

**KING’S OWN INSTITUTE\***

**Success in Higher Education**

# 

# INDIVIDUAL ASSIGNMENT COVERSHEET

Family Name: AUSTRIA Given Name: JOHN BENNY

Student Number: 12301175 Lecturer’s Name: DR. PRABHU JYOT SINGH

Subject Name: ICT740 Applied Cybersecurity

Assignment Title: Assessment 3: Countermeasures

**Declaration**

(This declaration must be completed by the student or the assignment will not be marked.)

I certify the following:

* I have read and understood the *Student Academic Misconduct Policy*
* This assignment is my own work based on my personal study and or research.
* I have acknowledged all material and sources used in the preparation of this assignment including any material generated in the course of my employment.
* The assignment has not previously been submitted for assessment.
* I have not copied in part or in whole or otherwise plagiarised the work of other students.
* I have read and I understand the criteria used for assessment.
* The assignment is within the word and page limits specified in the unit outline.
* The use of any material in this assignment does not infringe the intellectual property / copyright of a third party.
* I understand that this assignment may undergo electronic detection for plagiarism, and an anonymous copy of the assignment may be retained on the database and used to make comparisons with other assignments in future.
* By completing this coversheet in full and submitting this assignment electronically, I am bound by the conditions of the KOI’s *Student Academic Misconduct Policy* and the declaration on this coversheet.

J\_AUST

22 / 09 / 2024

Signature Date

----------------------------------------------------------------------------

**Assignment Receipt**

Family Name: AUSTRIA Student Number: 12301175

Given Name:(s) JOHN BENNY

Lecturer’s Name: DR. PRABHU JYOT SINGH

Subject Name: ICT740 Applied Cybersecurity

Assignment Title: Assessment 3: Countermeasures

J\_AUST

22 / 09 / 2024

Signature Date

INDIVIDUAL ASSIGNMENT COVER SHEET \* AUSTRALIAN INSTITUTE OF BUSINESS AND MANAGEMENT PTY LTD PAGE **1** OF **1**

1. JULY 2015 CRICOS 03171A ABN: 72 132 629

# TABLE OF CONTENTS

[INDIVIDUAL ASSIGNMENT COVERSHEET 1](#_Toc177906661)

[TABLE OF CONTENTS 2](#_Toc177906662)

[1.0. INTRODUCTION 3](#_Toc177906663)

[2.0. COUNTERMEASURES 4](#_Toc177906664)

[2.1. Ubuntu Firewall 5](#_Toc177906665)

[2.2. Secure Apache Web Server 7](#_Toc177906666)

[2.3. Hide Web Server Version and OS Information 8](#_Toc177906667)

[2.4. Enabling SSL 9](#_Toc177906668)

[2.5. Protect from DDOS 11](#_Toc177906669)

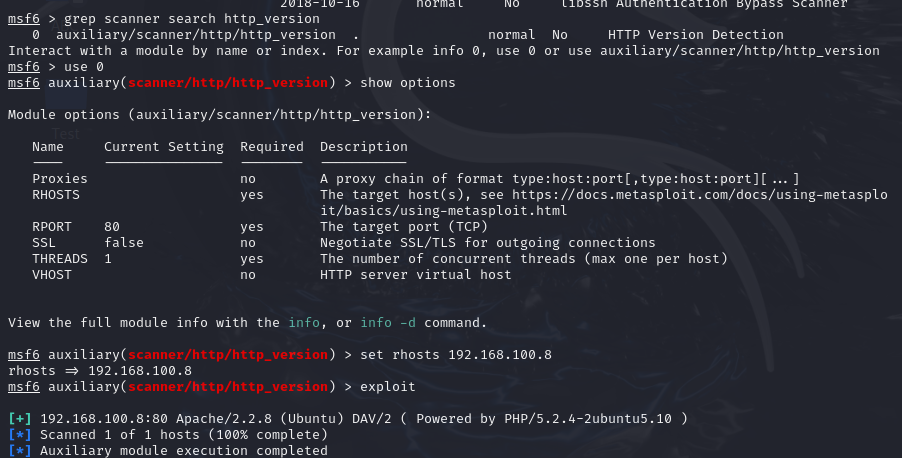
[3.0. CONCLUSIVE REMARKS 14](#_Toc177906670)

[4.0. REFERENCES 15](#_Toc177906671)

# INTRODUCTION

Quality of Service is one of the most important applications in the field of network traffic. Despite network traffic being improved every day, current approaches on each port number are unreliable. Port 80 as defined by Rouse (2023) is assigned to Hypertext Transfer Protocol (HTTP) that is utilized to send and receive data from unencrypted web pages.

