Report VM Ubuntu 20 on GCP Host [34.172.136.48]

Project 7 – Vulnerability Assessment and Remedition Plan

1- Configuration Management & Tools
   a. Install OS Ubuntu [20] - SSH 8.3p1
   b. Install Web server [nginx 1.8]
   c. Install [PHP 7.4]
   d. VM on prem kali lunix
   e. Install OpenVAS on kali lunix
2- Conduct vulnerability
   a. Perform vulnerability Scanning

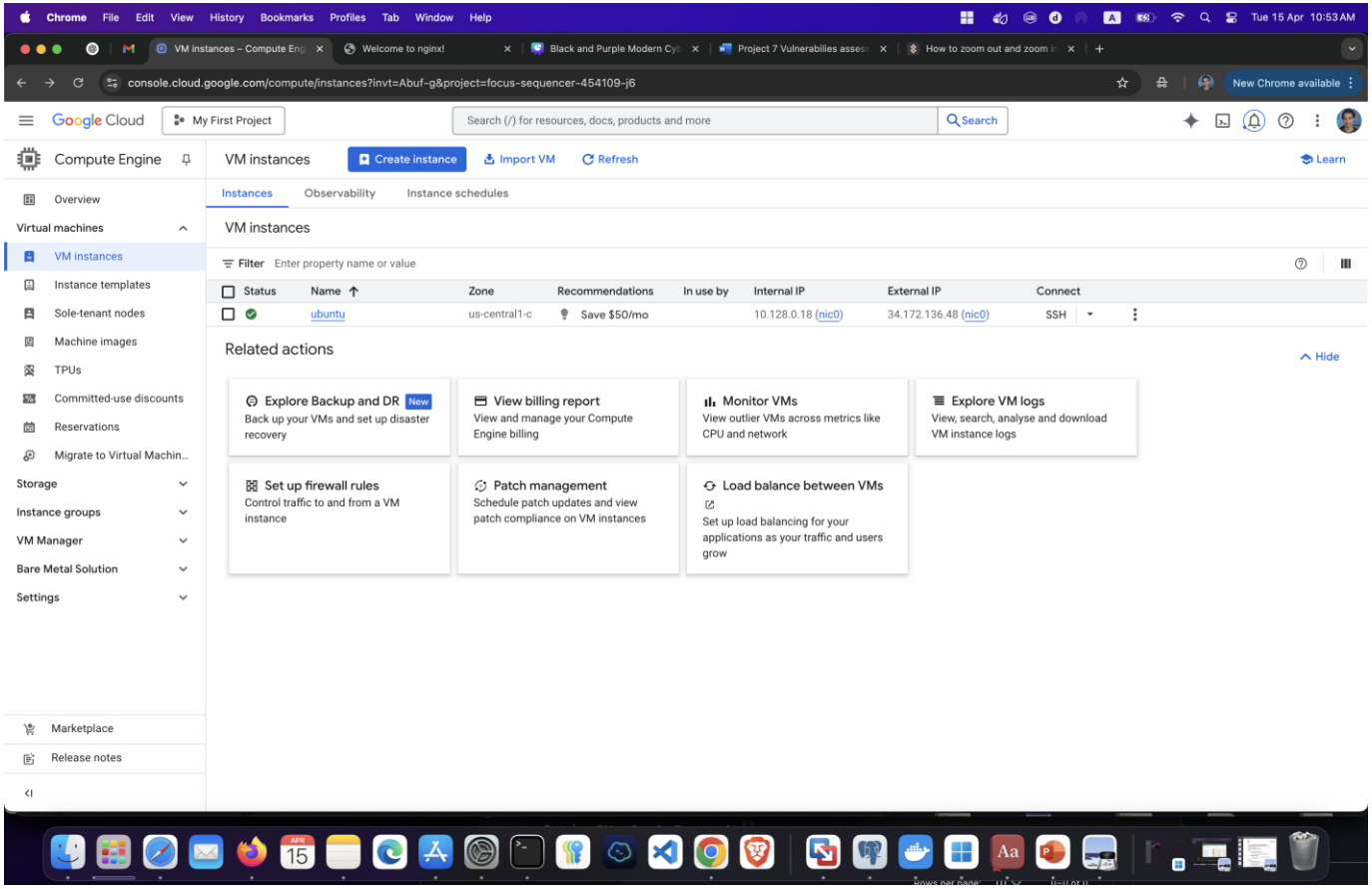
Vulnerability	Severity	Location
Nginx End of Life (EOL) Detection	High	80/tcp
PHP End of Life (EOL) Detection - Linux	High	80/tcp
PHP < 8.1.29, 8.2.x < 8.2.20, 8.3.x < 8.3.8 Multiple Vulnerabilities - Linux	High	80/tcp
PHP < 8.1.29, 8.2.x < 8.2.20, 8.3.x < 8.3.8 Multiple Vulnerabilities - Linux	High	22/tcp
PHP < 8.1.31, 8.2.x < 8.2.26, 8.3.x < 8.3.14 Multiple Vulnerabilities - Linux	High	80/tcp
PHP < 8.0.30, 8.1.x < 8.1.22, 8.2.x < 8.2.9 Security Update - Linux	High	80/tcp
PHP < 8.1.30, 8.2.x < 8.2.24, 8.3.x < 8.3.12 Multiple Vulnerabilities - Linux	High	80/tcp
PHP < 8.0.28, 8.1.x < 8.1.16, 8.2.x < 8.2.3 Security Update - Linux	High	80/tcp
PHP < 8.0.27, 8.1.x < 8.1.14, 8.2.x < 8.2.1 Security Update - Linux	High	80/tcp
OpenBSD OpenSSH <= 8.6 Command Injection Vulnerability	High	22/tcp
Nginx Multiple Vulnerabilities (Oct 2022)	High	80/tcp
nginx 0.6.18 - 1.20.0 1-byte Memory Overwrite Vulnerability	High	80/tcp
PHP 'CVE-2017-7189' Improper Input Validation Vulnerability - Linux	High	80/tcp
Diffie-Hellman Ephemeral Key Exchange DoS Vulnerability (SSH, D(HE)ater)	High	22/tcp
nginx <= 1.21.1 Information Disclosure Vulnerability	High	80/tcp
OpenSSH 8.2 < 8.5 Memory Corruption Vulnerability	High	22/tcp

OpenSSH 6.2 <= 8.7 Privilege Escalation Vulnerability	High	22/tcp
OpenBSD OpenSSH 6.8p1 - 9.9p1 MitM Vulnerability	Medium	22/tcp
OpenBSD OpenSSH < 9.6 Multiple Vulnerabilities (Terrapin Attack)	Medium	22/tcp
Prefix Truncation Attacks in SSH Specification (Terrapin Attack)	Medium	22/tcp
OpenBSD OpenSSH Information Disclosure Vulnerability (CVE-2020-14145)	Medium	22/tcp
PHP < 8.1.28, 8.2.x < 8.2.18, 8.3.x < 8.3.6 Security Update (GHSA-h746-cjrr-wfmr) - Linux	Medium	80/tcp
PHP < 8.0.22, 8.1.x < 8.1.9 Security Update - Linux	Medium	22/tcp
OpenSSH Information Disclosure Vulnerability (CVE-2016-20012)	Medium	80/tcp
phpinfo() Output Reporting (HTTP)	Medium	80/tcp
PHP < 8.1.32, 8.2.x < 8.2.28 Multiple Vulnerabilities - Linux	Medium	22/tcp
OpenBSD OpenSSH < 9.3 Unspecified Vulnerability	Medium	22/tcp
OpenBSD OpenSSH < 9.2 Unspecified Vulnerability	Medium	80/tcp
Source Control Management (SCM) Files/Folders Accessible (HTTP)	Medium	80/tcp
Nginx 1.5.13 - 1.27.0 Buffer Overread Vulnerability	Medium	80/tcp
PHP < 8.0.29, 8.1.x < 8.1.20, 8.2.x < 8.2.7 Security Update - Linux Nginx 1.11.4 - 1.27.3 TLS Session Resumption Vulnerability	Medium	80/tcp
OpenBSD OpenSSH < 9.1 Multiple Vulnerabilities	Medium	22/tcp
TCP Timestamps Information Disclosure	low	general
Weak MAC Algorithm(s) Supported (SSH)	low	22/tcp

