MIT WORLD PEACE UNIVERSITY

Vulnerability Identification and Penetration Testing
Third Year B. Tech, Semester 6

IT AUDIT, MALWARE ANALYSIS AND VULNERABILITY ASSESSMENT FOR REPORT GENERATION

ASSIGNMENT 8

Prepared By

Krishnaraj Thadesar
Cyber Security and Forensics
Batch A1, PA 10

April 21, 2024

Contents

1   Aim

To perform IT Audit, Malware Analysis and Vulnerability Assessment for Report Generation.

2   Objectives

1. To understand the concept of IT Audit, Malware Analysis and Vulnerability Assessment.

2. To perform IT Audit, Malware Analysis and Vulnerability Assessment.

3   Theory

3.1   IT Audit

An IT audit is the examination and evaluation of an organization's information technology infrastructure, policies and operations. Information technology audits determine whether IT controls protect corporate assets, ensure data integrity and are aligned with the business's overall goals.

3.2   Malware Analysis

Malware analysis is the process of determining the functionality, origin and potential impact of a given malware sample such as a virus, worm, trojan horse, rootkit, or backdoor. Malware analysts typically do not have access to the source code of the malware, which means they must extract as much information as possible from the compiled code.

3.3   Vulnerability Assessment

A vulnerability assessment is the process of defining, identifying, classifying and prioritizing vulnerabilities in computer systems, applications and network infrastructures and providing the organization doing the assessment with the necessary knowledge, awareness and risk background to understand the threats to its environment and react appropriately.

3.4   IT Audit Tools

1. Nikto: Web server scanner for identifying vulnerabilities and misconfigurations.

2. Wireshark: Network protocol analyzer for capturing and analyzing network traffic.

3. Nessus: Vulnerability scanner for identifying security vulnerabilities in networks, systems, and applications.

4. OpenVAS: Open-source vulnerability scanner for detecting security issues in networks and web applications.

5. Nexpose: Vulnerability management solution for discovering, assessing, and prioritizing vulnerabilities.

6. Retina: Vulnerability management and assessment tool for identifying and remediating security risks.

7. Qualys: Cloud-based security and compliance platform offering vulnerability management and threat protection.

8. SAINT: Security assessment and vulnerability management tool for identifying and mitigating security risks.

9. Core Impact: Penetration testing tool for simulating real-world attack scenarios and identifying vulnerabilities.

10. Metasploit: Penetration testing framework for exploiting security vulnerabilities in target systems.

11. Nmap: Network scanner for discovering hosts and services on a network and identifying potential security issues.

3.5 Nikto

3.6 Uses

- Performs comprehensive web server scanning to identify potential vulnerabilities and misconfigurations.

- Checks for common security issues such as outdated software, insecure server configurations, and known vulnerabilities.

- Provides detailed reports and recommendations for improving web server security posture.

3.7 Advantages

- Free and open-source tool, widely used in the cybersecurity community.

- Supports scanning of multiple web servers and protocols, including HTTP and HTTPS.

- Regularly updated with new checks and vulnerability signatures to detect the latest threats.

3.8 Disadvantages

- May produce false positives or miss certain vulnerabilities in complex web applications.

- Limited to web server scanning and may not cover all aspects of network security assessment.

- Requires careful interpretation of scan results and manual verification of findings.

3.9 Wireshark

3.10 Uses

- Captures and analyzes network traffic to troubleshoot network issues and investigate security incidents.

- Provides real-time monitoring of network packets, allowing for deep inspection of protocols and traffic patterns.

- Supports various protocols and data types, including TCP, UDP, HTTP, and VoIP.

3.11 Advantages

- Free and open-source packet analyzer, available for multiple platforms including Windows, macOS, and Linux.

- User-friendly interface with powerful filtering and analysis capabilities for both novice and experienced users.

- Offers extensive protocol support and customizable display options for detailed packet analysis.

3.12 Disadvantages

- High learning curve for beginners due to the complexity of network protocols and packet analysis techniques.

- May capture sensitive information if not configured properly, leading to privacy concerns.

- Requires adequate system resources for capturing and processing large volumes of network traffic.