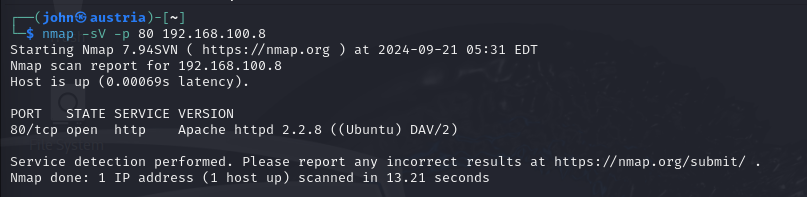
This assessment will focus on the vulnerability of Port 80 defined in Assessment 2. I used Metasploit Framework to exploit the data of Metasploitable2 in port 80. Through Metasploit, I have retrieved the Apache version of port 80 which is 2.2.8 and the version of PHP which is 5.2.4-2ubuntu5.10.



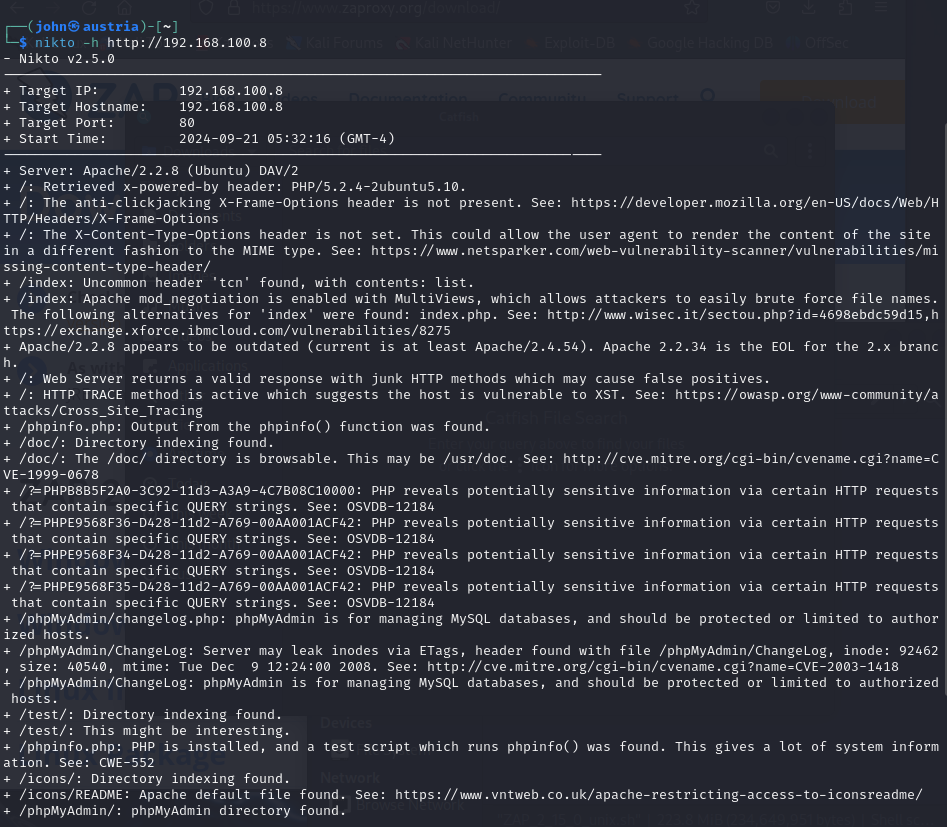
This paper will look at five countermeasures to tackle the vulnerabilities of port 80. The IP address of Metasploitable2 will be scanned by Nmap and Nikto to show the current status of Metasploitable2. Then, five countermeasures are installed and deployed in Metasploitable2 to harden the system of port 80. Finally, a conclusive remark to summarise the activities performed in Metasploitable2.

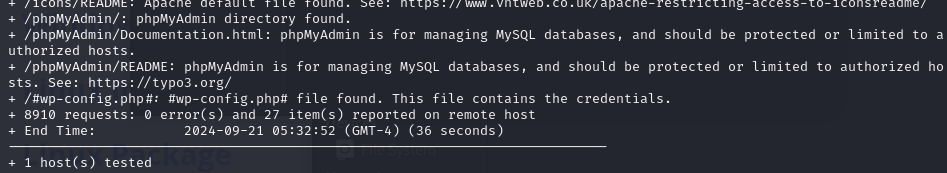
# COUNTERMEASURES

Before I started doing the countermeasure, I had to make sure that port 80 of Metasploitable2 is working. I entered ‘nmap -sV -p 80 192.168.100.8’. It showed that the host is up for the port 80. It also mentioned that port 80 is running in the service of http and in the version of apache httpd 2.2.8.



