ITS425: Ethical Hacking and Penetration Testing

Credit Hours: 3

Contact Hours: This is a 3-credit course, offered in accelerated format. This means that 16 weeks of material is covered in 8 weeks. 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 14-20 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:

This course provides students with the knowledge and practice needed to secure information systems against attacks such as viruses, worms, and other system weaknesses that pose significant danger to organizational data. Ethical hacking and penetration testing are applied to uncover common techniques used by cyber criminals to exploit system vulnerabilities.

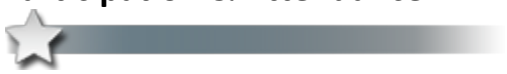
Course Overview:

ITS425 introduces to the application of ethical hacking techniques and penetration testing for IT security. Students undertake an extensive review of various hacking tools and methods that are commonly used to compromise computer systems. Ethical hacking, also known as penetration testing, is the act of hacking into a system *with permission and legal consent* from organization or individual who owns and operates the system, for the purpose of identifying vulnerabilities and strengthening the organization's security. ITS425 students will conduct hands-on penetration testing in a virtual lab environment that provides practice of the concepts presented in the course using versions of hacking tools that are used in the field. It is important to restate that ITS425 is an ethical hacking course, which implies that students will learn hacking techniques within a controlled environment toward the goal of better securing IT resources for their rightful owners.

Course Learning Outcomes:

1. Describe and analyze the differences between ethical and unethical penetration testing.
2. Describe and explain the phases of a penetration test.
3. Apply different tools and methods to conduct penetration tests.
4. Compare and contrast various methods of conducting network reconnaissance in penetration testing.
5. Describe the role and purpose of network scanning in penetration testing.
6. Apply different tools and methods to exploit systems during penetration testing.
7. Describe and utilize methods and tools to maintain access to systems during penetration testing.
8. Analyze and apply methods to report the results of penetration testing and make system recommendations.

Participation & Attendance



Prompt and consistent attendance in your online courses is essential for your success at CSU-Global Campus. Failure to verify your attendance within the first 7 days of this course may result in your withdrawal. If for some reason you would like to drop a course, please contact your advisor.

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.

Course Materials

Inclusive Access

This term your course will be included in CSU-Global's Inclusive Access program, which allows day one access to one or more of your required course materials — at a reduced cost. Click the "Course eBook" link located at the top of each module to access your materials. You will have access to these materials at no charge until the add/drop date, at which point your student account will be charged. If you decide you do not want to participate, you can Opt-Out of the Inclusive Access program by navigating to your course book and clicking "OPT-OUT" before the add/drop deadline. If you opt-out by the add/drop deadline, your student account will not be charged.

Required:

Bundled purchase including the following resources:

> Oriyano, S. P. (2014). *Hacker techniques, tools, and incident handling* (2nd ed.). Burlington, MA: Jones & Bartlett Learning.
>
> Access to vLab virtual lab environment with included virtual lab manual.

***All non-textbook required readings and materials necessary to complete assignments, discussions, and/or supplemental or required exercises will be provided within the course itself. Please read through each course module carefully.*

Course Schedule

Due Dates

The Academic Week at CSU-Global begins on Monday and ends the following Sunday.

- Discussion Boards: The original post must be completed by Thursday at 11:59 p.m. MT and Peer Responses posted by Sunday 11:59 p.m. MT. Late posts may not be awarded points.
- Mastery Exercises: Students may access and retake mastery exercises through the last day of class until they achieve the scores they desire.
- Critical Thinking Activities: Assignments are due Sunday at 11:59 p.m. MT.

