Project

Project Title
Linux-Based Web Application Infrastructure

Purpose
The purpose of this project is to evaluate, research, and recommend particular solutions for a Linux-based infrastructure, serving a financial institution's initiative to provide its customers with access to online banking and loan application submittals.

Learning Objectives and Outcomes
You will be able to:
- Explain regulations and legislations that a Linux-based infrastructure needs to address.
- Differentiate between various open source network services.
- Perform user and group account management.
- Configure mounting options for various filesystems.
- Explain the importance of designing a scalable and secure Linux-based infrastructure.
- Configure layers of security for a Linux-based Web server with a firewall, mandatory access control (MAC), and application layer filtering.
- Evaluate the pros and cons of building a custom Linux kernel and using a vendor-supplied kernel.
- Examine the use of a software management plan for Linux systems.
- Examine the use of Linux-based logging, file integrity, and scanning tools.
- Evaluate the need to install anti-virus software on Linux servers.
- Configure a remote logging process.
- Examine the importance of encrypting backup data.
- Design a backup and recovery plan for a Linux-based infrastructure.

Required Source Information and Tools
The following tools and resources will be needed to complete this project:
- Course textbook
- Access to the Internet
- Access to the ITT Tech Virtual Library
You will submit each project task and part as described in the table below. Your instructor will provide you inputs on each task so that you can create a good executive summary for each project part.

## Project Logistics

<table>
<thead>
<tr>
<th>Activity Name</th>
<th>Assigned</th>
<th>Due</th>
<th>% Grade</th>
</tr>
</thead>
<tbody>
<tr>
<td>Project Part 1: Executive Summary</td>
<td>Unit 1</td>
<td>Unit 4</td>
<td>8</td>
</tr>
<tr>
<td>▪ Project Part 1 Task 1: Outline Security Policy</td>
<td>Unit 1</td>
<td>Unit 2</td>
<td></td>
</tr>
<tr>
<td>▪ Project Part 1 Task 2: Provide Open Source Server Solutions</td>
<td>Unit 2</td>
<td>Unit 3</td>
<td></td>
</tr>
<tr>
<td>▪ Project Part 1 Task 3: Manage User Account Access</td>
<td>Unit 3</td>
<td>Unit 4</td>
<td></td>
</tr>
<tr>
<td>Project Part 2: Executive Summary</td>
<td>Unit 4</td>
<td>Unit 7</td>
<td>8</td>
</tr>
<tr>
<td>▪ Project Part 2 Task 1: Secure File Storage Server</td>
<td>Unit 4</td>
<td>Unit 5</td>
<td></td>
</tr>
<tr>
<td>▪ Project Part 2 Task 2: Secure Web and Database Servers</td>
<td>Unit 5</td>
<td>Unit 6</td>
<td></td>
</tr>
<tr>
<td>▪ Project Part 2 Task 3: Provide Layered Security</td>
<td>Unit 6</td>
<td>Unit 7</td>
<td></td>
</tr>
<tr>
<td>Project Part 3: Executive Summary</td>
<td>Unit 7</td>
<td>Unit 10</td>
<td>8</td>
</tr>
<tr>
<td>▪ Project Part 3 Task 1: Use a Kernel</td>
<td>Unit 7</td>
<td>Unit 8</td>
<td></td>
</tr>
<tr>
<td>▪ Project Part 3 Task 2: Recommend a Software Management Plan</td>
<td>Unit 8</td>
<td>Unit 9</td>
<td></td>
</tr>
<tr>
<td>▪ Project Part 3 Task 3: Monitor Logs and Baseline</td>
<td>Unit 9</td>
<td>Unit 10</td>
<td></td>
</tr>
<tr>
<td>Project Part 4: Executive Summary of the Project</td>
<td>Unit 10</td>
<td>Unit 11</td>
<td>8</td>
</tr>
<tr>
<td>▪ Project Part 4 Task 1: Design a Backup Plan</td>
<td>Unit 10</td>
<td>Unit 11</td>
<td></td>
</tr>
</tbody>
</table>

Please note that the tasks listed in the above table are informal submissions for which you can opt to receive formative feedback from the instructor.

