SEU CS566: Securing the Enterprise Infrastructure with Cyber Security Techniques

Credit Hours: 3

Contact Hours: This is a 3-credit course, offered in a 14-week format. The exact number of hours per week that you can expect to spend on each course will vary based upon the weekly coursework, as well as your study style and preferences. You should plan to spend 8-12 hours per week in each course reading material, interacting on the discussion boards, writing papers, completing projects, and doing research.

Faculty Information

Faculty contact information and office hours can be found on the faculty profile page.

Course Description and Outcomes

Course Description:

The course reinforces cyber security methods in critical infrastructures equipping students with the knowledge and hands on experience of protecting large Windows Based infrastructure services. Students will also gain insight into complex cyber security system design, deployment, and ongoing maintenance. Holistic security techniques will be covered to provide complete system and enterprise security. Patch management and vulnerability detection for Windows-based systems is also discussed.

Course Learning Outcomes:

1. Explain information security and how it applies to the Microsoft Windows operating systems.
2. Describe native security features of the Microsoft Windows operating systems.
3. Implement secure access controls for a given enterprise environment.
4. Define and apply Group Policy controls in Microsoft Windows.
5. Design techniques to protect enterprise networks from security vulnerabilities.
6. Develop an enterprise security administration framework to ensure your organization meets its security policy goals.
7. Identify and implement the most effective security controls to make computers and networks as secure as possible.
8. Apply best practices to securing enterprise computers, networks, and applications.

Participation & Attendance

Prompt and consistent attendance in your online courses is essential for your success. If for some reason you would like to drop a course, please contact Saudi Electronic University.

Online classes have deadlines, assignments, and participation requirements just like on-campus classes. Budget your time carefully and keep an open line of communication with your instructor. If you are having technical problems, problems with your assignments, or other problems that are impeding your progress, let your instructor know as soon as possible. **Any critical thinking assignment not completed within 7 days of the due date will not be graded and a score of zero will be assigned.** ***Important: There is no grace period for any Module 14 assignment; this includes the critical thinking assignment, discussion question, and all quizzes. Late work will not be accepted for these assignments or any other assignments not submitted by the last day of the course (including all quizzes and labs).***

Course Materials

Required:

Solomon, M. G. (2014). *Security strategies in Windows platforms and applications* (2nd ed.). Burlington, MA: Jones & Bartlett Learning. ISBN-13: 9781284031652

Access to vLab virtual lab environment with included virtual lab manual.

Course Schedule

Due Dates

The Academic Week begins on Sunday and ends the following Saturday. All assignments are due by Saturday at midnight Mountain Time of the week assigned. **Any critical thinking assignment not completed within 7 days of the due date will not be graded and a score of zero will be assigned.** ***Important: There is no grace period for any Module 14 assignment; this includes the critical thinking assignment, discussion question, and all quizzes. Late work will not be accepted for these assignments or any other assignments not submitted by the last day of the course (including all quizzes and labs).***

- **Discussion Activities**: Application of knowledge is an important step in the learning experience and every course has key discussions wherein students can apply and analyze content as well as move toward synthesis. This course has Discussion Forums that provide learners an extended opportunity to interact with one another in an instructor-facilitated dialogue that focuses on key course themes. Students will apply and synthesize knowledge learned to case studies simulating real-world decision-making***. Important: The original post must be completed by Wednesday at 11:59 p.m. Mountain Time and peer responses must be posted by Saturday at 11:59 p.m. Mountain time. No late postings, original or additional, will be accepted or graded.***
- **Quizzes:** These exercises will assess learner knowledge in specific topic areas.
- **Critical Thinking Application Assignments**: Each assignment will require students to apply their knowledge learned in the module to real-world scenarios.
- **Live Sessions**: Attending required live sessions helps students prepare for the midterm and final examinations, and gain a better understanding of the course materials.
- **Labs:** These are applied, hands-on assignments.

