Southern New Hampshire University

IT 320 Milestone One Guidelines and Rubric

Overview: You will be using the final project lab environment to complete this milestone. Instructions for navigating the environment are 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 first milestone that you will complete for your final project. In this milestone, you will:

- Begin drafting parts of your final project document focusing on Sections I and II, the network and vulnerability assessment pieces of your final project.
- 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 1: Configuring a Linux-Based Firewall to Allow Incoming and Outgoing Traffic	Test the current firewall and install the Linux firewall. Configure and test the Linux-based firewall using internal services from an external machine.
Lab 2: Patching, Securing Systems, and Configuring Antivirus	Secure and patch a Windows Server operating system to close security holes that can be leveraged by an attacker.
Lab 3: Vulnerability Scanners and Penetration Testing	Discover security holes/vulnerabilities by using tools (OpenVAS, Nmap) to scan a host.
Lab 4: Deep Dive Packet Analysis	Analyze network traffic (POP, FTP, etc.) using appropriate protocols and tools (Wireshark, NetworkMiner) to find relevant artifacts.

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 the first part of Milestone One, you will be assessing the network. This means you will be presenting whatever information you discover as a result of scanning, reviewing settings, etc. You will be asked to collect evidence to show your findings. The second part of the assignment has you interpreting the results of the scans/settings you have reviewed. This is where you provide more detail related to the vulnerabilities that were uncovered, describing the types of threats these vulnerabilities pose.

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

- **Network Assessment – Gathering Evidence of the Vulnerabilities:**
  In this part of your milestone, 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.
  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.
  c) Determine if there is **malicious software protection** in place using the tools provided to you. Support your response with evidence.
     - What kinds of antivirus software, malware protection, or other security software is in place?
     - What are the risks associated with the gaps in malicious software prevention?
     - 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.

- **Vulnerability Assessment – Interpreting Evidence of Vulnerabilities:**
  In this part of your milestone, 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.
  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?
  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?
  d) What are the vulnerabilities specific to the **network hardware** (firewall)? Explain what kind of security threats the vulnerabilities pose.

Rubric

Guidelines for Submission: The written portion of your submission should be 3 to 4 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 Element	Proficient (100%)	Needs Improvement (70%)	Not Evident (0%)	Value
Network Assessment: Firewall Threats	Determines threats to the firewall, supporting the response with evidence	Determines threats to the firewall but determination is cursory, contains inaccuracies, or is not supported by evidence	Does not determine threats to the firewall	11.1
Network Assessment: Virtual Machine Threats	Determines threats to the virtual machine, supporting the response with evidence	Determines threats to the virtual machine but determination is cursory, contains inaccuracies, or is not supported by evidence	Does not determine threats to the virtual machine	11.1
Network Assessment: Malicious Software Protection	Determines if there is malicious software protection in place using the tools provided, supporting the response with evidence	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	Does not determine if there is malicious software protection in place	11.1
Network Assessment: Intrusion Detection	Analyzes security threat findings in the output based on the network traffic and supports with evidence	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	Does not analyze security threat findings	11.1

Vulnerability Assessment: Network Traffic	Explains vulnerabilities specific to the network traffic and the security threats the vulnerabilities pose, supporting the explanation with evidence	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	Does not explain vulnerabilities specific to the network traffic and the security threats the vulnerabilities pose	11.1
Vulnerability Assessment: Anti-Malware Systems	Explains vulnerabilities specific to the anti-malware systems and the security threats the vulnerabilities pose, supporting the explanation with evidence	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	Does not explain vulnerabilities specific to the anti-malware systems and the security threats the vulnerabilities pose	11.1
Vulnerability Assessment: Operating Systems / Workstations	Explains vulnerabilities specific to the operating systems and workstations and the security threats the vulnerabilities pose, supporting the explanation with evidence	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	Does not explain vulnerabilities specific to the operating systems and workstations and the security threats the vulnerabilities pose	11.1
Vulnerability Assessment: Network Hardware	Explains vulnerabilities specific to the network hardware systems and the security threats the vulnerabilities pose, supporting the explanation with evidence	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	Does not explain vulnerabilities specific to the network hardware and the security threats the vulnerabilities pose	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%**