Week #	Readings	Assignments
1	• Chapters 1 & 2 in *Hacker Techniques, Tools, and Incident Handling* • PR, N. (2012, April 19). The Importance of Ethical Hacking: Emerging Threats Emphasise Need for Holistic Assessments, Says Frost & Sullivan. *PR Newswire US*. • PR, N. (2015, September 17). Austin-based security firm says the world needs more smart hackers. *PR Newswire US*. • Conniff, K. (2014). How to Hacker-Proof Your Home. *Time*, *184*(1), 60-61.	• Discussion (25 points) • Opening Exercise (0 points) • Mastery (10 points) • Critical Thinking (70 points)
2	• Chapters 3 & 4 in *Hacker Techniques, Tools, and Incident Handling* • Cryptography. (2015). *Funk & Wagnalls New World Encyclopedia*, 1p. 1. • Cochrane, P. (2015). The unsecurable. *Financial Director*, 22. • Ludwig, S. E. (2015). Mitigating Risk in Open Environments. *Security: Solutions for Enterprise Security Leaders*, 69. Meyer, C. (2015). Retain Your Relevance: Study Cybersecurity. *Security: Solutions For Enterprise Security Leaders*, 97-98.	• Discussion (25 points) • Opening Exercise (0 points) • Mastery (10 points) • Critical Thinking (70 points)
3	• Chapters 5 & 6 in *Hacker Techniques, Tools, and Incident Handling* • Glassman, J. K. (2016). My 10 Top Picks for 2016. *Kiplinger's Personal Finance*, *70*(1), 25-26. • Alsaleh, M., & Oorschot, P. (2013). Evaluation in the absence of absolute ground truth: toward reliable evaluation methodology for scan detectors.*International Journal Of Information Security*, *12*(2), 97-110. doi:10.1007/s10207-012-0178-1. • Anbar, M., Manasrah, A., & Manickam, S. (2012). Statistical cross-relation approach for detecting TCP and UDP random and sequential network scanning (SCANS). *International Journal Of Computer Mathematics*, *89*(15), 1952-1969. doi:10.1080/00207160.2012.696621.	• Discussion (25 points) • Opening Exercise (0 points) • Mastery (10 points)

4	• Chapters 7 & 8 in *Hacker Techniques, Tools, and Incident Handling* • Frenkel, K. A. (2015). Password Cracking Tops IT's Security Concerns. *CIO Insight*, 2. • Palenchar, J. (2015). UHD, Home Automation Take Lead in Broad-Based Custom Growth. *TWICE: This Week in Consumer Electronics*, *30*(18), 10. • Ablon, L., & Libicki, M. (2015). Hackers' Bazaar: The Markets for Cybercrime Tools and Stolen Data. *Defense Counsel Journal*, *82*(2), 143-152. • Pister, K., & Simon, J. (2014). Secure Wireless Sensor Networks Against Attacks. *Electronic Design*, *62*(6), 38.	• Discussion (25 points) • Opening Exercise (0 points) • Mastery (10 points) • Critical Thinking (70 points)
5	• Chapters 9 & 10 in *Hacker Techniques, Tools, and Incident Handling* • Lemos, R. (2014). Malware 'Mayhem' Follows Emergence of Shellshock Vulnerability. *Eweek*, 1. • Temizkan, O., Kumar, R. L., Park, S., & Subramaniam, C. (2012). Patch Release Behaviors of Software Vendors in Response to Vulnerabilities: An Empirical Analysis. *Journal of Management Information Systems*, *28*(4), 305-338. • Greenberg, A. (2012). Hackers Spill More Than 450,000 Email Addresses and Passwords, Blame A Yahoo! Database Vulnerability. *Forbes.Com*, 18.	• Discussion (25 points) • Opening Exercise (0 points) • Mastery (10 points) • Critical Thinking (80 points)
6	• Chapters 11 & 12 in *Hacker Techniques, Tools, and Incident Handling* • Rorot. (2015). Session hijacking cheat sheet. • Wedman, S., Tetmeyer, A., & Saiedian, H. (2013). An Analytical Study of Web Application Session Management Mechanisms and HTTP Session Hijacking Attacks. Information Security Journal: A Global Perspective, 22(2), 55-67. • Lemos, R. (2013). Large DoS Attacks More Than Quadruple in 2013: Study. Eweek, 7.	• Discussion (25 points) • Opening Exercise (0 points) • Mastery (10 points) • Critical Thinking (80 points)
7	• Chapters 13 & 14 in *Hacker Techniques, Tools, and Incident Handling* • Tetri, P., & Vuorinen, J. (2013). Dissecting social engineering. *Behaviour & Information Technology*, *32*(10), 1014-1023. doi:10.1080/0144929X.2013.763860. • Jansson, K., & von Solms, R. (2013). Phishing for phishing awareness. Behaviour & Information Technology, 32(6), 584-593. • Thurman, M. (2013). Security Manager's Journal. Computerworld, 47(8), 32.	• Discussion (25 points) • Opening Exercise (0 points) • Mastery (10 points)
8	• Chapter 15 in *Hacker Technologies, Tools, and Incident Handling* • Sampemane, G. (2015). Internal Access Controls. *Communications of The ACM*, *58*(1), 62-65. doi:10.1145/2687878.	• Discussion (25 points) • Opening Exercise (0 points) • Mastery (10 points) • Portfolio (350 points)