## Deliverables

### Overall Scenario

First World Bank Savings and Loan is a financial institution in the United States. The organization offers various banking services, such as loans and deposits. You have recently joined the organization as a Linux system administrator. The organization’s task team has made recommendations to evaluate and prototype a Linux-based infrastructure architecture. The recommendations are based upon factors such as total cost of ownership, scalability, and reliability. Your focus on this project is to ensure that the decisions and recommendations made by the task team and management are appropriate from the confidentiality, integrity, and availability (CIA) triad perspective. You will also research various aspects of the proposed architecture and make recommendations based upon your findings.
Project Part 1 Task 1: Outline Security Policy

Scenario
To stay competitive in the financial institution market, the First World Bank Savings and Loan wishes to provide all banking services online to its customers. These services also include the online use of credit cards for loan applications. The organization estimates over $100,000,000 a year in online credit card transactions for loan applications and other banking services.

A task team has been formed to study the cost, performance, and security of maintaining a Linux and open source infrastructure. According to rough estimates, annual cost savings in licensing fees alone can be up to $4,000,000. At the same time, the confidentiality, integrity, and availability (CIA) triad perspective needs to be taken into account for infrastructure maintenance.

The task team has engaged a network engineer with the network and routing design. The team has determined the following server services that would be needed to support the online transaction infrastructure:

- A database server
- A Web server
- A file server
- A Simple Mail Transfer Protocol (SMTP) server
- A Lightweight Directory Access Protocol (LDAP) server

All servers would be physically located in a third-party data center.

Tasks
You need to:

- Understand the business need of First World Bank Savings and Loan.
- Point out specific legislation and regulations that meet the statutory compliance criteria.
- Assess the feasibility of Linux and open source infrastructure in handling security demands listed by the legislation and regulations.
- Make recommendations to model a tiered architecture for the proposed online transaction in a Linux-based infrastructure.
- Identify a suitable security framework that forms the basis of your recommended security policy, providing a valid rationale for your recommendation.
- Create a professional summary report detailing the execution of each task assigned to you.
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 examined the business need of the organization and compliance with specific legislation and regulations.
- I have recommended a tiered architecture for the proposed online transaction.
- I have suggested an appropriate security framework for the security policy.
Project Part 1 Task 2: Provide Open Source Server Solutions

For the various servers at First World Bank Savings and Loan, you need to recommend the appropriate open source software for each server.

Tasks
You need to:

- Research and evaluate various open source software for each server considering the stability and security of the software.
- Recommend open source software for each server and explain reasons for selecting each software.

Submission Requirements

- Format: Microsoft Word
- Font: Arial, Size 12, Double-Space
- Citation Style: Chicago Manual of Style
- Length: 1–2 pages
- Due By: Unit 3

Self-Assessment Checklist

- I have researched and evaluated various open source software for each server.
- I have recommended open source software for each server providing rationale for my recommendation.
Project Part 1 Task 3: Manage User Account Access

Scenario
At First World Bank Savings and Loan, a group of Web administrators need to manage the Web servers. A group of Linux administrators need to manage user accounts and general system maintenance while the security analyst needs access to read log files. You need to design an account policy for granting user access permissions to these users.

Tasks
You need to:
- Summarize an account policy that can be used for all users.
- Describe special permissions, if any, required to create user or group accounts.

Submission Requirements
- Format: Microsoft Word
- Font: Arial, Size 12, Double-Space
- Citation Style: Chicago Manual of Style
- Length: 1–2 pages for the project task; 2–3 pages for the executive summary
- Due By: Unit 4

Self-Assessment Checklist for Project Part 1 Task 3
- I have created an account policy that can be used for all users.
- I have described special permissions that may be required to create user or group accounts.

