ISEC2700 – Introduction to Information Security Practices

Assignment #2

Pod #5\_6

September 24rd, 2024

Table of Contents

[Introduction 2](#_Toc157673648)

[Section #1 3](#_Toc157673649)

[Section #2 3](#_Toc157673650)

[Bibliography 4](#_Toc157673651)

# Introduction

In this Assignment we will research ways to harden a server, and then install a harden an Apache Webserver.

## Section #1

* This section will include the change log and testing plan for the Apache Web Server

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Install Log** | | | | | |
| **Project:** Ubuntu Web Server | | | | | **Date:** 09/24/24 |
| **Activity ID No.** | **Activity Name** | **Description of Work** | | | **Responsibility** |
| A001 | Documentation required for install and configuration. | [Ubuntu CLI Cheatsheet](https://ubuntu.com/download/server/thank-you?version=24.04.1&architecture=amd64&lts=true)  Naming Convention Document v1.3.24  ISEC2700\_Assign 2 v9.17.24 | | |  |
| A002 | Resources required for install. | Ubuntu Server 24.04.1 LTS  (ubuntu-24.04.1-live-server-amd64.iso) | | |  |
| A003 | Documentation of object names required for implementation. | **Specify object names in preparation for implementation** | | |  |
| **VM** Folder: | E:\2024 Semester 3\ISEC2700\ISEC2700-WB01 | |
| **VM** Name: | ISEC2700-WS01 | |
| **VM** OS (selected during VM build): | Ubuntu Server | |
| **System** Hardware Configuration: | Primary HD | 60GB |
| Additional HDs |  |
| RAM | 4GB |
| Processors/Cores | 2 / 1 |
| Network | IP Address (Static/DHCP) | DHCP  (192.168.208.132) |
| Subnet Mask |  |
| G/W Address |  |
| DNS Server Addresses (2) | *Primary*  *Secondary* |
| Installation Mode | New Installation | |
| Time Zone: | AST | |
| Server Type | Web Server | |
| **Server** “Administrator” Password: | Sysop\_pod5  Passw0rd | |
| **Server** Host Name: | WS01C1U30 | |
| Domain Name: | isec2700.pod5.ca | |
| **Additional** User: | Only if required. | |
| Additional User Password: | Only if required. | |
| DSRM Password: | Only if required. | |
|  | | |
| *Name and description of each snapshot to be taken during install.*  *Create a schedule of regular rollback points of the server and take regular snapshots of your server in shutdown state.* |  | |
| A004 | Required configurations or settings applied during initial install. | Accept all defaults during installation, except to enable DHCP. Do not proceed without a network. | | |  |
| A005 | “Backup” information: Regular rollback points, snapshots, etc. | Snapshots to be taken before and after each assignment following the “PostA1”, “PreA1” naming conventions. | | |  |
| A006 | “Gold” Copy information: Rollback or restore options for the system. | Backups located at E:\2024 Semester 3\ISEC2700\GoldCopies | | |  |
| A007 | Install OpenSSH Server | Do not add any additional snap-ins, do not import an SSH identity, leave as default. | | |  |
| A008 | Update Time Zone | Use command “timedatectl1” to set time zone to Halifax (AST) | | |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Change No.** | **Change Type** | **Description of Change** | **Date Completed** | **Status** | **Comments / Troubleshooting notes** |
| CR001 | Timezone Configuration | “timedatectl set-timezone “America/Halifax” | 09/24/24 | Completed | Confirmed via standalone “timedatectl” command, showing Halifax. |
| CR002 | IP Configuration | “ip addr show && ip route show” | 09/24/24 | Completed | A computer screen with white text  Description automatically generated |
| CR003 | Apache Daemon Installation | Installed Web Server via “tasksel” | 09/24/24 | Completed | “sudo apt install tasksel”  “sudo tasksel”  Selected Web Server from list, installed |
| CR004 | PHP Installation | “sudo apt install php php-cli”  “sudo apt install libapache2-mod-php”  “sudo systemctl restart apache2” | 09/24/24 | Completed | Installs both PHP, PHP Command Line and PHP libraries, followed by a restart of the Apache service. |
| CR005 | Enable SSH | “sudo systemctl status ssh” | 09/24/24 | Complete | SSH is usually enabled and active by default, if it is not (dead), enable it with this command. |
| CR006 | Server Hardening | Added lines to /etc/apache2/apache2.conf | 09/24/24 | Complete | Added:  “TraceEnable off  ServerTokens Prod  ServerSignature Off  <IfModule mod\_headers.c> (underscore between mod and headers)  Header unset Server  Header unset X-powered-By  </IfModule> |
| CR007 | Added User and Group | Created group “apachegroup” with user “apacheuser” | 09/24/24 | Complete | Added said group and user to /etc/apache2/envvars under “APACHE\_RUN\_USER” and “…GROUP” respectively. |
| CR008 | Users Added, SSH Permissions Modified | Added user “test” and “remotetest”, edited /etc/ssh/ssh\_config permissions | 09/24/24 | Complete | Added default user (sysop\_pod5) and “remoteuser” to AllowUsers line,  Added “test” user to DenyUsers line  (both new users passwords are “student@2024”) |