Week #	Readings	Assignments

1	• Chapter 1 in *Security Strategies in Windows Platforms and Applications* • Akhtar, S. (2016, October 23). Addressing the cyber security challenge. *ArabianBusiness.com* • Chatterjee, S., Sarker, S., & Valacich, J. S. (2015). The behavioral roots of information system security: Exploring key factors related to unethical IT use. *Journal of Management Information Systems, 31*(4), 49-87. • Sloan, R., & W. P. (2017, March 23). Cyber matters: The importance of cybersecurity vocabulary. *Wall Street Journal.*	• Discussion (10 points) • Lab (30 points) • Live Session (0 points)
2	• Chapter 2 in *Security Strategies in Windows Platforms and Applications* • Chen, Z. Chen, K. Jiang, J., Zhang, L., Wu, S., Qi, Z., . . .Kang, Z. (2017). Evolution of cloud operating system: From technology to ecosystem. *Journal of Computer Science and Technology, 32*(2), 224-241.	• Discussion (10 points) • Lab (30 points) • Weeks 1-2 Quiz (15 points)
3	• Chapter 3 in *Security Strategies in Windows Platforms and Applications* • Choi, Y., Lee, Y., Moon, J., & Won, D. (2017). Security enhanced multi-factor biometric authentication scheme using bio-hash function. *PloS ONE, 12*(5), 1-32. • Milić, D. C., Kovačević, D., & Štefanac, K. (2017). Synergy of information communication technologies and the banking system in the functioning of successful banking operations. *Ekonomski Vjesnik, 30*(2), 473-488.	• Critical Thinking (50 points) • Live Session (0 points)
4	• Chapter 4 in *Security Strategies in Windows Platforms and Applications* • Brennan, S. (2016). The importance of developing cyber security resilience in the middle east. *ArabianBusiness.com.* • Nelson, S. D., Simek, J. W., & Maschke, M. C. (2017). Technology and cybersecurity policies help lawyers manage technology (instead of it managing them). *Computer and Internet Lawyer, 34*(7), 14-36.	• Discussion (10 points) • Lab (30 points) • Weeks 3-4 Quiz (15 points)
5	• Chapter 5 in *Security Strategies in Windows Platforms and Applications* • Lima, A., Sousa, B., Cruz, T., & Simões, P. (2017). *Security for mobile device assets: A survey.* Paper presented at the International Conference on Cyber Warfare and Security (pp. 227-XVI). Reading, UK: Academic Conferences International Limited. • Shah, N., & Farik, M. (2017). Ransomware – Threats, vulnerabilities and recommendations. *International Journal of Scientific & Technology Research, 6*(6), 307-309.	• Critical Thinking (50 points) • Live Session (0 points)
6	• Chapter 6 in *Security Strategies in Windows Platforms and Applications* • Leonhard, W. (2017). 5 fatal flaws that dog the new Windows 10. *InfoWorld.com.*	• Discussion (10 points) • Lab (30 points) • Weeks 5-6 Quiz (15 points)

	• Microsoft unveils a bonanza of security capabilities. (2017, February 11). *Global Data Point.*	
7	• Chapter 7 in *Security Strategies in Windows Platforms and Applications* • Bhuse, V., & Hekhuis, K. (2018). Support for secure code execution in server operating systems. Paper presented at the International Conference on Cyber Warfare and Security (pp. 21-30, XI). Reading, UK: Academic Conferences International Limited. • Lenghel, R. D., & Vlad, M. P. (2017) Information systems auditing. *Quaestus, 11*, 178-182.	• Critical Thinking (60 points) • Live Session (0 points)
8	• Chapter 8 in *Security Strategies in Windows Platforms and Applications* • Dreyer, I. (2017). Extract more value from your backup than just backup. Cape Town: SyndiGate Media, Inc. • Li, X., & Qian, L. (2017). A hybrid disaster-tolerant model with DDF technology for MooseFS open-source distributed file system. *Journal of Supercomputing, 73*(5), 2052-2068.	• Discussion (10 points) • Lab (30 points)
9	• Chapters 9 & 10 in *Security Strategies in Windows Platforms and Applications* • Cybersecurity in the middle east - the legal perspective. (2017). *Gulf Business.* • Niemimaa, E., & Niemimaa, M. (2017). Information systems security policy implementation in practice: From best practices to situated practices. *European Journal of Information Systems, 26*(1), 1-20.	• Critical Thinking (60 points) • Lab (30 points) • Live Session (0 points)
10	• Chapter 11 in *Security Strategies in Windows Platforms and Applications* • Gkioulos, V., Wangen, G., & Katsikas, S. K. (2017). User modelling validation over the security awareness of digital natives. *Future Internet, 9*(3), 32. • Yuryna Connolly, L., Lang, M., Gathegi, J., & Tygar, D. J. (2017). Organisational culture, procedural countermeasures, and employee security behavior. *Information and Computer Security, 25*(2), 118-136.	• Discussion (10 points) • Lab (30 points) • Weeks 9-10 Quiz (15 points)
11	• Chapter 12 in *Security Strategies in Windows Platforms and Applications* • Radisavljevic-Gajic, V., Park, S., & Chasaki, D. (2018). Vulnerabilities of control systems in internet of things applications. *IEEE Internet of Things Journal, 5*(2), 1023-1032. • Takyi, H., Watzlaf, V., Judith, T. M., Zhou, L., & DeAlmeida, D. (2017). Privacy and security in multi-user health kiosks. *International Journal of Telerehabilitation, 9*(1), 3-14.	• Critical Thinking (60 points) • Live Session (0 points)
12	• Chapter 13 in *Security Strategies in Windows Platforms and Applications* • Khajouei, H., Kazemi, M., & Moosavirad, S. H. (2017). Ranking information security controls by using fuzzy analytic	• Discussion (10 points) • Lab (30 points) • Weeks 11-12 Quiz (15 points)