Self-Assessment Checklist for Project Part 1: Executive Summary
- I have summarized the organization’s business model as it relates to e-commerce.
- I have explained the need to secure the Linux platform.
- I have demonstrated the design of a tiered e-commerce platform architecture.
- I have explained the benefits of creating group accounts and managing user account access.
- I have described how data can be shared with the Web server in a secure fashion.
Project Part 2 Task 1: Secure File Storage Server

Scenario
There is a requirement to read customer confidential data located in the local area network (LAN) of First World Bank Savings and Loan. The organization needs to deliver highly confidential customer data in Portable Document Format (PDF) format for its online customers. This data is typically uploaded to a Linux file server by the bank employees within the LAN. However, online customers need to have access to their particular data. At the same time, the customers should not be able to modify the data.

Tasks
You need to:
- Design a file storage server architecture for the proposed Web-based infrastructure to support customers.
- Describe specifically how data can be shared with the Web server in a secure fashion.

Submission Requirements
- Format: Microsoft Word
- Font: Arial, Size 12, Double-Space
- Citation Style: Chicago Manual of Style
- Length: 1–2 pages
- Due By: Unit 5

Self-Assessment Checklist
- I have explained how a Linux server can read data from a secure server in the local network.
- I was able to understand Linux filesystem mounting options.
- I have recommended an appropriate network sharing service.
Project Part 2 Task 2: Secure Web and Database Servers

Scenario
First World Bank Savings and Loan needs to service its customers online with a Web application using a database that contains highly sensitive information. The Web application has been designed to work well with open source Web and database servers. The front end of the Web application, which is accessed by users, is served by a Web server. The Web server communicates with a database server to deliver the data. In other words, the Web server interacts with the database server. The users do not need to interact directly with the database server.

Tasks
You need to:
- Research and make recommendations about how the organization should implement the Web and database servers. Defend your recommendations in terms of security and stability.
- Explain how Web and database administrators will be able to access the servers remotely.

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 recommended a database and Web server architecture and provided adequate explanations for the recommendation based upon security and stability.
- I was able to specify a remote access solution for the Web and database administrators that can be considered secure.
**Project Part 2 Task 3: Provide Layered Security**

**Scenario**
First World Bank Savings and Loan requires layered security for its public-facing Web server. The Web server is a bastion host that uses Secure Sockets Layer (SSL) for customer activity. In addition, the server provides Secure Shell (SSH) access to administrators. Even though the security team has a hardware solution for the firewall in the demilitarized zone (DMZ), you need to provide additional layers of security on the Web server by using firewall, Transmission Control Protocol (TCP) Wrappers, and Security Enhanced Linux (SELinux).

**Tasks**
You need to:
- Access the Web server using SSH from the Internet.
- Discuss how TCP Wrappers can be used for providing security. What are the other options that can be configured in TCP Wrappers?
- Summarize the changes that need to be made in SELinux, if it is turned off.
- Explain ways in which the Web server can be allowed to serve Web pages to customers.

**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 for the project task; 2–3 pages for the executive summary
- Due By: Unit 7

**Self-Assessment Checklist for Project Part 2 Task 3**
- I have designed firewall rules and explained when it is appropriate to use TCP Wrappers.
- I was able to manage objects using SELinux.

**Self-Assessment Checklist for Project Part 2: Executive Summary**
- I have explained remote mounting options and the implications of selecting read-write versus read-only options.
- I have demonstrated a secure architecture design for common Web-based e-commerce platforms using Web and database servers.
- I have described layered security as part of a bastion host’s configuration by using a minimum mandatory access control (MAC) and a firewall.
Project Part 3 Task 1: Use a Kernel

First World Bank Savings and Loan's Linux-based infrastructure requires an in-house custom kernel or a kernel provided by a vendor.

Tasks
You need to:

- Make recommendations whether the organization should use a custom kernel, compile stock kernels from sources, or use a vendor-supplied kernel.
- Explain the pros and cons of each of the kernel options and support your recommendations with a valid rationale.

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 recommended the appropriate kernel that can be used by the organization.
- I have explained the advantages and disadvantages of using each of the kernel options with a valid rationale.
Project Part 3 Task 2: Recommend a Software Management Plan

Scenario
The original task team at First World Bank Savings and Loan has concerns about the support and software management of the organization’s Linux-based infrastructure. The team wants you to recommend a software management plan keeping in mind the various servers and the cost.

