The utilization of VMs to understand the principles of ethical hacking has become common within cybersecurity. In this assignment, we will walk through the basics of vulnerability analysis and show the ease with which a vulnerability can be exploited to gain root access of a system.

View the "Lab 3 Your First Hack Part 2 Lab" video within the "Video Playlist: Penetration Testing and Risk Management," located in the topic resources. Utilizing your Kioptrix 1 machine from last week, gain root access to the device. Begin by adding a user to the system with full root access. There are various ways to hack into the provided machine, all of which result in the same outcome of gaining root access.

The director of IT has asked you to present your mitigation strategy at a conference. As usual, your meeting was hastily increased in scope to include a training class for the C-suite with regard to common attacks used against the company in the last 30 days. Create a video presentation outlining how to gain access to the system. Provide a brief summary on the mitigation techniques you would employ to secure the system from privilege escalation and assume upgrading and replacement is not an option. Define the taxonomy of attacks by providing a definition, summary, and categorization of the following attack families:

* Buffer overflow
* Privilege escalation
* Rootkits
* Trojans
* Backdoors
* Viruses
* Return-oriented programming
* Common social engineering attacks

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.