Southern New Hampshire University

IT 320 Final Project Guidelines and Rubric

Overview

The final project for this course is the creation of a vulnerability report. This is an important type of report in the information security industry, and will be the culmination of your work in IT 320. This is your opportunity to bring all that you have learned together to analyze a network, evaluate vulnerabilities and risks, and recommend mitigation strategies.

A vulnerability report typically includes the following:

- A security assessment of a computer network
- Identification of vulnerabilities, supported with evidence
- An interpretive analysis of risks, including benchmarking or ranking risk using levels or similar metrics
- Recommended mitigation steps or solutions

Vulnerability reports are written for a diverse audience within an organization. Therefore, they include an executive summary for managers and decision-makers as well as technical data for analysis by other IT professionals. Organizations may require vulnerability reports to meet compliance requirements or may have internal policies that call for a vulnerability assessment and completion of a report on a fixed schedule.

Vulnerability reports are often researched and produced by information security experts from outside the organization. As you will see in the assignment prompt below, you will play the role of an information security consultant as you complete this final project.

Your work on this project is supported by **two milestones**, in **Modules Three** and **Five**, that are designed to support you as you go through the final project lab and gather the information you need to create your vulnerability report draft. These milestones are important practice opportunities from which you will gain critical feedback that will inform your final draft of this project that you will submit in **Module Seven**.

Your practice work and your instructor feedback will be especially important as you craft your executive summary for this project. This executive summary section is *not contained* within the milestone activities. It would not make sense to create that final summary piece until you have completed your drafts, received your instructor feedback, and are ready to finalize your final project draft in **Module Seven**.

In this assignment, you will demonstrate your mastery of the following course outcomes:

- IT-320-01: Assess in-house, distributed, or cloud-based networks for their current security posture
- IT-320-02: Recommend mitigation strategies for hardening network operating systems, applications, and network devices based on National Institute of Standards and Technology (NIST) standards
- IT-320-03: Implement network hardening solutions for addressing vulnerable network security postures

- IT-320-04: Interpret data from networking and system logs for building security assurance

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.

Specifically, you must address the **critical elements** listed below. Most of the critical elements align with a particular course outcome (shown in brackets).

I. **Executive Summary:** Provide background information and the high-level findings of your report to establish a detailed context based on your assessment of the network, the evidence you collected (your Milestone One work), and the mitigation strategy, recommendations, and solutions (your Milestone Two work) you addressed.
   a) What is the **purpose** of the vulnerability report? How should it be used and interpreted by the enterprise? [IT-320-02]
   b) What was your **methodology** for identifying security vulnerabilities? This is where you should briefly describe the tools and techniques that you used to find the vulnerabilities. [IT-320-01]
   c) Overall, what was your **determination** about the enterprise's current **security posture.** [IT-320-01]

II. **Network Assessment – Gathering Evidence of the Vulnerabilities:**
In this part of your project, you will assess the security posture of this network to find what security vulnerabilities currently exist using the appropriate scanning tools and techniques looking at both the pfSense firewall and the Windows Server firewall for the Windows Server host (192.168.1.10). Please see the Final Project navigation pane in the InfoSec environment for a diagram of the systems, users IDs, and passwords you will need to use in that environment. Be sure your responses and supporting evidence address the following questions:
   a) **Firewall**: Determine **threats** to the firewall. For example, are there any ports that are open unnecessarily or unused? Support your response with evidence. [IT-320-01]
   b) **Virtual Machine (host)**: Determine **threats** to the virtual machine (host). For example, are there any ports that are open unnecessarily or unused? Support your response with evidence. [IT-320-01]
   c) Determine if there is **malicious software protection** in place using the tools provided to you. Support your response with evidence. [IT-320-01]:
      i. What kinds of antivirus software, malware protection, or other security software is in place?
      ii. What are the risks associated with the gaps in malicious software prevention?
      iii. What are the risks associated with leaving the malicious software prevention strategies as they are now?
   d) **Intrusion Detection**: What security threats are you finding in the output as you analyze the **network traffic**? Support your response with evidence from your Wireshark and NetworkMiner tools. [IT-320-01]

III. **Vulnerability Assessment – Interpreting Evidence of Vulnerabilities**:

In this part of your project, you will interpret evidence gathered from the network assessment you conducted in Section I to discuss what security vulnerabilities currently exist. In particular, look closely at the scan you performed on the firewall and your Nmap and Zenmap results. Interpret the output from these tools. Be sure your responses and supporting evidence address the following questions:

a) What are the vulnerabilities specific to the **network traffic**? Explain what kind of security threats the vulnerabilities pose. [IT-320-04]

b) What are the vulnerabilities specific to the **anti-malware systems** (especially centrally managed solutions with aggregated reporting)? Explain what kind of security threats the vulnerabilities pose. For example, what do the Windows security settings tell you? [IT-320-04]

c) What are the vulnerabilities specific to the **operating systems** and **workstations**? Explain what kind of security threats the vulnerabilities pose. For example, what did you find when you used the OpenVAS tool? [IT-320-04]

d) What are the vulnerabilities specific to the **network hardware** (firewall)? Explain what kind of security threats the vulnerabilities pose. [IT-320-04]

IV. **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. For Parts e and f, it may be helpful to organize your information in a table format for organizational purposes. A sample is provided for you in the Supporting Information section.

