BSCSIA Course Kick Start Guide– C844

Course Applicability: C844, Emerging Technologies in Cybersecurity

The C844 course focuses on a comparison of evolving technologies to address the security requirements of an organization. Students learn underlying principles critical to the operation of secure networks and the adoption of new technologies. You will gain a working knowledge of WiresharkMAP tool functionality for identifying vulnerabilities, as well as explore WLAN and mobile device security concepts.

Prerequisite Courses:

Typically, successful students complete the course in ~**41 days.**

About This Guide

This Kick Start Guide can be used as a supplemental resource to help you get started with the course, get answers to frequently asked questions, and be leveraged to help with completing the performance assessment for the course. You can find the primary course material for the course by clicking the "Go To Course Material" button on your course page. Reach out to your assigned course instructor for additional guidance once assigned.

Guide Contents

What's Required to complete the Course

What to Produce

C844 has two tasks that must be completed and passed for you to complete the course. You must provide sufficient responses to the questions in the task requirements, capturing responses in a file type listed in the file restrictions section of your task requirements. The most common submissions are in the form of a .ppt or .doc document.

File Restrictions. File name may contain only letters, numbers, spaces, and these symbols: ! - _ . * ' ( ) File size limit: 200 MB File types allowed: doc, docx, rtf, xls, xlsx, ppt, pptx, odt, pdf, txt, qt, mov, mpg, avi, mp3, wav, mp4, wma, flv, asf, mpeg, wmv, m4v, svg, tif, tiff, jpeg, jpg, gif, png, zip, rar, tar, 7z

Page/Word Count and Formatting

Page/Word Count Minimum and Format

There is **no specified minimum or maximum page or word count requirement** for the tasks. You should simply look to provide complete responses to each question that satisfies what the task requirements and rubric call for. There is **no specific formatting or writing style** such as APA, MLA etc. requirement. You should, however, format your work using section headers that correlate to the specific task requirements/rubric points. Provide your responses to the specific task requirement points in the corresponding section of your work.

Format Recommendations: (1) Select the type of document you want to use (.doc, .ppt etc.), (2) create a title page containing your name, the course, and task number at minimum, and (3) include section/paragraph headers for each question (i.e. a header called "Describe network topology," as the header for task one, section A of the requirements). Provide the response to that section under the corresponding header in your work. Continue on the same path for each section of both tasks. Conclude with a reference page for the sources cited in your work.

Performance Assessments and Originality and Similarity Standards

Performance Assessments Basics and Unicheck

Need help getting started with your Performance Assessment, view the video Planning & Pre-writing a Performance Assessment, and the WGU Knowledge Center article Performance Assessment Submission, which covers assessment submission from start to finish.

Your submission must be your original work. No more than a combined total of ***30%*** of the submission and no more than a ***10%*** match to any one individual source can be directly quoted or closely paraphrased from sources, even if cited correctly. View Video linked here for similarity check procedures: ***Video on Reviewing Unicheck Reports-**

Sources and Citations FAQ

Sources and Citations Requirements

Q: Do I have to include in-text/in-line citations in my work?

A: yes, you do. Please be especially cognizant of this with working of your papers. If you choose to quote, paraphrase, or summarize content from a source, THEN you must acknowledge that source using in-text/in-line citations and an accompanying reference page/reference slide. Your work can be 100% original work if you choose.

Q: If I quote, paraphrase, or summarize content from a source, do I have to use APA format?

A: No, you do not. There is no specific writing style requirement for the assignment. This absence of a standard writing style however introduces ambiguity in what information is required for citations and reference lists that often leads to task returns for missing information. So, if you choose to quote, paraphrase, or summarize content from a source you should look to, at a minimum, include the core elements of author, date, and title for your citations and accompanying reference lists. A safe bet is to just optionally employ APA, or another style for the citation and references portion of your work regardless of how you format the whole work.

Q: If I want to quote, paraphrase, or summarize content from a source, where can I get help with formatting the citations and references?

A: There is no specified writing style you must use for the assignment, but there is a plethora of information on APA citations and references within the WGU Writing Center.

Q: How much of my work can be quoted, paraphrased, or summarized content from a source?

A: *No more than a combined total of 30% of the submission and no more than a 10% match to any one individual source.*

Q: Is properly cited information subject to the 30% total similarity threshold?

A: Yes. Your submission can have n*o more than a combined total of 30% similarity* ***even if cited correctly***.

Writing and Proofreading Help

Writing Center

WGU Writing Center

At the WGU Writing Center students will acquire the skills and resources they need to become stronger writers.