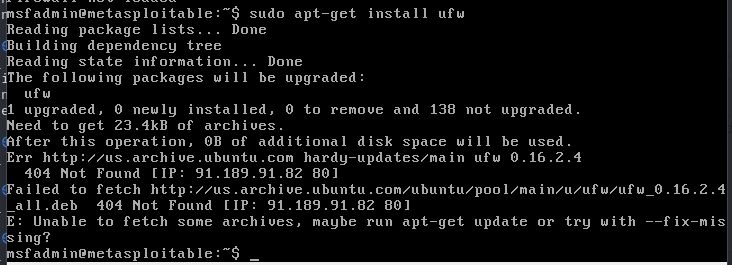
To fully scan the port 80 of Metasploitable2, I have used Nikto to display its current vulnerabilities. The scan from Nikto proved that port 80 has a lot of vulnerabilities shown.





## Ubuntu Firewall

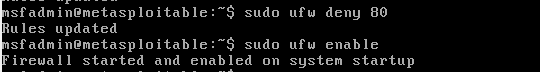
To address the vulnerabilities of port 80 in Metasploitable2, the first countermeasure is to install ubuntu firewall in the system. By typing ‘sudo apt-get install ufw’ in the prompt bar then pressing enter, Ubuntu Firewall is installed in a flash. Ubuntu Server (2024) states that “The default firewall configuration tool for Ubuntu is ufw.”



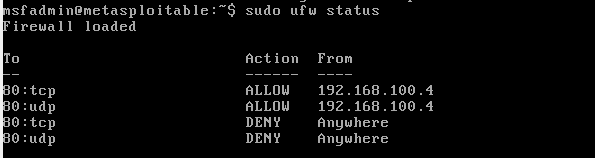
After ubuntu firewall has been installed, I only allowed my Kali Linux to have access to port 80 in Metasploitable 2. 192.168.100.4 is the IP address for my Kali Linux. To do this, I have prompt ‘sudo ufw allow from 192.168.100.4 to any port 80’ in the prompt bar. The rules of the firewall has been updated after I allowed my Kali Linux to be the only one to have access.



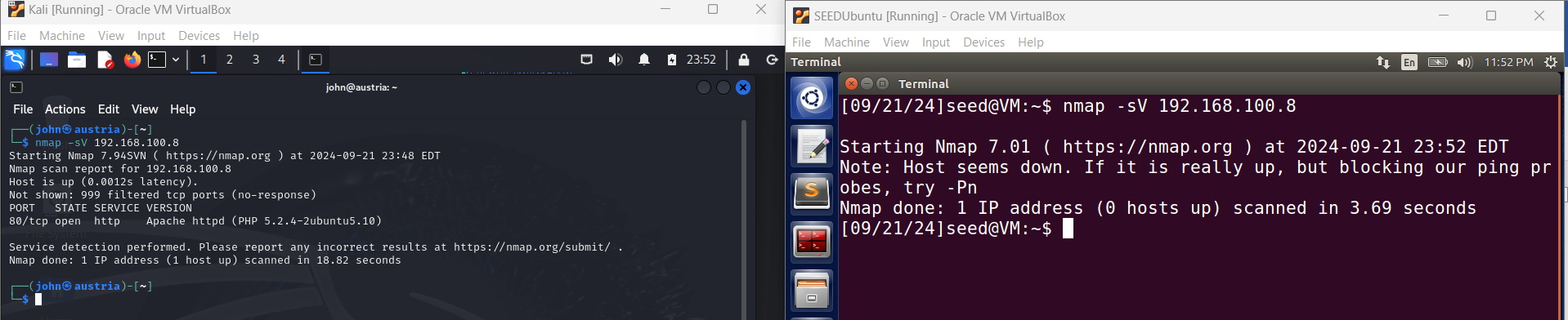
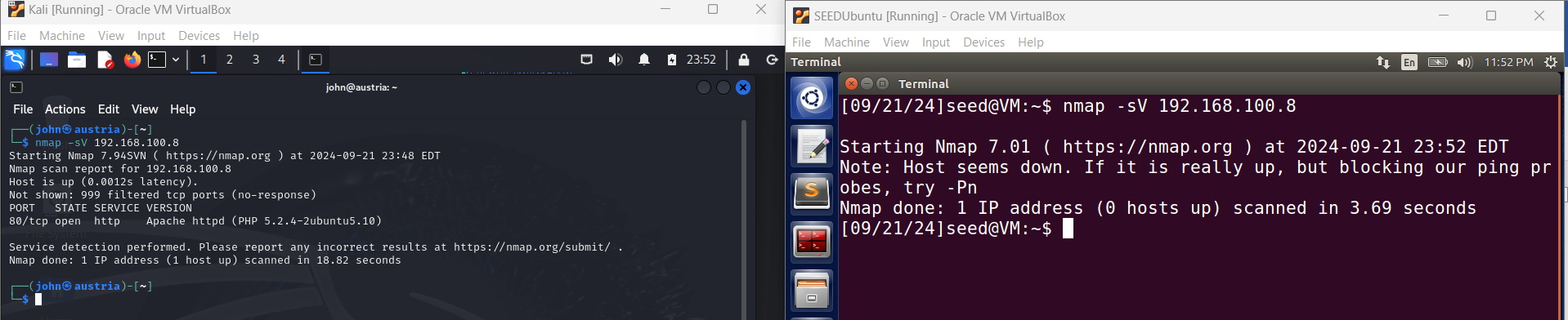
I need to make sure that my Kali Linux will be the only one to have access to port 80 of metasploitable2 by denying entry to other addresses. I entered ‘sudo ufw deny 80’ in the prompt bar to deny everyone else except for my Kali Linux. Shortly, I prompted ‘sudo ufw enable’ to make sure that the firewall has started and is enabled on the system startup.