**Testing Plan**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Project (Activity) for testing:** | | Ubuntu Web Server | | |  |  |  |
| **Date:** |  | 09/24/24 | |  |  |  |  |
|  |  |  |  |  |  |  |  |
| **Test ID** | **Description** | **Action** | **Expected result** | **Tech** | **Status** | **Repeat test** | **Notes:** |
| A001 | Test Apache Installation | Enter “apachectl -v” | The correct version of Apache should be displayed | KW | Complete | 1 | Current Version Installed |
| A002 | Test Network Connectivity | Ping “8.8.8.8” | All pings should return | KW | Complete | 1 | Network connectivity established |
| A003 | Confirm server configuration | Use command “hostname” and command “ip” | Hostname should match documentation as well as network settings | KW | Complete | 1 | System configured as per install log |

## Section #2

* This section will include the Security Plan for the Apache Web Server

Section #1 – Firewall Settings

* For configuring settings for the Firewall
* Change default password and username

**Command: sudo passwd <username>**

* Allow of necessary ports required for our application

**Command: sudo ufw allow 80/tcp**

**sudo ufw allow 22/tcp**

**sudo ufw enable**

Section #2 – Server Hardening

* For Ubuntu Sever Hardening Configuration
* Secure SSH Access

**Command: sudo nano /etc/ssh/sshd­\_config**

**PermitRootLogin no**

**PasswordAuthentication no**

**sudo systemctl restart sshd**

* Install fail2ban

**(it's a good idea to do update first to get newest version. Better safe than sorry.)**

**Command: sudo apt update**

**sudo apt install fail2ban**

**sudo cp /etc/fail2ban/jail.conf /etc/fail2ban/jail.local**

**sudo systemctl start fail2ban**

**sudo systemctl enable fail2ban**

Section #3 – System Access

* For System Access Security Configuration
* Account Permissions (Admin Password)

**Command: sudo nano /etc/security/pwquality.conf**

* Disable Remote Access to the Root Admin Account

**Command: sudo nano /etc/ssh/sshd\_config**

**PermitRootLogin no**

**sudo systemctl restart sshd**

Section #4 – HTTP or TCP/IP Hardening

* For HTTP or TCP/IP Hardening Configuration
* Disabling IPv6

**Command: sudo sysctl -w net.ipv6.conf.all.disable\_ipv6=1**

**sudo sysctl -w net.ipv6.conf.default.disable\_ipv6=1**

* Enabling IP spoofing protection

**Command: sudo sysctl -w net.ipv4.conf.all.rp\_filter=1**

**sudo sysctl -w net.ipv4.conf.default.rp\_filter=1**

Section #5 – Logging or Auditing

* For Logging or Auditing
* Enable Log Rotation

**Command: sudo nano /etc/logrotate.conf**

**(edit items in there such as a weekly or monthly rotation, rotate a certain number of archived files, etc...)**

* Enable utmpdump for detecting Log Tampering

**Command:** **sudo apt instasll sysvinit-utils**

**(To read the logs, use: sudo utmpdump /var/log/wtmp)**

## Section #3

* This section will include the screenshot of the gold copy properties created for the Apache Web Server.

