Colorado State University
GLOBAL CAMPUS

ISM531: CYBER SECURITY DEFENSE AND COUNTERMEASURES

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:

The Cyber Security Defense and Countermeasures course prepares students to defend enterprise networks and protect enterprise data assets from Web-based and internal attacks using techniques such as system hardening, encryption, policy enforcement, and software/hardware intrusion detection systems.

Course Overview:

This course looks at management issues and practical implications related to securing information systems. It focuses on the following topics: threat environment; security policy and planning; cryptography, secure networks; access control; firewalls; host hardening; application security; data protection; incident response; and networking and a review of TCP/IP. A clear theoretical understanding supports a large practical component where students learn to audit information systems and use contemporary security software.

Course Learning Outcomes:

1. Evaluate techniques to improve network security defense against regional and international threats.
2. Analyze a network for vulnerabilities to common cyber based attacks.
3. Summarize encryption techniques for securing enterprise data.
4. Recommend a strategy to protect digital assets from virus, malware, and other cyber-attacks.
5. Demonstrate an ability to analyze organizational networks and provide sound recommendations to protect digital assets from virus, malware, and other cyber-attacks.

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

Required:
Boyle, R. J., & Panko, R. R. (2015). *Corporate computer security* (4th ed.). Upper Saddle River, NJ: Pearson Education. ISBN-13: 9780133545197

***NOTE:** All non-textbook required readings and materials necessary to complete assignments, discussions, and/or supplemental or required exercises are 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 at 11:59 p.m. MT. Late posts may not be awarded points.
- **Critical Thinking:** Assignments are due Sunday at 11:59 p.m. MT.

Weekly Reading and Assignment Details

Module 1

Readings

- Chapter 1 in *Corporate Computer Security*
- Willingham, T., Henderson, C., Kiel, B., Haque, M. S., & Atkison, T. (2018). Testing vulnerabilities in bluetooth low energy. In Proceedings of the ACMSE 2018 Conference: Article (6), 1–7. doi.org/10.1145/3190645.3190693
- Le, D. C., Khanchi, S., Zincir-Heywood, A. N., & Heywood, M. I. (2018). Benchmarking evolutionary computation approaches to insider threat detection. In Proceedings of the Genetic and Evolutionary Computation Conference, 1286–1293. doi.org/10.1145/3205455.3205612

Discussion (25 points)

Module 2

Readings

- Chapters 1 & 2 (pages 27-80) in *Corporate Computer Security*
- TutorialsPoint (2018) Ethical hacking. Retrieved from https://www.tutorialspoint.com/ethical_hacking/ethical_hacking_tutorial.pdf
- Slatalla, M (2018) Hackers’ hall of fame. Retrieved from http://www.dvara.net/hk/hackers'_hall_of_fame.pdf

Discussion (25 points)

Critical Thinking (90 points)

Choose one of the following two assignments to complete this week. Do *not* complete both assignments. Identify your assignment choice in the title of your submission. Note that while there are two options for the Critical Thinking assignment, there is only one rubric. Review the rubric to confirm you are meeting the assignment requirements.

Option #1: Compliance Assessment Report

You have been hired as chief information security officer at a large publicly traded company. The company currently has a network of 25 offices nationwide. Each of these offices handles financial, medical, and payment information for thousands of clients.

Your CEO has asked you to prepare a report to point out what laws and regulations your organization needs to be compliant with, so they can share that information with the board of directors, who has asked for this report.

Your well-written paper should meet the following requirements:

- Be 3-4 pages in length.
- Contain an illustrative table or a diagram created from properly cited external references.
- Include two credible external references in addition to the textbook.
- Formatted according to the CSU-Global Guide to Writing and APA. The length is not inclusive of the title and reference pages. Be clear, concise, and focused.

Option #2: External Threats Report

You have been hired as chief information security officer at a large international company. The US-based company currently has ten (10) offices worldwide, nine (9) of which are in foreign countries. Each of these offices handles financial, confidential medical, and payment information for the clients within its national borders.

Your CEO has asked you to prepare a report to point out what external criminal and hacking threats exist, and what foreign laws and regulations your organization needs to be compliant with, so they can share that information with the board of directors, who has asked for this report.

