



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.

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:

In ITS425, you are introduced to the application of ethical hacking techniques and penetration testing for IT security. You will 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. You 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 you 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.

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

Textbook Information is located in the CSU-Global Booklist on the Student Portal.

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 at 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:** Assignments are due Sunday at 11:59 p.m. MT.

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!

WEEKLY READING AND ASSIGNMENT DETAILS

Module 1 Introduction to Computer Hacking

Readings

- Chapters 1 & 2 in *Hacker Techniques, Tools, and Incident Handling*
- CISSP online training: Telecommunications and networking. (2016, June 30). *ICT Monitor Worldwide*.
- Dsouza, Z. (2018). Are cyber security incident response teams (csirts) redundant or can they be relevant to international cyber security? *Federal Communications Law Journal*, 69(3), 201.
- French, L. (2017). Virtual case notes: \$7 Hacking tool swipes passwords with ease. *Forensic Magazine*.
- Martin, C. (2017). Taking the high road white hat, black hat: the ethics of cybersecurity. *ACM Inroads*, 8(1), 33-35.
- McDonald, T. (2018). Addressing cybersecurity: UK nao efforts to tackle increasing challenges. *International Journal of Government Auditing*, 45(2), 18-19.

Opening Exercise (0 points)

Discussion (25 points)

Critical Thinking (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, three-commerce Web application server is acting as an external point-of-entry into the network: <ul style="list-style-type: none">• 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, and

- Schedule.

Your penetration testing plan should be 2-3 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.

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 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 1 page in length that describes the challenges you faced and explains what you learned from the lab activity.

Mastery Exercise (10 points)

Module 2 Network Reconnaissance

Readings

- Chapters 3 & 4 in *Hacker Techniques, Tools, and Incident Handling*
- Cryptography. (2017). *Funk & Wagnalls New World Encyclopedia*, 1p. 1.
- Meyer, C. (2015). Retain your relevance: Study cybersecurity. *Security: Solutions for Enterprise Security Leaders*, 52(11), 97-98.
- Schneider, J. D. (2016). Lights out. *Energy Law Journal*, 37(2), 433-443.
- Why everything is hackable; Computer security. (2017). *The Economist*, 423(9035), 71.

Opening Exercise (0 points)

Discussion (25 points)

Critical Thinking (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 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 1 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 1 page in length that describes the challenges you faced and explains what you learned from the lab activity.

Mastery Exercise (10 points)

Live Classroom (0 points)

1-hour session with provided PowerPoint presentation

Module 3 Footprinting, Port Scanning and Systems Reconnaissance

Readings

- Chapters 5 & 6 in *Hacker Techniques, Tools, and Incident Handling*
- Domas, S. (2018, February). Top 6 challenges in tackling cybersecurity of medical devices in hospitals. *Security Technology Executive*, 28, 12-12,14.
- Glassman, J. K. (2016). My 10 top picks for 2016. *Kiplinger's Personal Finance*, 70(1), 25-26.
- Rashid, F. Y. (2016). Nmap security scanner gets new scripts, performance boosts. *InfoWorld.com*.

Opening Exercise (0 points)

Discussion (25 points)

Mastery Exercise (10 points)

Module 4 System Enumeration and Wireless Security

Readings

- Chapters 7 & 8 in *Hacker Techniques, Tools, and Incident Handling*
- Frenkel, K. A. (2015). Password cracking tops IT's security concerns. *CIO Insight*, 2.
- Kamping-Carder, L. (2016). Keep your smart home safe from hackers; As internet-connected devices in homes grow more popular, so do the risks of unwanted intruders. *Wall Street Journal (Online)*, p. N/a.
- Talbot, C. M., Temple, M. A., Carbino, T. J., & Betances, J. A. (2018). Detecting rogue attacks on commercial wireless Insteon home automation systems. *Computers & Security*, 74, 296-307.

Opening Exercise (0 points)

Discussion (25 points)

Critical Thinking (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; and
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 1-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 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 1-page in length that describes the challenges you faced and explains what you learned from the lab activity.

Mastery Exercise (10 points)

Module 5 Web Based Attacks and System Malware Threats

Readings

- Chapters 9 & 10 in *Hacker Techniques, Tools, and Incident Handling*
- Dennis, C. (2018). Why is patch management necessary? *Network Security*, 2018(7), 9-13.
- Millard, W. (2017). Where bits and bytes meet flesh and blood: hospital responses to malware attacks. *Annals of Emergency Medicine*, 70(3), A17-A21.
- PR Newswire. (2017). More than three quarters of vulnerabilities are disclosed on dark web and security sources before national vulnerability database publication.

