**LAS CA2 Report**

Proof of concept system for ABC Company



Submitted on: 2th February 2020

*Done by:*

*Lee Yi Terng (1904189)*

*Sean Chye (1904189)*

# 1. Introduction

## 1.1 Purpose of the Document

This document details the information regarding the Proof of Concept system developed for ABC Company.

The Proof of Concept was developed to allow ABC Clients to browse ABC products on sale, as well as to allow ease of access for ABC staff to update said price list remotely.

The preparation of this document will be followed up by a demonstration based on the demonstration agenda below.

## 1.2 Factors Considered

This proof of concept system was developed with the following factors in mind:

Maximum of three virtual machines used;

Only two or three sample price lists needed;

Web content will be HTML based;

At least five security features;

The general public can browse the price lists;

Authorised ABC staff can upload/update price lists.

## 1.3 Document Structure

This document is organised in the following sections:

Section 2: SYSTEM OVERVIEW

Section 2 states the overview of the Proof of Concept System, assumptions made when creating it as well as including the network design with a diagram and listing out required services in order to run the Proof of Concept System properly.

Section 3: OPERATION PROCEDURES

This section highlights instructions and detailed explanations on how clients and staff of ABC can carry out their operations in its intended manner.

Section 4: SECURITY MEASURES

This section offers detailed explanations of each of the security measures put in place to harden the server and reduce the possibility of successful attacks. The section also indicates the importance of each measure. Measures explained in this section include but are not limited to, removing root login, firewall and SELinux.

Section 5: FUTURE IMPROVEMENTS

This section describes and discusses future considerations and measures that can be implemented to better enhance the Proof of Concept System’s security or functionality.

Section 6: DEMONSTRATION AGENDA

This section describes the agenda that will be used for the demonstration of the Proof of Concept system and will be strictly adhered to.

# 2. System Overview

## 2.1 Overview

The Proof of Concept system was designed to provide customers and staff alike a convenient way to carry out their respective tasks.

For customers, they can access the site via their web browser.

For staff, they can remotely update and change the price lists of products as to the needs of ABC Company.

## 2.2 Assumptions

While designing the Proof of Concept System, the assumptions listed below were made:

Only one group of ABC staff needed to access the server besides the administrator;

The staff of ABC only needed to update the price lists at work, whilst on the same network as the server itself;

## 2.3 Network Design

### 2.3.1 Virtual Machines Used

In this proof of concept system, two virtual machines were used. One to act as the web server and one to act as a client for the customers and employees. The use of a third virtual machine will be needed should enhancements be implemented. (Refer to Section 5.4 and Section 5.5)

### 2.3.2 Specifications

Operating System: CentOS 7

Minimum: 4GB RAM, 2 GB memory

Preferred: 8GB RAM, 10GB memory

The Proof of Concept system is developed with growth and expansion in mind. While 4GB of RAM should be adequate at this point in time, should ABC Company’s customer base grows, the server would need to handle more requests and the increased amount of RAM will enable it to be able to handle these requests without sacrificing speed. The storage memory of the system has also been decided with expansion in mind. Should the number of products sold by ABC company ever increase, there will be adequate memory space to store the price lists.

### 2.3.3 Network Diagram

### 

## 2.4 Required Services

### 2.4.1 Apache Web Server (HTTPD)

The httpd service for the Apache Web Server is of utmost importance. It hosts the websites and allows client and customer access via HTTP protocols using their web browsers. The HTML files for the webpage “[www.abcstore.com](http://www.abcstore.com)” is stored in “/var/www/ABC”.

The Apache Web Server is enabled to start upon boot-up of the server. A status page can also be configured to be displayed for troubleshooting purposes in the future if necessary.

### 2.4.2 SSHD Service

The SSHD service is used to allow authorized employees of ABC Staff to remotely edit the price lists from their own workstations. The service is enabled on both the server and the employee’s clients.

Employees will SSH into the server in order to do their edits and upload or update price lists.

The SSHD Port 22 and service is set to be permanently on for the server in order to allow round the clock access for employees to edit whenever necessary. Firewalls are configured to allow connections to the SSHD service. While this allows anyone to attempt an SSH connection to the server, a valid account and its credentials are required for a successful SSH connection to be established.

# 3. Operation Procedures

## 3.1 General Public

Clients, customers or the general public can access the price list by using their web browser and browsing to “<http://www.abcstore.com>”. This will bring them to the home page of the website, where they can choose from the options available to view the price list of their preference. At the price list pages, there are back buttons to let them go back to the home page should they want to view another price list.

The web browser uses HTTP protocols to access the webpage.