	hierarchy process. *Information Systems and eBusiness Management, 15*(1), 1-19. • Middle East businesses suffer more cybercrime than globally. (2016, May 18). *Gulf News.*	
13	• Chapter 14 in *Security Strategies in Windows Platforms and Applications* • Khan, S., Parkinson, S., & Qin, Y. (2017). Fog computing security: A review of current applications and security solutions. *Journal of Cloud Computing, 6*(1), 1-22. • Nkukwana, S., & Terblanche, N. H. D. (2017). Between a rock and a hard place: Management and implementation teams' expectations of project managers in an agile information systems delivery environment. *South African Journal of Information Management, 19*(1).	• Discussion (10 points) • Live Session (0 points)
14	• Chapter 15 in *Security Strategies in Windows Platforms and Applications* • Bucko, J. (2017). Security of smart banking applications in Slovakia. *Journal of Theoretical and Applied Electronic Commerce Research, 12*(1), 42-52. • Bucşă, R. (2017). OwnCloud solution for small businesses. *Economy Transdisciplinarity Cognition, 20*(2), 30-35.	• Discussion (10 points) • Weeks 13-14 Quiz (15 points)

Assignment Details

This course includes the following assignments/projects:

Module 1

Lab: Implementing Access Controls with Windows Active Directory (30 Points)

Lab Details:

In this lab, you will use the Active Directory Domain Controller to secure the CIA triad, ensuring the confidentiality and integrity of network data. You will create users and global security groups and assign the new users to security groups. You will follow a given set of access control criteria to ensure authentication on the remote server by applying the new security groups to a set of nested folders. Finally, you will verify that authentication by using the new user accounts to access the secured folders on the remote server.

Follow these steps to complete this assignment:

1. Carefully read through the **Student Lab Guide**. It provides detailed instructions for accessing and completing the labs in this course.
2. Open the **Lab 1 Assessment Worksheet**. Save a copy of the worksheet to your computer; this will allow you to fill it out electronically and save your answers. You will complete this worksheet and submit it to your instructor after completing the hands-on portion of the lab. However, it is strongly recommended that you read through the worksheet before you begin.
3. Click the **Lab Access** in the Module Folder to enter the virtual lab environment.
4. Read through all the material under the Intro and Steps tabs before you start working.

5. Follow the step-by-step instructions under the Steps tab to perform the lab. *Note:* You will not be completing a lab report, so you can disregard instructions to make screen captures.
6. After completing the hands-on lab, complete and submit the Lab 1 Assessment Worksheet. Use the worksheet that you saved to your computer. Be sure to save it again before submitting it.

Module 2

Lab: Using Access Control Lists to Modify File System Permissions on Windows Systems (30 points)

Lab Details:

In this lab, you will use the Windows command-line utility, icacls.exe, to establish file-level permissions following a set of access control requirements. You will test those permissions by remotely accessing the Windows server and attempting to modify files in the secured folders.

