American Public University System

The Ultimate Advantage is an Educated Mind

School of Science and Technology
Department of Information Technology
ISSC344: Open Source System Security
3 Credit Hours
8 Week Course
Prerequisite(s): None

Table of Contents

Instructor Information

Instructor: (Bio)
Email:
Office Hours:

Course Description (Catalog)

This course is an introductory study of the principles, practices, procedures, and methodologies to provide security on Linux systems. It assesses the security risks, threats and vulnerabilities related to individual and enterprise Linux environments. Course topics include: user privileges and permissions, file systems volumes and encryption and kernel security risk mitigation.

Course Scope

This course covers various security aspects of Linux as a network operating system. The risks, threats and vulnerabilities associated with Linux are explained. Practices for taking advantage of the layers of security in Linux, and building a layered security strategy for Linux environments are presented. A set of hands-on laboratories are performed online to strengthen learning and acquire practical skills.

Course Objectives

The successful student will fulfill the following learning objectives:

CO-1: Analyze the Basic Components of Linux Security

CO-2: Examine Networked File systems and Remote Access

CO-3: Apply security to Networks, Firewalls, and Applications

CO-4: Identify the components in a layered Linux Security Strategy

CO-5: Develop Best Practices for Emerging Technologies

CO-6: Create Testing and Reporting plans

Course Delivery Method

This is an 8-week course delivered online in the APUS Sakai classroom. A faculty member is assigned to support the students throughout the 8-week course. Lecture slides for the weekly lessons are available in the classroom for students to download. Students must complete 4 laboratory assignments online by logging into a Linux virtual lab environment accompanying the textbook. The lab manual is available in the classroom for students to download. Students are responsible for actively participating in the weekly discussion forums, performing the lab activities, answering review questions in a set of assignments, and taking two one-hour quizzes.

Resources

Required Textbook

Jang, Michael (2011) *Security Strategies in Linux Platforms and Applications,* Jones & Bartlett Learning. ISBN: 978-0-7637-9189-6

Laboratory Manual to accompany Security Strategies in Linux Platforms and Applications, Jones & Bartlett Learning

References

Terpstra , J. et al. (2004*). Hardening Linux*. New York, New York: McGraw-Hill/Osborne

Siddiqui, S. (2002). Linux Security. Premier Press

Kabir, M.J. (2002). *Red Hat Linux Security and Optimization*. John Wiley & Sons

Krishnamurthy, M. (2008). *How to Cheat at Securing Linux*. Singress Publishing

Barret, D., Byrnes, R., Silverman, R. (2003). *Linux Security Cookbook*. O'Reilly

Schryen, G. (2011). *Is Open Source Security a Myth?* Communications of the ACM, 54, 5, 130-140

Turnbull, J. (2005). Hardening Linux. New York, NY:Springer-Verlag

Web-based Readings

Odhner, N. (2005). *Security in Open Source Environments.* Retrieved from http://www.faulkner.com.ezproxy2.apus.edu/products/securitymgt/

Green, A. (2003). Linux Security. Retrieved from: http://www.faulkner.com.ezproxy2.apus.edu/products/securitymgt/

Mearian, L. (2002). Wall St. leans toward Linux. *Computerworld*. Retrieved from http://www.computerworld.com/s/article/75271/Wall_St._leans_toward_Linux

Wyk, K. V. (2007). Linux vs. Windows: which is most secure? Retrieved from http://www.esecurityplanet.com/views/article.php/3665801/Linux-vs-Windows-Which-is-Most-Secure.htm

Haas, J. (2011) Linux, the ultimate UNIX. Retrieved from http://linux.about.com/cs/linux101/a/linux_2.htm

Noyes, K. (2010). Why Linux is more secure than Windows. Retrieved from http://www.pcworld.com/businesscenter/article/202452/why_linux_is_more_secure_than_windows.html

LinuxQuestions.org (2010). Sample squid proxy log files. Retrieved from: http://www.linuxquestions.org/questions/linux-server-73/sample-squid-proxy-log-files-837345

Fenzi, K., Wreski, D. (2004). Linux Security HOWTO. Retrieved from: http://www.tldp.org/HOWTO/Security-HOWTO/

Gite, V. (2009). 20 Linux Server Hardening Security Tips. Retrieved from: http://www.cyberciti.biz/tips/linux-security.html