Your well-written paper should meet the following requirements:

- Be 3-4 pages in length.
- Contain an illustrative table or a diagram created from properly cited external references.
- Include two credible external references in addition to the textbook.
- Formatted according to the CSU-Global Guide to Writing and APA. The length is not inclusive of the title and reference pages. Be clear, concise, and focused.

Portfolio Milestone (25 points)

Submit your Portfolio Topic to your instructor for preliminary approval. Provide reasons for your choice. Your submission should contain no more than 1 page of content, framed by a cover page and references page. This assignment is required and is worth 25 points.

Module 3

Readings

- Chapter 2 (pages 81-120) and Chapter 3 in *Corporate Computer Security*
- Paletov, R., Tsankov, P., Raychev, V., & Vechev, M. (2018). Inferring crypto API rules from code changes. In Proceedings of the 39th ACM SIGPLAN Conference on Programming Language Design and Implementation, 450–464. doi.org/10.1145/3192366.3192403
- Arezki, S., & Elhissi, Y. (2018). Toward an IT governance maturity self-assessment model using EFQM and CobiT. In Proceedings of the International Conference on Geoinformatics and Data Analysis, 198–202. doi.org/10.1145/3220228.3220265

Discussion (25 points)

Critical Thinking (90 points)

Choose one of the following two assignments to complete this week. Do *not* complete both assignments. Identify your assignment choice in the title of your submission. Note that while there are two options for the Critical Thinking assignment, there is only one rubric. Review the rubric to confirm you are meeting the assignment requirements.

Option #1: Hands-On Project—Enigma® Machine Simulator
This project uses an Enigma® machine simulator. It functions like the Enigma machines used during WWII. This example has been included to help you better understand how encryption worked in the early days. It is a great learning tool for when you first start exploring the subject of cryptography. Enigma machines provided good encryption strength for their day. Modern cryptographic systems are much more secure than Enigma machines.

Pay attention to the colored paths as you type. The red path goes through the three rotors, bounces off the reflector, becomes green, and then goes back through the three rotors. The right rotor moves with each keystroke. If it completes one full cycle, it will advance the middle rotor and, subsequently, the left rotor as well.

Directions:

1. Open a web browser and go to http://enigmaco.de/enigma/enigma.swf.
2. Use the left and right arrows to move each of the top three rotors so that each has the letter "A" selected in blue.
3. Click in the Input text box in the bottom of your screen.
4. Slowly type your first name and last name without a space. (If you make a typing error you can start over by pressing the backspace key.)
5. *Take a screenshot.*

   Note: The text in the Input text box is what you typed. The text in the Output text box is what you would send. You are now going to reset the dials to their original position (in this case AAA) and type the encrypted text (cipher text) you produced in the Output text box. You can copy the cipher text from the screenshot you just took. Subsequently, you should see your name reproduced in the bottom box. This is the equivalent of decrypting the message.

6. Click in the Input text box and backspace your name. (The rotors should be set back to their AAA position.)
7. Refer back to the screenshot you just took and copy down the output (cipher text).
8. Type the cipher text into the Input text box. (Type slowly so you do not make a mistake and have to start over.)
9. *Take a screenshot* with your name showing in the Output text box.
10. Backspace the text in the Input text box.
11. Slowly press the A key ten times and notice how a different encrypted letter is chosen as output through the rotating dials even though you are hitting the same key each time.
12. *Take a screenshot.*

Submit your screenshots and answer the following questions:

- Why did Enigma machines use multiple rotors?
- How did WWII cryptographers know which rotor settings to use?

Your well-written paper should meet the following requirements:

- Be 3-4 pages in length.
- Contain an illustrative table or a diagram created from properly cited external references.

- Include two credible external references in addition to the textbook.
- Formatted according to the CSU-Global Guide to Writing and APA. The length is not inclusive of the title and reference pages. Be clear, concise, and focused.

Option #2: Security Plan Assessment
You have been hired as chief information technology officer at a rapidly growing company. The company is young and has only 50 employees, and there is no security plan in place yet.

Your CEO has asked you to prepare a report and recommendation about which of the following three frameworks—1) COSO, 2) CobiT, and 3) ISO/IEC 27000 Family—should be adopted by the company in order to create a security plan.

Your well-written paper should meet the following requirements:

- Be 3-4 pages in length.
- Contain an illustrative table or a diagram created from properly cited external references.
- Include two credible external references in addition to the textbook.
- Formatted according to the CSU-Global Guide to Writing and APA. The length is not inclusive of the title and reference pages. Be clear, concise, and focused.