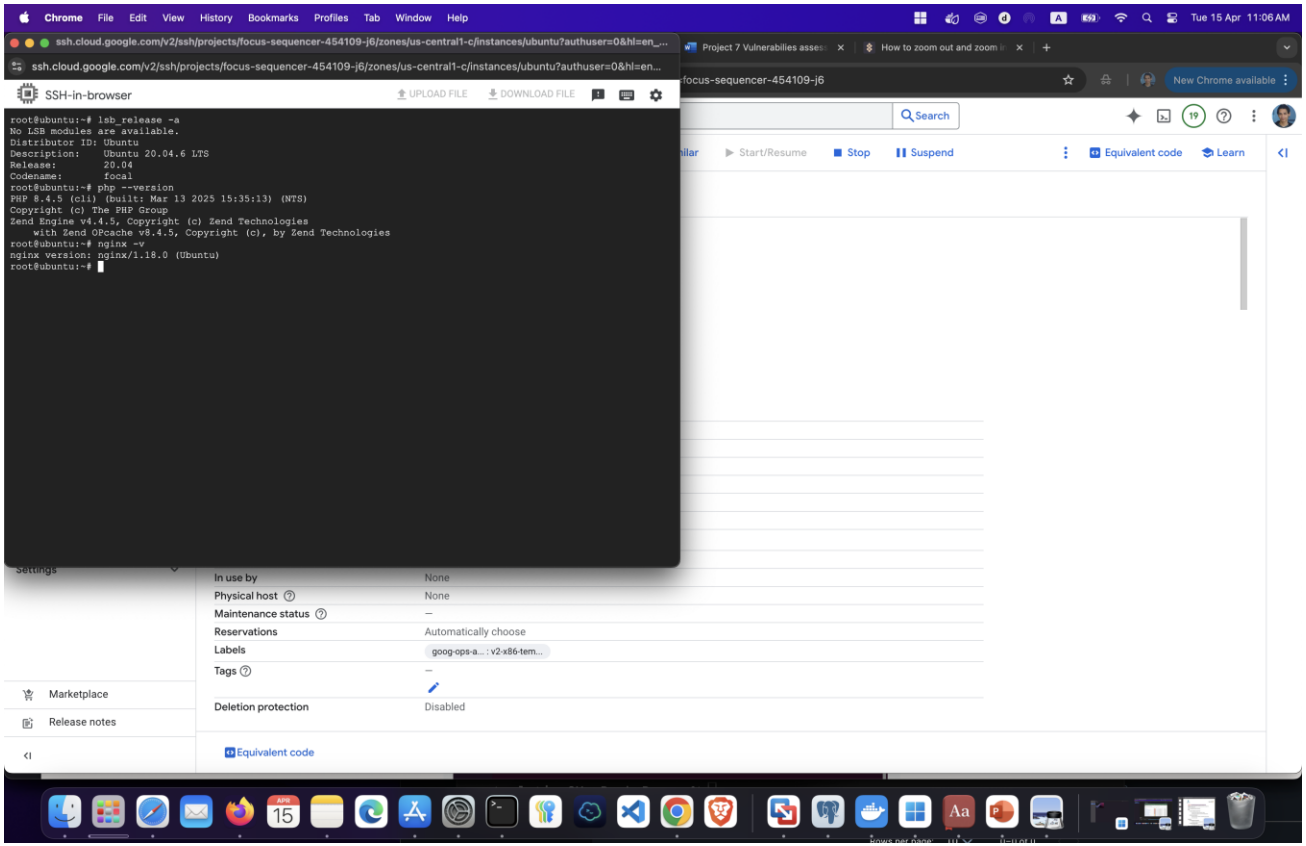
b. Analyze Vulnerability Scanning:
    i. 17 High
    ii. 15 Medium
    iii. 2 Low

- Impact:
  - Nginx 1.8 Vulnerabilities: An **EOL version of Nginx is not receiving any security updates from the vendor. Unfixed security vulnerabilities might be leveraged by an attacker to compromise the security of this host.**
  - *PHP7.4 Vulnerability*: Lack **in system hackers can exploit and expect brute force attach and DDos attack**
  - **OpenSSH *Vulnerability*: Successful exploitation would allow an attacker to execute**
  - arbitrary code on the target machine.
  - Source Control Management (SCM) Files/Folders Accessible (HTTP): Based on the information provided in these files/folders an attacker might be able to gather additional info about the structure of the system and its Applications.
  - weak MAC algorithms

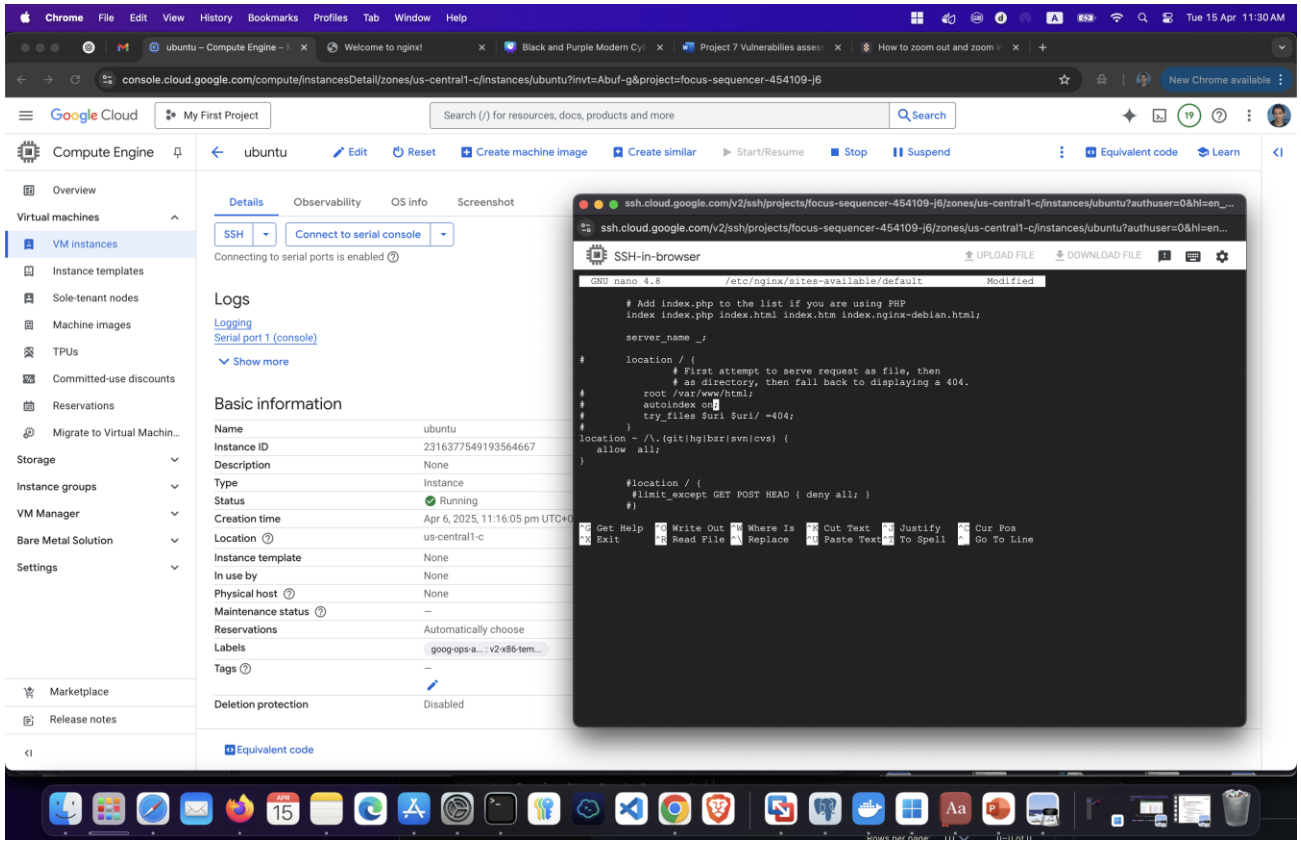
- Solutions:
  - Upgrade Nginx patch to version on the remote host or later
  - Upgrade PHP patch to version 8.1.3 or later.
  - Upgrade SSH patch version to 9.3 or later
  - Hardening nginx configuration by off autoindex
  - Harding nginx by remove signature of version
  - Harding by off autoindex direct root or any alias path in nginx Configuration
  - Remove phpinfo() from any php code
  - Restrict access to the SCM files/folders for authorized systems
  - Only.
  - Disable the reported weak MAC algorithm(s).