## 3.2 Staff

Authorized ABC Employees who need to update, edit or upload the price lists can do so remotely from their own workstation. From their workstation, they must ensure their client has the SSH-Client installed. This will allow them to attempt an SSH connection to the server and log in using their account credentials.

Current Accounts for demonstration purposes:

Username: ABC\_Employee\_1   
Password: centos

Username: ABC\_Employee\_2   
Password: centos

Username: ABC\_Employee\_3  
Password: centos

Upon successful login, they can change their directories to “var/www/ABC” where they will be able to view and edit the HTML files of the price lists using the text editor of their choice. The home page “index.html” cannot be edited by any ABC Employees except the administrator for security purposes. The employees are also unable to change or alter any other directories or files not authorized to them.

To exit the SSH session, simply type “exit”.

## 3.3 Administrator

The administrator holds Sudo privileges over the entire system and is expected to carry out the required measures properly in order to ensure the adequate security and protection of the system. He has the power to change user permissions, create new users, change file permissions and many other functions.

Current Admin Account for Demonstration Purposes:

Username: admin

Password: admin

# 4. Security Measures

Security is of utmost importance to any system, and the Proof of Concept System has been designed with that in mind. Below are detailed descriptions of each security measure that has been put in place for the system. They are rated in importance level as well for priority sake. (Low, Medium, High)

## 4.1 SELinux

Security-enhanced Linux (SELinux) is an essential part of securing the Linux OS. It is a Linux kernel security module that provides a mechanism for supporting access control security policies, including mandatory access controls. SELinux is a set of kernel modifications and user-space tools that have been added to various Linux distributions. SELinux is currently enabled to start upon boot-up of the server and set to “Enforcing Mode”. This ensures that SELinux is always on and monitoring.

Importance: **High**

## 4.2 Firewall

The firewall is configured to only open essential ports such as HTTP-80 and SSH-22. The other unnecessary ports and services are all disabled to minimise weak points in the system which attackers can exploit. This is to ensure that the firewall protects the system from outside attacks as much as possible.

Importance: **High**

## 4.3 Disabled Root Login

By disabling Root login it forces users to use the ‘Sudo’ command. Sudo has a greater command of logging and auditing, which means the owner can track the actions of that particular user for malicious or suspicious activity. This can be very useful for forensic investigation and analysis. Moreover, disabling the root login means the attackers cannot try to hack their way into a root account, which would give them unlimited power over the system.

Importance: **High**

## 4.4 Drop Ping Requests

By pinging a system, hackers will be able to find out whether the system is online or if it exists at all. By dropping the ping request, it would not return any information about the system and make it seem that the system is offline or dead. This will make the system more secure as hackers will not be able to attack a dead or non-existent system.

Importance: **Medium**

## 4.5 SSHD Brute Force Protection

Hackers can easily brute force SSHD login by repeatedly entering usernames and passwords without a limit. A maximum count of logins, 3 in this case, in a specific time can be implemented, by installing the fail2ban firewall and configuring it to only allow up to a few failed logins before they are timed out for a period of 10 minutes.

Importance: **High**

## 4.6 Hiding Apache Version

The version of the website can provide useful information for the hacker to use and exploit. A hacker can use Nmap and cross-check the information on the common vulnerabilities website and exploit it. The common vulnerabilities website provide an in-depth explanation of loopholes and exploits in previous systems. They also sometimes will contain information on how to exploit that particular system in the form of scripts, downloadable software and even detailed walkthrough. Therefore by hiding the version of apache, it would require the hacker to do more work and research thus, reducing the chances of the hacker getting into the system.

Importance: **Medium**

## 4.7 XSS Protection

Cross-site scripting is an application-layer vulnerability in the Apache server. Without protection, the website will not be able to identify whether the script is trust or not and will run the script nonetheless. The script might allow a hacker to gain information about the tokens, session cookies or other sensitive information retained by the browser and used with that site.

By enabling cross-site scripting protection, it prevents the hacker from running and injection client-side scripts into web pages that were viewed by other users.

Importance: **Low**

## 4.8 Clickjacking Attack Immunity

Clickjacking is a well-known web application vulnerability. There are ways to protect against clickjacking attacks. X-Frame-Options in the HTTP response header can be used to indicate whether or not a browser should be allowed to open a page in frame or iframe via HTML.

There are three settings for X-Frame-Options:

1. SAMEORIGIN: This will allow the page to be displayed in a frame on the same origin as the page itself
2. DENY: This will prevent a page from manifest in a frame or an iframe
3. ALLOW-FROM uri: This setting will check the frame for a specific origin and only allow the page to be displayed on that

Importance: **Medium**

## 4.9 Secure Apache Using Modules

Mod\_security is an apache module works as a firewall for web applications and allows monitoring of traffic on a real-time basis. It also helps to protect the server from brute force attacks

Mod\_evasive is a very efficient module that prevents DDOS attacks from being as effective and also enables it to handle HTTP brute force and Dos or DDOS attacks. It detects attacks by checking the number of requests made to the page per second and many more.