- Shameli-Sendi, A., & Dagenais, M. (2014). ARITO: Cyber-attack response system using accurate risk impact tolerance. International Journal Of Information Security, 13(4), 367-390.
- Eesa, A. S., Orman, Z., & Brifcani, A. A. (2015). A new feature selection model based on ID3 and bees algorithm for intrusion detection system.Turkish Journal Of Electrical Engineering & Computer Sciences, 23(2), 615-622.
- Hayatle, O., Otrok, H., & Youssef, A. (2013). A Markov Decision Process Model for High Interaction Honeypots. Information Security Journal: A Global Perspective, 22(4), 159-170.

Assignment Details

This course includes the following assignments/projects:

Module 1

CRITICAL THINKING ASSIGNMENT (70 points)

Choose one of the following two assignments to complete this week. Do not do both assignments. Identify your assignment choice in the title of your submission.

Option #1: Attack and Penetration Test Plan

Prepare a written proposal for the penetration test plan that describes your firm's approach to performing the penetration test and what specific tasks, deliverables, and reports you will complete as part of your services.

Scenario: You are the owner and operator of a small information security consulting firm. You have received a request from one of your clients, Infusion Web Marketing, to provide a written proposal for performing a penetration test on the company's production Web servers and corporate network.

Environment:

Scope	Production e-commerce Web application server, thee-commerce Web application server is acting as an external point-of-entry into the network: • Ubuntu Linux 10.04 LTS Server (TargetUbuntu01) • Apache Web Server running the e-commerce Web application server • Credit card transaction processing occurs on all web servers.
Intrusive or Non-Intrusive	Intrusive. The test will include penetrating past specific security checkpoints.
Compromise or No Compromise	No compromise. The test can compromise with written client authorization only.
Scheduling	Between 2:00 a.m-6:00 a.m. MST weekend only (Saturday or Sunday)

Deliverables:

Based on the scenario above, provide a written attack and penetration testing plan. The plan should include these sections:

- Table of Contents
- Project Summary
- Goals and Objectives
- Tasks
- Reporting
- Schedule.

Your penetration testing plan should be two to three pages in length and should discuss and cite at least three credible or academic references other than the course materials. The CSU-Global Library is an excellent place to search for credible academic sources. Document and citation formatting should be in conformity with *CSU-Global Guide to Writing and APA Requirements*.

Helpful Resources:

The SANS Institute provides several resources that you might find helpful for this assignment: http://www.sans.org/reading-room/whitepapers/testing

The National Institute for Standards and Technologies (NIST) also provides guidance on the topic of security and penetration testing: http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf

Option #2: Assessing and Securing Systems on a Wide Area Network (WAN)

This Critical Thinking lab assignment will make use of the student virtual lab environment (VSCL) purchased in conjunction with your textbook.

Assignment Details:

For this assignment, complete Lab #1 in the virtual lab environment (VSCL). This assignment allows you to practice skills associated with assessing and securing systems.

During the lab you are asked to record information and results from your activities in a Microsoft Word document.

Deliverables:

Submit a Microsoft Word document with document formatting and any citations in conformity with the *CSU-Global Guide to Writing and APA Requirements*. Include the following:

1. Report your results from Lab #1, including screen captures for Part 1, Step 7; Part 2, Steps 6, 16, and 20; Part 3, Step 25; and Part 4, Steps 6 and 24. Make sure you collect this information in a single Microsoft Document that will be your deliverable for this assignment and serve as proof that you have completed the lab.
2. Write a summary narrative at least one page in length that describes the challenges you faced and explains what you learned from the lab activity.

PORTFOLIO PROJECT REMINDER

A Portfolio Project is due at the end of the course. Read and think about the full Portfolio Project description on the **Week 8 Assignments** page and review the Portfolio Project grading rubric, which you can access from the **Course Information** page. Be sure to begin preparing to complete this assignment early in the course and continue to work on the Portfolio Project throughout the eight weeks of the course. The statement "You cannot complete this project the last week of the course" is a fact and not a challenge!

