, click on either the “Writing Center” or “Tutoring Center” and then click “Smarthinking.” All login information is available.

Selected Bibliography

- Bejtlich, R. (2005). *Extrusion detection: security monitoring for internal intrusions*. Boston: Addison-Wesley Professional.
- Bejtlich, R. (2004). *The tao of network security monitoring: beyond intrusion detection*. Boston: Addison-Wesley Professional.
- Crothers, T. (2002). *Implementing intrusion detection systems: a hands-on guide for securing the network*. Hoboken, NJ: Wiley.
- Endorf, C., Schultz, G., & Mellander, J. (2003). *Intrusion detection and prevention*. Emeryville, CA: McGraw-Hill Osborne Media.
- Holden, G. (2003). *Guide to firewalls and network security: intrusion detection and vpns*. Boston: Course Technology.
- Jones, K., Bejtlich, R., & Rose, C. (2005). *Real digital forensics: computer security and incident response*. Boston: Addison-Wesley Professional.
- Kruegel, C., Valeur, F., & Vigna, G. (2004). *Intrusion detection and correlation: challenges and solutions*. New York: Springer.
- Northcutt, S., & Novak, J. (2002). *Network intrusion detection*. 3rd ed. Indianapolis, IN: Sams.
- Northcutt, S., Zeltser, L., Winters, S., & Fredrick, K. (2002). *Inside network perimeter security: the definitive guide to firewalls, virtual private networks (vpns), routers, and intrusion detection systems*. Indianapolis, IN: Sams.
- Tulloch, M. (2003). *Microsoft encyclopedia of security*. Redmond, WA: Microsoft Press.

Appendix A – Grading Rubric

All written assignments will be assessed according to this rubric. Note that a score of 0 may be assigned in any category where your work does not meet the criteria for the beginning level.

APUS Assignment Rubric Undergraduate Level 300-400	EXEMPLARY LEVEL 4	ACCOMPLISHED LEVEL 3	DEVELOPING LEVEL 2	BEGINNING LEVEL 1	TOTAL POINTS
FOCUS/THESIS	Student exhibits a defined and clear understanding of the assignment. Thesis is clearly defined and well constructed to help guide the reader throughout the assignment. Student builds upon the thesis of the assignment with well-documented and exceptional supporting facts, figures, and/or statements.	Establishes a good comprehension of topic and in the building of the thesis. Student demonstrates an effective presentation of thesis, with most support statements helping to support the key focus of assignment.	Student exhibits a basic understanding of the intended assignment, but the thesis is not fully supported throughout the assignment. While thesis helps to guide the development of the assignment, the reader may have some difficulty in seeing linkages between thoughts. While student has included a few supporting facts and statements, this has limited the quality of the assignment.	Exhibits a limited understanding of the assignment. Reader is unable to follow the logic used for the thesis and development of key themes. Introduction of thesis is not clearly evident, and reader must look deeper to discover the focus of the writer. Student's writing is weak in the inclusion of supporting facts or statements.	10
CONTENT/SUBJECT KNOWLEDGE	Student demonstrates proficient command of the subject matter in the assignment. Assignment shows an impressive level of depth of student's ability to relate course content to practical examples and applications. Student provides comprehensive analysis of details, facts, and concepts in a logical sequence.	Student exhibits above average usage of subject matter in assignment. Student provides above average ability in relating course content in examples given. Details and facts presented provide an adequate presentation of student's current level of subject matter knowledge.	The assignment reveals that the student has a general, fundamental understanding of the Resource. Whereas, there are areas of some concern in the linkages provided between facts and supporting statements. Student generally explains concepts, but only meets the minimum requirements in this area.	Student tries to explain some concepts, but overlooks critical details. Assignment appears vague or incomplete in various segments. Student presents concepts in isolation, and does not perceive to have a logical sequencing of ideas.	20