Follow these steps to complete this assignment:

1. Carefully read through the **Student Lab Guide**. It provides detailed instructions for accessing and completing the labs in this course.
2. Open the **Lab 2 Assessment Worksheet**. Save a copy of the worksheet to your computer; this will allow you to fill it out electronically and save your answers. You will complete this worksheet and submit it to your instructor after you have completed the hands-on portion of the lab. However, it is strongly recommended that you read through the worksheet before you begin.
3. Click the **Lab Access** in the Module Folder to enter the virtual lab environment.
4. Read through all the material under the Intro and Steps tabs before you start working.
5. Follow the step-by-step instructions under the Steps tab to perform the lab. *Note:* You will not be completing a lab report, so you can disregard instructions to make screen captures.
6. After completing the hands-on lab, complete and submit the Lab 2 Assessment Worksheet. Use the worksheet that you saved to your computer. Be sure to save it again before submitting it.

Module 3

Critical Thinking: Systems and Controls Assessment (50 points)

Assignment Details:

Assume you are a manager in a large international organization. You have been asked to assess the company's information systems and security controls.

- Describe identification, authentication, and authorization.
- Explore whether or not you would use Windows ACLs and explain your reasoning.
- Evaluate best practices for managing Microsoft Windows and application vulnerabilities.

Keep in mind, we are more interested in your ability to describe the steps you would take to review security goals than providing an answer to this scenario. Remember the strategy of Think, Plan, Design, Implement, and Evaluate.

Deliverables:

Your paper should be 4-5 pages in length and formatted according to Saudi Electronic University academic writing standards and APA style guidelines. Use at least two scholarly sources as well as information from your module to support your decision.

Module 4

Lab: Configuring BitLocker and Windows Encryption (30 points)

Lab Details:

In this lab, you will use the Microsoft Encrypting File System (EFS) to encrypt files and folders on a Windows Server 2012 machine. You will document the success or failure of your encryption efforts. You will install Microsoft BitLocker Drive Encryption, a data protection feature that is used to resist data theft and the risk of exposure from lost, stolen, or decommissioned computers. You will encrypt a data drive on the server and decrypt it using a recovery key.

Follow these steps to complete this assignment:

1. Carefully read through the **Student Lab Guide**. It provides detailed instructions for accessing and completing the labs in this course.
2. Open the **Lab 3 Assessment Worksheet**. Save a copy of the worksheet to your computer; this will allow you to fill it out electronically and save your answers. You will complete this worksheet and submit it to your instructor after you have completed the hands-on portion of the lab. However, it is strongly recommended that you read through the worksheet before you begin.
3. Click the **Lab Access** in the Module Folder to enter the virtual lab environment.
4. Read through all the material under the Intro and Steps tabs before you start working.
5. Follow the step-by-step instructions under the Steps tab to perform the lab. *Note:* You will not be completing a lab report, so you can disregard instructions to make screen captures.
6. After completing the hands-on lab, complete and submit the Lab 3 Assessment Worksheet. Use the worksheet that you saved to your computer. Be sure to save it again before submitting it.

Module 5

Critical Thinking: Malware (50 points)

Assignment Details:

In an essay, answer the following questions based on the readings from this module:

- How do you determine the type and location of malware present on the computer or device? Explain your rationale.
- In your opinion, do you think that vulnerabilities can be minimized in the future? Why or why not?

Provide information from your readings to support your statements.

Deliverables:

Your essay should be 4-5 pages in length, incorporating at least two academic resources from the Library in addition to the case study. Cite all sources using Saudi Electronic University academic writing standards and APA style guidelines found in the Library, citing references as appropriate.

Module 6

Lab: Managing Group Policy within the MS Windows Environment (30 points)

Lab Details:

In this lab, you will create and link Active Directory Group Policy Objects (GPO) to domain computers and use the Group Policy Manager Console (GPMC) to deploy security policies across the domain. You also will generate policy audit reports from the GPMC and the Windows Command Prompt to analyze the existence of and effectiveness of the GPO.