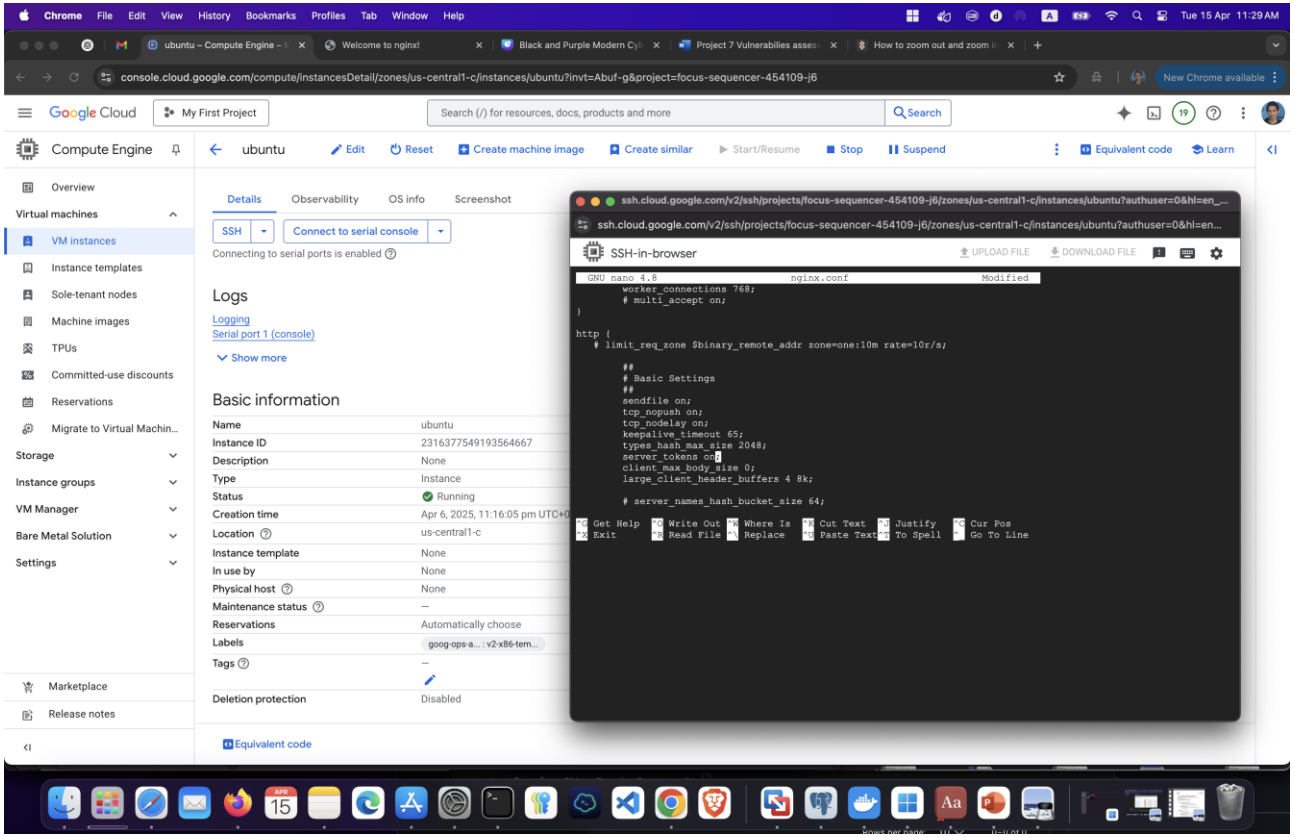
1.1 Configuration Management & Tools [VM OS Ubuntu 20]



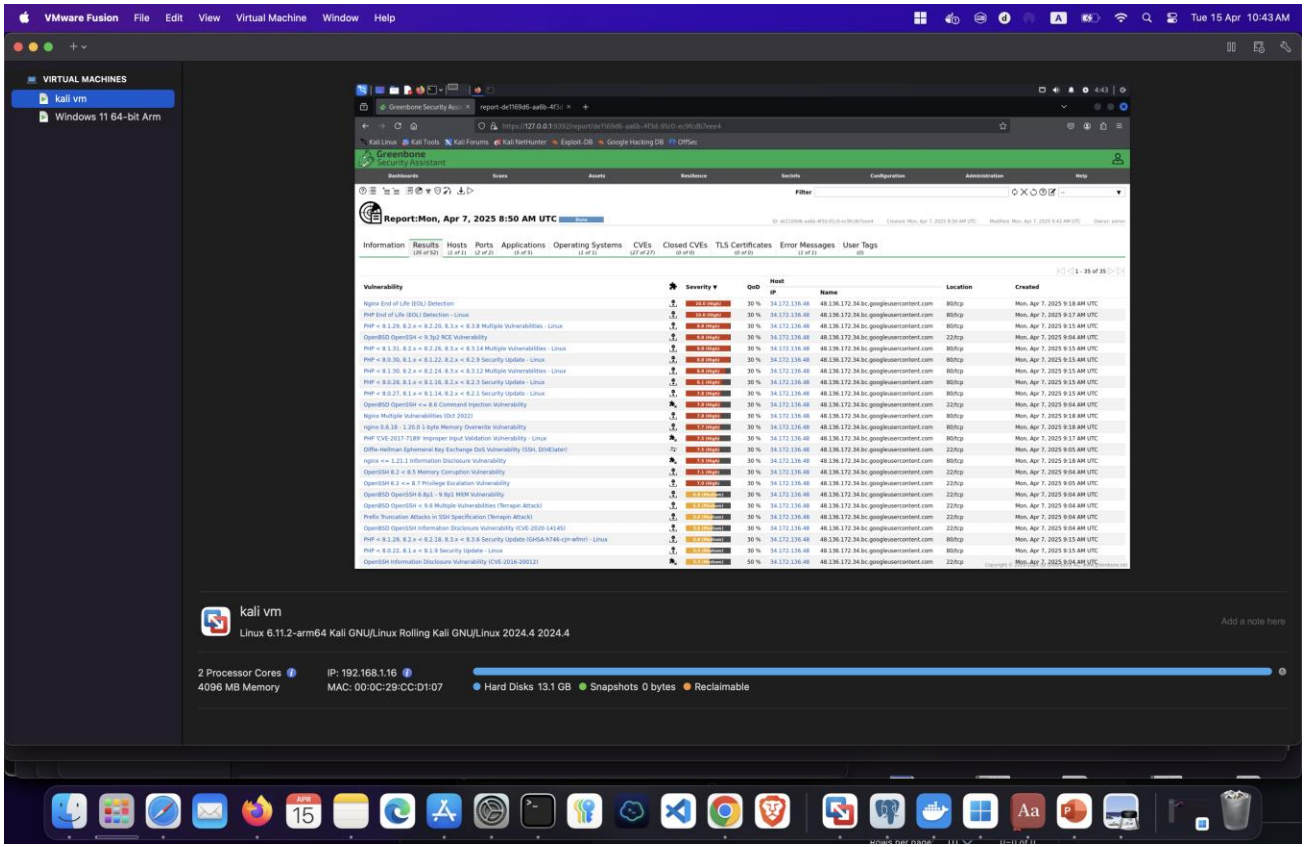
1.2 Configuration Management & Tools [nginx – php]



