Akshatha K

Penetration Tester

TASK 1:

Perform a half-open scan against the target network to quickly identify all open ports in the network

ANSWER for Task1:

Cmd:

Sudo nmap -sS TARGET_IP

(or)

Sudo nmap -sS -p- -T4 -oN Result_scan.txt TARGET_IP

-sS: This flag tells Nmap to perform a SYN scan.

-T4 for faster scanning

TARGET_IP: Replace this with the IP address or range you want to scan.

TASK 2:

Perform an aggressive mode that enables OS detection, version detection, script scanning, and traceroute in the network

ANSWER for Task2:

Cmd:

Sudo nmap -A TARGET_IP

(or)

Sudo nmap -A -oN aggressive_scan.txt TARGET_IP

-A: Enables aggressive scan mode, which includes:

- **OS Detection**: Attempts to determine the operating system of the target.
- **Version Detection**: Identifies the versions of services running on open ports.
- **Script Scanning**: Runs a set of default Nmap scripts for additional information.
- **Traceroute**: Traces the route packets take to reach the target.

TASK 3:

While examining web server logs, you notice some HyperText Transfer Protocol (HTTP) GET requests that look suspicious. You need to carefully examine the logs, identify the attacks, and determine the appropriate mitigation control.

Log #1:

```
"18.66.78.71 - - [22/Dec/2021:16:18:20 +0300] "GET /media/system/js/caption.js HTTP/1.1" 200 751
"http://18.66.78.71/?wvstest=javascript:domxssExecutionSink(1,%22'%5C%22%3E%3Cxssta g%3E()locxss%22)" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.21""
```

Log #2

```
"18.66.78.71 - - [22/Dec/2021:15:20:03 +0300] "GET /DVWA/vulnerabilities/fi/?page=%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2fetc%2f passwd HTTP/1.1" 200 2190 "http://18.66.78.71/DVWA/" "Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2272.16 Safari/537.36""
```

Log #3

```
"18.66.78.71 - - [22/Dec/2021:15:19:59 +0300] "GET /DVWA/vulnerabilities/fi/?page=%27AND%201%3dcast(0x5f21403264696c656d6d61%20as %20varchar(8000))%20or%20%271%27%3d%27 HTTP/1.1" 200 1433
"http://18.66.78.71/DVWA/" "Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2272.16 Safari/537.36""
```

ANSWER for Task3:

Log #1:

Analysis:

- **Attack Type**: This log entry shows a potential **DOM-based Cross-Site Scripting (XSS)** attack. The `wvstest` parameter in the URL includes a JavaScript payload designed to execute a script in the client's browser, which could lead to unauthorized actions or data theft.
- **Mitigation Control**:
    - **Input Validation and Sanitization**: Ensure that all input fields are properly validated and sanitized to prevent the execution of malicious scripts.
    - **Content Security Policy (CSP)**: Implement CSP headers to restrict the types of content that can be executed or loaded by the browser.
    - **Escape Outputs**: Ensure that all user-generated content is properly escaped before being rendered on the web page.

Log #2:

Analysis:

- **Attack Type**: This log entry indicates a **Directory Traversal Attack**. The attacker is attempting to access sensitive files (`/etc/passwd`) by exploiting the file inclusion vulnerability in the application.
- **Mitigation Control**:
    - **Input Validation**: Implement strict validation on file paths to prevent directory traversal.
    - **Use Safe APIs**: Avoid using APIs or functions that allow direct file system access based on user input.
    - **Least Privilege**: Ensure that the web server process runs with the least privilege necessary to limit the impact of successful attacks.

Log #3:

Analysis:

- **Attack Type**: This log entry indicates a **SQL Injection Attack**. The attacker is attempting to exploit a SQL injection vulnerability in the application by injecting malicious SQL code into a query.
- **Mitigation Control**:
    - **Parameterized Queries**: Use parameterized queries or prepared statements to prevent SQL injection attacks.
    - **Input Validation and Escaping**: Validate and escape all user inputs before using them in SQL queries.
    - **Database Permissions**: Restrict database user permissions to the minimum necessary for application functionality.