To show the status of ubuntu firewall, I entered ‘sudo ufw status’ in the prompt bar, and it shows the latest status of firewall in which 192.168.100.4 is the only IP address that can access port 80 and the other addresses are denied.



Here are comparisons of nmap between Kali Linux and Seed Ubuntu. We could see that Kali Linux is able to access the port 80 of Metasploitable2 while Seed Ubuntu cannot access Metasploitable2.

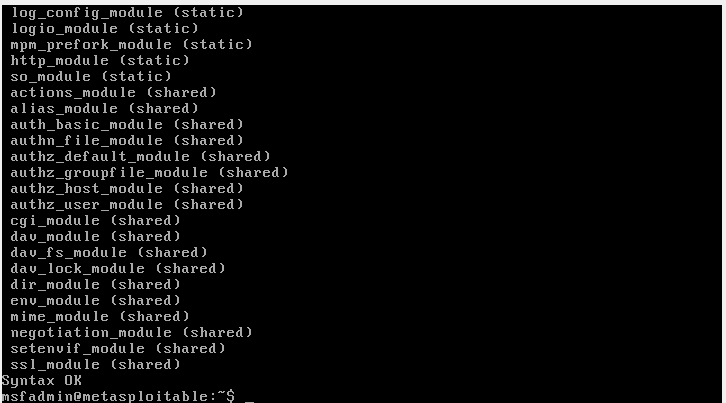


## Secure Apache Web Server

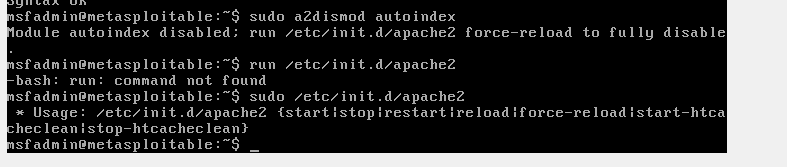
Apache is a software based on web server that has the main task of accepting HTTP requests from visitors and responding back with the requested information (Giaquinto, 2022). Securing Apache Web Server of Metasploitable2 can be done by disabling some modules of Apache. Entering ‘sudo apache2ctl -M’ in the prompt bar of Metasploitable2 will give us a glimpse of the enabled modules in the Apache.

****

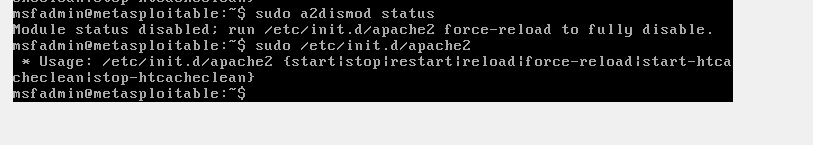
From the photo below, it shows that we have a lot of modules enabled in the system. We are going to disable the autoindex and status module in this process. Disabling autoindex will prevent any unauthorized person from viewing the directory listing and discovering the sensitive files of the system. In complementary, disabling status module will prevent the hackers from having knowledge regarding the performance of the server and its current activity.

****

To disable autoindex, I have typed ‘sudo a2dismod autoindex’ in the prompt bar. The terminal then instruct me to run ‘sudo etc/init.d/apache2’ to disable autoindex. After I run the command, autoindex is fully disabled.

****

Disabling status module is the same with disabling autoindex. I just entered ‘sudo a2dismod status’ in the prompt bar and run the command ‘sudo /etc/init.d/apache2’, then status module is already disabled.