Module 2

CRITICAL THINKING ASSIGNMENT (70 points)
Choose one of the following two assignments to complete this week. Do not do both assignments. Identify your assignment choice in the title of your submission.

Option #1: Information Gathering and Website Footprinting

This Critical Thinking lab assignment will make use of the student virtual lab environment (VSCL) and lab manual purchased in conjunction with your textbook.

Assignment Details:

For this assignment, complete Lab #3 in the virtual lab environment (VSCL). This assignment allows you to practice information gathering and website footprinting. Footprinting is the first step of the hacking process and allows you to gather information about the organization you will be targeting for a penetration and security test.

Complete Lab # 3. During the lab you are asked to record information and results from your footprinting activities in a Microsoft Word document.

Deliverables:
Submit a Microsoft Word document with document formatting and any citations in conformity with the *CSU-Global Guide to Writing and APA Requirements*. Include the following:

1. Report your results from Lab #3, including screen captures for Part 1, Steps 5, 7, 18, and 22 and Part 2, Step 4. Make sure you collect this information in a single Microsoft Document that will be your deliverable for this assignment and serve as proof that you have completed the lab.
2. Write a summary narrative at least one page in length that describes the challenges you faced and explains what you learned from the lab activity.

Option #2: Applying Encryption and Hashing Algorithms for Secure Communications
This Critical Thinking lab assignment will make use of the student virtual lab environment (VSCL) purchased in conjunction with your textbook.
Assignment Details:
For this assignment, complete Lab #2 in the virtual lab environment (VSCL). This assignment allows you to practice skills associated with assessing and securing systems.
During the lab you are asked to record information and results from your activities in a Microsoft Word document.

Deliverables:
Submit a Microsoft Word document with document formatting and any citations in conformity with the *CSU-Global Guide to Writing and APA Requirements*. Include the following:

1. Report your results from Lab #2, including screen captures from Part 2, Steps 6, 10, 14, and 18; Part 3, Steps 4 and 6; Part 4, Steps 16 and 24; Part 5, Step 7; and Part 6, Steps 8 and 18. Make sure you collect this information in a single Microsoft Document which will be your deliverable for this assignment and serve as proof that you have completed the lab.
2. Write a summary narrative at least one page in length that describes the challenges you faced and explains what you learned from the lab activity.

Module 3 – N/A

Module 4

CRITICAL THINKING ASSIGNMENT (70 points)
Choose one of the following two assignments to complete this week. Do not do both assignments. Identify your assignment choice in the title of your submission.

Option #1: Compromise and Exploit a Vulnerable Microsoft Workstation

This Critical Thinking lab assignment will make use of the student virtual lab environment (VSCL) purchased in conjunction with your textbook.

Assignment Details:

For this assignment, complete Lab #4 in the virtual lab environment. This lab will introduce various security tools used to footprint and attack a given system.

Deliverables:

Submit a Microsoft Word document with document formatting and any citations in conformity with *CSU-Global Guide to Writing and APA Requirements*. Include the following:

1. Report your results from Lab #4, including screen captures from Part 3, Steps 18 and 20;
2. Ping scan on 172.30.0.0_24.xml;
3. Intense scan on 172.30.0.30.xml;
4. *yourname*_Victim_VulnerabilityScan.pdf. Make sure you collect this information in a single Microsoft Document which will be your deliverable for this assignment and serve as proof that you have completed the lab.
5. Write a summary narrative at least one page in length that describes the challenges you faced and explains what you learned from the lab activity.

Option #2: Attacking a Vulnerable Web Application and Database

This Critical Thinking lab assignment will make use of the student virtual lab environment (VSCL) purchased in conjunction with your textbook.

Assignment Details:

For this assignment, complete Lab #5 in the virtual lab environment. This lab will introduce various security tools used to footprint and attack a given system.

Deliverables:

Submit a Microsoft Word document with document formatting and any citations in conformity with *CSU-Global Guide to Writing and APA Requirements*. Include the following:

1. Report your results from Lab #5, including screen captures from Part 2, Steps 5 and 8; Part 3, Steps 18 and 20; and Part 4, Step 8. Make sure you collect this information in a single Microsoft Document that will be your deliverable for this assignment and serve as proof that you have completed the lab.
2. Write a summary narrative at least one page in length that describes the challenges you faced and explains what you learned from the lab activity.