CRITICAL THINKING SKILLS	Student demonstrates a higher-level of critical thinking necessary for 300-400 level work. Learner provides a strategic approach in presenting examples of problem solving or critical thinking, while drawing logical conclusions which are not immediately obvious. Student provides well-supported ideas and reflection with a variety of current and/or world views in the assignment. Student presents a genuine intellectual development of ideas throughout assignment.	Student exhibits a good command of critical thinking skills in the presentation of material and supporting statements. Assignment demonstrates the student's above average use of relating concepts by using a variety of factors. Overall, student provides adequate conclusions, with 2 or fewer errors.	Student takes a common, conventional approach in guiding the reader through various linkages and connections presented in assignment. However, student presents a limited perspective on key concepts throughout assignment. Student appears to have problems applying information in a problem-solving manner.	Student demonstrates beginning understanding of key concepts, but overlooks critical details. Learner is unable to apply information in a problem-solving fashion. Student presents confusing statements and facts in assignment. No evidence or little semblance of critical thinking skills.	20
ORGANIZATION OF IDEAS/FORMAT	Student thoroughly understands and excels in explaining all major points. An original, unique, and/or imaginative approach to overall ideas, concepts, and findings is presented. Overall format of assignment includes an appropriate introduction (or abstract), well- developed paragraphs, and conclusion. Finished assignment demonstrates student's ability to plan and organize research in a logical sequence. Student uses at least of 5-7 references in assignment.	Student explains the majority of points and concepts in the assignment. Learner demonstrates a good skill level in formatting and organizing material in assignment. Student presents an above average level of preparedness, with a few formatting errors. Assignment contains less than 5 resources.	Learner applies some points and concepts incorrectly. Student uses a variety of formatting styles, with some inconsistencies throughout the paper. Assignment does not have a continuous pattern of logical sequencing. Student uses less than 3 sources or references.	Assignment reveals formatting errors and a lack of organization. Student presents an incomplete attempt to provide linkages or explanation of key terms. The lack of appropriate references or source materials demonstrates the student's need for additional help or training in this area. Student needs to review and revise the assignment.	20
WRITING CONVENTIONS (GRAMMAR & MECHANICS)	Student demonstrates an excellent command of grammar, as well as presents research in a clear and concise writing style. Presents a thorough, extensive	Student provides an effective display of good writing and grammar. Assignment reflects student's ability to select appropriate word usage	Assignment reflects basic writing and grammar, but more than 5 errors. Key terms and concepts are somewhat vague and not completely explained by	Topics, concepts, and ideas are not coherently discussed or expressed in assignments. Student's writing style is weak and needs	20

	understanding of word usage. Student excels in the selection and development of a well-planned research assignment. Assignment is error-free and reflects student's ability to prepare a high-quality academic assignment.	and present an above average presentation of a given topic or issue. Assignment appears to be well written with no more than 3-5 errors. Student provides a final written product that covers the above-minimal requirements.	student. Student uses a basic vocabulary in assignment. Student's writing ability is average, but demonstrates a basic understanding of the subject matter.	improvement, along with numerous proofreading errors. Assignment lacks clarity, consistency, and correctness. Student needs to review and revise assignment.	
USE OF COMPUTER TECHNOLOGY/ APPLICATIONS	Student provides a high-caliber, formatted assignment. Learner exhibits excellent use of computer technology in the development of assignment. Quality and appropriateness of stated references demonstrate the student's ability to use technology to conduct applicable research. Given assignment includes appropriate word processing, spreadsheet and/or other computer applications as part of the final product.	Assignment presents an above-average use of formatting skills, with less than 3 errors. Students has a good command of computer applications to format information and/or figures in an appropriate format. Student uses at least two types of computer applications to produce a quality assignment.	Student demonstrates a basic knowledge of computer applications. Appearance of final assignment demonstrates the student's limited ability to format and present data. Resources used in assignment are limited. Student may need to obtain further help in the use of computer applications and Internet research.	Student needs to develop better formatting skills. The student may need to take additional training or obtain help from the Educator Help Desk while preparing an assignment. Research and resources presented in the assignment are limited. Student needs to expand research scope. The number of formatting errors is not acceptable.	10
TOTAL POINTS					100