Penetration testing provides valuable insight into how a system or network performs from the outside in. In this assignment, students will take the lead on a basic penetration test to gain valuable information in order to provide a defensive strategy to mitigate vulnerabilities. View the "Lab 5 Challenge Your Hacking Skills" video within the "Video Playlist: Penetration Testing and Risk Management," located in the topic Resources.

Create a 6- to 8-minute PowerPoint presentation with an embedded video. Show professionalism in your speech and appearance. Use an online video platform such as Loom, YouTube, or Vimeo to upload your completed video. Ensure that others can access and view your linked video prior to submitting to the LMS. In the video, be sure to detail the following, using screenshots:

Part A

* Explain how you would plan, organize, and perform penetration testing on your Metasploitable 2 VM.
* Provide a brief summary of why a penetration test is valuable to an organization.
* Describe how you would handle failures in following procedures.

Part B

Utilizing your Kali VM, conduct the following scans against your Metasploitable 2 VM and provide screenshots in your video:

* NMAP Scan
* Nikto Scan
* OWASP – Zap scan
* Use the Nessus vulnerability scans from Topic 5.

Part C

* Perform a risk assessment and gap analysis based upon your findings from the Part B scans and current trends in cybersecurity.
* Propose and analyze countermeasures to mitigate vulnerabilities.
* Describe your expected results.
* Explain how your strategy to establish mitigation of the vulnerabilities identified in your scans.
* Explain how strategy reduces risk and hardens your system.

Part D

* Login locally to your Metasploitable 2 VM (msfadmin:msfadmin) and implement at least three of the changes described in Part C.

Part E

* Explain why you chose to implement the changes you did (cost, expedience, criticality).
* Describe which vulnerabilities were impacted by the change.
* How were your expected results different from your actual results?
* What are some lessons learned from hardening your system?

**Note:** Retain a copy of this assignment for the "Business Continuity Plan," which will be finalized and submitted in either CYB-690 or ITT-660, depending on your major.

APA style is not required, but solid academic writing is expected.

This assignment uses a rubric. Please review the rubric prior to beginning the assignment to become familiar with the expectations for successful completion.

You are not required to submit this assignment to LopesWrite.

***Benchmark Information***

*This benchmark assignment assesses the following programmatic competencies:*

*MS-Cybersecurity*

*1.3: Conduct risk assessments and evaluate vulnerabilities, threats and gaps in an organization's infrastructure to identify appropriate security measures to reduce risks' impact to business processes.*