Module 4

Readings

- Chapters 4 & 5 in *Corporate Computer Security*
- Bertino, E., Jabal, A. A., Calo, S., Verma, D., & Williams, C. (2018). The challenge of access control policies quality. *Journal of Data and Information Quality, 10*(2), 1–6. doi.org/10.1145/3209668
- Mukherjee, P., & Mazumdar, C. (2018). Attack difficulty metric for assessment of network security. In Proceedings of the 13th International Conference on Availability, Reliability and Security, 1–10. doi.org/10.1145/3230833.3232817

Discussion (25 points)

Critical Thinking (90 points)

Choose one of the following two assignments to complete this week. Do *not* complete both assignments. Identify your assignment choice in the title of your submission. Note that while there are two options for the Critical Thinking assignment, there is only one rubric. Review the rubric to confirm you are meeting the assignment requirements.

Option #1: Hands-On Project—Password Testing
Let us evaluate the strength of one of your current passwords. Just because an attacker steals your password database does not mean he or she automatically knows your password. He or she still must crack it. Creating a strong password can make it impractical for an attacker to crack your password.

There are several online tools that help users learn more about strong passwords. These tools can help you understand the differences between strong and weak passwords.

Directions:

1. Go to: https://howsecureismypassword.net/.
2. Enter one of the passwords you use on a regular basis with a minor change.
3. *Take a screenshot.*
4. Take note of the problems with your password (e.g., a number sequence and a dictionary word).
5. Try entering a password you might actually use that you think is strong.

6. *Take a screenshot of the results.*

Submit your screenshots and answer the following questions:

- Why do special characters (e.g., @, #, $, %, ^, &, or *) make passwords difficult to crack?
- Why does a change of case help make a stronger password?
- How did you choose the password you currently have?
- Could others follow the same logic and choose a similar password?
- Do you use the same password for multiple accounts? Why would this be a security risk?

Your well-written paper should meet the following requirements:

- Be 3-4 pages in length.
- Contain an illustrative table or a diagram created from properly cited external references.
- Include two credible external references in addition to the textbook.
- Formatted according to the CSU-Global Guide to Writing and APA. The length is not inclusive of the title and reference pages. Be clear, concise, and focused.

Option #2—Network Security and Access Control

You are a senior network security professional at your company. Your company has 150 employees. Each employee has his or her own terminal to access the company's network. There are also 15 wireless access points to support access for portable devices.

You are charged with the task of assessing the current wireless network vulnerabilities and pointing out how threats can exploit theses vulnerabilities to launch security breaches. In addition, you are required to provide recommendations related to access control to reduce possible risks.

Your well-written paper should meet the following requirements:

- Be 3-4 pages in length.
- Contain an illustrative diagram for the network and the suggested access control.
- Include two credible external references in addition to the textbook.
- Formatted according to the CSU-Global Guide to Writing and APA. The length is not inclusive of the title and reference pages. Be clear, concise, and focused.

Portfolio Milestone (25 points)

Submit an outline of your Portfolio Project.

- State your paper topic.
- Provide four scholarly articles that you might consider using for your final Portfolio Project. Give a short reason why each would be pertinent to your project. This is not expected to be a final list. The goal here is to motivate you to begin examining research that might help you in your final Portfolio Project.
- Add a reference section for your research sources.
- Format your outline according to the CSU-Global Guide to Writing and APA.

Module 5

Readings

- Chapter 6 in *Corporate Computer Security*
- Module "A," pages 578-617, in *Corporate Computer Security*
- Dixit, V. H., Kyung, S., Zhao, Z., Doupé, A., Shoshitaishvili, Y., & Ahn, G.-J. (2018). Challenges and preparedness of SDN-based firewalls. In Proceedings of the 2018 ACM International Workshop on

Security in Software Defined Networks & Network Function Virtualization, 33–38. doi.org/10.1145/3180465.3180468

Discussion (25 points)

Critical Thinking (90 points)

Choose one of the following two assignments to complete this week. Do *not* complete both assignments. Identify your assignment choice in the title of your submission. Note that while there are two options for the Critical Thinking assignment, there is only one rubric. Review the rubric to confirm you are meeting the assignment requirements.