A screenshot of a computer

Description automatically generated

# Bibliography

* Securinc TeamSecurinc is a leading cybersecurity consulting firm dedicated to helping businesses navigate the complex world of information security. Since our inception, & Team, S. (2023, October 7). 10 tips for hardening your firewalls. Securinc. <https://www.securinc.io/blog/tips-for-hardening-your-firewalls/>
* KL, A. (2024, September 4). Ubuntu server security: Top hardening tips. TheSecMaster. <https://thesecmaster.com/blog/the-ultimate-guide-to-harden-the-ubuntu-server-linux-server-hardening>
* Boelen, M. (2024, June 18). Ubuntu system hardening guide for desktops and servers. Linux Audit. <https://linux-audit.com/ubuntu-server-hardening-guide-quick-and-secure/#accounts>
* How to view and configure linux system logs on ubuntu 20.04. Better Stack Community. (n.d.). <https://betterstack.com/community/guides/logging/how-to-view-and-configure-linux-logs-on-ubuntu-20-04/>
* Using linux utmpdump for forensics and detecting log file tampering. Sandfly Security - Agentless Linux EDR and Incident Response. (2022, October 6). <https://sandflysecurity.com/blog/using-linux-utmpdump-for-forensics-and-detecting-log-file-tampering/>
* How to protect SSH with fail2ban on ubuntu 20.04. DigitalOcean. (n.d.). <https://www.digitalocean.com/community/tutorials/how-to-protect-ssh-with-fail2ban-on-ubuntu-20-04>
* Ltd, F. (n.d.). Ubuntu - Enable & Secure SSH server (18.04, 20.04, 21.04 & 22.04). <https://farbyte.uk/blog/ubuntu-enable-secure-ssh-server>

## Work Journals

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Work Journals: Assignment 2 |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
| **Name** = Riley |  |  |  |  |  |  |  |  |  |  |  |
| **Role** = Researcher/Author |  |  |  |  |  |  |  |  |  |  |  |
| **Work Details:** |  |  |  |  |  |  |  |  |  |  |  |
| Monday Sept 24 | |  |  |  |  |  |  |  |  |  |  |
| 2 hours researching security plan  2 hours compiling security plan, applying CLI commands  1 hour editing document, spell checking, bibliography | | | | |  |  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Work Journals: Assignment 2 |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
| **Name** = Jacob Collett |  |  |  |  |  |  |  |  |  |  |  |
| **Role** = Researcher/Author |  |  |  |  |  |  |  |  |  |  |  |
| **Work Details:** |  |  |  |  |  |  |  |  |  |  |  |
| Monday Sept 24 | |  |  |  |  |  |  |  |  |  |  |
| 2 hours researching security plan  2 hours applying security plan to VM | | | | |  |  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Work Journals: Assignment 2 |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
| **Name** = Kyle Walker |  |  |  |  |  |  |  |  |  |  |  |
| **Role** = Researcher/Author/TL |  |  |  |  |  |  |  |  |  |  |  |
| **Work Details:** |  |  |  |  |  |  |  |  |  |  |  |
| Monday Sept 24 | |  |  |  |  |  |  |  |  |  |  |
| 6 hours writing install plan, change log, testing plan and creating VM | | | | |  |  |  |  |  |  |  |

## Rubric Entries

**Jacob:**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ***Category*** | ***% of Mark*** | **4** | **3** | **2** | **1** | **0** |
| **Attendance** | **30%** | Student attends all team meetings as well as classes (100%). As well as submitting a work journal of homework/work whenever done. | Student attends most team meetings and most classes (75%). As well as submitting work journal 75% of the time whenever homework/work was completed. | Student sometimes attends team meetings and classes (50%). As well as submitting work journal 50% of the time whenever  homework/work was completed. | Student rarely attends team meetings and classes (25%). As well as submitting work journal 25% of the time whenever homework/work was completed. | Student does not attend team meetings or classes. As well as not submitting work journal. |
| **Communication** | **20%** | Student can always be contacted and replies in a timely manner. Can communicate with others in a respectful manner all the time. Team consensus averaged 4 for communication | Student can most of the time be contacted and replies in a timely manner most of the time. Can communicate with others in a respectful manner most of the time. Team consensus averaged 3 for communication | Student sometimes be contacted and replies in a timely manner sometimes. Can sometime communicates with others in a respectful manner. Team consensus averaged 2 for communication | Student rarely replies in a timely manner and is hard to contact most of the time. Cannot communicate with others in a respectful manner most of the time. Team consensus averaged 1 for communication | Student cannot be contacted and expected to reply in a timely manner. Student cannot communicate in a respectful manner. Team consensus averaged 0 for communication |
| **Quality of Submitted Work** | **20%** | Student submits quality work that meets expectations every time asked.  When compared to assignment rubric, team consensus determines quality is excellent (100%-80%). Comment on Dropbox from each member will score out of 10 | Student submits quality work that meets expectations most of the time. When compared to assignment rubric, team consensus determines quality is acceptable (80%-70%) Comment on Dropbox from each member will score out of 10. | Student submits mediocre work, that sometimes meets expectations. When compared to assignment rubric, team consensus determines quality is mediocre (70% -50%). Comment on Dropbox from each member will score out of 10. | Student submits mediocre work most of the time, and the work rarely meets expectations. When compared to assignment rubric, team consensus determines quality is poor (>50%). Comment on Dropbox from each member will score out of 10. | Student does not submit quality work or any work at all, anything submitted rarely or never meets expectations. When compared to assignment rubric, team consensus determines quality is very poor and is not worth submitting. Comment on Dropbox will score out of 10. |
| **Deadlines** | **30%** | Student completes work before all deadlines. | Student completes all work by the **24-hour** team deadline. | Student completes all work by 12 hours post **24-hour** team deadline (12 hours remaining on Brightspace due date) | Student completes all work by 18-hour post **24-hour** team deadline (6 hours remaining on Brightspace due date) | Student does not complete work before Brightspace due date. Work is not accepted after 1 hour until Brightspace due date. |