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: [IT-320-03]

   i. At least one issue associated with the firewall

   ii. At last one issue associated with one or more client machines

   iii. At least one issue associated with one or more server machines

   iv. At least one issue associated with a Windows host

b) Indicate the **impact** of the vulnerability. [IT-320-03]

c) Indicate the **likelihood** of the vulnerability. [IT-320-03]

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. [IT-320-02]

e) **Prioritize** the recommended strategies for the company. Use the matrix in the Supporting Information section to assess the priority. [IT-320-02]

f) Explain the **rationale** of the prioritization you have chosen for each solution. [IT-320-02]

V. **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 and support your response with evidence. [IT-320-03]

b) **Harden the server(s)** using at least one method and support your response with evidence. [IT-320-03]

Supporting Information

Matrix (for Section IV, Parts e and f)

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.

Table Sample (for Section IV, Parts e and f)

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.

Final Project Rubric

Guidelines for Submission: The written portion of your submission should be 5 to 6 pages in length (in addition to small screenshots, the title page, and references). Use double spacing, 12-point Times New Roman font, and one-inch margins. Sources should be cited according to APA style.

Critical Elements	Exemplary	Proficient	Needs Improvement	Not Evident	Value
Executive Summary: Purpose	Meets “Proficient” criteria and examples demonstrate a nuanced understanding of the case and overall value of network security for enterprises (100%)	Explains the purpose of the vulnerability report and how it should be used and interpreted by the enterprise (85%)	Explains the purpose of the vulnerability report and how it should be used and interpreted by the enterprise but explanation is cursory, contains inaccuracies, or is illogical (55%)	Does not explain the purpose of the vulnerability report (0%)	5

Executive Summary: Methodology	Meets “Proficient” criteria and chosen methodology reflects keen insight or is particularly well supported by network security principles (100%)	Describes the methodology used for identifying security vulnerabilities specific to the tools and techniques used (85%)	Describes the methodology used for identifying security vulnerabilities specific to the tools and techniques used but explanation is cursory, contains inaccuracies, or is illogical (55%)	Does not describe the methodology used for identifying security vulnerabilities (0%)	5
Executive Summary: Determination About Security Posture	Meets “Proficient” criteria and overall determination and supporting findings reflect an in-depth or nuanced understanding of network security principles (100%)	Makes an accurate, overall determination about the enterprise’s current security posture (85%)	Makes an overall determination about the enterprise’s current security posture, but determination is cursory, contains inaccuracies, or is illogical (55%)	Does not make an overall determination about the enterprise’s current security posture (0%)	5
Network Assessment: Firewall Threats	Meets “Proficient” criteria and determination reflects an in-depth or nuanced understanding of network security principles (100%)	Determines threats to the firewall, supporting the response with evidence (85%)	Determines threats to the firewall but determination is cursory, contains inaccuracies, or is not supported by evidence (55%)	Does not determine threats to the firewall (0%)	5
Network Assessment: Virtual Machine Threats	Meets “Proficient” criteria and assessment reflects an in-depth or nuanced understanding of network security principles (100%)	Determines threats to the virtual machine, supporting the response with evidence (85%)	Determines threats to the virtual machine but determination is cursory, contains inaccuracies, or is not supported by evidence (55%)	Does not determine threats to the virtual machine (0%)	5
Network Assessment: Malicious Software Protection	Meets “Proficient” criteria and assessment reflects an in-depth or nuanced understanding of network security principles (100%)	Determines if there is malicious software protection in place using the tools provided, supporting the response with evidence (85%)	Determines if there is malicious software protection in place using the tools provided but determination is cursory, contains inaccuracies, or is not supported by evidence (55%)	Does not determine if there is malicious software protection in place (0%)	5
Network Assessment: Intrusion Detection	Meets “Proficient” criteria and interpretation reflects an in-depth or nuanced understanding of network security principles (100%)	Analyzes security threat findings in the output based on the network traffic and supports with evidence (85%)	Analyzes security threat findings in the output but there are inaccuracies, the assessment is not comprehensive, or the specific resulting security risks are not supported by evidence (55%)	Does not analyze security threat findings (0%)	5

