Southern New Hampshire University

IT 320 Final Project Milestone Two Guidelines and Rubric

Overview: You will continue to use the final project lab environment to complete this milestone. Remember to refer to the instructions for navigating the environment located within the lab pane. Once you complete your lab, use your lab notebook, experience in the final project lab environment, and accompanying screen captures of your results in the final project lab. Refer back to your lab tips Visual Aid to review how your work during the module lab activities can help inform your work in your final project lab.

This assignment is the second milestone that you will complete for your final project. In this milestone, you will do the following:

- Continue identifying the vulnerabilities that you uncovered in Milestone One focusing on Sections IV and V, the recommendations and solutions portions of your final project.
- List the vulnerability along with the mitigation tactics/strategies you deem the most appropriate based on NIST standards.
- Use the likelihood/impact chart to determine the level of impact and likelihood.
- Organize the vulnerabilities in order by priority that would address them.
- This assignment is an important practice opportunity for you to draft and get feedback from your instructor to improve your final draft
- The rubric for scoring in this assignment has been adjusted to reflect that this is a practice opportunity. You should focus on getting the necessary information into your draft. No draft is perfect. That is why it is a draft.
- Follow the critical elements as a guide. These are the elements you will be graded on in the final project submission.

Ensure that you *set aside uninterrupted time* to work in your lab. The server does not provide a persistent environment. It will provide you with a 90-minute window to complete your lab. There are separate segments in each lab. Monitor yourself and ensure you complete the segments within that window. If you cannot complete all the segments in the 90-minute window, you will need to ask your instructor to reset the lab. However, you should only need to go back and complete the remaining segments you have not yet finished as you should already have documented the results on the completed segments.

Ideally, you should record your engagement with the lab for yourself. Then you can go back and watch your recording and screenshot of whatever pieces of the experience are necessary.

Labs You Should Be Using as Reference Material for This Milestone (including your lab notebook and lab worksheets):

Lab Name	**Learning Objectives From These Labs**
Lab 5: Social Engineering	Identify how social engineering techniques can be utilized.
Lab 6: Crafting and Deploying Malware	Identify how an attacker creates and deploys malware to a victim's machine. Demonstrate how hackers steal data from the victim's network.

Southern New Hampshire University

Lab 7: Intrusion Detection Using Snort	Enumerate hosts on the network using various tools. 1. Setting Up the Sniffer 2. Detecting Unwanted Incoming Attacks 3. Detecting Unwanted Outgoing Traffic
Lab 8: Securing the pfSense Firewall	Harden the firewall by closing unnecessary ports. Remove insecure and unnecessary protocols. Add secure service to a firewall.

Prompt: ABC Manufacturing has hired you as a security consultant to identify security vulnerabilities, provide recommendations, and implement approved changes. Management at ABC has provided you with access to their server networking environment. When the network was set up, the network technician was unfamiliar with the firewall appliance and may have opened up more ports than necessary. Only web services (HTTP and HTTPs) and map service (SMTP) should be allowed from outside of the network.

The client's internal team has provided a list of tests they want performed based on their own initial analysis:

- Scan the firewall for open ports using the tools available to you in the lab environment
- Determine what the settings on the firewall are for incoming traffic that is allowed. What is it set on? What vulnerabilities does it pose if they are not set?
- Use Microsoft Security Essentials on the client and server Windows machines to determine if vulnerabilities exist.
- Conduct a vulnerability scan on each host desktop using the OpenVAS application on the Kali 2 Linux Box.
- Find vulnerabilities specific to intrusion detection and prevention systems using Wireshark and NetworkMiner.

In Milestone One, you assessed the network and presented your findings including the evidence behind them. You then interpreted the results of the scans/settings you reviewed and provided detail related to the vulnerabilities that were uncovered and the types of threats these vulnerabilities pose.

In Milestone Two, you will take the next steps toward a complete vulnerability report. First, you will identify what aspects of the network should be examined to address the network security posture and assess these areas using risk criteria. You will then recommend mitigation strategies for addressing these issues, prioritize these strategies, and explain your rationale. You will then implement the recommended solutions for at least one issue that you have uncovered and provide evidence of this implementation.

Specifically, the following **critical elements** must be addressed in Milestone Two:

- **Network Security Posture Recommendations:**
  In this area, you will identify what aspects of the network should be examined to address the network security posture. Use your knowledge from research, readings, and activities in the course to help you.

a) Identify key aspects of the network that should be examined to address the **network security posture** ensuring the following key criteria have been included:
   - At least one issue associated with the firewall
   - At last one issue associated with one or more client machines
   - At least one issue associated with one or more server machines
   - At least one issue associated with a Windows host

b) Indicate the **impact** of the vulnerability.
c) Indicate the **likelihood** of the vulnerability.
d) What **mitigation strategies** do you recommend be implemented for addressing all of the issues uncovered in your network assessment above? Support your response with evidence from your lab work and coursework.
e) **Prioritize** the recommended strategies for the company. Use the matrix provided below to assess the priority.
f) Explain the **rationale** of the prioritization you have chosen for each solution.

- **Implementation Solutions:**
  In this area, you will add a brief written summary following your charts that demonstrates you actually implemented the solutions you recommended in your lab environment. Your written responses should include evidence in the form of a screenshot or screen capture that demonstrates you have executed your proposed recommendations.
  a) **Execute** your proposed strategy specific to at least one of the issues you have uncovered with firewalls supported by evidence.
  b) **Harden the server(s)** using at least one method supported by evidence.