- writingcenter@wgu.edu
- Schedule an Appointment(Opens a new window)
- https://my.wgu.edu/success-centers/writing-center

Writing Center Help Line
(877) 435-7948 x2967

Back To Table of Contents

C844 Task Best Practices

1. Use Headers. Include headers in your submission that correspond to each task requirement/rubric section. This can be as simple as using the task letter code or an abbreviated version of the section (i.e. “A,” or “Describe the network topology” as the header for the first question, Task section A). Provide the response to that section under the corresponding header in your work.

2. Provide responses to answer the question, not necessarily for overall flow. Each section is evaluated as a standalone against the rubric. An essay/storyline approach often leaves actual answers to questions overlooked or hidden in paragraphs (I see many, many task returns due to this). Making your responses clear, complete, and organized under headers matching rubric points the way the templates I shared are structured, makes it easy for your evaluator to find them, which makes things better for you.

3. Pay attention to tenses. Look out for items that are plural in the requirements and ensure you provide two or more where applicable. For instance, section E states, “ Recommend solutions for eliminating or minimizing *all* identified vulnerabilities or anomalies from Wireshark and Nmap.” Here you would be mindful not to overlook the word “all” and make sure you recommend solutions for all identified vulnerabilities and anomalies.

4. Be blatant and alleviate guesswork/interpretation for your evaluator. Don’t assume the person evaluating your work can read your mind. Provide clarity in your responses by restating key parts of the questions in your responses.

5. Check spelling and grammar. Be sure to run spell check and proofread your work before submitting to avoid a task return for professional communication.

6. Run your similarity check. Be sure to run your similarity check and adjust your work to meet similarity requirements before submitting your work. Submitting work that doesn’t meet similarity results in an automatic task return with no feedback on content as no evaluation will be conducted.

7. Leverage the task guide, recorded cohorts, and templates!

Task 1

Requirement	**Guidance**	**Response steps**
A. Describe the network topology you found when running Nmap. Include screenshots as evidence of running Nmap.	Run a Nmap scan on the specified network in the lab environment.	You must take multiple screenshots of the results of running Nmap. You must also describe each host on the network. The description includes things like (IP address, # of open ports, type of operation system used, etc.)

Requirement	**Guidance**	**Response steps**
B. Summarize the vulnerabilities on the network and their potential implications based on your Nmap results.	From the Nmap results, identify at least three vulnerabilities and the associated implication of that vulnerability.	Vulnerabilities will include things like outdated operating systems, software that has known issues, and protocols that run in the clear. Do not forget to list an associated implication of each vulnerability.

Requirement	Guidance	Response to steps
C. Describe the anomalies you found when running Wireshark, on the network capture file, and include evidence of the range of packets associated with *each* anomaly.	Here you will use Wireshark and analyze the prepopulated PCAPS file to identify anomalies in the file. The PCAPS file is located on the desktop of the home screen of the lab environment. There are four PCAPS files in the folder, and you can use any file in the folder for this section of the task	In this section, you will be looking for similar issues as you identified in the Nmap scan. You are looking for anything (protocol, software, multiple tcp requests) that would cause harm or disruption to your network. The recommendation is to find three anomalies. Also, you must take a screenshot of the range of packets as your graphical representation of the issue you are referring to.

Requirement	Guidance	Response steps
D. Summarize the potential implications of not addressing *each* of the anomalies found when running Wireshark.	You must list an implication specific to the anomaly identified	You must list an implication for "each" anomaly

Requirement	Guidance	Response steps
E. Recommend solutions for eliminating or minimizing *all* identified vulnerabilities or anomalies from Wireshark and Nmap. Use current, industry-respected, reliable research and sources to support your recommendations for *each* vulnerability or anomaly.	You must recommend a solution for each identified vulnerability (Nmap) and *anomaly* (Wireshark).	Each issue identified must have a recommended solution on how to remediate it. The solution must be specific to that issue and must be supported by a reliable academic source. Sources include, but are not limited to, Microsoft, SANS, and cve.mitre.org. **You must use in-text citations here.**

Requirement	Guidance	Response steps
F. Acknowledge sources, using in-text citations and references, for content that is quoted, paraphrased or summarized.	You must acknowledge all sources used in section E.	The in-text citations must correlate to a work on your reference page 1 to 1

Requirement	Guidance	Response steps
G. Demonstrate professional communication in the content and presentation of your submission.	You must demonstrate professional communication.	You must present a well-written paper. Spelling, structure, flow, grammar, and proper tense are a few examples of professional communication.

Task 2

INTRODUCTION

As wireless and mobile technologies continue to grow in presence and popularity, the world is becoming more and more connected. Unfortunately, this also means that devices and networks are becoming more and more vulnerable to outside threats. Businesses must identify and mitigate these vulnerabilities and threats in order to protect employees' personal information and ensure the organization is secure from passive leaking of proprietary information.