1.3 Configuration Management & Tools [nginx configuration]



1.4 Configuration Management & Tools [nginx configuration]



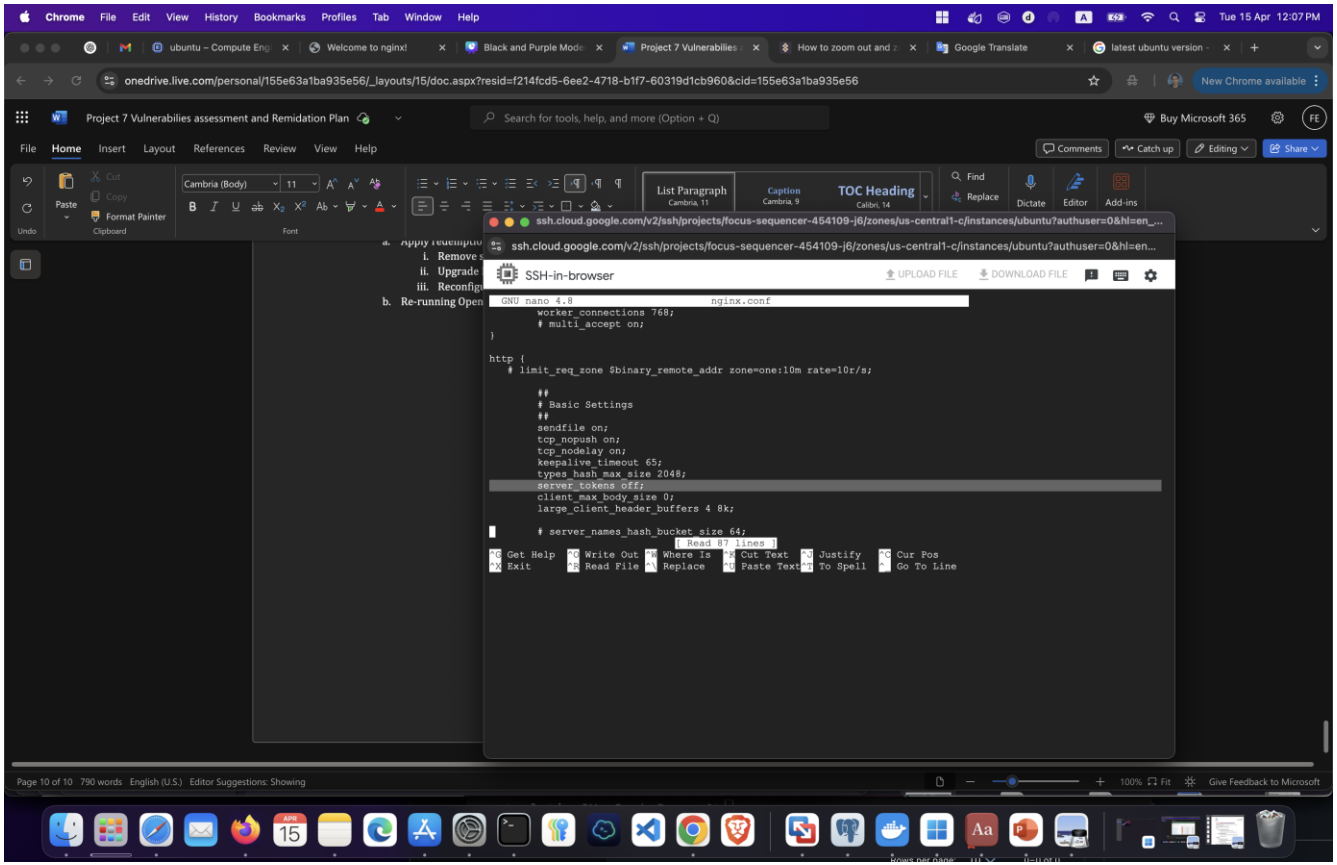
2.1 Perform vulnerability Scanning [Report 1]

3- DEVELOP Remediation Plan

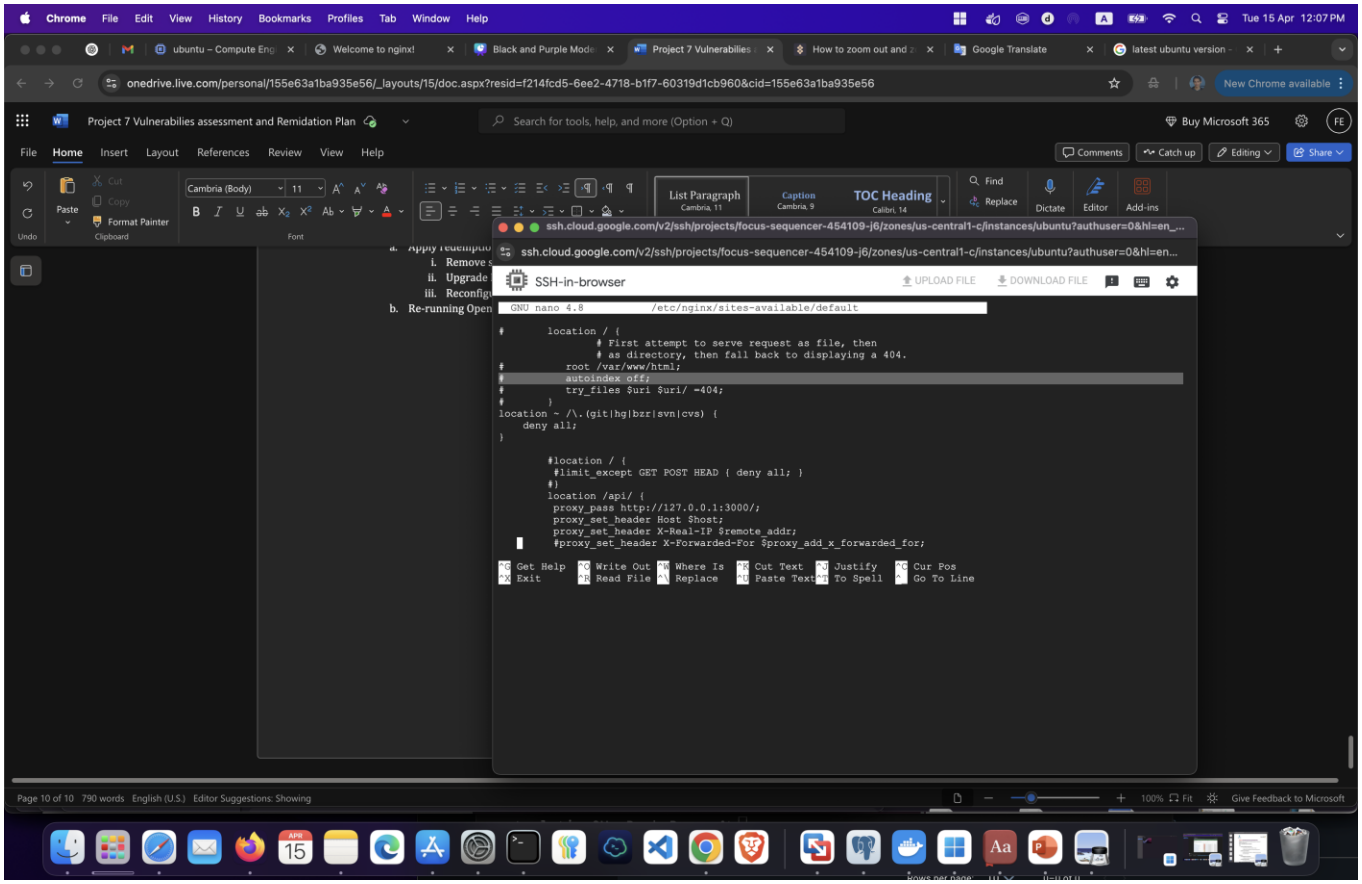
a. Define high and medium severities vulnerability to be fix As soon As possible.
b. Take backup from nginx configuration and any other configurations in OS
c. Create firewall rules to filter all open ports & update patches.
d. Timeline and assign tasks to soc team.
e. Redemption plan to upgrade to ubuntu 24.10
f. Upgrade ssh to 9.3

Name	Vulnerabilities	Time	Status
Fady William	10 High	3 Days	New
Ahmed Saad	7 High	2 Days	New
Ahmed Abdulmutallab	7 Medium	1 Day	New
Tarek Mohamed	8 Medium	4 Days	New

