STUDENT COPY

The following sections contain student copies of the assignments. These must be distributed to students prior to the due dates for the assignments. Online students will have access to these documents in PDF format, which will be available for downloading at any time during the course.

Graded Assignment Requirements

Assignment Requirements documents provided below must be printed and distributed to students for guidance on completing the assignments and submitting them for grading.

Instructors must remind students to retain all handouts and assignment documents issued in every unit, as well as student-prepared documentation and graded deliverables. Some or all these documents will be used repeatedly across different units.

Unit 1 Discussion 1: Securing a Linux System

Learning Objectives and Outcomes

- You will present different views on security related to a Linux system.
- You will be able to identify risks related to the implementation of a Web application in a Linux environment.

Assignment Requirements

A small community bank is studying the prospect of maintaining its own in-house Linux Web server for a Web application. The Web application will allow the bank's customers to login, view their loan details, and check and save account balances. The company sends you a request for your services as a Linux and open source consultant. You grab the opportunity because you are dissatisfied with your current job.

It is your first day in the community bank, and you are told that your role as a consultant will be to analyze all probable risks related to the prospective Web application. Your manager introduces you to the other employees, including Bob, who is an intern working on the development of the Web application. Bob is also the system administrator as he currently supports the local area network (LAN) environment. You discuss the Web application and its functioning in detail with Bob.

Bob tells you that the server will be hosted at the bank's location since the other servers are presently supporting their Microsoft Windows-based LAN. The Web application will run on any of the popular open source servers. Knowing your background, Bob is very excited to learn Linux and use this learning to make the Web application more effective and less vulnerable.

Bob shares the following server requirements with you:

- A Web server
- A database server
- A Simple Mail Transfer Protocol (SMTP) server
- A file server for customers' loan applications and other personal data files

Your manager asks you to prepare a brief presentation on the areas of high risk for this project and to present it before the board of directors the next day.

Discuss and share three top areas of risk providing a suitable rationale for your selection. Participate in this discussion with your classmates by engaging in a meaningful debate regarding risks expected in this project. Summarize your thoughts in a document and submit it to your instructor.

Required Resources

None

Submission Requirements

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

Self-Assessment Checklist

- I have identified at least three areas of risk.
- I have recognized areas that were not previously considered as a risk.

Unit 2 Discussion 1: Identifying Layers of Access Control in Linux

Learning Objectives and Outcomes

- You will be able to identify various layers of access control in a Linux server environment.
- You will make security recommendations using different layers of access control.

Assignment Requirements

Really Cheap Used Computers, Inc. is an online seller of old school computers. The organization’s e-commerce Web site runs on a Linux server. The server is located at the organization’s local office in Boston, Massachusetts. The company has experienced tremendous growth and has hired you as the new security analyst. You access the server and find that there are virtually no layers of security other than the passwords set for user accounts.

Discuss at least three layers of access control that can be put in place on this server to create a more secure environment. Rationalize whether the given scenario represents discretionary access control (DAC) or mandatory access control (MAC).

Participate in this discussion by engaging in a meaningful debate regarding your choices of the three layers of access control in Linux. You must defend your choices with a valid rationale. Summarize your thoughts in a Word document and submit it to your instructor.

Required Resources

None

Submission Requirements

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

Self-Assessment Checklist

- I have demonstrated a basic understanding of access control mechanisms.
- I was able to identify and differentiate between the different layers of access control.

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.

Unit 6 Discussion 1: Determining Firewall Rules

Learning Objectives and Outcomes

- You will be able to explore design and firewall rules for a bastion host.
- You will examine how a bastion host allows administrators to access Samba and Secure Shell (SSH) for remotely managing a server.

Assignment Requirements

As the Linux system administrator of insurance company Secure All, Inc., you need to design firewall rules for the organization's bastion host file server, which uses Samba. This server is located in the local area network (LAN) with the network address 172.16.0.0/12 and subnet 255.240.0.0. The server should also allow Web application access for its online transaction platform to mount the filesystem. The Web application resides on the Web server located in the demilitarized zone (DMZ). This server has two interface cards. One card, which is for the traffic from the DMZ firewall, is linked to the wide area network (WAN). This card's IP address is 192.168.1.5. The other interface card has the IP address 172.16.1.5 and is linked to the LAN.

Which firewall rules should be written using iptables for the server hosting Samba? Discuss and suggest firewall rules to allow administrators to remotely manage the server using SSH. Use the concept of "default deny" when designing the rules.

Participate in this discussion by engaging in a meaningful debate regarding the firewall rules that can be written using iptables. 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

None

Submission Requirements

- Format: Microsoft Word
- Font: Arial, Size 12, Double-Space
- Citation Style: Chicago Manual of Style
- Length: 1–2 pages
- Due By: Unit 6

Self-Assessment Checklist

- I have provided suitable iptables rules for the server hosting Samba using the concept of “default deny.”
- I have explained key points of how a bastion host should allow administrators to access Samba and SSH for remotely managing the server.

Unit 8 Discussion 1: Using Community and Vendor Support for Managing Software

Learning Objectives and Outcomes

- You will be able to explore options available to maintain Linux servers and its open source software through various support methods.
- You will examine situations in which an organization may consider subscription-based support or community-based support.

Assignment Requirements

Community-supported software refers to free software support offered in the open source community. On the other hand, vendor-supported software refers to paid software subscriptions provided by a vendor. Organizations providing Linux support may or may not make money for providing the support.

Many open source software users do not pay for Linux support and instead use forums, mailing lists, and Internet Relay Chat (IRC) to find solutions to a problem. This free “community support” is quite popular for keeping the software updated and addressing configuration and production issues.

Discuss the pros and cons of Linux support provided by the community and by vendors. What are the situations where an organization may consider subscription-based support or community-based support and why?

Participate in this discussion by engaging in a meaningful debate regarding situations where an organization may consider subscription-based support or community-based support. Support your answers with a suitable rationale. At the end of the discussion, write a summary of your learning from the discussion and submit it to your instructor.

Required Resources

None

Submission Requirements

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

- Due By: Unit 8

Self-Assessment Checklist

- I have described the advantages of Linux support provided by the community and vendors.
- I have explained the situations in which an organization may consider subscription-based support or community-based support.

Unit 10 Discussion 1: Creating a Backup Plan

Learning Objectives and Outcomes

- You will be able to explore the criticality of taking data backup.
- You will examine the appropriate frequency of a backup.
- You will explore a plan to verify the reliability of backups.

Assignment Requirements

As the Linux system administrator for First World Bank Savings and Loan's proposed Linux-based infrastructure, it is imperative that you take a backup of the “right” data, keep the data safe, and restore the data when the need arises.

Discuss a suitable backup plan considering the different servers of the organization. In your plan, include suggestions for verifying backups with periodic restores.

Answer the following questions:

- What is the critical data from each server in the infrastructure that requires a backup?
- Will it be necessary to encrypt backup data?
- How often do you need to take the backup of the data?
- Where will you store the backup data?
- How often will you verify the backups?

Required Resources

None

Submission Requirements

- Format: Microsoft Word
- Font: Arial, Size 12, Double-Space
- Citation Style: Chicago Manual of Style
- Length: 1–2 pages
- Due By: Unit 10

Self-Assessment Checklist

- I have discussed a suitable backup plan explaining the critical data that requires a backup.

- I have clarified whether encryption is necessary or not.
- I have discussed the frequency of taking a backup.
- I have clarified the periodicity of verifying the backup.