Task - 9

Vidit Sharma
21BCY10055

Date:6/9/2023

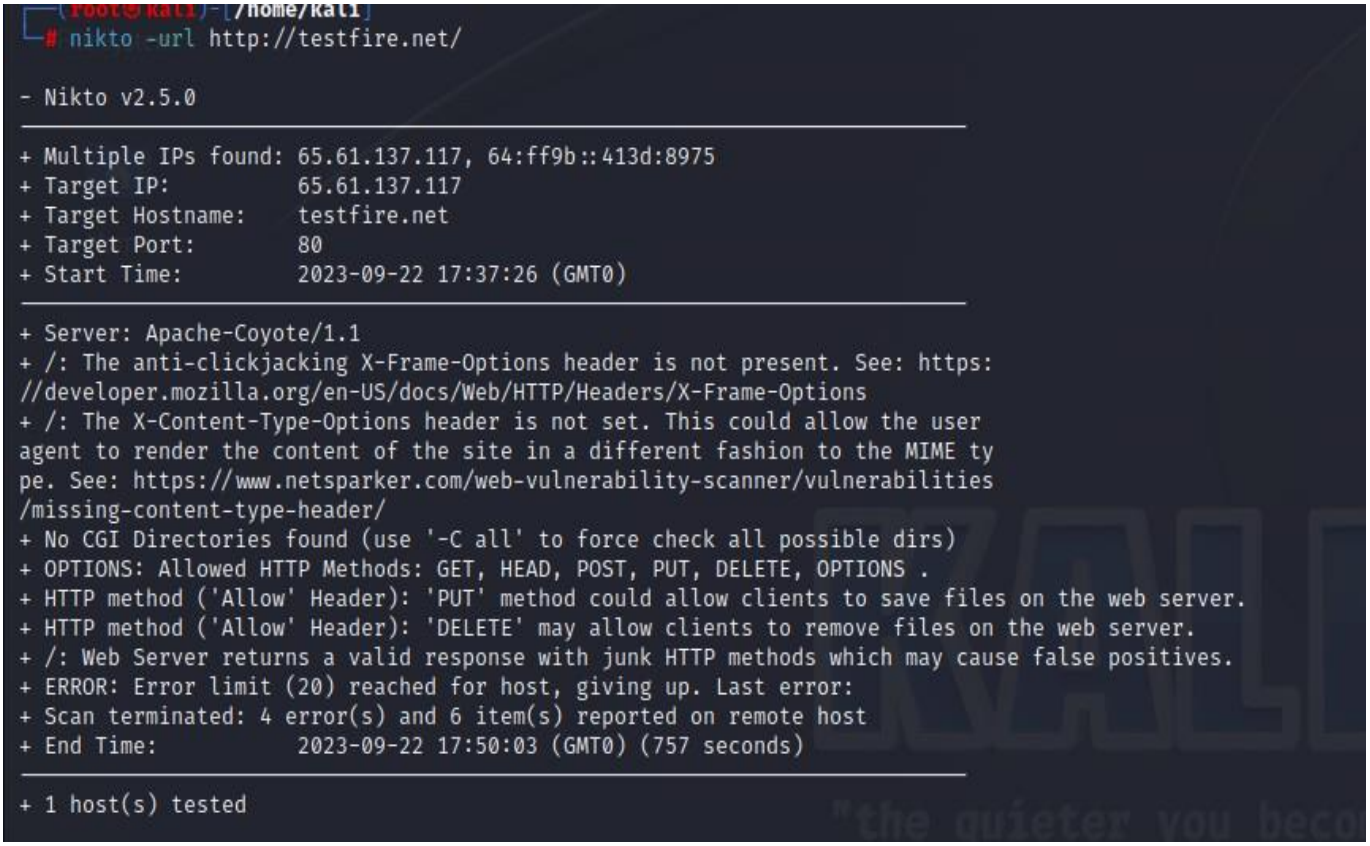
Nikto Tool-

Nikto is an open-source web server scanner tool used for discovering various security vulnerabilities in web servers and web applications. It performs a comprehensive set of tests against a web server to identify potential issues, such as outdated software, misconfigurations, and known security vulnerabilities.