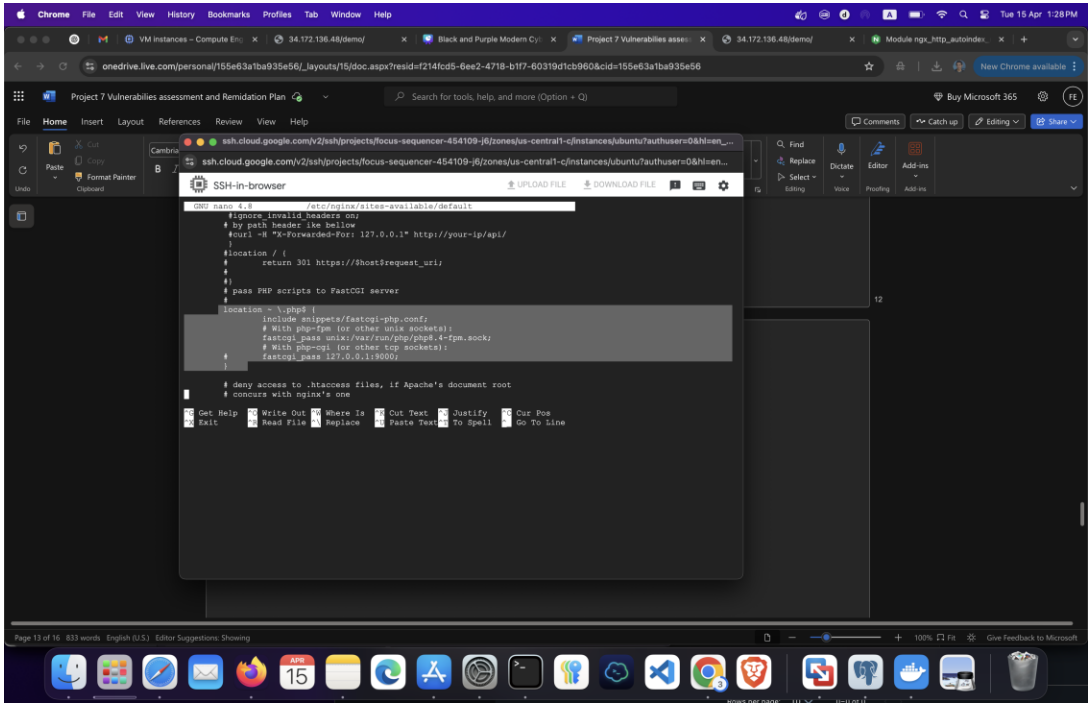
4- Implement and Verify Fixes
    a. Apply redemption
        i. Remove ssh 8.3pl that not compatible with ubuntu 20
        ii. Upgrade PHP version to 8.3
        iii. Reconfigure nginx to off autoindex and server token and signature
    b. Re-running OpenVAS and scan VM again



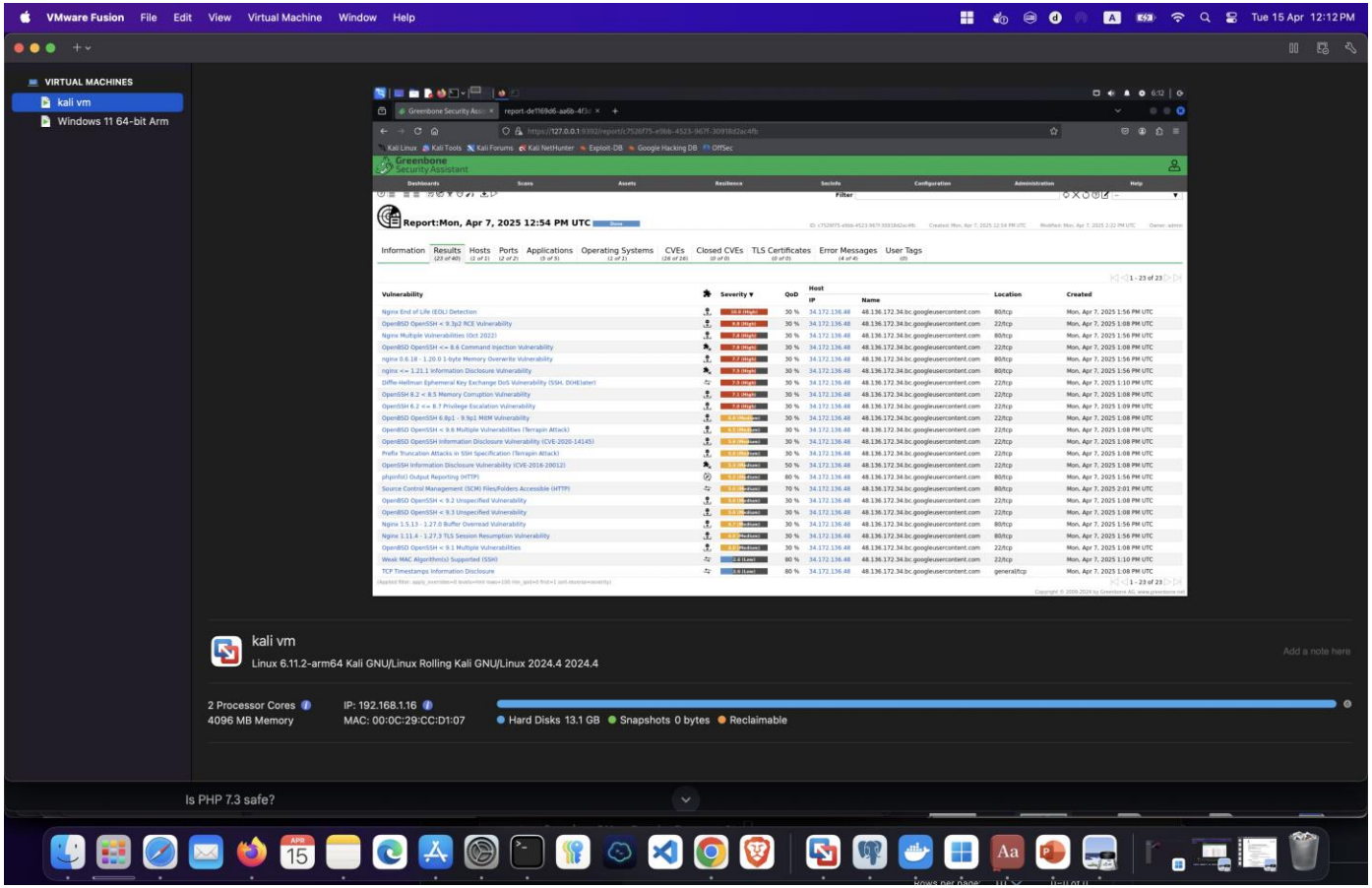
4- Implement and Verify Fixes screenshot 1