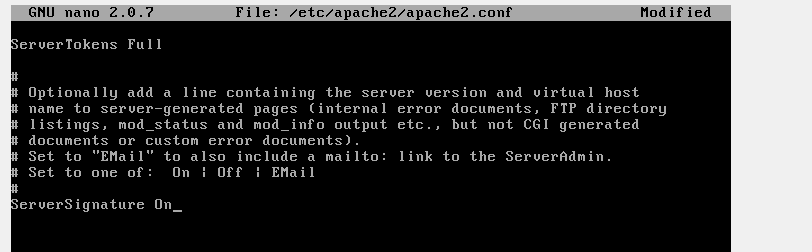
****

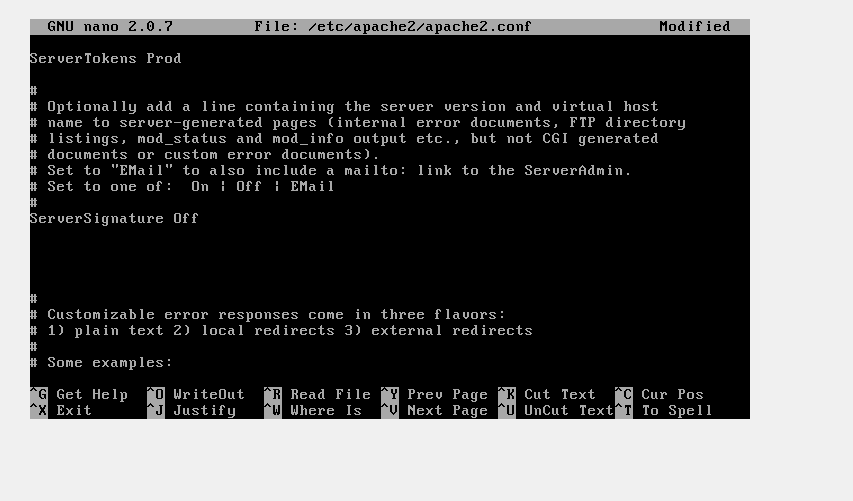
## Hide Web Server Version and OS Information

In this countermeasure, I’m going to hid the web server version and OS Information to any potential hackers. Hiding this valuable information is done by accessing the apache file. I entered sudo nano /etc/apache/apache2.conf’ then typed my password to gain access to the file.



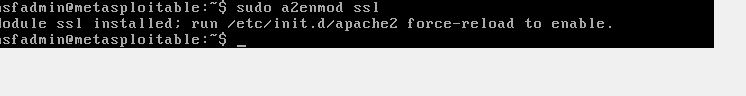
After gaining access to the file, I noticed that the ServerTokens is currently at “Full” status. I have modified the ‘Full’ status to ‘Prod’ status to limit the information of apache provides to the server. At the same time, ServerSignature is currently ‘On’, turning this ‘Off’ will make the Apache display error messages rather than providing the details of the server version.

****

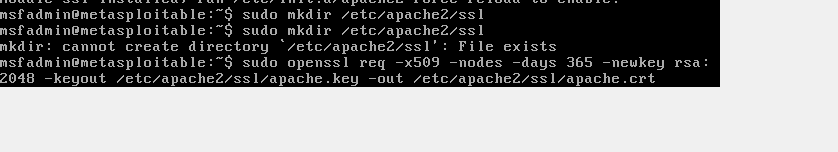
****

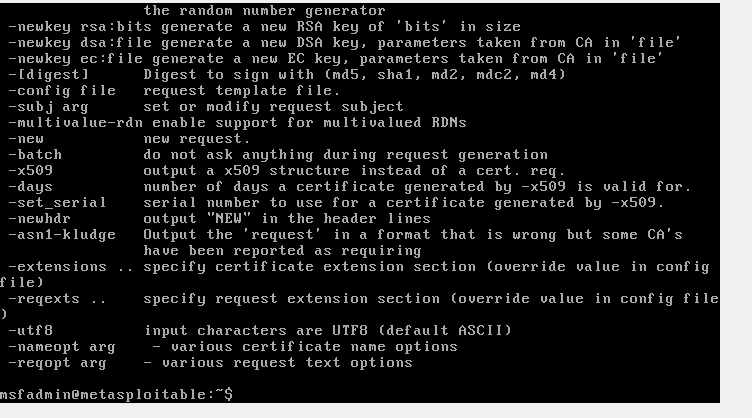
## Enabling SSL

The next countermeasure is to enable Secure Sockets Layer (SSL) in Metaspoitable2. SSL is a digital certificate that establishes a connection which is encrypted between a browser and a server (Digicert, 2023). To enable SSL, we must install the module of ssl, entering ‘sudo a2endmod ssl’ in the prompt bar will install the module.

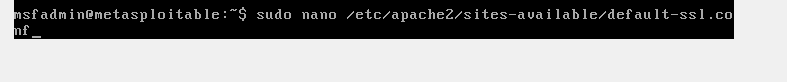
****

After SSL has been installed, I must go to the directory of ssl through ‘sudo mkdir /etc/apache2/ssl’, then I will generate a SSL certificate by ‘sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/apache2/ssl/apache.key -out /etc/apache2/ssl/apache.crt’

****

****

Then, I need to configure the apache for SSL. Prompting ‘sudo nano /etc/apache2/sites-available/default-ssl.conf’ will help me open the file for ssl in the apache.