Option #1: Hands-On Project—Firewall Rules

In this project, you will create two simple firewall rules in Windows Advanced Firewall. This may be the first time you have made a modification to the firewall on your computer. The first rule will block all ICMP traffic. This will effectively prevent you from using the ping command to send ICMP packets to other computers. You will use a command prompt to verify the rule was effective.

The second rule will block all outgoing Port 80 traffic. Port 80 is traditionally associated with web traffic (HTTP). Once you create and enable the rule, all outgoing Port 80 traffic will be blocked. You will use a web browser to verify the rule was effective; however, secure web traffic (HTTPS) running over Port 443 will still be accessible.

Both of the rules in this project will apply to outgoing traffic only. It is important to remember to disable the rules at the end of the project so your ICMP and Port 80 traffic will not be blocked.

Directions:

1. Click Start.
2. In the search box, type cmd
3. Press Enter.
4. Type ping www.google.com
5. Press Enter. (This will ping www.Google.com)
6. Type time
7. Press Enter twice.
8. Take a screenshot.
9. Click Start, Control Panel, System and Security, and Windows Firewall.
10. Click Advanced settings.
11. Click Outbound Rules.
12. Click New Rule (right-hand pane).
13. Click Custom, Next, and Next.
14. Change the dropdown box to ICMPv4.
15. Click Next, Next, Next, and Next.
16. Name the rule YourName_Block_ICMP. (Replace YourName with your first and last names. In this case, it was RandyBoyle_Block_ICMP.)
17. Click Finish.
18. Return to your command prompt.
19. Type ping www.google.com
20. Press Enter. (This will ping www.google.com. You should get a "General failure" error.)
21. Type time
22. Press Enter twice.
23. Take a screenshot.
24. Open a web browser.
25. Browse to www.Google.com. (This will verify that you do have internet access.)
26. Return to the Windows Advanced Firewall window.

27. Click Outbound Rules.
28. Click New Rule (right-hand pane).
29. Click Port, and Next.
30. Type “80” into the text box for Specific remote ports. (This will effectively block all outgoing web traffic from your computer. You will disable/delete this rule later.)
31. Click Next, Next, and Next.
32. Name the rule YourName_Block_Port_80. (Replace YourName with your first and last names. In this case, the rule was named RandyBoyle_Block_Port_80.)
33. Click Finish.
34. Return to your web browser.
35. Browse to any non-secure (not HTTPS) website of your choosing. You can browse to any website as long as it does not make an HTTPS connection (Port 443). The rule you made only blocks Port 80 web traffic.
36. Take a screenshot of the blocked website. (In this case, it was www.Microsoft.com.)
37. Return to the Windows Advanced Firewall window.
38. Select both of the rules you created.
39. Right-click the selected rules.
40. Click Disable Rule. (If you do not disable the rules, your ICMP and web traffic will still be blocked.)
41. Take a screenshot of your disabled rules.

Submit your screenshots and answer the following questions:

- How could blocking all ICMP traffic protect you?
- Could you still access some websites with your Port 80 rule enabled? Why?
- Why would you want to allow incoming (not outgoing) Port 443, but block incoming Port 80?
- Could malware rename itself in order to get through a firewall? Why would this work?

Your well-written paper should meet the following requirements:

- Be 2-4 pages in length.
- Contain an illustrative table or a diagram created from properly cited external references.
- Include two credible external references in addition to the textbook.
- Formatted according to the CSU-Global Guide to Writing and APA. The length is not inclusive of the title and reference pages. Be clear, concise, and focused.

Option # 2: Hands-On Project—Wireshark

One of the most well-known packet sniffers is called **Wireshark**® (formerly Ethereal®). It is a powerful tool that can capture, filter, and analyze network traffic. It can promiscuously capture traffic on both wired and wireless networks. It is used by security and networking professionals to troubleshoot networking problems.

In this project, you will install Wireshark, capture packets, and look at the contents of a packet.

1. Download Wireshark from: http://www.wireshark.org/download.html.
2. Click Download Windows Installer. (Download the latest stable release.)
3. Click Save.
4. Save the file in your download folder.
5. If the program does not automatically open, browse to your download folder.
6. Double-click Wireshark-setup-2.2.0.exe. (The software version numbers will be slightly different as newer versions are released. Use latest “Stable Version”)
7. Click Next, I Agree, Next, Next, Next, and Install.
8. Click Next to install WinPCap.