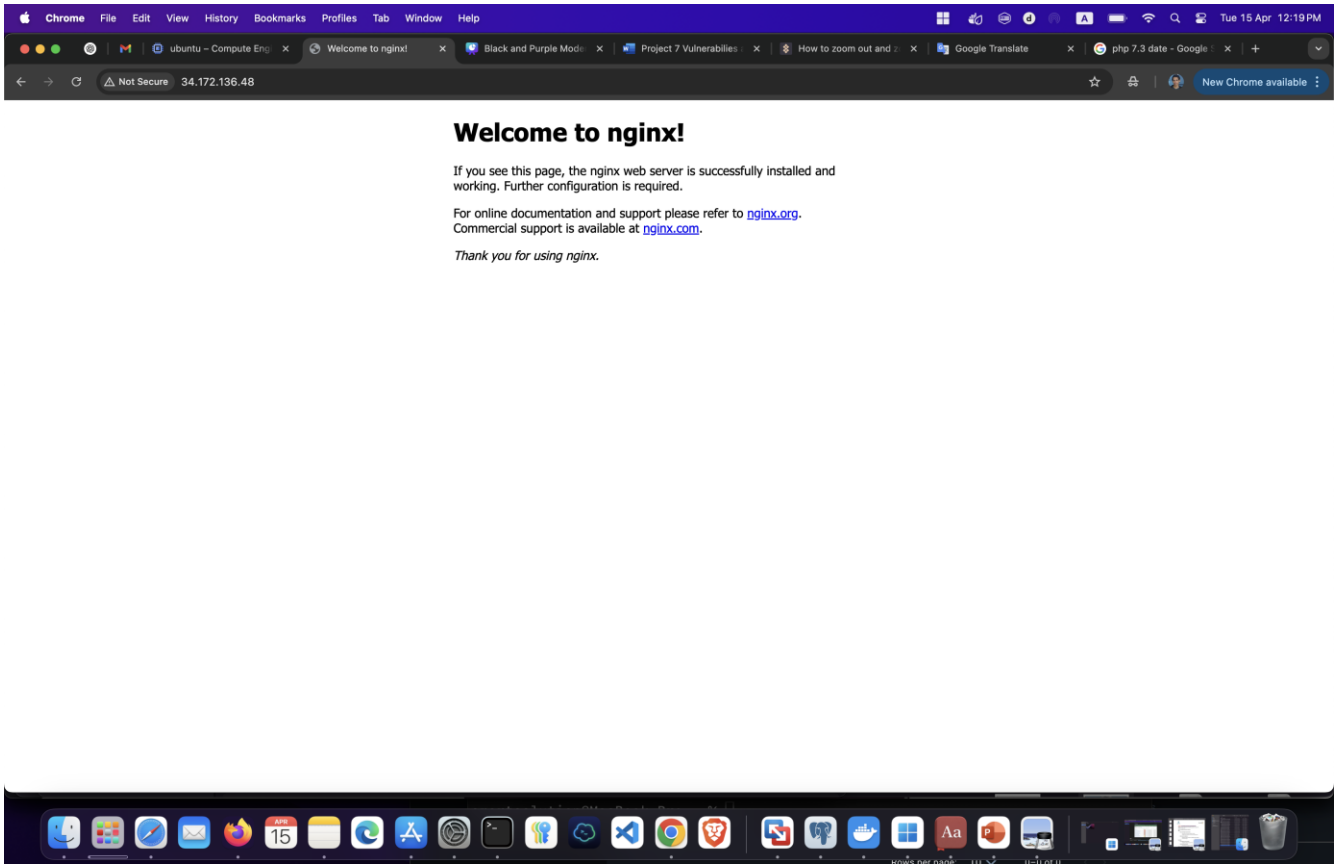
4- Implement and Verify Fixes screenshot 2



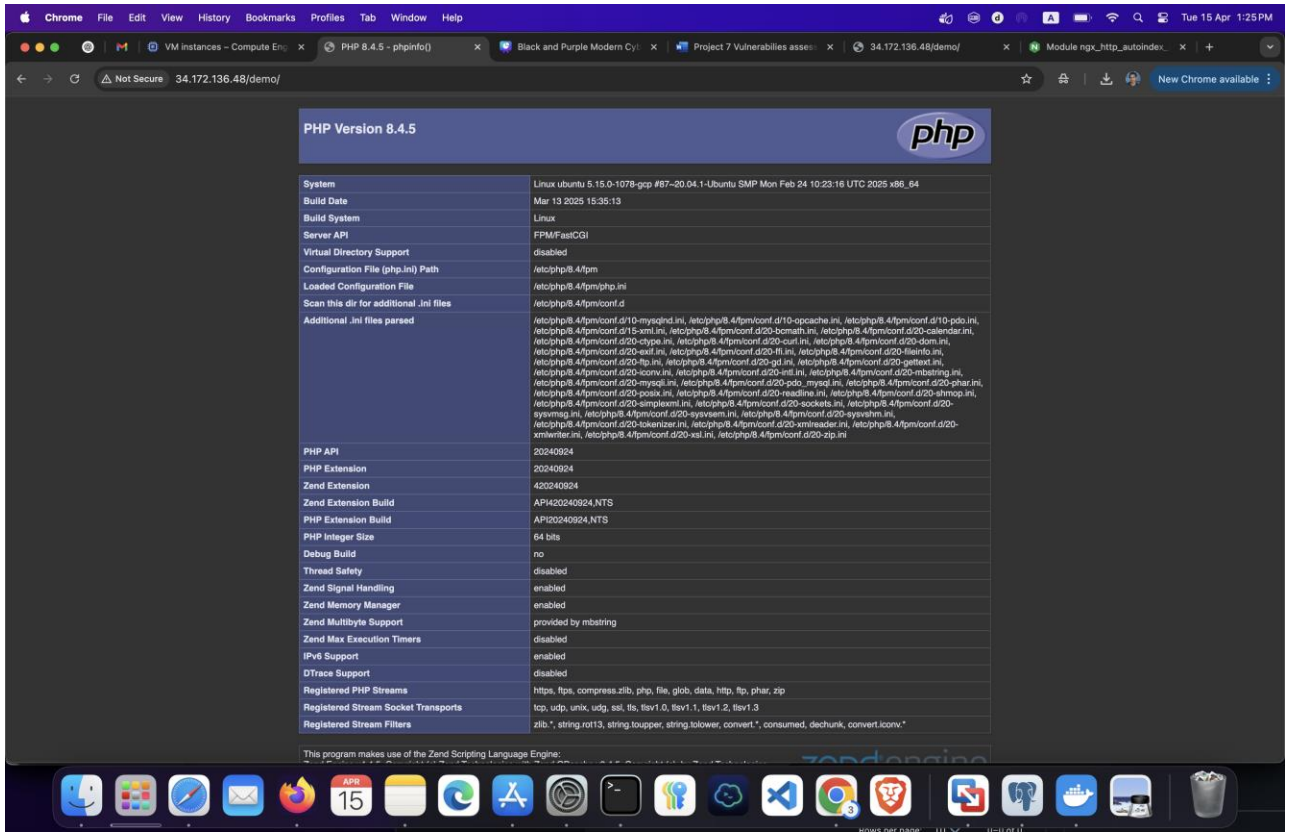
4- Implement and Verify Fixes [configure php 8.3]



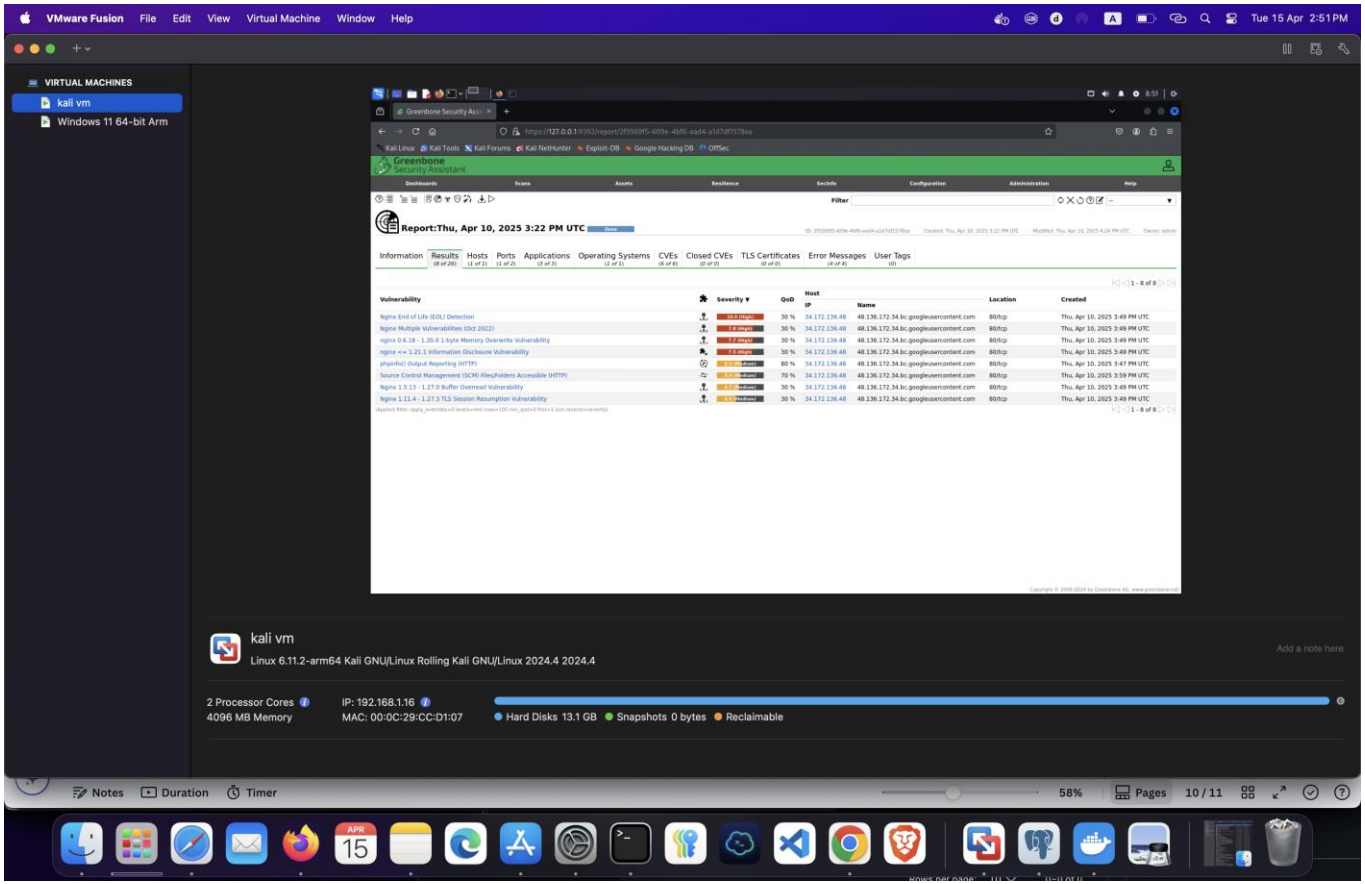
4- Implement and Verify Fixes [report 2 fix php version]