Tasks
You need to:
- Make a recommendation for a software management plan. Consider options available from the open source community and from vendors. If you select a vendor, specify the software it will support and how it will support.
- Explain the need to install anti-virus software on Linux servers providing a rationale in support of your answer.
- Summarize a plan for applying patches and security updates to the Linux system.

Submission Requirements
- Format: Microsoft Word
- Font: Arial, Size 12, Double-Space
- Citation Style: Chicago Manual of Style
- Length: 1–2 pages
- Due By: Unit 9

Self-Assessment Checklist
- I have recommended a suitable software management plan.
- I have explained the need to install anti-virus software on Linux servers.
- I have explained how to manage critical and noncritical security-related updates.
Project Part 3 Task 3: Monitor Logs and Baseline

Scenario
The task team at First World Bank Savings and Loan wants you to research appropriate monitoring tools for the organization’s Linux-based tiered infrastructure.

Tasks
You need to:

- Summarize the benefits of remote logging.
- Recommend tools for:
  - Alerting administrators when files in the operating system have changed.
  - Checking for rootkits.
  - Checking for new open ports, files, and system resources.
- Explain how logwatch can be configured to deliver a daily report from each server summarizing events found in log files.
- Recommend a schedule and a software application or service to periodically scan the servers to satisfy Payment Card Industry (PCI) Data Security Standard (DSS) compliance requirements.

Submission Requirements
- Format: Microsoft Word
- Font: Arial, Size 12, Double-Space
- Citation Style: Chicago Manual of Style
- Length: 1–2 pages for the project task; 2–3 pages for the executive summary
- Due By: Unit 10

Self-Assessment Checklist for Project Part 3 Task 3
- I have recommended a file integrity checker and explained the purpose of a rootkit checker.
- I have explained the use of common GNU’s Not UNIX (GNU) utility tools.
- I have described the configuration of logwatch and recommended a service or tool for periodic server scans.

Self-Assessment Checklist for Project Part 3: Executive Summary
- I have recommended appropriate kernel options for the organization and explained the pros and cons of each option.
- I have described the importance of a software management plan.
- I have explained the use of installing anti-virus software on Linux servers.
• I have summarized monitoring and logging techniques used in a typical Linux infrastructure.
• I have described the importance of a suitable backup plan, while maintaining data confidentiality using encryption.
**Project Part 4 Task 1: Design a Backup Plan**

For the various servers that are part of First World Bank Savings and Loan's Linux-based infrastructure, you have to research and design a backup plan using open source and commercial software. You can create the design based on your discussions with peers in Unit 10 Discussion 1 titled “Creating a Backup Plan.”

**Tasks**

You need to:

- Recommend software, both open source and commercial, to use for the backup plan. Explain reasons for your recommendation.
- Recommend a design of the backup plan. Answer the following questions:
  - Will you use a dedicated server or a service provider for backups?
  - Will backups be stored on hard disks, tape media, or any other media?
  - Who will be responsible for verifying backups and restoring data?
- Summarize the need for encrypting backup data.

**Submission Requirements**

- Format: Microsoft Word
- Font: Arial, Size 12, Double-Space
- Citation Style: Chicago Manual of Style
- Length: 1–2 pages for the project task; 3–5 pages for the executive summary
- Due By: Unit 11

**Self-Assessment Checklist for Project Part 4 Task 1**

- I have recommended open source and commercial software options for the backup.
- I have designed a plan for full and incremental backups and explained the need for encrypting backup data.
- I have designed a process for backup verification and restoring.

**Self-Assessment Checklist for Project Part 4: Executive Summary of the Project**

- I have demonstrated how to secure a Linux platform using installed commands and other available open source software.
- I have explained the use of bastion hosts to secure architecture design.
- I have examined best practices to mitigate security risks to a Linux server using a suitable software management plan.
- I have demonstrated the use of a layered security approach on Linux servers.
- I have described backup, recovery, and incident response in a Linux architecture.