Follow the steps below to complete this assignment:

1. Carefully read through the **Student Lab Guide**. It provides detailed instructions for accessing and completing the labs in this course.
2. Open the **Lab 5 Assessment Worksheet**. Save a copy of the worksheet to your computer; this will allow you to fill it out electronically and save your answers. You will complete this worksheet and submit it to your instructor after you have completed the hands-on portion of the lab. However, it is strongly recommended that you read through the worksheet before you begin.
3. Click the **Lab Access** in the Module Folder to enter the virtual lab environment.
4. Read through all the material under the Intro and Steps tabs before you start working.
5. Follow the step-by-step instructions under the Steps tab to perform the lab. *Note:* You will not be completing a lab report, so you can disregard instructions to make screen captures.
6. After completing the hands-on lab, complete and submit the Lab 5 Assessment Worksheet. Use the worksheet that you saved to your computer. Be sure to save it again before submitting it.

Module 7

Critical Thinking: Critical Thinking: System Security Goals (60 points)

Assignment Details:

In an essay, answer the following questions based on this week's module:

- How do you know if your system is meeting your security goals?
- You can verify that controls are working, but how do you know if they are getting the job done?
- What auditing practices or procedures would you implement for your organization? Why?

Deliverables:

Provide information from your readings to support your statements. Your well-written essay should be 4-5 pages in length, incorporating at least two academic resources from the Library in addition to the case study. Cite all sources using Saudi Electronic University academic writing standards and APA style guidelines found in the Library, citing references as appropriate.

Module 8

Lab: Creating a Scheduled Backup and Replicating System Folders (30 points)

Lab Details:

In this lab, you will install the Windows Distributed File System and Windows Server Backup features from the PowerShell command line. You will schedule a daily backup of the C:\ERPdocuments folder on the TargetWindows01 server and replicate this backup to the TargetWindows02 server using the DFS Replication feature.

Follow these steps to complete this assignment:

1. Carefully read through the **Student Lab Guide**. It provides detailed instructions for accessing and completing the labs in this course.
2. Open the **Lab 6 Assessment Worksheet**. Save a copy of the worksheet to your computer; this will allow you to fill it out electronically and save your answers. You will complete this worksheet and submit it to your instructor after you have completed the hands-on portion of the lab. However, it is strongly recommended that you read through the worksheet before you begin.
3. Click the **Lab Access** in the Module Folder to enter the virtual lab environment.
4. Read through all the material under the Intro and Steps tabs before you start working.
5. Follow the step-by-step instructions under the Steps tab to perform the lab. *Note:* You will not be completing a lab report, so you can disregard instructions to make screen captures.
6. After completing the hands-on lab, complete and submit the Lab 6 Assessment Worksheet. Use the worksheet that you saved to your computer. Be sure to save it again before submitting it.

Module 9

Critical Thinking: Windows Networks (60 points)

Assignment Details:

Microsoft Windows computers can be very useful by themselves, but they are far more effective when they are able to communicate with one another. In an essay, address the following:

- Discuss the techniques that many organizations use to ensure that their Windows networks are secure.
- Additionally, examine how to connect computers together without risking your organization's information to loss, alteration, or disclosure.
- Provide an example of how each principle of the CIA triad can be used to secure the network

Provide information from your readings to support your statements.

Deliverables:

Your well-written essay should be 4-5 pages in length, incorporating at least two academic sources from the Library in addition to the case study. Cite all sources using Saudi Electronic University academic writing standards and APA style guidelines found in the Library, citing references as appropriate.

Lab: Securing Servers with the Security Configuration Wizard and the Windows Firewall (30 points)

Lab Details:

In this lab, you will create and apply a new security policy to a Windows Server 2012 machine using the Windows Security Configuration Wizard (SCW). Next, you will further harden security on a Windows Server 2008 machine by manually disabling unnecessary services, which can also optimize performance. You will then use built-in Windows Firewall to prevent unauthorized access to the server. Finally, you will review the existing configuration and recommend changes that will harden security.

Follow the steps below to complete this assignment:

1. Carefully read through the **Student Lab Guide**. It provides detailed instructions for accessing and completing the labs in this course.
2. Open the **Lab 7 Assessment Worksheet**. Save a copy of the worksheet to your computer; this will allow you to fill it out electronically and save your answers. You will complete this worksheet and submit it to your instructor after you have completed the hands-on portion of the lab. However, it is strongly recommended that you read through the worksheet before you begin.
3. Click the **Lab Access** in the Module Folder to enter the virtual lab environment.
4. Read through all the material under the Intro and Steps tabs before you start working.
5. Follow the step-by-step instructions under the Steps tab to perform the lab. *Note:* You will not be completing a lab report, so you can disregard instructions to make screen captures.
6. After completing the hands-on lab, complete and submit the Lab 7 Assessment Worksheet. Use the worksheet that you saved to your computer. Be sure to save it again before submitting it.