**Score: 20/20 – 100%**

**Kyle:**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ***Category*** | ***% of Mark*** | **4** | **3** | **2** | **1** | **0** |
| **Attendance** | **30%** | Student attends all team meetings as well as classes (100%). As well as submitting a work journal of homework/work whenever done. | Student attends most team meetings and most classes (75%). As well as submitting work journal 75% of the time whenever homework/work was completed. | Student sometimes attends team meetings and classes (50%). As well as submitting work journal 50% of the time whenever  homework/work was completed. | Student rarely attends team meetings and classes (25%). As well as submitting work journal 25% of the time whenever homework/work was completed. | Student does not attend team meetings or classes. As well as not submitting work journal. |
| **Communication** | **20%** | Student can always be contacted and replies in a timely manner. Can communicate with others in a respectful manner all the time. Team consensus averaged 4 for communication | Student can most of the time be contacted and replies in a timely manner most of the time. Can communicate with others in a respectful manner most of the time. Team consensus averaged 3 for communication | Student sometimes be contacted and replies in a timely manner sometimes. Can sometime communicates with others in a respectful manner. Team consensus averaged 2 for communication | Student rarely replies in a timely manner and is hard to contact most of the time. Cannot communicate with others in a respectful manner most of the time. Team consensus averaged 1 for communication | Student cannot be contacted and expected to reply in a timely manner. Student cannot communicate in a respectful manner. Team consensus averaged 0 for communication |
| **Quality of Submitted Work** | **20%** | Student submits quality work that meets expectations every time asked.  When compared to assignment rubric, team consensus determines quality is excellent (100%-80%). Comment on Dropbox from each member will score out of 10 | Student submits quality work that meets expectations most of the time. When compared to assignment rubric, team consensus determines quality is acceptable (80%-70%) Comment on Dropbox from each member will score out of 10. | Student submits mediocre work, that sometimes meets expectations. When compared to assignment rubric, team consensus determines quality is mediocre (70% -50%). Comment on Dropbox from each member will score out of 10. | Student submits mediocre work most of the time, and the work rarely meets expectations. When compared to assignment rubric, team consensus determines quality is poor (>50%). Comment on Dropbox from each member will score out of 10. | Student does not submit quality work or any work at all, anything submitted rarely or never meets expectations. When compared to assignment rubric, team consensus determines quality is very poor and is not worth submitting. Comment on Dropbox will score out of 10. |
| **Deadlines** | **30%** | Student completes work before all deadlines. | Student completes all work by the **24-hour** team deadline. | Student completes all work by 12 hours post **24-hour** team deadline (12 hours remaining on Brightspace due date) | Student completes all work by 18-hour post **24-hour** team deadline (6 hours remaining on Brightspace due date) | Student does not complete work before Brightspace due date. Work is not accepted after 1 hour until Brightspace due date. |