Some key features of Nikto include:

- Vulnerability Scanning: Nikto scans web servers for a wide range of potential vulnerabilities, including outdated software, known security issues, and misconfigurations.
- SSL/TLS Support: It can also check the SSL/TLS configuration of a web server to identify weak encryption settings or certificate issues.
- Full HTTP Method Support: Nikto supports various HTTP methods, including GET, POST, PUT, and DELETE, allowing it to thoroughly test web applications.
- Plugin Architecture: Users can extend Nikto's functionality through custom plugins, enabling the tool to check for specific vulnerabilities or issues.
- Reporting: Nikto generates detailed reports outlining the discovered vulnerabilities, providing information on potential risks and remediation steps.

1. Scanning testfire.net website on port 80 (HTTP) using Nikto tool-



Command used - nikto -url http://testfire.net/

Information gathered-

- Two IP addresses are associated with the target, one IPv4 (65.61.137.117) and one IPv6 (64:ff9b::413d:8975).
- Target IP: The primary IP address of the target is 65.61.137.117.
- Target Hostname: The target is identified as "testfire.net," which is the domain or hostname associated with the IP address.
- Start Time: The scan was initiated on September 22, 2023, at 17:37:26 GMT.
- Server Information: The web server running on the target is identified as "Apache-Coyote/1.1." This information can be valuable for understanding the server's technology stack.
- Security Findings:
    a. X-Frame-Options Header: The anti-clickjacking X-Frame-Options header is not present. This header helps prevent clickjacking attacks.
    b. X-Content-Type-Options Header: The X-Content-Type-Options header is not set. This header can help control how content is rendered in the user's browser.
    c. CGI Directories: No CGI directories were found during the scan.
    d. Allowed HTTP Methods: The server allows various HTTP methods, including GET, HEAD, POST, PUT, DELETE, and OPTIONS.
    e. HTTP Methods ('Allow' Header): The scan identifies that the server allows PUT and DELETE HTTP methods, which could have security implications.

f. Web Server Response: The web server returns a valid response with unexpected or unusual HTTP methods, potentially causing false positives.

- Scan Termination: The scan was terminated due to encountering errors. It reports four errors and six items reported on the remote host.
- End Time: The scan was completed on September 22, 2023, at 17:50:03 GMT, lasting for 757 seconds (approximately 12.6 minutes).

This information is essential for assessing the security posture of the web server, identifying potential vulnerabilities or misconfigurations, and taking appropriate actions to address any security issues. The findings related to missing security headers and allowed HTTP methods suggest areas where security improvements may be needed to reduce potential risks.

2. Scanning for Metasploitable 2-

IP address 192.168.10.5 on port 80 (HTTP)

- Target IP: The target server's IP address is 192.168.10.5.
- Target Hostname: The target hostname matches the IP address, which is common in local network scans.
- Target Port: The scan is performed on port 80, which is commonly used for HTTP web traffic.

- Start Time: The scan was initiated on September 22, 2023, at 18:12:58 GMT.
- Server Information: The web server running on the target is identified as "Apache/2.2.8 (Ubuntu) DAV/2." This information provides details about the server's software stack.

Security Findings:

1. PHP Version: The server is running PHP version 5.2.4-2ubuntu5.10. This is essential information for potential attackers, as it could be used to exploit known vulnerabilities in this PHP version.
2. X-Frame-Options Header: The anti-clickjacking X-Frame-Options header is not present. This header helps prevent clickjacking attacks and is considered an important security measure.
3. X-Content-Type-Options Header: The X-Content-Type-Options header is not set. This header is valuable for controlling how content is rendered in the user's browser and can help prevent certain types of attacks.
4. Outdated Apache Version: The detected Apache version (2.2.8) is flagged as outdated, and it's noted that Apache 2.2.34 is the End-of-Life (EOL) version for the 2.x branch. Using outdated software may expose the server to known vulnerabilities.
5. HTTP TRACE Method: The HTTP TRACE method is active on the server, suggesting that the host may be vulnerable to Cross-Site Tracing (XST) attacks. This is a security concern.
6. Directory Indexing: Directory indexing was found in several directories, making them browsable. This can potentially expose directory structures and files to unauthorized users, revealing sensitive information.
7. phpMyAdmin: The presence of phpMyAdmin, a tool for managing MySQL databases, was detected. It's crucial to protect or limit access to such tools to prevent unauthorized access and potential data breaches.
8. WordPress Configuration File: The scan identified the presence of a "wp-config.php" file, which often contains sensitive credentials. Exposing this file can pose a significant security risk, especially if it contains database login details.

- Scan Termination: The scan was completed with 27 items reported on the remote host, and there were no reported errors.
- End Time: The scan finished on September 22, 2023, at 18:13:22 GMT, lasting for 24 seconds.