Unit 4 Discussion 1: Compromising an Online System

Learning Objectives and Outcomes

- You will be able to explore how a Linux system can get compromised.
- You will examine ways in which a well-secured Linux filesystem can mitigate risks.

Assignment Requirements

The Apache Software Foundation (ASF) is a reputable open source foundation that has a history of developing and maintaining many open source products, including the Apache Web Server. In April 2010, the ASF discovered that their server hosting issue-tracking software was “hacked.”

You can read a report on the incident on the following Web link:

- https://blogs.apache.org/infra/entry/apache_org_04_09_2010

This report documents how a vulnerability was exploited, which solutions worked, which didn't work, and the measures planned by the Apache Infrastructure Team to mitigate future risks.

Security is a layered process. Although the hackers took advantage of a vulnerable third-party Web application to gain root access to ASF’s Linux infrastructure, you need to focus on the layers of security that worked and failed on the Linux infrastructure, and how this vulnerability could have been avoided with a more secure Linux server.

Discuss how the hackers took advantage of the JIRA daemon. What role did Pluggable Authentication Modules (PAM) play in this process? What are the security measures that you would recommend to mitigate such risks in the future?

Participate in this discussion by engaging in a meaningful debate regarding the role of the JIRA daemon and PAM in the system breach and suggest security measures. You must defend your choices with a valid rationale. At the end of the discussion, write a summary of your learning from the discussion and submit it to your instructor.

Required Resources

- Access to the Internet

Submission Requirements

- Format: Microsoft Word
- Font: Arial, Size 12, Double-Space
- Citation Style: Chicago Manual of Style
- Length: 1–2 pages
- Due By: Unit 4

Self-Assessment Checklist

- I have provided key points about how security is compromised through various vulnerabilities.
- I have explained how users are able to login with passwords even when password-based logins are disabled for Secure Shell (SSH).
- I have described security risks and how such risks can be mitigated.