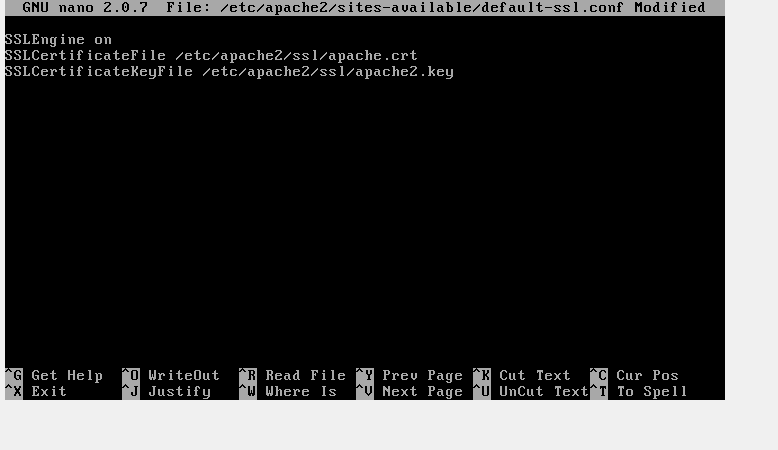
****

I have included the following commands to make the SSL compatible with Apache:

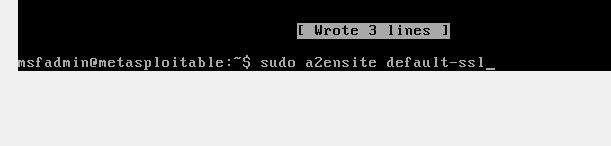
SSLEngine on

SSLCertificateFile /etc/apache2/ssl/apache.crt

SSLCertificateKeyFile /etc/apache2/ssl/apache.key

****

After the configuration, it is time to start the SSL virtual host. To start the virtual host, I entered ‘sudo a2ensite default-ssl’ in the prompt bar.

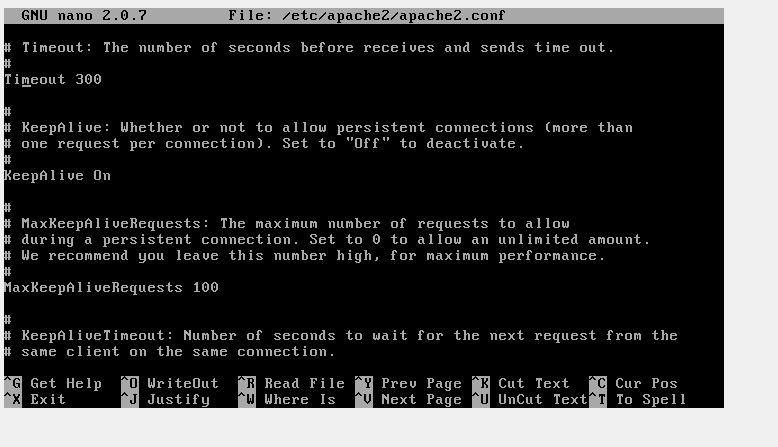
****

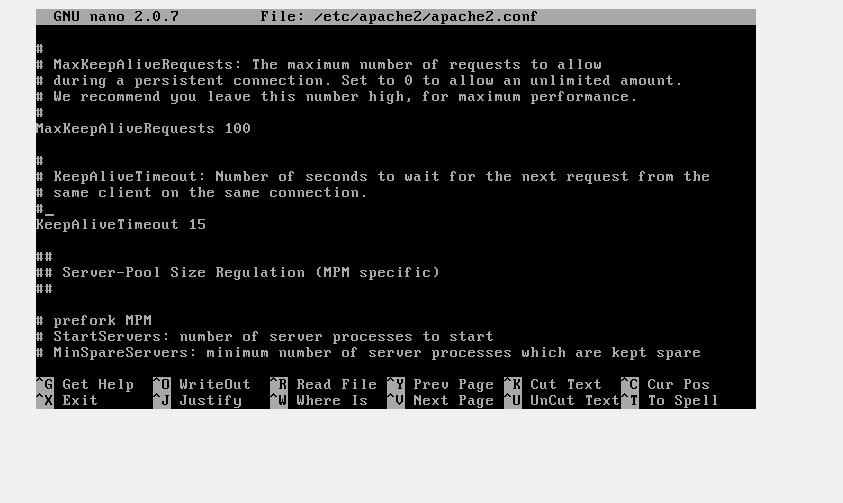
## Protect from DDOS

The last countermeasure for port 80 exploitation is to protect the port from Distributed Denial of Service (DDOS). The process is almost the same with hiding the web browser and OS Information. I just entered ‘sudo nano /etc/apache/apache2.conf’ to have access to the apache file.