Module 5

CRITICAL THINKING ASSIGNMENT (80 points)
Choose one of the following two assignments to complete this week. Do not do both assignments. Identify your assignment choice in the title of your submission.

Option #1: Identifying and Preventing Malware

This Critical Thinking lab assignment will make use of the student virtual lab environment (VSCL) and lab manual purchased in conjunction with your textbook.

Assignment Details:

For this assignment, complete Lab #6 in the virtual lab environment. This lab will prepare you to use antivirus and anti-malware tools to identify system viruses and malware. You will then use security software to remove malicious software from the system.

Deliverables:

Submit a Microsoft Word document with formatting and any citations in conformity with *CSU-Global Guide to Writing and APA Requirements*. Include the following:

1. Report your results from Lab #6, including screen captures from Part 3, Steps 4 and 13;
2. *yourname*_AVG-scan.csv;
3. *yourname*_ResidentShield-scan.csv. Make sure you collect this information in a single Microsoft Document that will be your deliverable for this assignment and serve as proof that you have completed the lab.
3. Write a summary narrative at least one page in length that describes the challenges you faced and explains what you learned from the lab activity.

Option #2: Challenge Question: Identifying and Preventing Malware

This Critical Thinking lab assignment will make use of the student virtual lab environment (VSCL) and lab manual purchased in conjunction with your textbook.

Assignment Details:

For this assignment, complete the challenge questions for Lab #6 in the virtual lab environment. The following challenge questions are provided to allow independent, unguided work, similar to what you will encounter in a real situation. You should aim to improve your skills by getting the correct answer in as few steps as possible. Use screen captures in your lab document where possible to illustrate your answers.

Deliverables:

Submit a Microsoft Word document with formatting and any citations in conformity with *CSU-Global Guide to Writing and APA Requirements*. Include the following:

1. Describe the steps needed to update AVG offline (without using Internet access from the infected machine). Why might someone want to update their antivirus software offline?
2. Workstation and desktop devices are prone to viruses, malware, and malicious software, especially if the user has access to the Internet. Assuming that users will be connected to the Internet, what security countermeasures can organizations implement to help mitigate the risk from viruses, malware, and malicious software? Make sure you collect this information in a single Microsoft Document that will be your deliverable for this assignment and serve as proof that you have completed the lab.

Module 6

CRITICAL THINKING ASSIGNMENT (80 points)

Choose one of the following two assignments to complete this week. Do not do both assignments. Identify your assignment choice in the title of your submission.

Option #1: Audit and Implement a Secure WLAN Solution

This Critical Thinking lab assignment will make use of the student virtual lab environment (VSCL) purchased in conjunction with your textbook.

Assignment Details:

For this assignment, complete Lab #8 in the virtual lab environment (VSCL). This lab will introduce the principles of securing and auditing a WLAN.

Deliverables:

Submit a Microsoft Word document with formatting and any citations in conformity with *CSU-Global Guide to Writing and APA Requirements*. Include the following:

1. Report your results from Lab #8, including screen captures of Part 3, Step 4. Make sure you collect this information in a single Microsoft Document which will be your deliverable for this assignment and serve as proof that you have completed the lab.
2. Write a summary narrative at least one page in length that describes the challenges you faced and explains what you learned from the lab activity.

Option #2: Challenge Question: Audit and Implement a Secure WLAN Solution

This Critical Thinking lab assignment will make use of the student virtual lab environment (VSCL) purchased in conjunction with your textbook.

Assignment Details:

For this assignment, complete the challenge question for Lab #8 in the virtual lab environment (VSCL). The following challenge questions are provided to allow independent, unguided work, similar to what you will encounter in a real situation. You should aim to improve your skills by getting the correct answer in as few steps as possible. Use screen captures in your lab document where possible to illustrate your answers.