**Score: 18/20 – 90%**

**Riley:**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ***Category*** | ***% of Mark*** | **4** | **3** | **2** | **1** | **0** |
| **Attendance** | **30%** | Student attends all team meetings as well as classes (100%). As well as submitting a work journal of homework/work whenever done. | Student attends most team meetings and most classes (75%). As well as submitting work journal 75% of the time whenever homework/work was completed. | Student sometimes attends team meetings and classes (50%). As well as submitting work journal 50% of the time whenever  homework/work was completed. | Student rarely attends team meetings and classes (25%). As well as submitting work journal 25% of the time whenever homework/work was completed. | Student does not attend team meetings or classes. As well as not submitting work journal. |
| **Communication** | **20%** | Student can always be contacted and replies in a timely manner. Can communicate with others in a respectful manner all the time. Team consensus averaged 4 for communication | Student can most of the time be contacted and replies in a timely manner most of the time. Can communicate with others in a respectful manner most of the time. Team consensus averaged 3 for communication | Student sometimes be contacted and replies in a timely manner sometimes. Can sometime communicates with others in a respectful manner. Team consensus averaged 2 for communication | Student rarely replies in a timely manner and is hard to contact most of the time. Cannot communicate with others in a respectful manner most of the time. Team consensus averaged 1 for communication | Student cannot be contacted and expected to reply in a timely manner. Student cannot communicate in a respectful manner. Team consensus averaged 0 for communication |
| **Quality of Submitted Work** | **20%** | Student submits quality work that meets expectations every time asked.  When compared to assignment rubric, team consensus determines quality is excellent (100%-80%). Comment on Dropbox from each member will score out of 10 | Student submits quality work that meets expectations most of the time. When compared to assignment rubric, team consensus determines quality is acceptable (80%-70%) Comment on Dropbox from each member will score out of 10. | Student submits mediocre work, that sometimes meets expectations. When compared to assignment rubric, team consensus determines quality is mediocre (70% -50%). Comment on Dropbox from each member will score out of 10. | Student submits mediocre work most of the time, and the work rarely meets expectations. When compared to assignment rubric, team consensus determines quality is poor (>50%). Comment on Dropbox from each member will score out of 10. | Student does not submit quality work or any work at all, anything submitted rarely or never meets expectations. When compared to assignment rubric, team consensus determines quality is very poor and is not worth submitting. Comment on Dropbox will score out of 10. |
| **Deadlines** | **30%** | Student completes work before all deadlines. | Student completes all work by the **24-hour** team deadline. | Student completes all work by 12 hours post **24-hour** team deadline (12 hours remaining on Brightspace due date) | Student completes all work by 18-hour post **24-hour** team deadline (6 hours remaining on Brightspace due date) | Student does not complete work before Brightspace due date. Work is not accepted after 1 hour until Brightspace due date. |

Score: 20/20 – 100%

**Shash:**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ***Category*** | ***% of Mark*** | **4** | **3** | **2** | **1** | **0** |
| **Attendance** | **30%** | Student attends all team meetings as well as classes (100%). As well as submitting a work journal of homework/work whenever done. | Student attends most team meetings and most classes (75%). As well as submitting work journal 75% of the time whenever homework/work was completed. | Student sometimes attends team meetings and classes (50%). As well as submitting work journal 50% of the time whenever  homework/work was completed. | Student rarely attends team meetings and classes (25%). As well as submitting work journal 25% of the time whenever homework/work was completed. | Student does not attend team meetings or classes. As well as not submitting work journal. |
| **Communication** | **20%** | Student can always be contacted and replies in a timely manner. Can communicate with others in a respectful manner all the time. Team consensus averaged 4 for communication | Student can most of the time be contacted and replies in a timely manner most of the time. Can communicate with others in a respectful manner most of the time. Team consensus averaged 3 for communication | Student sometimes be contacted and replies in a timely manner sometimes. Can sometime communicates with others in a respectful manner. Team consensus averaged 2 for communication | Student rarely replies in a timely manner and is hard to contact most of the time. Cannot communicate with others in a respectful manner most of the time. Team consensus averaged 1 for communication | Student cannot be contacted and expected to reply in a timely manner. Student cannot communicate in a respectful manner. Team consensus averaged 0 for communication |
| **Quality of Submitted Work** | **20%** | Student submits quality work that meets expectations every time asked.  When compared to assignment rubric, team consensus determines quality is excellent (100%-80%). Comment on Dropbox from each member will score out of 10 | Student submits quality work that meets expectations most of the time. When compared to assignment rubric, team consensus determines quality is acceptable (80%-70%) Comment on Dropbox from each member will score out of 10. | Student submits mediocre work, that sometimes meets expectations. When compared to assignment rubric, team consensus determines quality is mediocre (70% -50%). Comment on Dropbox from each member will score out of 10. | Student submits mediocre work most of the time, and the work rarely meets expectations. When compared to assignment rubric, team consensus determines quality is poor (>50%). Comment on Dropbox from each member will score out of 10. | Student does not submit quality work or any work at all, anything submitted rarely or never meets expectations. When compared to assignment rubric, team consensus determines quality is very poor and is not worth submitting. Comment on Dropbox will score out of 10. |
| **Deadlines** | **30%** | Student completes work before all deadlines. | Student completes all work by the **24-hour** team deadline. | Student completes all work by 12 hours post **24-hour** team deadline (12 hours remaining on Brightspace due date) | Student completes all work by 18-hour post **24-hour** team deadline (6 hours remaining on Brightspace due date) | Student does not complete work before Brightspace due date. Work is not accepted after 1 hour until Brightspace due date. |

Score: 2/20 – 10%