9. Click Next, I Agree, Install, and Finish.
10. Click Next, and Finish.
11. Double-click the Wireshark icon on your desktop. (You can also access it through your Start menu.)
12. Click Interface List. (This will display a list of all available network interfaces on your computer. You will want to want to note the description and IP address of the interface with the most traffic. You will need to select this interface in the following steps.)
13. Note the interface with the most traffic. (You will select this interface in the following steps.) If there are duplicate names for the Network Interface Card (NIC), you can use the last three or four values of the MAC address to identify the appropriate NIC.
14. Close the Capture Interfaces window.
15. Click Capture, and Options.
16. Select your Network Interface Card (NIC) if it is not already selected.
17. Take a screenshot.
18. Close *all* other programs you currently have open except your word processing program (MS Word, or LibreOffice Writer®, for example).
19. Click Start.
20. Let it run for 10 seconds.
21. While you are waiting open a web browser and go to www.google.com.
22. Return to your Wireshark window.
23. In the file menu click Capture and Stop (or use the keyboard shortcut—Ctrl+E).
24. Scroll up until you see a green and blue area. (These are the packets you captured when you requested Google's main page.)
25. Take a screenshot.
26. Scroll down until you see a line that has GET / HTTP/1.1. (You may have to try more than one until you get to the packet that shows "www.google.com" in the bottom pane.)
27. Select that row.
28. In the bottom pane, you will see a bunch of numbers to the left. (It is the packets contents in hexadecimal.) Just to the right you will see the content of the packet in a column.
29. Select the text: www.google.com.
30. Take a screenshot.

Submit your screenshots and answer the following questions:

- What do the different colors in the Wireshark packet capture listing mean?
- Identify the traffic you see coming in and out of the network?
- What Hostnames are being requested and who is requesting them?
- Is surfing the web anonymous? Using the Wireshark exercise, explain you answer.

Your well-written paper should meet the following requirements:

- Be 2-4 pages in length.
- Contain an illustrative table or a diagram created from properly cited external references.
- Include two credible external references in addition to the textbook.
- Formatted according to the CSU-Global Guide to Writing and APA. The length is not inclusive of the title and reference pages. Be clear, concise, and focused.

Module 6

Readings

- Chapters 7 & 8 in *Corporate Computer Security*
- Kapoor, N. (2018). Host hardening – Achieve or avoid. Retrieved from https://www.owasp.org/images/8/83/Host_review_owasp_2016.pdf

- Thomas, T. W., Tabassum, M., Chu, B., & Lipford, H. (2018). Security during application development: an application security expert perspective. 2018 CHI Conference on Human Factors in Computing Systems, 1–12. https://doi.org/10.1145/3173574.3173836
- Kara, O., Ergüler, İ., & Anarim, E. (2016). A new security relation between information rate and state size of a keystream generator. *Turkish Journal of Electrical Engineering & Computer Sciences, 24*(3), 1916-1929. doi:10.3906/elk-1311-54.

Discussion (25 points)

Critical Thinking (90 points)

Choose one of the following two assignments to complete this week. Do *not* complete both assignments. Identify your assignment choice in the title of your submission. Note that while there are two options for the Critical Thinking assignment, there is only one rubric. Review the rubric to confirm you are meeting the assignment requirements.

Option #1: Facility Network Security: Assessment and Recommendations

You are the chief information technology officer at a small outpatient health care facility in Riyadh. The medical facility employs five specialist physicians, ten certified nurses, five administrative assistants, and two technicians. There are 25 clinical rooms. Each room is equipped with a computer. In addition, five computers are used by the administrative assistants for patients' appointments and records. All these computers are connected using a local area network. Physicians are supplied with portable devices that they can use to write e-prescriptions. These devices are connected wirelessly to the rest of the network.

As the chief information technology officer, you are charged with the task of evaluating the security status of the facility network and developing a report to recommend the directions that should be followed soon.

Your report should include the following materials:

- Existing and potential vulnerabilities and threats
- Suggestions and discussions of methods or tools that can be used to overcome the existing and potential security threats
- Discussion of encryption techniques that can be used for the wireless network and the selection and justification of a proper technique for this facility
- Discussion of the prevention of cyber-attacks and the proper maintenance needed to achieve this goal.