Matrix (for Section IV, Parts e and f)

Use this risk rating matrix to evaluate and rate the risks or vulnerabilities you identify:

Likelihood	(5)	Medium (3)	High (4)	High (4)	Very High (5)	Very High (5)
	(4)	Medium (3)	Medium (3)	Medium (3)	High (4)	Very High (5)
	(3)	Low (2)	Medium (3)	Medium (3)	Medium (3)	High (4)
	(2)	Very Low (1)	Low (2)	Medium (3)	Medium (3)	Medium (3)
	(1)	Very Low (1)	Very Low (1)	Low (2)	Low (2)	Medium (3)
		(1)	(2)	(3)	(4)	(5)
		Impact				

Figure 3: Risk Rating Matrix. Reprinted from "Cyber Security Assessment Sample Report," by Honeywell International Inc., retrieved from https://www.honeywellprocess.com/library/marketing/notes/honeywell-iits-cyber-assesssment-sample-report.pdf Copyright 2012 by Honeywell International Inc.

Format your findings and recommendations in a table, such as the one below.

Description of Vulnerability	Impact (1–5)	Likelihood (1–5)	Priority (1–5)	Recommendations
Example: Switches do not have spanning tree feature enabled. This feature prevents communication loops from crashing the network.	*2*	*3*	*3*	*Example: Enable spanning tree feature.*

Table 6: CSVA Findings. Reprinted from "Cyber Security Assessment Sample Report," by Honeywell International Inc., retrieved from https://www.honeywellprocess.com/library/marketing/notes/honeywell-iits-cyber-assesssment-sample-report.pdf Copyright 2012 by Honeywell International Inc.

Matrix Key

Very High (5) – The results of this finding can cause total loss of the generating asset to support reliable operation, and are almost certain to result in human death or serious injury and to significantly violate, harm, or impede the organization's mission, reputation, or interest.

High (4) – The results of this finding can cause impairment of the generating asset to support reliable operation of the bulk electric system. They may also result in human death or serious injury, and may significantly violate, harm, or impede the organization's mission, reputation, or interest.

Medium (3) – The results of this finding can cause partial or short-term (<7 days) impairment of generating asset to support reliable operation of the bulk electric system. They may result in human injury and may violate, harm, or impede the organization's mission, reputation, or interest.

Low (2) – The results of this finding can cause short-term impairment (<24 days) of the generating asset to support reliable operation of the bulk electric system and may noticeably affect the organization's mission, reputation, or interest.

Very Low (1) – The results of this finding will NOT cause impairment of the generating asset to support reliable operation of the bulk electric system and are unlikely to noticeably affect the organization's mission, reputation, or interest.

Figure 3: Risk Rating Matrix. Adapted from "Cyber Security Assessment Sample Report," by Honeywell International Inc., retrieved from https://www.honeywellprocess.com/library/marketing/notes/honeywell-iits-cyber-assesssment-sample-report.pdf Copyright 2012 by Honeywell International Inc.

Southern New Hampshire University

Rubric

Guidelines for Submission: Your submission should include an explanation of the changes made to the network topology and screenshots of these changes. It should be about 2 to 4 pages in length.

Critical Element	Proficient (100%)	Needs Improvement (70%)	Not Evident (0%)	Value
Network Security Posture Recommendations: Network Security Posture	Identifies what aspects of the network should be examined to address the network security posture ensuring all key criteria have been included	Identifies what aspects of the network should be examined to address the network security posture but identification is inaccurate, is illogical, or does not include all key criteria	Does not identify what aspects of the network should be examined	11.1
Network Security Posture Recommendations: Impact	Indicates the impact of the vulnerability	Indicates the impact of the vulnerability but explanation is cursory, inaccurate, or illogical	Does not indicate the impact of the vulnerability	11.1
Network Security Posture Recommendations: Likelihood	Indicates the likelihood of the vulnerability	Indicates the likelihood of the vulnerability but explanation is cursory, inaccurate, or illogical	Does not indicate the likelihood of the vulnerability	11.1
Network Security Posture Recommendations: Mitigation Strategies	Proposes mitigation strategies that comprehensively address the issues uncovered in the network assessment section supported by evidence from lab work and coursework	Proposes mitigation strategies that comprehensively address the issues uncovered in the network assessment section but proposal contains inaccuracies, is illogical, or is not supported by evidence	Does not propose mitigation strategies	11.1
Network Security Posture Recommendations: Prioritization	Appropriately prioritizes mitigation strategies based on the given keys and organizes information logically into the provided table format	Prioritizes mitigation strategies, but not all are appropriate, based on the given keys, or are not organized logically into the provided table format	Does not prioritize mitigation strategies	11.1
Network Security Posture Recommendations: Rationale	Explains rationale of the prioritization chosen for each solution	Explains rationale of the prioritization chosen for each solution but explanation is cursory, inaccurate, or illogical	Does not explain rationale of the prioritization	11.1
Implementation Solutions: Execute	Executes a proposed strategy specific to at least one of the issues uncovered with firewalls and supports with evidence	Executes a proposed strategy specific to at least one of the issues uncovered with firewalls but execution is inaccurate, illogical, or not supported by evidence	Does not execute on proposed strategy	11.1
Implementation Solutions: Hardening the Server(s)	Includes a screenshot or screen capture that demonstrates successfully hardening the server(s)	Includes a relevant screenshot or screen capture, but image does not constitute evidence of successfully hardening the server(s)	Does not include a relevant screenshot or screen capture of hardening the server(s)	11.1

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	11.2
			Total	**100%**