Importance: **Low**

## 4.10 Disable TRACE HTTP Requests

‘TRACE' is an HTTP request method used for debugging which echo's back input back to the user. There was a report posted that a hacker could use the HTTP TRACE method to steal information including cookies, and possibly website credentials. It is a good idea to only enable HEAD, POST, and GET for web applications.

Importance: **Low**

## 4.11 Least Privilege

ABC Employees who need to update the price list only have access to the folder with the HTML files for the website and can only replace the price list webpages. They do not have access to any other folders or files in the system. This is to ensure the employee accounts have just enough privilege to carry out their jobs and nothing else for the sake of security. This can be changed only by the system administrator.

If the employee accounts are given more privilege than they need, they can access files they should not be accessing and alter certain files or folders. Employing the least privilege helps to improve the protection of data and limit malicious behaviour, be it from the employee themselves or a hacker who has gained control of an employee account.

Importance Level: **High**

# 5. Future Improvements

As we believe that to remain relevant, we must continually improve ourselves and gain new skill sets, we believe the Proof of Concept system still has much to offer in the future. Listed below are some potential improvements that can be implemented in the future to give the system better functionality and features as well as more security.

## 5.1 SAMBA

A samba file system can be set up as an alternative to SSH for employees to update, edit or upload price lists. It allows end-users to access files, printers, and other shared resources. The file shares will be accessible from all devices on your network. This can be done by installing the samba and samba-client packages on the server and employee clients.

## 5.2 SFTP

Secure file transfer protocol (SFTP) is the more secure counterpart of the File transfer protocol (FTP). SFTP is a part of the SSH protocol suite. It provides full authentication and security functionality of the SSH protocol, Including SSH keys.

## 5.3 Chroot Jail

Chroot jail prevents a remote SSH user from accessing other directories other than the one that it is allowed to. Chroot jail is important as it prevents users with malicious intent from accessing important directories they should not have access to.

## 5.4 Remote Log Files

Normally log files are stored locally, because of that when the computer crashes the log files cannot be recovered. The hacker can also delete the log files so as to cover up their tracks, they are not very reliable. Remote logging files are far more reliable as they will send a backup of their log files to another computer in the same network. Therefore, when the initial computer is compromised the log files can still be recovered.

## 5.5 Reverse Proxy

By setting up a reverse proxy, it prevents attackers from spamming ping requests to the website by setting up another identical website as a proxy and redirecting the ping requests to that proxy. Therefore, significantly reducing the amount of spam that the original website receives as most of the traffic is sent to the proxy.

# 6. Demonstration Agenda

Listed below is the demonstration agenda that will be used and strictly followed for the Proof of Concept system.

1. Demonstrate website and customer access
2. Show the employee SSH using a client VM and accounts
3. Show employee able to edit the pages remotely
4. Show employee least privilege
5. Show admin account with sudo privileges
6. Show SELinux in enforcing
7. Show disabled root login
8. Show dropping ping requests using client VM
9. Show brute force protection

# 7. Conclusion

This concludes the Proof of Concept system report. Based on the requirements and security features implemented, we feel this is a quality system that will bring benefits to ABC Company.

*End of report*

References:

Boyle, I., ABC Magazine practical parenting advice. ABC Magazine. Available at: https://abcmag.co.uk/ [Accessed January 24, 2020].

HostAdvice. (2020). *How to Harden the Apache web server on a CentOS 7 VPS or Dedicated Server | HostAdvice*. [online] Available at: https://devops.ionos.com/tutorials/how-to-harden-the-apache-web-server-on-centos-7/ [Accessed 28 Jan. 2020].

Devops.ionos.com. (2020). *How to Harden the Apache Web Server on CentOS 7 | IONOS DevOps Central*. [online] Available at: https://devops.ionos.com/tutorials/how-to-harden-the-apache-web-server-on-centos-7/ [Accessed 28 Jan. 2020].

Owasp.org. (2020). *Cross Site Scripting (XSS) | OWASP*. [online] Available at: https://owasp.org/www-community/attacks/xss/ [Accessed 30 Jan. 2020].

Lehman, D. (2020). *Disable Trace HTTP Request in Apache*. [online] nowhereLAN. Available at: https://www.nowherelan.com/2018/12/28/disable-trace-http-request-in-apache/ [Accessed 30 Jan. 2020].