Your well-written paper should meet the following requirements:

- Be 3-4 pages in length.
- Contain illustrative diagrams for the considered systems.
- Include at least five credible external references in addition to the textbook.
- Formatted according to the CSU-Global Guide to Writing and APA. The length is not inclusive of the title and reference pages. Be clear, concise, and focused.

Option #2: Hands-On Project—Microsoft Windows Event Viewer®

Good administrators check their logs regularly. They need to know what went on when they were away. They need to look for intruders, compromised machines, stolen or deleted files, and so on. The list of things to look for can be extensive.

Microsoft Windows Event Viewer® is a simple program that organizes these logs in a way that makes them easy to view. Learning how Event Viewer works is a great training platform for beginners. It is also a useful diagnostic tool.

In this example, you will enable logging of security events, log in and out of your machine, and then look up the event in Event Viewer.

1. Click Start, Control Panel, System and Security, Administrative Tools, and Local Security Policy.
2. Click on Local Policies, and Audit Policy.
3. Double-click on the policy labeled “Audit account logon events.”
4. Select both Success and Failure.
5. Click OK.
6. Double-click on the policy labeled “Audit logon events.”
7. Select both Success and Failure.
8. Click OK.
9. Take a screenshot.
10. In the control panel, click System and Security, Administrative Tools, and Event Viewer.
11. Click Windows Logs, and Security.
12. Take a screenshot.
13. Log off your computer by clicking Start, the drop-down menu next to Shut down, and Log Off. (You do not need to shut all the way down.)
14. Log onto your computer by clicking your username and entering your password.
15. In the control panel, click System and Security, Administrative Tools, and Event Viewer.
16. Click Windows Logs, and Security.
17. Take a screenshot.
18. Double-click on the Logon/Logoff event that was just recorded.
19. Take a screenshot.
20. Click Close.
21. Click Applications and Services Logs, and Microsoft Office Sessions.
22. Click on one of the log events.
23. Take a screenshot.

Submit your screenshots and answer the following questions:

- Will these security logs track failed logon attempts? From remote machines too?
- Will it track security events other than just logon/logoff events?
- Can you use Event Viewer to view other logs?
- Why is there a log that tracks which Microsoft office programs you use and how long you use them?

Your well-written paper should meet the following requirements:

- Be 3-4 pages in length.
- Contain an illustrative table or a diagram created from properly cited external references.
- Include two credible external references in addition to the textbook.
- Formatted according to the CSU-Global Guide to Writing and APA. The length is not inclusive of the title and reference pages. Be clear, concise, and focused.

Module 7

Readings

- Chapters 9 & 10 (pages 525-562) in *Corporate Computer Security*
- Tesfay, W. B., Hofmann, P., Nakamura, T., Kiyomoto, S., & Serna, J. (2018). I read but don’t agree: Privacy policy benchmarking using machine learning and the EU GDPR. Presented at the Companion Proceedings of The Web Conference, 163–166. https://doi.org/10.1145/3184558.3186969

- Smith, J. M., Greenlee, E., & Ferber, A. (2017). Demo: Akatosh: Automated cyber incident verification and impact analysis. In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, 2463–2465. doi.org/10.1145/3133956.3138854

Discussion (25 points)

Module 8

Readings

- Chapter 10 (pages 563-578) in *Corporate Computer Security*
- Lee, K. H., Kwong, C. K., Zaki, R., Emig, K., & Tucker, J. (2018). Dawn: Improving hurricane response for citizens and local governments. Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems, 1–6. doi.org/10.1145/3170427.3180650

Discussion (25 points)

Portfolio Project (300 points)

Choose one of the following two Portfolio Projects to complete. Do not do both assignments. Identify your assignment choice in the title of your submission. Review the Portfolio Project grading rubric to understand how you will be graded on your project.

Option #1: Hands-On Project—HoneyBOT®

HoneyBOT® is a simple honeypot for beginners to use. Honeypots can give you a good idea of how many people are probing your machine for weaknesses. Without a honeypot, you may not be able to tell if anyone is scanning your machine.

In this example, you will use your qweb browser to generate some entries in HoneyBOT. You will try to make FTP and HTTP connections with your own computer. The honeypot will record the IP address of the remote machine that is scanning your computer and each port that was scanned.