4 Implementation

4.1

Syntax

```
$ nikto -h <target> -Tuning x
```

Command

```
$ nikto -h www.thisislegal.com -Tuning x
```

Purpose
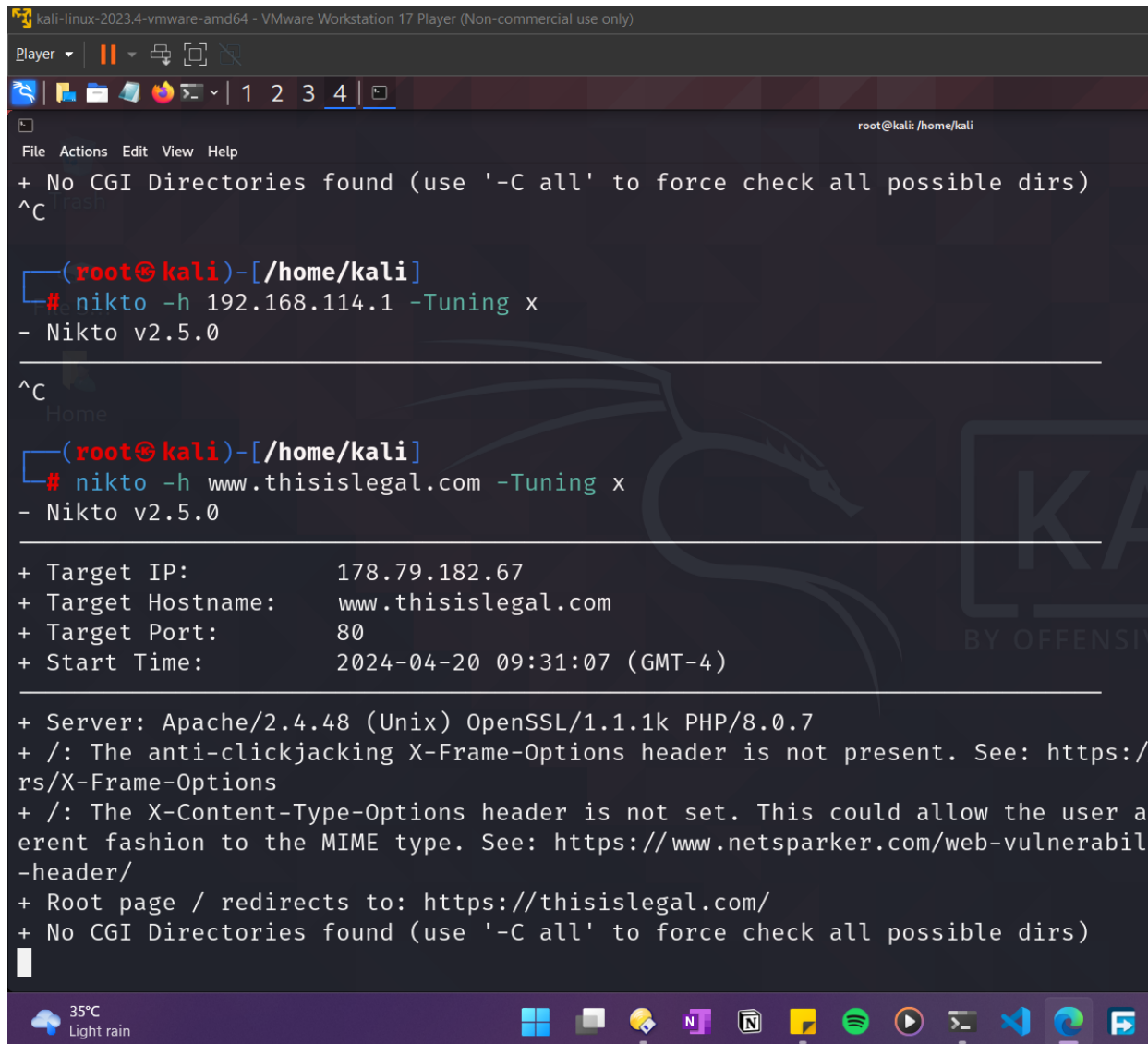
This command performs a web server scan on the target host "www.thisislegal.com".
Tuning Levels in Nikto:

- 0: File Upload

- 1: Interesting File / Seen in logs

- 2: Misconfiguration / Default File

- 3: Information Disclosure

- 4: Injection (XSS/Script/HTML)

- 5: Remote File Retrieval - Inside Web Root

- 6: Denial of Service

- 7: Remote File Retrieval - Server Wide

- 8: Command Execution / Remote Shell

- 9: SQL Injection

Meaning of Tuning Level x, is that it will scan for all the vulnerabilities from level 0 to level 9.