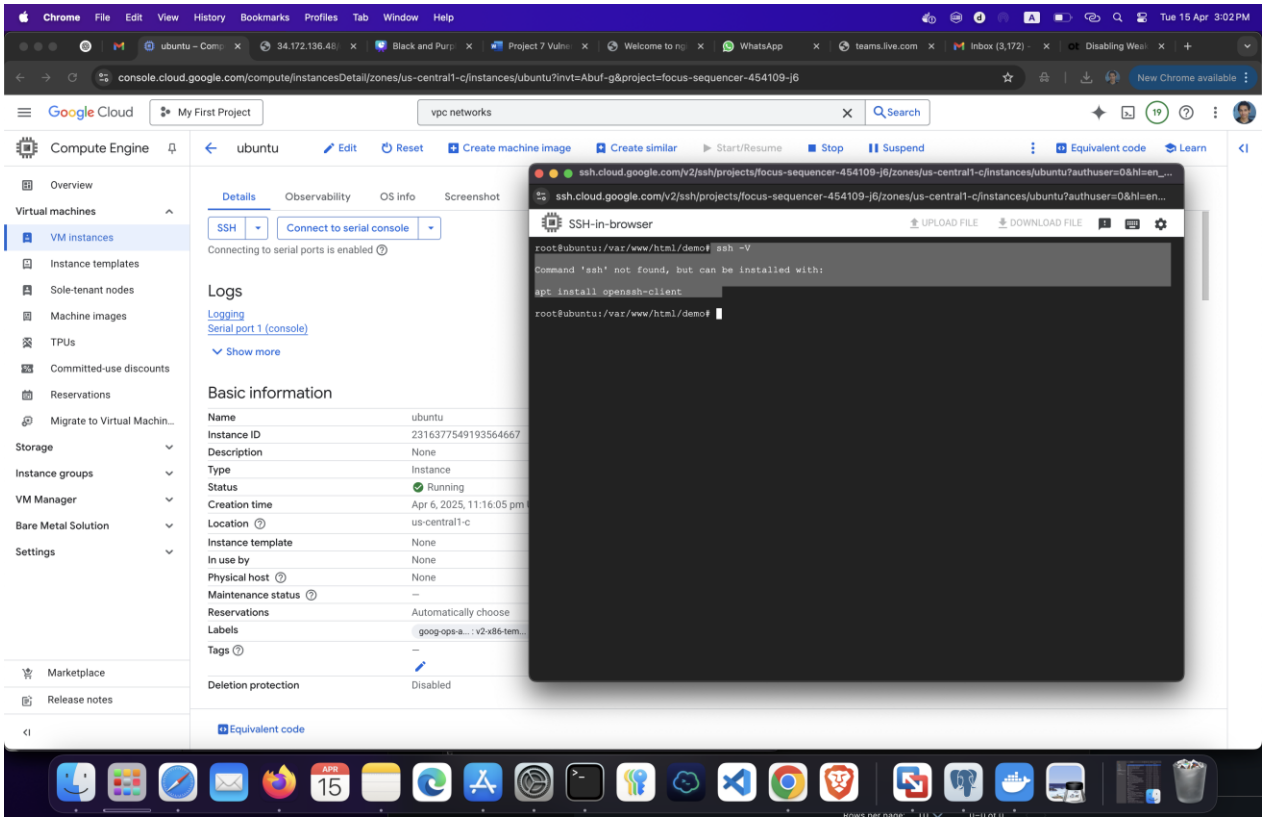
4- Implement and Verify Fixes [system is up screenshot]



4- Implement and Verify Fixes [PHP 8.3 is running screenshot]

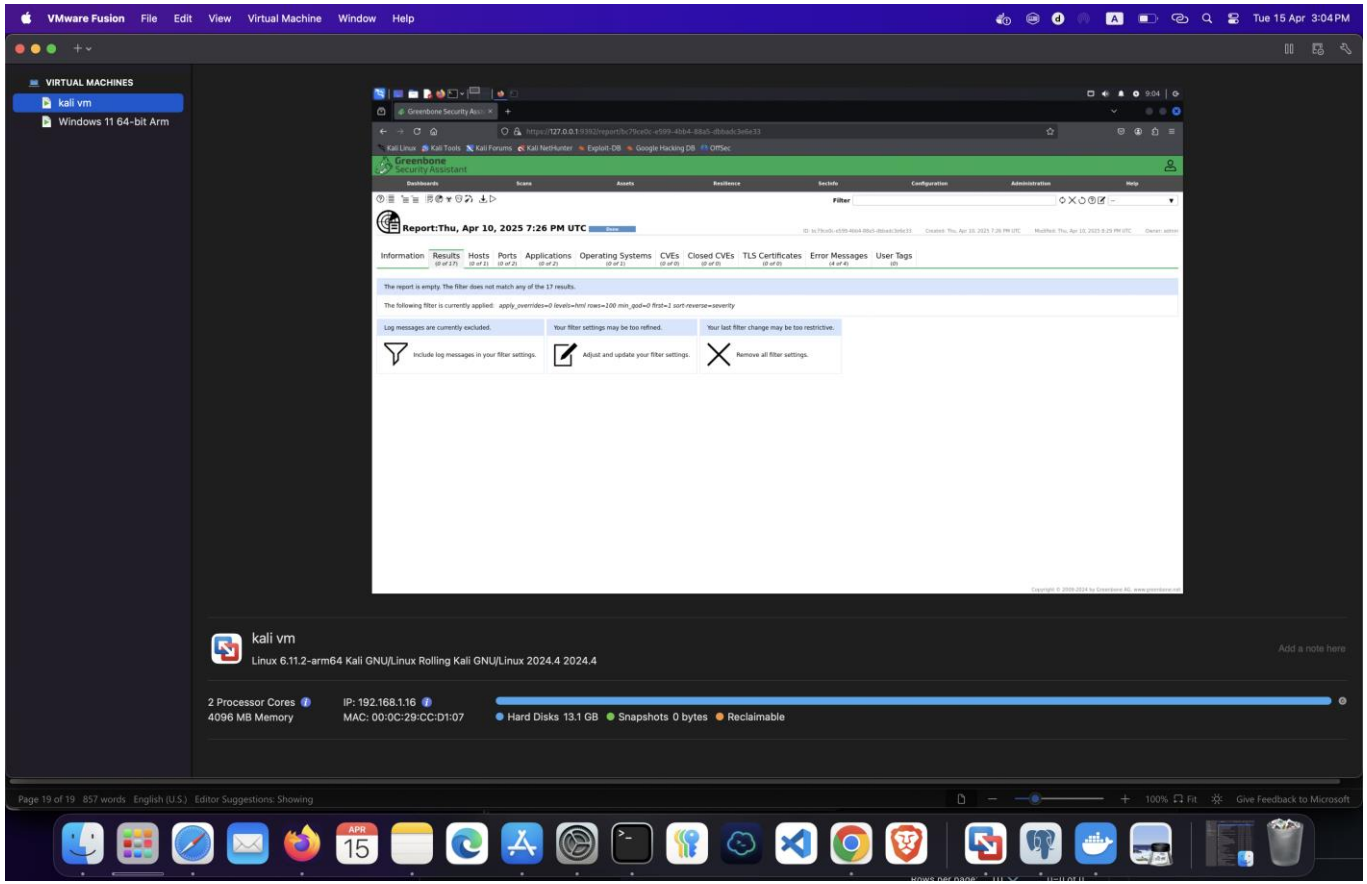


4- Implement and Verify Fixes [OpenSSH , MAC algorithm]