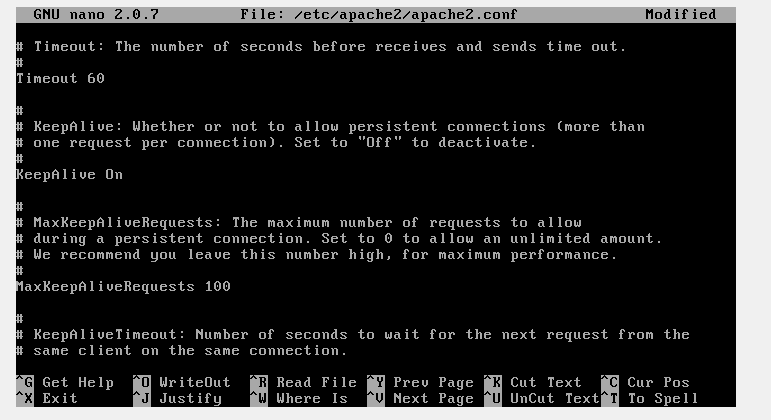


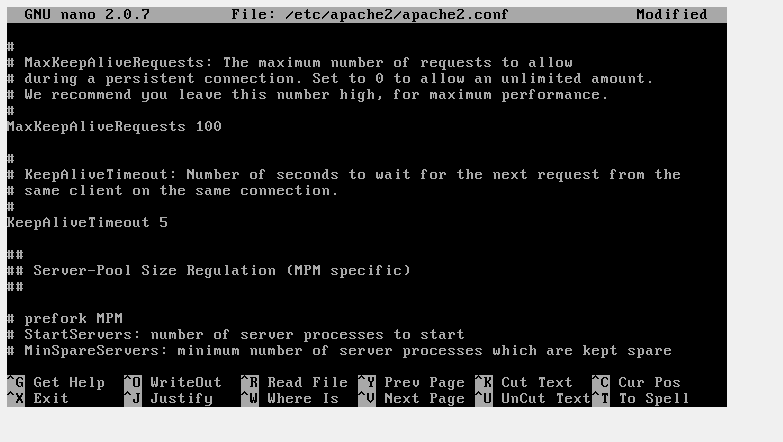
After gaining access, I am going to modify Timeout, KeepAlive MaxKeepAliveRequests, and KeepAliveTimeout. The timeout is normally at 300, KeepAlive is turned on, MaxKeepAliveRequests at 1000 and KeepAliveTimeout is at 15.



****

I’m going to leave the KeepAlive and MaxKeepAliveRequests as they are and I’m just going to modify the Timeout and KeepAliveTimeout. I set the value of 60 for Timeout and KeepAliveTimeout for 5. Doing this will mitigate any type of slow-request attacks such as Slowloris and will prevent any hackers from holding open connections for long periods of time.