LinuxLinks (2012). 80 of the Best Linux Security Applications. Retrieved from: http://www.linuxlinks.com/article/20080429140249467/Security.html

Chavakin, A. (n.d.). *FTP Attack Case Study Part I: The Analysis*. Retrieved from http://www.linuxsecurity.com/content/view/117644/49/

Chavakin, A. (n.d.). FTP Attack Case Study Part II: the Lessons. Retrieved from: http://www.linuxsecurity.com/content/view/117696/

Fox, M., Giordano, J., Stotler, L.,Thomas, A. (n.d.). *SELinux and grsecurity: A Case Study Comparing Linux Security Kernel Enhancements*. Retrieved from: http://www.cs.virginia.edu/~jcg8f/GrsecuritySELinuxCaseStudy.pdf

Cruz, V. (2005). Linux and Security at Salem Hospital: A Case Study. Retrieved from: http://www.linuxjournal.com/article/8014

Harris, S. (2005). Telecommunications and Networking Security. In All In One CISSP. Emeryville, California: McGraw-Hill/Osborne.

Software Requirements

1. Microsoft Office (MS Word, MS Excel, MS PowerPoint)
2. Adobe Acrobat Reader (Click here for free download)

3. TargetRedHat01 VM and the vWorkstation Virtual environment

Evaluation Procedures

The course has a strong laboratory component. Students must complete a set of lab activities using the online TargetRedHat01 VM environment. The grading will be based on four graded assignments, eight weekly Forum discussions, four laboratory assignments, and two open-book quizzes.

1. There will be **four assignments (5% each) counting a total of 20% of the final grade**. The assignments will follow each of the major milestones of the course. These assignments are drawn from Lesson Reviews in the textbook. They are selected to provide the student with information to understand the concepts discussed. Assignments should be prepared in Microsoft Word and uploaded into the student folder by the due date.
2. There will be **eight weekly Forum discussions you will need to respond to**. Answers should be 3-4 paragraphs with a **topic sentence** that **restates the question** and **supporting sentences** using the terms, concepts, and theories from the required readings. Each answer should be a **minimum of 250 - 400 words** (about 6 to 8 good sentences). You may **attack**, **support** or **supplement** other students' answers using the terms, concepts and theories from the required readings. All responses should be a **courteous paragraph** that contains a **topic sentence** with good **supporting sentences**. You may respond multiple times with a continuous discussion with points and counter points. The key requirement is to express your idea and then **support your position** using the terms, concepts and theories from the required readings to demonstrate to me that you understand the material. The Forum postings will count as **24%** (3% for each discussion posting) of the final grade.
3. There will be four laboratory assignments throughout the course **(28%)**. These labs are important activities, and are contained in the lab manual accompanying the textbook. Students follow the lab procedures described in the Lab manual. The lab manual is available in electronic form for students to download.
4. There will be a term paper which counts as **12%** of the final grade.
5. There will be a one hour long and non-proctored quiz in Week 8 which counts as **16%** of the final grade. It will be a combination of multiple-choice and true-false and will be open book and open note.

All assignments, labs, Forum question responses, and the quiz are due by 12:00 midnight Eastern Time Sunday of the week assigned.

Grade Instruments	Points Possible	% of Final Grade
Assignments (Weeks 1, 3, 5, 7) (5 points each)	**20**	**20%**
Forum Discussions (Weeks 1 to 8) (3 points each)	**24**	**24%**
Quiz (Week 4)	**16**	**16%**
Paper topic (Week 1)	**1**	**1%**
Paper outline (Week 3)	**1**	**1%**

Paper (Week 7)	**10**	**10%**
Lab assignments (Weeks 2, 4, 6, 8)	**28**	**28%**
TOTAL	**100 Points**	**100%**

Project Paper (Topic, Outline, and Paper)
Week 1: topic selection due
Week 3: outline due
Week 7: Paper due

The paper may be of type:

- Traditional narrative (on a subject related to open-source (Linux) security)
- Case study (analysis, design, or implementation of a security aspect of Linux)

A list of suggested topics will be provided to the students via class announcement and Messages (in Week 1)

Details of Project Paper (12%):
Prepare a 10-15 page paper in Microsoft Word in APA format (see writing expectations in the Policies section). Include at least 10 references.