Deliverables:

Submit a Microsoft Word document with formatting and any citations in conformity with *CSU-Global Guide to Writing and APA Requirements*. Include the following:

As a field representative for your company, you are accustomed to traveling and working from hotels on the road. You always stay in a hotel with free WiFi so that you work and check your email, as well as Skype with your family. What are the risks of using a public WiFi? Short of finding a more secure network, what could you do to use this wireless network in a more secure fashion? What options do you have if you are traveling for personal reasons and not as an employee? Make sure you collect this information in a single Microsoft Document that will be your deliverable for this assignment and serve as proof that you have completed the lab.

Module 7
N/A

Module 8

PORTFOLIO PROJECT (350 points)

Choose one of the following two assignments to complete this week. Do not do both assignments. Identify your assignment choice in the title of your submission.

Option #1: Report on Organizational Security Threats and Vulnerabilities

Prepare a detailed written report discussing the potential security threats and vulnerabilities of a fictitious organization, Adventure Scuba and Diving Institute (ASDI).

Please see the Specification section for more details on assignment submission requirements.

Scenario:

Adventure Scuba and Diving Institute (ASDI) is located in the United States and offers training and certification programs for scuba and deep sea diving. ASDI is a premier training school in the area of diving and scuba and has developed a wealth of proprietary training resources, videos, guides and manuals. The school suspects that competitors have tried to breach the organization's computer systems to gain access to these training materials.

ASDI's network is comprised of two web servers, two file servers, one email server, 50 employee workstations, and a 50-workstation student computer lab. The school also has public and private Wi-Fi availability throughout the campus.

Your firm has been hired as the IT security analyst to review, evaluate, and make recommendations with respect to maintenance of security of the organization's computer and network systems. You have been charged by your supervisor to prepare a preliminary report documenting the most critical security threats that ASDI faces. Your supervisor has given you the following resources that might be useful in your research and analysis:

- An article on the Help Net security Web site (*http://www.net-security.org/secworld.php?id=10154*)
- Common Vulnerabilities and Exposure (CVE) database search (*http://cve.mitre.org/find/index.html*)
- Security organizations, such as Secunia (*http://secunia.com/*)

Your supervisor has asked you to consider and account for the following questions as you shortlist the threats and prepare your report:

1. What threats are new this year and which have become more prevalent?
2. Why are these threats more common and why are they important?
3. What threats remain constant from year to year? Why?
4. What threats do you believe will become more critical in the next twelve months? Why?
5. Has an exploit been released?
6. What is the likelihood of an exploit?
7. How widely used is the software or system?

Specifications for this Assignment:

1. Submit the report as a single document in Word format.
2. Eight to ten pages in length
3. Document and citation formatting should be in conformity with the *CSU-Global Guide to Writing and APA Requirements*.
4. Cite and discuss at least three credible sources other than (or in addition to) the course textbook. The three sources recommended in this assignment description may be among these sources, which may also include sources found via Web search or in the CSU-Global Library.
5. Include in your report a network diagram of how you propose the network structure should be configured for optimum security. You can create this diagram using any drawing tool, including those embedded in Word, or by drawing the diagram by hand, scanning into an image file, and then pasting into your report.
6. The sections of your report should be as follows:
    - Cover Page
    - Table of Contents
    - Executive Summary (*provide a project overview and summary here)*
    - Body of the report in narrative form in two sections: Section 1 of the on Vulnerabilities and Threats in narrative form, providing responses to each of the questions posed in the assignment scenario, and Section 2 on Countermeasures and Prevention
    - Network Diagram
    - References.

Option #2: Presentation on Organizational Security Threats and Vulnerabilities

Prepare a professional-quality, APA-formatted PowerPoint presentation with slide notes discussing the potential security threats and vulnerabilities of a fictitious organization, Adventure Scuba and Diving Institute (ASDI).

Please see the Specification section for more details on assignment submission requirements.

Scenario:

Adventure Scuba and Diving Institute (ASDI) is located in the United States and offers training and certification programs for scuba and deep sea diving. ASDI is a premier training school in the area of diving and scuba and has

developed a wealth of proprietary training resources, videos, guides and manuals. The school suspects that competitors have tried to breach the organization's computer systems to gain access to these training materials.

ASDI's network is comprised of two web servers, two file servers, one email server, 50 employee workstations, and a 50-workstation student computer lab. The school also has public and private Wi-Fi availability throughout the campus.