In this task you will assume the role of an IT professional who is responsible for identifying wireless and mobile vulnerabilities, as outlined in the scenario below. You will then present your findings and recommend solutions to mitigate these risks and prevent future threats.

SCENARIO

You are a network professional on the IT team at Alliah Company, a new but fast-growing social media provider. One year ago, Alliah launched a social media website aimed at young professionals. The company also released a mobile app for accessing the site from cellular devices. Alliah was able to launch its website with money generated by a crowd-funded campaign, but most of the funds were spent on the site and app development, with relatively little money (and time) devoted to the internal office network infrastructure.

Alliah has 35 full-time employees, all of whom have offices or shared work spaces in a three-story building that serves as the company headquarters. The building is an old warehouse that was converted for office use and is approximately 10,000 square feet. Currently, the employees occupy only two floors; the third floor is vacant and available for expansion.

The Alliah WLAN has a gigabit managed switch, a multiservice wireless LAN controller, and seven wireless access points strategically located to provide coverage to office staff. One access point services a large back patio area for employee use. The network is protected by a firewall. The Alliah website servers are located in a data center 100 miles from Alliah headquarters.

Five employees are account representatives who are on the road at least 80 percent of the time, and each rep has a company-issued laptop, tablet, and smartphone. They use a large, shared office in the headquarters building when they are not traveling.

Employees use company-owned computers that connect to the WLAN, and, in an effort to control costs during the launch, Alliah has a bring your own device (BYOD) policy.

The IT staff consists of five employees; three are devoted to website maintenance, one manages the headquarters' computers and network, and another employee assists with the website and the office network. IT staff uses wired Ethernet connections to remotely access the website servers.

The Alliah website is successful, attracting more and more visitors each month. Jennifer, the CEO, anticipates hiring more employees and is considering a strategy that would take the company public within a few years. In preparation, she wants to ensure that Alliah's wireless networking infrastructure is highly secure, especially because it may need to grow quickly in a short period of time, and she wants to understand the security risks the company faces. She also wants to decide if Alliah should continue allowing BYOD or restrict network access to company-owned devices only, or if a compromise solution is available.

Requirement	**Guidance**	**Response to steps**
A. Describe **two** WLAN vulnerabilities that present risks for Alliah, based on the details in the scenario.	Describe **two** wireless LAN (WLAN) vulnerabilities that could present a risk to the company.	List two specific WLAN vulnerabilities. Chapter four of the course material has a few great examples.

Requirement	Guidance	Response to steps
B. Describe **two** mobile vulnerabilities that present risks for Alliah, based on the details in the scenario.	Describe **two** mobile device vulnerabilities that could present a risk to the company.	List two specific mobile device vulnerabilities. Chapter four of the course material has a few great examples.

Requirement	Guidance	Response to steps
C. Summarize the steps for mitigating *each* identified WLAN and mobile vulnerability, including the specific tools or documentation that will be needed for mitigation.	You must list steps the mitigate the identified vulnerabilities	You will list specific tools and technologies to mitigate the vulnerabilities listed in sections A and B. Make sure your mitigation is applicable to the vulnerability.

Requirement	Guidance	Response to steps
D. Recommend preventive measures to maintain the security posture of WLAN and mobile environments in a small business, such as Alliah. Reference federal, state, or industry regulations that justify these measures.	List a preventative measure to maintain the security posture of the WLAN and the mobile device environment.	List one preventative measure for each environment. You must also use a federal regulation to support the measures. Applicable regulations can be found in chapter four of the course material in the section labeled *regulatory compliance.* **In-text citation is required here**. **NIST's and ISO's will not suffice for this section.**

Requirement	Guidance	Response to steps
E. Recommend a solution for the company's BYOD approach, including research to justify your recommendation.	Recommend a BYOD approach for the company.	Recommend a BYOD approach. You can recommend any approach (CYOD, BYOD, etc.) you like. However, your approach must be supported by a reliable academic source that supports your position. **In-text citation is required here.**

Requirement	Guidance	Response steps
Acknowledge sources, using in-text citations and references, for content that is quoted, paraphrased or summarized.	You must acknowledge all sources used in sections D & E.	The in-text citations must correlate to a work on your reference page 1 to 1.

Requirement	Guidance	Response steps
G. Demonstrate professional communication in the content and presentation of your submission.	You must demonstrate professional communication.	You must present a well-written paper. Spelling, structure, flow, grammar, and proper tense are a few examples of professional communication.

Back To Table of Contents