Opening Exercise (0 points)

Discussion (25 points)

Critical Thinking (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; yourname_ResidentShield-scan.csv*. 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.
3. Write a summary narrative at least 1-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 which will be your deliverable for this assignment and serve as proof that you have completed the lab.

Mastery Exercise (10 points)

Live Classroom (0 points)

1-hour session with provided PowerPoint presentation; may be in Week 5 or 6 (but not both)

Module 6 Maintaining System Access

Readings

- Chapters 11 & 12 in *Hacker Techniques, Tools, and Incident Handling*

- Dao, N., Kim, J., Park, M., & Cho, S. (2016). Adaptive suspicious prevention for defending DOS attacks in SDN-based convergent networks. *PLoS One*, 11(8), E0160375.
- Merlo, A., Costa, G., Verderame, L., & Armando, A. (2016). Android vs. SEAndroid: An empirical assessment. *Pervasive and Mobile Computing*, 30, 113-131.
- Rorot. (2015). Session hijacking cheat sheet. Retrieved from <http://resources.infosecinstitute.com/session-hijacking-cheat-sheet/>

Opening Exercise (0 points)

Discussion (25 points)

Critical Thinking (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 1-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 used 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 which will be your deliverable for this assignment and serve as proof that you have completed the lab.

Mastery Exercise (10 points)

Live Classroom (0 points)

1-hour session with provided PowerPoint presentation; may be in Week 5 or 6 (but not both)

Module 7 Elements of Social Engineering and IT Security Incident Response

Readings

- Chapters 13 & 14 in *Hacker Techniques, Tools, and Incident Handling*
- Junger, M., Montoya, M., & Overink, F. J. (2017). Priming and warnings are not effective to prevent social engineering attacks. *Computers in Human Behavior*, 66(C), 75-87.
- Van der Kleij, R., Kleinhuis, G., & Young, H. J. (2017). Computer security incident response team effectiveness: A needs assessment.

Opening Exercise (0 points)

Discussion (25 points)

Mastery Exercise (10 points)

Module 8 Defending and Protecting IT Systems

Readings

- Chapter 15 in *Hacker Techniques, Tools, and Incident Handling*
- Aburomman, A. A., & Reaz, M. B. I. (2017). A survey of intrusion detection systems based on ensemble and hybrid classifiers. *Computers & Security*, 65, 135-152.
- Van der Kleij, R., Kleinhuis, G., & Young, H. J. (2017). Computer security incident response team effectiveness: A needs assessment.

Opening Exercise (0 points)

Discussion (25 points)

Mastery Exercise (10 points)

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 website
- Common Vulnerabilities and Exposure (CVE) database search
- Security organizations, such as Secunia

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

- What threats are new this year and which have become more prevalent?
- Why are these threats more common and why are they important?
- What threats remain constant from year to year? Why?
- What threats do you believe will become more critical in the next 12 months? Why?
- Has an exploit been released?
- What is the likelihood of an exploit?
- How widely used is the software or system?

Specifications for this Assignment:

- Submit the report as a single document in Word format.
- 8-10 pages in length
- Document and citation formatting should be in conformity with the CSU-Global Guide to Writing and APA Requirements.
- 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.
- 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.
- The sections of your report should be as follows:
 - Cover Page
 - Table of Contents
 - Executive Summary (*provide a project overview and summary in this section*)
 - 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 (350 Points)

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 website

- Common Vulnerabilities and Exposure (CVE) database search
- Security organizations, such as Secunia

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 12 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. 10-15 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 in this section*)
 - 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

Grading Scale	
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

Course Grading

20% Discussion Participation
8% Mastery Exercises
37% Critical Thinking Assignments
35% Final Portfolio Project

SAMPLE

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 /repurposing your own work (see CSU-Global Guide to Writing & APA 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 & APA when citing in APA (based on the most recent APA style manual) for all assignments. A link to this guide should also be provided within most assignment descriptions in your course.

Disability Services Statement

CSU-Global is committed to providing reasonable accommodations for all persons with disabilities. Any student with a documented disability requesting academic accommodations should contact the Disability Resource Coordinator at 720-279-0650 and/or email ada@CSUGlobal.edu for additional information to coordinate reasonable accommodations for students with documented disabilities.

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.