Southern New Hampshire University

ISE 620 Milestone Three Guidelines and Rubric

Overview: The final project for this course is the creation of a security posture and response analysis report. Throughout this course, there will be key milestone activities that will give you adequate time to research, analyze, and put together your report. These milestones are designed to build upon each other so that you can get started on key aspects of your final project and receive feedback from your instructor for improving your work as you draft your report.

Prompt: Submit a **tools and results brief**. The scoring of this milestone activity is based on 1) your ability to evaluate the tools you would use to detect network security vulnerabilities for HealthNet, 2) your use of the Nessus scan and Snort report to identify attacks that happened, why they happened, and the weaknesses that the attacker exploited, and 3) your ability to analyze these reports to inform your recommendations on what needs to be done to improve upon HealthNet's security posture. Remember to **review your Final Project Guidelines and Rubric document** for how you will be scored on your final submission.

Specifically, the following **critical elements** must be addressed:

I. **Importance of the Tools and Systems:** In this section, you will evaluate the tools and systems you have used throughout the course to address how you would use them to detect network security vulnerabilities if a more in-depth security assessment of HealthNet were to be conducted. You will apply the knowledge and skills gained from using the tools during this course to the following:

   A. How would you use **network intrusion detection software** to detect a problem in the organization's network? Examples of potential network intrusions that you could discuss include exploit attempts, port scans, and worms.
   B. How would you use a **network protocol analyzer** to monitor this network for security threats? In your response, ensure that you address sniffing packets for usernames and passwords.
   C. Evaluate the **effectiveness** of the tools and systems that you would use to analyze the network or computing devices for known vulnerabilities. For instance, based on your experience with this tool/system during the course, were there any gaps or problems in how they would allow you to monitor or detect security threats for this organization?

II. **Analyzing Results:** You should now begin to review the results of the preliminary vulnerability assessments already gathered by your practice director in the Nessus scan and Snort report . It appears that the attacker used Metasploit and Meterpreter. Note that for this scenario, the Nessus scan and the Snort report have different addresses, but it is the same attacker. In this instance, you would consider that the destination IP in Snort (10.5.11.173) and the Nessus IP address (192.168.118.80) are the same for our purposes. Specifically, in this part of your report, you should do the following:

   A. Correlate the known **vulnerabilities** in the Nessus scan with those in the Snort report. What does the information in the Snort report tell you? What problems can you identify at this stage? In other words, identify some of the nefarious activities from those highlighted in the report. Sample at least four of the activities for the purposes of this milestone.

III. **Needs and Recommendations:** Now that you have completed the analysis of the vulnerabilities in the Nessus scan and Snort report, you will address your recommendations to meet HealthNet's needs.

A. Recommend a potential strategy or method for **communicating** these results to stakeholders of the network. You will have an opportunity to discuss potential strategies with your peers in an upcoming discussion forum. In your final project, you will want to build out on this strategy or method based on your instructor feedback from this milestone.

B. What do your results tell you specific to the needs of future **security controls** for this organization? For example, how can the results be used to mitigate security risks and vulnerabilities?

C. Describe at least two new **policies** or policy updates that need to be created to ensure the confidentiality, integrity, and availability of the organization's data. Your response should be based on the results of your network vulnerability scanning tools. In your final project, you will want to build out on what policies or policy updates are necessary based on your instructor feedback from this milestone.

D. How will the future security controls and new or updated policies aid the organization in **restoring availability** of their network and other information services after a security incident?

E. Suggest how these new security **countermeasures** can be communicated to stakeholders of the network and associated information systems. In other words, what strategies or methods can you recommend to communicate the future security controls and new policies to stakeholders?

Guidelines for Submission: Your paper must be submitted as a 2- to 3-page Microsoft Word document with double spacing, 12-point Times New Roman font, one-inch margins, and at least three sources cited in APA format.

Critical Elements	Attempted With Minimal or No Functional Issues (100%)	Attempted With Significant Functional Issues (75%)	Not Evident (0%)	Value
Importance of the Tools and Systems: Network Intrusion Detection Software	Explains how network intrusion detection software can be used to detect problems in organization's network, using examples with minimal or no errors in explanation	Explains how network intrusion detection software is used to detect problem in organization's network, but with significant errors in explanation or lack of examples	Does not explain how network intrusion detection software is used to detect problem in organization's network	10
Importance of the Tools and Systems: Network Protocol Analyzer	Explains how network protocol analyzer would be used to monitor network for security threats, addressing sniffing packets for usernames and passwords in response, with minimal or no errors in explanation	Explains how network protocol analyzer would be used to monitor network for security threats, addressing sniffing packets for usernames and passwords in response, but with significant errors in explanation	Does not explain how network protocol analyzer would be used to monitor network for security threats	10
Importance of the Tools and Systems: Effectiveness	Evaluates how effective the tools and systems used in the course would be to analyze the network or computing devices for known vulnerabilities, with minimal or no errors in evaluation	Evaluates how effective the tools and systems used in the course would be to analyze the network or computing devices for known vulnerabilities, but with significant functional errors	Does not evaluate effectiveness of tools and systems that would be used to analyze the network or computing devices for known vulnerabilities	10

Analyzing Results: Vulnerabilities	Correlates results from the Snort and Nessus reports to identify at least four nefarious activities, with minimal or no errors	Correlates results from the Snort and Nessus reports to identify nefarious activities, with significant functional errors, or lacks at least four examples	Does not correlate results from Snort and Nessus reports to identify nefarious activities	15
Needs and Recommendations: Communicating	Recommends an appropriate strategy or method for communicating results to network's stakeholders, with minimal or no errors in suitability of recommendation	Recommends strategy or method for communicating results to network's stakeholders, but with significant functional errors in suitability of recommendation	Does not recommend strategy or method for communicating results to network's stakeholders	10
Needs and Recommendations: Security Controls	Determines how results of network assessments will affect organization's future security controls, with minimal or no errors in suitability	Determines how results of network assessments will affect organization's future security controls, but with significant errors in suitability	Does not determine how results of network assessments will affect organization's future security controls	10
Needs and Recommendations: Policies	Describes at least two new policies or policy updates that need to be created to ensure the confidentiality, integrity, and availability of the organization's data, based on results of analysis of the vulnerabilities, with minimal or no errors	Describes at least two new policies or policy updates that need to be created to ensure the confidentiality, integrity, and availability of the organization's data, but with significant errors, or only one new policy or update is included	Does not describe new policies or policy updates that need to be created to ensure the confidentiality, integrity, and availability of the organization's data	10
Needs and Recommendations: Restoring Availability	Explains how future security controls and new or updated policies will aid organization in restoring availability of network and other information services after a security incident, with minimal or no errors	Explains how future security controls and new or updated policies will aid organization in restoring availability of network and other information services after a security incident, but with significant errors	Does not explain how future security controls and new or updated policies will aid organization in restoring availability of network and other information services after a security incident	10
Needs and Recommendations: Countermeasures	Determines how new security countermeasures can be communicated to stakeholders of network and associated information system, with minimal or no errors	Determines how new security countermeasures can be communicated to stakeholders of network and associated information system, but with significant errors	Does not determine how new security countermeasures can be communicated to stakeholders of network and associated information system	10
Articulation of Response	Submission has no major errors related to citations, grammar, spelling, syntax, or organization	Submission has major errors related to citations, grammar, spelling, syntax, or organization that negatively impact readability and articulation of main ideas	Submission has critical errors related to citations, grammar, spelling, syntax, or organization that prevent understanding of ideas	5
			Total	**100%**