You may use resources from the APUS Online Library, any library, government library, or any peer-reviewed reference (Wikipedia and any other publicly-reviewed source is not accepted). The paper must by at least 10 pages double-spaced, 1" margin all around, black12 point fonts (Times New Roman or Arial) with correct citations of all utilized references/sources, (pictures, graphics, etc... are extra - allowed but extra for the minimum page count). The title page and references are also required but don't count in the minimum page count. A minimum of 10 references are needed.

Turnitin. The paper will be subjected to checking against plagiarism. The paper must follow acceptable originality criteria (no more than 15% max total, and 2% per individual source match are allowed).

Save the file using the following file naming convention: ISSC344_Project_First_Last.doc(x) (where first and last are your first and last names resp.) and submit the file in this assignment area
Here are the originality report requirements:
1.The originality report must be less than 15% match
2.No single source shall be above 2%
3.You must submit the originality report with your paper to your AMU classroom

If you don't follow these three requirement instructions you will get a 0 for your project paper assignment. You will have the chance to rework your papers until an acceptable level of match is achieved.
If turnitin.com matches more than 40% you may be subject to academic reporting.

Grading Scale

Please see the student handbook to reference the University's grading scale.

Course Outline

Week	Topics	Learning Objectives	Reading(s)	Graded Assignment(s)
1	Security threats in Linux	CO1	Chapter 1 Lesson 1 slides	Forum: DQ#1 Week 1 Assignment Paper Topic
2	Linux security: components and facilities	CO1	Chapters 2, 3 Lesson 2 slides	Forum: DQ#2 Week 2 Lab
3	User privileges and permissions	CO2	Chapter 4, Lesson 3 slides	Forum: DQ#3 Week 3 Assignment Paper Outline
4	File systems, volumes, encryption	CO2	Chapter 5, Lesson 4 slides	Forum: DQ#4 Week 4 Assignment Quiz
5	Networks, firewalls, SELinux	CO3	Chapter 7 Lesson 5 slides	Forum: DQ#5 Week 5 lab
6	Networked filesystems & remote access	CO3, C04	Chapter 8 Lesson 6 slides	Forum: DQ#6 Week 6 Assignment
7	Networked application security	CO4-CO5	Chapter 9 Lesson 7 slides	Forum: DQ#7 Week 7 lab Paper
8	Testing & reporting; best practices for emerging technologies	CO5-CO6	Chapters 13, 15 Lesson 8 slides	Forum: DQ#8 Week 8 Assignment

Policies

TOC

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

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.

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

TOC

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.
- ***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

TOC

Baclit, R., Sicam C., Membrey P., Newbigin, J. (2009). *Foundation of CentOs Linux:Enterprise Linux on the Cheap*. Apress

Petersen, R. (2008). *Linux: The Complete Reference*. 6th edition, McGraw-Hill/Osborne

Greiner, L. (2011). Linux-Based Application Development. Retrieved from http://www.faulkner.com.ezproxy1.apus.edu/products/faccts/

Rash, M. (2007). *Linux firewalls: attack detection and response with iptables, psad, and fwsnort.* [electronic resource], San Francisco: No Starch Press. Available at: http://library.books24x7.com.ezproxy1.apus.edu/toc.asp?bookid=23672

Koconis, D. (2003). *Securing Linux: a survival guide for Linux security*. Bethesda, MD: SANS Press. Available at http://library.books24x7.com.ezproxy1.apus.edu/toc.asp?bookid=8451

Mookhey, K.K., Burghate, N. (2005). Linux: Security, audit and control features. Rolling Meadows, Ill.: Information Systems Audit and Control Association. Available at: http://library.books24x7.com.ezproxy1.apus.edu/toc.asp?bookid=30839

Sutherland, E. (2012). Protecting NASA from hackers is not rocket science, say analysts.*Technewsworld*. Retrieved from http://www.technewsworld.com/story/Protecting-NASA-From-Hackers-Is-Not-Rocket-Science-Say-Analysts-74569.html

Harris, S. (2005). Telecommunications and Networking Security. In All In One CISSP. Emeryville, California: McGraw-Hill/Osborne.

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**	**BEGINNNIG 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 concerning 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