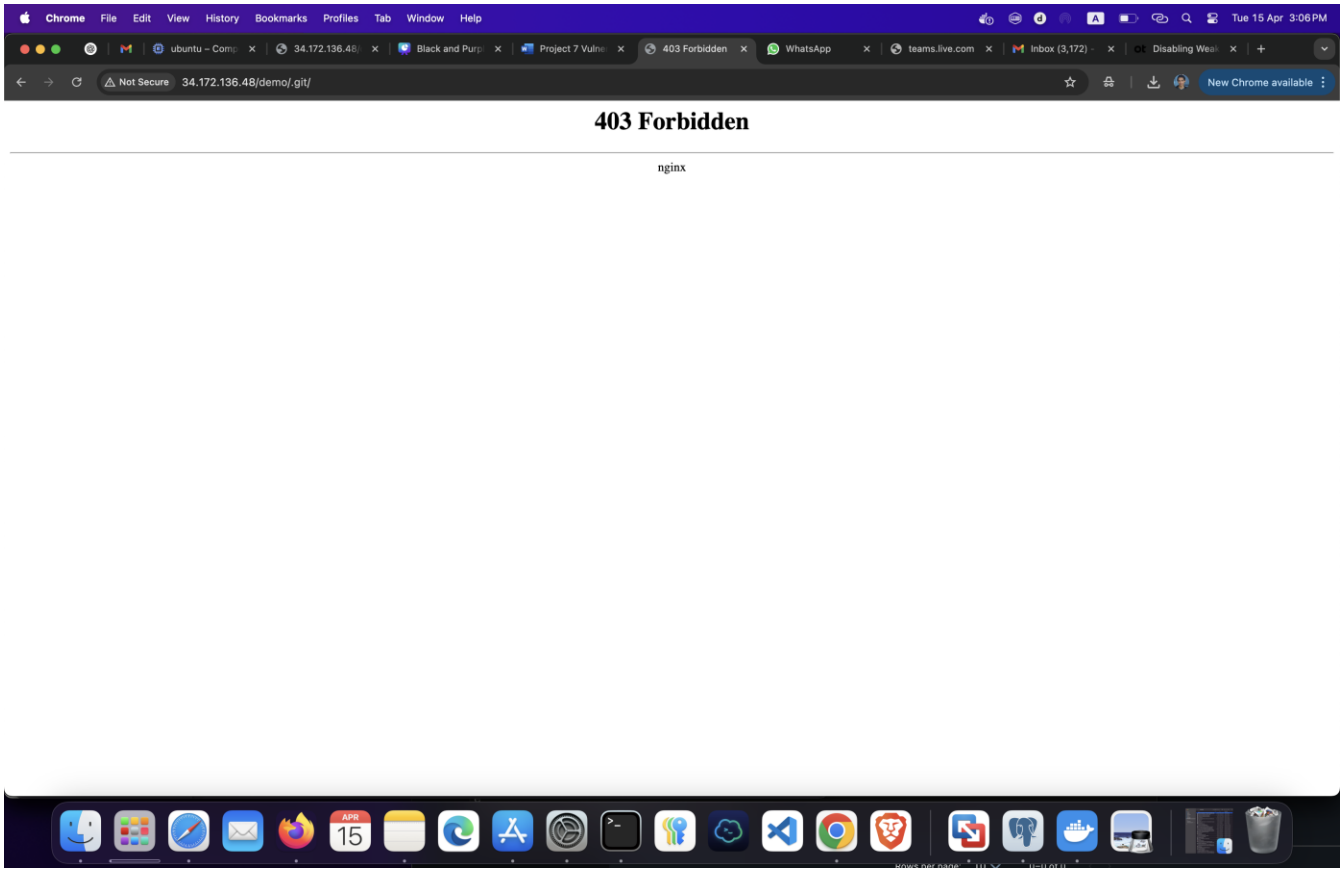


4- Implement and Verify Fixes [Remove SSH]

5- Verification report

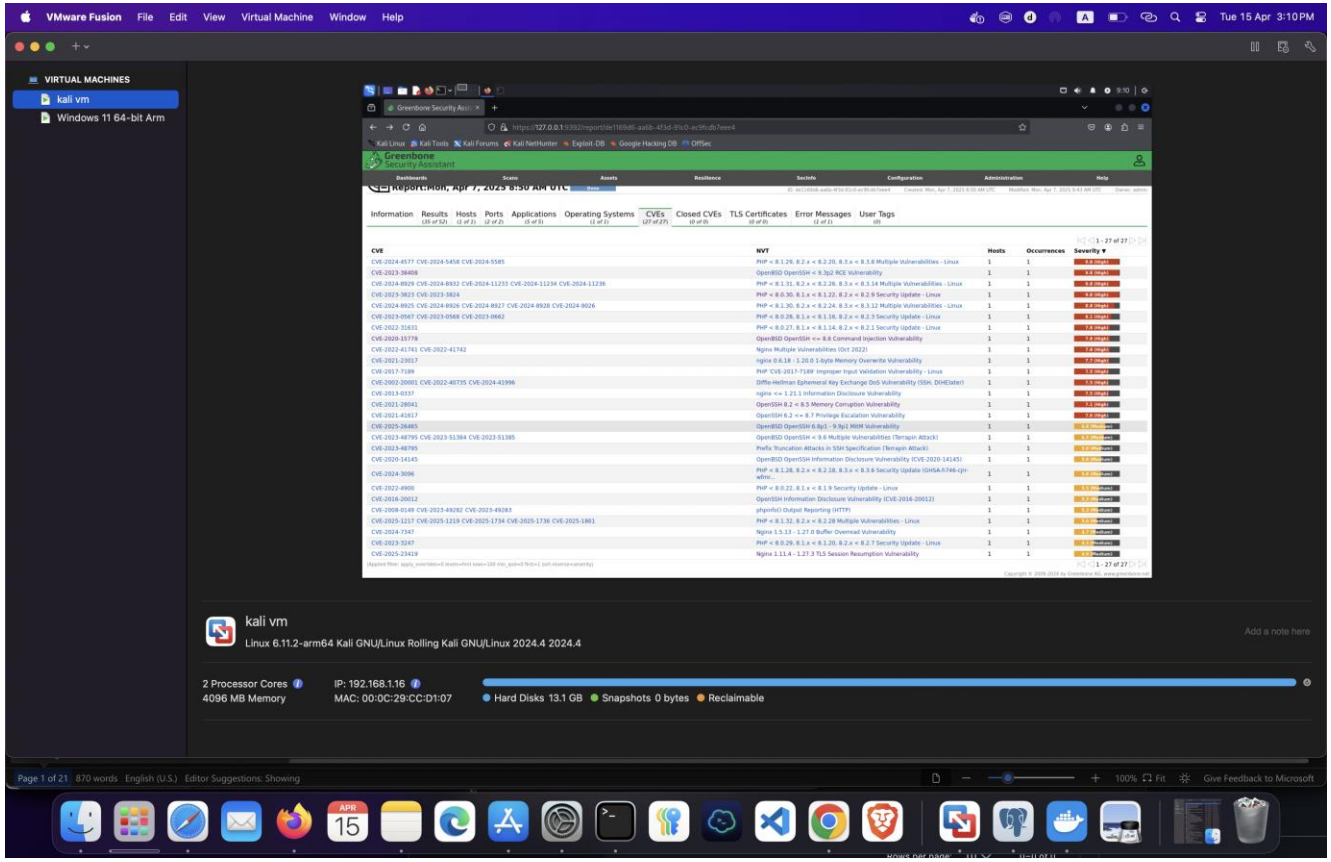


6- Verification report [Fix access directory]



Fix access directory

7- References:



CVS