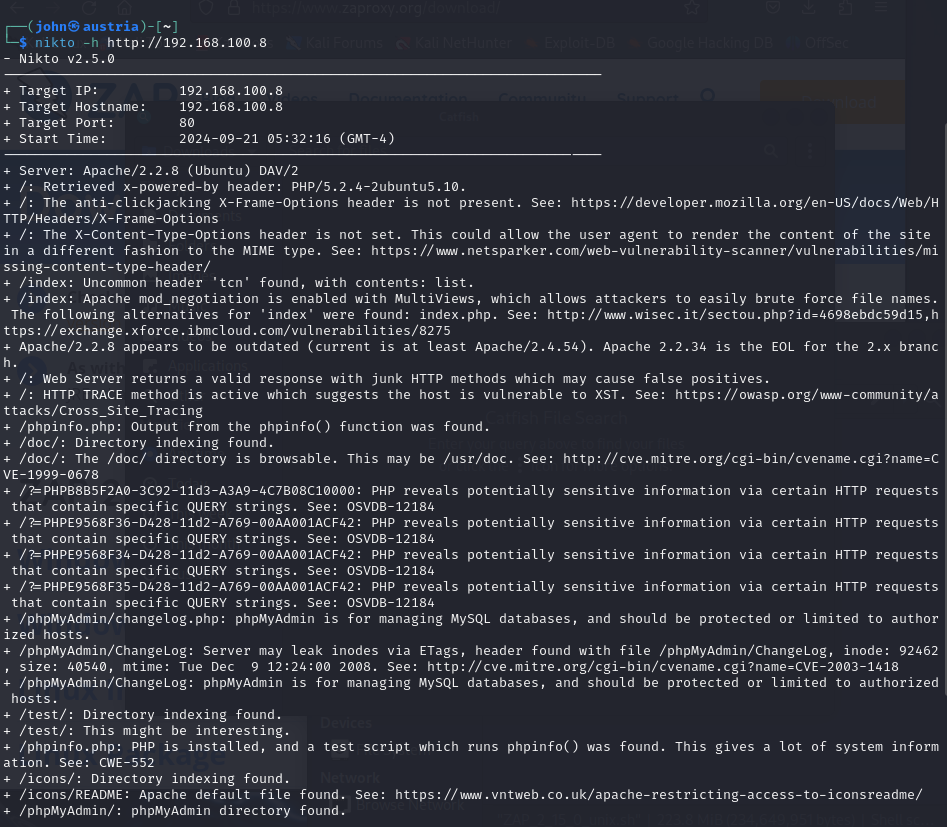
****

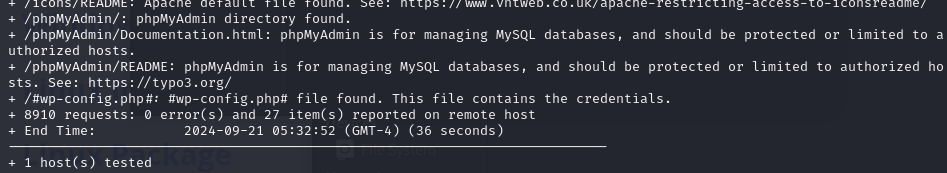
# CONCLUSIVE REMARKS

This assessment utilized five countermeasures to tackle the vulnerabilities of port 80 in Metasploitable2. The five countermeasures are ubuntu firewall, securing web apache server, hiding web server version and OS information, enabling SSL, and Protect from DDOS. The countermeasure proved to be useful as I only need to install some of the countermeasures and configure the values from the Apache file.

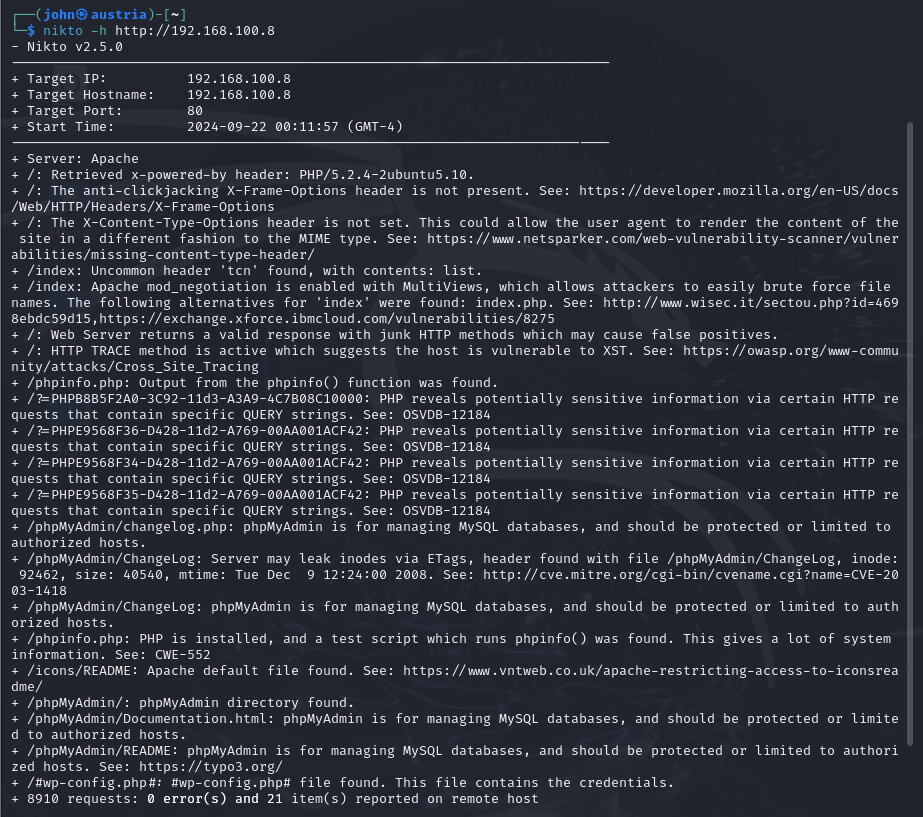
To fully test the countermeasures stated above, I have used nikto once more to scan Metasploitable2. I typed ‘nikto -h http://192.168.100.8’ in the prompt server then pressed enter. The scan returned with fewer vulnerabilities compared to the first scan in chapter 2. The red squares are the vulnerabilities from chapter 2 that did not return in the last scan.

Scan in chapter 2:





New Scan:



# REFERENCES

Digicert (2023). *What is SSL, TLS and HTTPS? | DigiCert*. [online] www.digicert.com. Available at: https://www.digicert.com/what-is-ssl-tls-and-https.

Giaquinto, R. (2022). *What is Apache and What Does it Do for Website Development?* [online] GreenGeeks Blog. Available at: https://www.greengeeks.com/blog/what-is-apache/.

Rouse, M. (2023). *What is Port 80? - Definition from Techopedia*. [online] Techopedia.com. Available at: https://www.techopedia.com/definition/15709/port-80.

Ubuntu Server (2024). *Firewalls*. [online] Ubuntu.com. Available at: https://ubuntu.com/server/docs/firewalls.