Output

Figure 1: Output of the command

4.2 Running Nikto with Tuning Level 6

Syntax

```
$ nikto -h <target> -Tuning x 6
```

Command

```
$ nikto -Tuning x 6 -h example.com
```

Purpose

This command will perform a web server scan on the target host "example.com" with all tuning levels except for 6 (Denial of Service).

Output

Figure 2: Output of the command

4.3

Syntax

```
$ nikto -Tuning <number> -h <target>
```

Command

```
$ nikto -Tuning 9 -h example.com
```

Purpose

This command will perform a web server scan on the target host "example.com" with tuning level 9 (SQL Injection).

Output

Figure 3: Output of the command

4.4

Syntax

```
$ nikto -h <target> -o <output> -F txt
```

Command

```
$ nikto -h www.thisislegal.com -o outputnikto -F txt
```

Purpose

This command performs a web server scan on the target host "www.thisislegal.com" and saves the output in a text file named "outputnikto".

Output

Figure 4: Output of the command

4.5   outputnikto file

Figure 5: Output of the command

4.6   Using Wireshark to Capture Packet and get password details.

Figure 6: Filtering by target ip

Figure 7: Login Request from ip
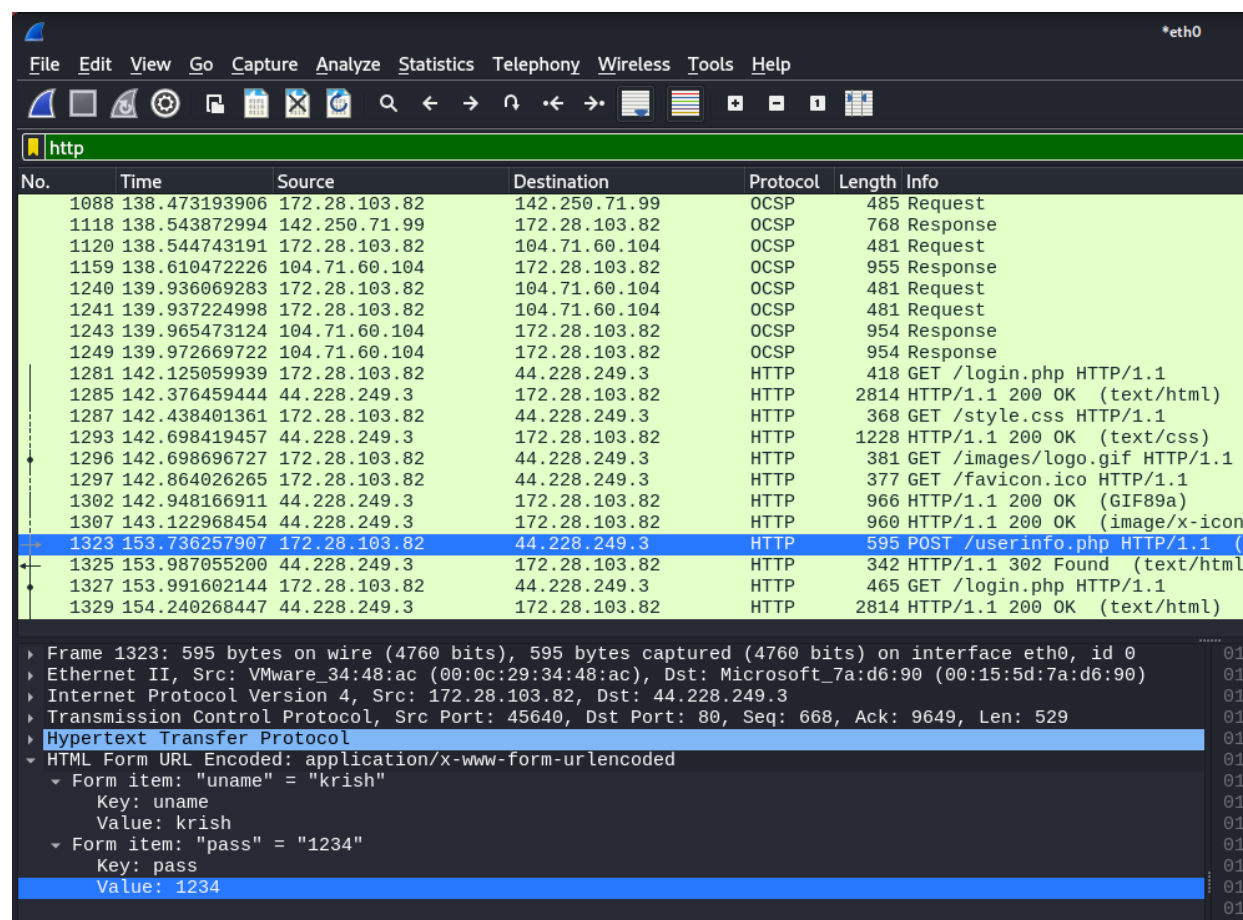
Figure 8: Viewing Http packets to get username and password