Vulnerability Assessment: Network Traffic	Meets "Proficient" criteria and interpretation reflects an in-depth or nuanced understanding of network security principles (100%)	Explains vulnerabilities specific to the network traffic and the security threats the vulnerabilities pose, supporting the explanation with evidence (85%)	Explains vulnerabilities specific to the network traffic and the security threats the vulnerabilities pose but explanation is cursory, contains inaccuracies, is illogical, or is not supported by evidence (55%)	Does not explain vulnerabilities specific to the network traffic and the security threats the vulnerabilities pose (0%)	5
Vulnerability Assessment: Anti-Malware Systems	Meets "Proficient" criteria and interpretation reflects an in-depth or nuanced understanding of network security principles (100%)	Explains vulnerabilities specific to the anti-malware systems and the security threats the vulnerabilities pose, supporting the explanation with evidence (85%)	Explains vulnerabilities specific to the anti-malware systems and the security threats the vulnerabilities pose but explanation is cursory, contains inaccuracies, is illogical, or is not supported by evidence (55%)	Does not explain vulnerabilities specific to the anti-malware systems and the security threats the vulnerabilities pose (0%)	5
Vulnerability Assessment: Operating Systems/ Workstations	Meets "Proficient" criteria and interpretation reflects an in-depth or nuanced understanding of network security principles (100%)	Explains vulnerabilities specific to the operating systems and workstations and the security threats the vulnerabilities pose, supporting the explanation with evidence (85%)	Explains vulnerabilities specific to the operating systems and workstations and the security threats the vulnerabilities pose but explanation is cursory, contains inaccuracies, is illogical, or is not supported by evidence (55%)	Does not explain vulnerabilities specific to the operating systems and workstations and the security threats the vulnerabilities pose (0%)	5
Vulnerability Assessment: Network Hardware	Meets "Proficient" criteria and interpretation reflects an in-depth or nuanced understanding of network security principles (100%)	Explains vulnerabilities specific to the network hardware systems and the security threats the vulnerabilities pose, supporting the explanation with evidence (85%)	Explains vulnerabilities specific to the network hardware and the security threats the vulnerabilities pose but explanation is cursory, contains inaccuracies, is illogical, or is not supported by evidence (55%)	Does not explain vulnerabilities specific to the network hardware and the security threats the vulnerabilities pose (0%)	5
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 (100%)	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 (55%)	Does not identify what aspects of the network should be examined (0%)	5

Network Security Posture Recommendations: Impact		Indicates the impact of the vulnerability (100%)	Indicates the impact of the vulnerability but explanation is cursory, inaccurate, or illogical (55%)	Does not indicate the impact of the vulnerability (0%)	5
Network Security Posture Recommendations: Likelihood		Indicates the likelihood of the vulnerability (100%)	Indicates the likelihood of the vulnerability but explanation is cursory, inaccurate, or illogical (55%)	Does not indicate the likelihood of the vulnerability (0%)	5
Network Security Posture Recommendations: Mitigation Strategies	Meets “Proficient” criteria and proposes strategies that reflect an in-depth or nuanced understanding of network security principles (100%)	Proposes mitigation strategies that comprehensively address the issues uncovered in the network assessment section supported by evidence from lab work and coursework (85%)	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 (55%)	Does not propose mitigation strategies (0%)	5
Network Security Posture Recommendations: Prioritization		Appropriately prioritizes mitigation strategies based on the given keys and organizes information logically into the provided table format (100%)	Prioritizes mitigation strategies, but not all are appropriate, based on the given keys, or are not organized logically into the provided table format (55%)	Does not prioritize mitigation strategies (0%)	5
Network Security Posture Recommendations: Rationale	Meets “Proficient” criteria and rationale reflects an in-depth or nuanced understanding of network security principles (100%)	Explains rationale of the prioritization chosen for each solution (85%)	Explains rationale of the prioritization chosen for each solution but explanation is cursory, inaccurate, or illogical (55%)	Does not explain rationale of the prioritization (0%)	5
Implementation Solutions: Execute	Meets “Proficient” criteria and rationale reflects an in-depth or nuanced understanding of network security principles (100%)	Executes a proposed strategy specific to at least one of the issues uncovered with firewalls and supports with evidence (85%)	Executes on proposed strategy specific to at least one of the issues uncovered with firewalls but execution is inaccurate, illogical, or not supported by evidence (55%)	Does not execute on proposed strategy (0%)	5
Implementation Solutions: Hardening the Server(s)		Includes a screenshot or screen capture that demonstrates successfully hardening the server(s) (100%)	Includes a relevant screenshot or screen capture, but image does not constitute evidence of successfully hardening the server(s) (55%)	Does not include a relevant screenshot or screen capture of hardening the server(s) (0%)	5

Articulation of Response	Submission is free of errors related to citations, grammar, spelling, syntax, and organization and is presented in a professional and easy-to-read format (100%)	Submission has no major errors related to citations, grammar, spelling, syntax, or organization (85%)	Submission has major errors related to citations, grammar, spelling, syntax, or organization that negatively impact readability and articulation of main ideas (55%)	Submission has critical errors related to citations, grammar, spelling, syntax, or organization that prevent understanding of ideas (0%)	5
				Total	**100%**