This week, you will submit the second project, VM Scanner Background Report, based on the [Nessus Report](https://learn.umgc.edu/d2l/common/dialogs/quickLink/quickLink.d2l?ou=550118&type=coursefile&fileId=My_Basic_Network_Scan_qw3e2d+(2).html). As you are writing your report, you may want to refer back to the CEO’s video in Week 1 to make sure your analysis and recommendations align with the CEO’s priorities and concerns.

You should link your analysis to the kinds of organizational functions and data associated with a transportation company (e.g., protecting order data, customer lists, sales leads, Payment Card Industry (PCI) compliance for processing credit, proprietary software, etc.) and provide your recommendation if Mercury USA should purchase the Nessus tool. This report should be four to six pages in length and include a title/cover page. Include in-text citations and a reference page with three quality sources in a citation style of your choice.

|  |
| --- |
| **How Will My Work Be Evaluated?**  For this assignment, you are asked to provide your supervisor, Judy, with a technical evaluation of a vulnerability scanner. By documenting your results in an effective background report, you are showing how you use your technical knowledge to convey your ideas to others in a professional setting. Your ability to express your findings using the right mix of technical detail in a business context is an important workplace skill.  The following evaluation criteria aligned to the competencies will be used to grade your assignment:   * 1.3.1: Identify potential sources of information that can be used to develop and support ideas. * 1.4.1: Produce grammatically correct material in standard academic English that supports the communication. * 10.1.1: Identify the problem to be solved. * 12.2.1: Identify systems for the risk assessment. * 12.3.1: Select controls. * 13.2.1: Evaluate vendor recommendations in the context of organization requirements. |

If you haven’t already downloaded it last week, download the [VM Scanner Background Report Template](https://learn.umgc.edu/d2l/common/dialogs/quickLink/quickLink.d2l?ou=550118&type=lti&rcode=UMUC-5840726&srcou=539254) now and follow the instructions in the document.

There should intext citation

Transcript

**Message from the CEO**

**Transcript**

Hello, as many of you know, I am the CEO and the chairman of the board of directors.

Recently, one of our company’s biggest competitors was the victim of the ransomware known as Wannacry. You may have seen the news reports.

From their initial investigation, our rival found out that their network was compromised by a trick bot on Windows 7 and Windows 8.1 desktops.

The hackers worked their way up to the Windows Server 2012 R2, where the company stored their mission-critical data. Customer data such as shipping records, credit card information, and other pertinent information were encrypted by the ransomware.

The company lost access to customer data and more importantly, lost customer confidence. It is reflected in their stock price.

We can’t afford to let this happen to us. We are going to take steps to ensure that our customers’ data is safe from these kinds of attacks. We’ve got a lot invested in our data, and we don’t want to face a situation where we would be tempted to pay a lot of ransom money with no real guarantee that the bad actors would even provide the key to decrypt our files.

In this competitive market, we need to be proactive to stay relevant.

So, stay tuned, and thanks for all the hard work that you do for our company.