Your firm has been hired as the IT security analyst to review, evaluate, and make recommendations with respect to maintenance of security of the organization's computer and network systems. You have been charged by your supervisor to prepare a preliminary report documenting the most critical security threats that ASDI faces. Your supervisor has given you the following resources that might be useful in your research and analysis:

- An article on the Help Net security Web site (*http://www.net-security.org/secworld.php?id=10154*)
- Common Vulnerabilities and Exposure (CVE) database search (*http://cve.mitre.org/find/index.html*)
- Security organizations, such as Secunia (*http://secunia.com/*)

Your supervisor has asked you to consider and account for the following questions as you shortlist the threats and prepare your report:

1. What threats are new this year and which have become more prevalent?
2. Why are these threats more common and why are they important?
3. What threats remain constant from year to year? Why?
4. What threats do you believe will become more critical in the next twelve months? Why?
5. Has an exploit been released?
6. What is the likelihood of an exploit?
7. How widely used is the software or system?

Specifications for this Assignment:

1. Submit the report as a single presentation in Microsoft PowerPoint format.
2. –Ten to fifteen content slides in length (Slides should follow the 6x6 rule – no more than six bullets and no more than six words in each bullet.)
3. Presentation and citation formatting should be in conformity with the *CSU-Global Guide to Writing and APA Requirements*.
4. Cite and discuss at least three credible sources other than (or in addition to) the course textbook. The three sources recommended in this assignment description may be among these sources, which may also include sources found via Web search or in the CSU-Global Library.
5. Include in your presentation a network diagram of how you propose the network structure should be configured for optimum security. You can create this diagram using any drawing tool, including those embedded in PowerPoint, Visio, or by drawing the diagram by hand, scanning into an image file, and then pasting into your report.
6. The sections of your report should be as follows:
    - Cover Page (Slide 1, not included in total number of slides)
    - Table of Contents (Slide 2, not included in total number of slides)

- Executive Summary (*provide a project overview and summary here)*
- Body of the report in in two sections: Section 1 of the on Vulnerabilities and Threats in narrative form, providing responses to each of the questions posed in the assignment scenario, and Section 2 on Countermeasures and Prevention
- Network Diagram
- References (not part of total number of slides).

Course Policies

Course Grading

20% Discussion Participation
8% Mastery Exercises
37% Critical Thinking Activities
35% Final Portfolio Paper

Grading Scale and Policies

A	95.0 – 100
A-	90.0 – 94.9
B+	86.7 – 89.9
B	83.3 – 86.6
B-	80.0 – 83.2
C+	75.0 – 79.9
C	70.0 – 74.9
D	60.0 – 69.9
F	59.9 or below

In-Classroom Policies
For information on late work and Incomplete grade policies, please refer to our **In-Classroom Student Policies and Guidelines** or the Academic Catalog for comprehensive documentation of CSU-Global institutional policies.

Academic Integrity
Students must assume responsibility for maintaining honesty in all work submitted for credit and in any other work designated by the instructor of the course. Academic dishonesty includes cheating, fabrication, facilitating academic dishonesty, plagiarism, reusing /re-purposing your own work (see *CSU-Global Guide to Writing and APA Requirements* for percentage of repurposed work that can be used in an assignment), unauthorized possession of academic materials, and unauthorized collaboration. The CSU-Global Library provides information on how students can avoid plagiarism by understanding what it is and how to use the Library and Internet resources.

Citing Sources with APA Style
All students are expected to follow the *CSU-Global Guide to Writing and APA Requirements* when citing in APA (based on the APA Style Manual, 6th edition) for all assignments. For details on CSU-Global APA style, please review the APA resources within the CSU-Global Library under the "APA Guide & Resources" link. A link to this document should also be provided within most assignment descriptions in your course.

Netiquette
Respect the diversity of opinions among the instructor and classmates and engage with them in a courteous, respectful, and professional manner. All posts and classroom communication must be conducted in accordance

with the student code of conduct. Think before you push the Send button. Did you say just what you meant? How will the person on the other end read the words?

Maintain an environment free of harassment, stalking, threats, abuse, insults or humiliation toward the instructor and classmates. This includes, but is not limited to, demeaning written or oral comments of an ethnic, religious, age, disability, sexist (or sexual orientation), or racist nature; and the unwanted sexual advances or intimidations by email, or on discussion boards and other postings within or connected to the online classroom.

If you have concerns about something that has been said, please let your instructor know.