5   Platform

Operating System: Arch Linux X8664
IDEs or Text Editors Used: Visual Studio Code

6   FAQs

1. **Detailing of output file "outputnikto". (EXPLAIN ALL VULNERABILITIES):**

   The output file "outputnikto" contains the results of a scan performed by the Nikto web server scanner on the target host "www.thisislegal.com" on port 80. Below are explanations for each vulnerability identified:

   - The anti-clickjacking X-Frame-Options header is not present.
     - This vulnerability exposes the website to clickjacking attacks, where an attacker can trick users into clicking on malicious elements by overlaying them on legitimate web content.
   - The X-Content-Type-Options header is not set.

- This vulnerability may allow attackers to manipulate the content type of the website, potentially leading to content spoofing or other attacks.
- PHP/8.0.7 appears to be outdated.
  - Outdated software versions may contain known vulnerabilities that could be exploited by attackers to compromise the web server.
- Apache/2.4.48 appears to be outdated.
  - Similarly, outdated versions of web server software like Apache may contain vulnerabilities that could be exploited by attackers.
- OpenSSL/1.1.1k appears to be outdated.
  - Outdated versions of OpenSSL may contain security vulnerabilities that could be exploited to intercept or manipulate encrypted communications.
- HTTP TRACE method is active which suggests the host is vulnerable to XST.
  - The HTTP TRACE method can be exploited in cross-site tracing (XST) attacks to steal sensitive information from users' cookies.
- Retrieved x-powered-by header: PHP/8.0.7.
  - Revealing server details like the PHP version in HTTP headers can provide attackers with information to tailor their attacks.
- Cookie PHPSESSID created without the httponly flag.
  - Cookies without the httponly flag may be accessible to client-side scripts, increasing the risk of cookie theft via cross-site scripting (XSS) attacks.
- phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
  - Exposing phpMyAdmin to unauthorized access may allow attackers to gain unauthorized access to the MySQL database and its contents.
- Directory indexing

2. **What is OSVDB. Enlist top 10 vulnerabilities supported by OSVDB:**

OSVDB (Open Sourced Vulnerability Database) was a project dedicated to collecting and sharing information about security vulnerabilities. However, it has been discontinued, and its data is no longer maintained. Nevertheless, here are the top 10 vulnerabilities commonly supported by OSVDB:

- SQL Injection (SQLi)
- Cross-Site Scripting (XSS)
- Remote Code Execution (RCE)
- Directory Traversal
- Authentication Bypass
- Information Disclosure
- Buffer Overflow
- Cross-Site Request Forgery (CSRF)
- Command Injection

- Denial of Service (DoS)

3. **Write one page information on Wireshark (basic terminologies and working):**

   Wireshark is a network protocol analyzer used for capturing and analyzing network traffic. Below is an overview of basic terminologies and working of Wireshark:

   - **Packet**: Unit of data transmitted over a network.
   - **Protocol**: Set of rules defining how data is transmitted and received.
   - **Capture Filter**: Criteria used to select specific packets for analysis.
   - **Display Filter**: Criteria used to filter and display specific packets in Wireshark.
     Wireshark captures network traffic through a process called packet capture. It then analyzes these captured packets to understand network communication. Users can apply capture and display filters to focus on relevant packets and interpret packet details such as source, destination, protocol, and payload. Wireshark offers features like live capture, packet decoding, protocol support, and export and save options for offline analysis and reporting.

7 Conclusion

In this assignment, we performed IT Audit, Malware Analysis, and Vulnerability Assessment using tools like Nikto and Wireshark. We identified potential vulnerabilities in a web server and analyzed network traffic to understand network communication. These activities are essential for maintaining the security and integrity of information systems and protecting against cyber threats.