GRP1 — GRP1 TASK 1: NMAP AND WIRESHARK

EMERGING TECHNOLOGIES IN CYBERSECURITY — C844
PRFA — GRP1

COMPETENCIES

4042.5.3 : Mapping and Monitoring
The graduate executes network mapping and monitoring procedures using industry-standard software for identifying vulnerabilities and threats.

INTRODUCTION

In the changing field of cybersecurity, you will need to continually identify new threats to your network as evidenced in the network itself and the traffic on that network. You will need to know how to run network mapping and monitoring software to find vulnerabilities and anomalies that could impact the security of your network in order to recommend sound solutions.

For this task, you will use the virtual world at the "Performance Assessment Lab" web link and access the files and lab environment necessary to run both Nmap and Wireshark on the network associated with this task. You will need to save the output of both Nmap and Wireshark to include in your submission. You will then recommend solutions to address any issues you find.

REQUIREMENTS

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. An originality report is provided when you submit your task that can be used as a guide.

You must use the rubric to direct the creation of your submission because it provides detailed criteria that will be used to evaluate your work. Each requirement below may be evaluated by more than one rubric aspect. The rubric aspect titles may contain hyperlinks to relevant portions of the course.

A. Describe the network topology you found when running Nmap. Include screenshots as evidence of running Nmap.

B. Summarize the vulnerabilities on the network and their potential implications based on your Nmap results.

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.

D. Summarize the potential implications of not addressing *each* of the anomalies found when running Wireshark.

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.

F. Acknowledge sources, using in-text citations and references, for content that is quoted, paraphrased, or summarized.

G. Demonstrate professional communication in the content and presentation of your submission.

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, csv, 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

RUBRIC

A:NMAP SUMMARY

NOT EVIDENT	APPROACHING COMPETENCE	COMPETENT
The submission does not describe the network topology.	The submission inaccurately describes the network topology or does not include screenshots showing evidence of running Nmap.	The submission accurately describes the network topology and includes screenshots showing evidence of running Nmap.

B:NMAP VULNERABILITIES

NOT EVIDENT	APPROACHING COMPETENCE	COMPETENT
The submission does not summarize the vulnerabilities on the network or does not include the potential implications.	The submission inaccurately summarizes the vulnerabilities on the network, or does not provide plausible potential implications.	The submission accurately summarizes the vulnerabilities on the network, and provides plausible potential implications.

C:WIRESHARK ANOMALIES

NOT EVIDENT	APPROACHING COMPETENCE	COMPETENT
The submission does not describe the anomalies found when running Wireshark.	The submission inaccurately describes the anomalies found when running Wireshark or includes insufficient evidence of the range of packets associated with each anomaly.	The submission accurately describes the anomalies found when running Wireshark and includes evidence of the range of packets associated with each anomaly.

D:IMPLICATIONS OF ANOMALIES

NOT EVIDENT	APPROACHING COMPETENCE	COMPETENT
The submission does not summarize potential implications for each anomaly.	The submission summarizes potential implications for each anomaly, but the provided implications are not plausible.	The submission summarizes the potential implications of taking no action for each anomaly, and the provided implications are plausible.

E:SOLUTIONS

NOT EVIDENT	APPROACHING COMPETENCE	COMPETENT
The submission does not recommend any solutions.	The submission includes recommendations, but the solutions do not eliminate or minimize all identified vulnerabilities and anomalies. Or the recommendations are not supported by reliable research or sources.	The submission recommends solutions that eliminate or minimize all identified vulnerabilities and anomalies. The recommendations are supported by reliable research and sources.

F:SOURCES

NOT EVIDENT	APPROACHING COMPETENCE	COMPETENT
The submission does not include both in-text citations and a reference list for sources that are quoted, paraphrased, or summarized.	The submission includes in-text citations for sources that are quoted, paraphrased, or summarized and a reference list; however, the citations or reference list is incomplete or inaccurate.	The submission includes in-text citations for sources that are properly quoted, paraphrased, or summarized and a reference list that accurately identifies the author, date, title, and source location as available.

G:PROFESSIONAL COMMUNICATION

NOT EVIDENT	APPROACHING COMPETENCE	COMPETENT
Content is unstructured, is disjointed, or contains pervasive errors in mechanics, usage, or grammar. Vocabulary or tone is unprofessional or distracts from the topic.	Content is poorly organized, is difficult to follow, or contains errors in mechanics, usage, or grammar that cause confusion. Terminology is misused or ineffective.	Content reflects attention to detail, is organized, and focuses on the main ideas as prescribed in the task or chosen by the candidate. Terminology is pertinent, is used correctly, and effectively conveys the intended meaning. Mechanics, usage, and grammar promote accurate interpretation and understanding.

WEB LINKS

Performance Assessment Lab

Skillable Labs Knowledge Base Article
Please consult this WGU Knowledge Base article for general FAQs regarding your Skillable lab environment.