Module 10

Lab: Securing Internet Client and Server Applications on Windows Systems (30 points)

Lab Details:

Both IIS and Internet Explorer can be hardened to improve confidentiality, integrity, and availability (CIA). In this lab you will identify security hardening opportunities for the IIS application, then make those changes on a Windows Server 2012 machine. Next, you will identify and modify the Internet Options for the Internet Explorer browser. Finally, you will document the changes you make and provide an explanation for how each change helps achieve CIA.

Follow the steps below to complete this assignment:

1. Carefully read through the **Student Lab Guide**. It provides detailed instructions for accessing and completing the labs in this course.
2. Open the **Lab 8 Assessment Worksheet**. Save a copy of the worksheet to your computer; this will allow you to fill it out electronically and save your answers. You will complete this worksheet and submit it to your instructor after you have completed the hands-on portion of the lab. However, it is strongly recommended that you read through the worksheet before you begin.
3. Click the **Lab Access** in the Module Folder to enter the virtual lab environment.
4. Read through all the material under the Intro and Steps tabs before you start working.
5. Follow the step-by-step instructions under the Steps tab to perform the lab. *Note:* You will not be completing a lab report, so you can disregard instructions to make screen captures.

6. After completing the hands-on lab, complete and submit the Lab 8 Assessment Worksheet. Use the worksheet that you saved to your computer. Be sure to save it again before submitting it.

Module 11

Critical Thinking: Critical Thinking: Software Security (60 points)

Assignment Details:

In an essay, review the following statements based on the readings from this week's module:

- Once your operating system is secure, you can focus on securing the software that runs in the operating system.
- Evaluate some of the most popular Microsoft applications and analyze how to make an application more secure to protect your organization's data. Describe at least three techniques used to secure an application.

Provide information from your readings to support your statements.

Deliverables:

Your well-written essay should be 4-5 pages in length, incorporating at least two academic resources from the Library in addition to the case study. Cite all sources using Saudi Electronic University academic writing standards and APA style guidelines found in the Library, citing references as appropriate.

Module 12

Lab: Protecting Digital Evidence, Documentation, and the Chain of Custody (30 points)

Lab Details:

In this lab, you will first use the Windows Event Viewer utility to search for failed logon attempts, which could indicate a possible intrusion by an unauthorized user. You will also generate your own errors by attacking the Windows Server 2012 machine and then review the Internet Information Services (IIS) logs to find those errors. Finally, you will document your findings and recommend remediation steps.

Follow the steps below to complete this assignment:

1. Carefully read through the **Student Lab Guide**. It provides detailed instructions for accessing and completing the labs in this course.
2. Open the **Lab 9 Assessment Worksheet**. Save a copy of the worksheet to your computer; this will allow you to fill it out electronically and save your answers. You will complete this worksheet and submit it to your instructor after you have completed the hands-on portion of the lab. However, it is strongly recommended that you read through the worksheet before you begin.
3. Click the **Lab Access** in the Module Folder to enter the virtual lab environment.
4. Read through all the material under the Intro and Steps tabs before you start working.
5. Follow the step-by-step instructions under the Steps tab to perform the lab. *Note:* You will not be completing a lab report, so you can disregard instructions to make screen captures.

6. After completing the hands-on lab, complete and submit the Lab 9 Assessment Worksheet. Use the worksheet that you saved to your computer. Be sure to save it again before submitting it.

Course Policies

Course Grading

13% Quizzes
13% Discussion Participation
34% Labs
40% Critical Thinking Activities

Any critical thinking assignment not completed within 7 days of the due date will not be graded and a score of zero will be assigned. ***Important: There is no grace period for any Module 14 assignment; this includes the critical thinking assignment, discussion question, and all quizzes and labs. Late work will not be accepted for these assignments or any other assignments not submitted by the last day of the course (including all quizzes).***