1. Download HoneyBOT from: http://www.atomicsoftwaresolutions.com/honeybot.php.
2. Click on the Download link in the left-hand menu.
3. Click on the appropriate "here" link to download the latest version of HoneyBOT.
4. Click Save.
5. Select your downloads folder.
6. Browse to your downloads folder.
7. Double-Click HoneyBOT_018.exe. (The version number may be different as newer releases become available.)
8. Click Run, Next, I Accept, Next, Next, and Next.
9. Check Create desktop icon.
10. Click Next, Install, and Finish.
11. Press the Start button or click File, and Start.
12. HoneyBOT may ask you to select an adapter if you have multiple NICs in your computer; select your current IP address. (It could be a non-routable IP that starts with "192.168" or it could be a typical IP address.)
13. Click OK.
14. Take a screenshot showing the total number of sockets loaded in the bottom status bar.
15. Click Start.
16. Open a web browser and go to FTP://[Your IP Address]. (Replace Your IP Address with the IP address that is being used by HoneyBOT. In this example, it was ftp://155.97.74.45.)
17. When prompted for a username, enter your first name.

18. Enter your last name for the password. (Entering your first and last name as username and password will record them in the HoneyBOT log. You do not really have an FTP server running. It is being "faked" by HoneyBOT.)
19. Open a web browser and go to HTTP://[Your IP Address]. (Replace Your IP Address with the IP address that is being used by HoneyBOT.)
20. Return to HoneyBOT and take a screenshot.
21. Double-click on one of the entries with the local port listing 21. (The remote IP and local IP should be the same.)
22. Take a screenshot of the HoneyBOT log entry showing your first and last name being used to access an FTP server.

Submit your screenshots and answer the following questions:

- What impact would more open ports have on the ability of your honeypot to attract hackers?
- Can hackers tell that you have a honeypot running?
- Do they have honeypots for spammers to keep them from harvesting emails from your webpages?
- Do you think law enforcement agencies (e.g., CIA, FBI, and NSA) in the United States run honeypots to track criminal behavior?

Directions:

- The content of the paper must be 8-10 pages in length and formatted according to the CSU-Global Guide to Writing and APA.
- A minimum of six references (in addition to course materials, like the textbook or articles), with at least two of these being peer-reviewed articles. The CSU-Global Library is a good place to search for credible, scholarly sources.

Option 2: Portfolio Project Hands-On Project—Recuva®
Recuva® is a useful program by Piriform® that will scan the empty memory space on your computer to see if there are any files that can be recovered. It can also securely delete files, so they cannot be recovered.

Most users errantly believe that data is gone forever when they empty it from the Recycle Bin. This is incorrect. It merely marks the space as open to be written over if another file needs to be stored. Your operating system writes over these open spaces and subsequently “damages” the previously deleted file.

1. Download Recuva from: http://www.recuva.com/download (or, http://www.piriform.com/recuva/download).
2. Click Download from FileHippo.com.
3. Click Download Latest Version.
4. Click Save.
5. If the program does not automatically open, browse to your download folder.
6. Run the installation program.
7. Select Run, Ok, Next, I Agree, Install, and Finish.
8. Click Start, Programs, Recuva, and Recuva (or you can double-click the Recuva desktop icon).
9. Select the drive from which you want to recover files. (Your C: drive will work, but it will take longer to complete the scan. The scan will complete much more quickly on a USB drive.)
10. Click Scan.
11. After the scan completes, click on any of the recovered files listed with a graphic extension (e.g., .jpg or .bmp) until you see a picture on the right-hand side of the screen.
12. Take a screenshot.

13. Click on the Info tab to see the details for the file.
14. Take a screenshot.
15. Check one of the recoverable graphic files. (Even some of the “unrecoverable” files are actually recoverable.)
16. Click Recover.
17. Save it to your desktop.
18. Open the picture you recovered.
19. Take a screenshot.

Submit your screenshots and answer the following questions:

- Does Piriform offer software that works like Recuva on your cell phone?
- What effect does the “condition” of the file have on its ability to be recovered?
- What other recovery options does Recuva come with?
- Does Recuva have the ability to find a deleted file by its specific file name, and if so, how?

Directions:

- The content of the paper must be 8-10 pages in length and formatted according to the CSU-Global Guide to Writing and APA.
- A minimum of six references (in addition to course materials, like the textbook or articles), with at least two of these being peer-reviewed articles. The CSU-Global Library is a good place to search for credible, scholarly sources.

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
45% Critical Thinking Assignments
35% Final Portfolio Project

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.