Lab - Recommend Remediation Based on Findings

Objectives

In this lab, you will complete the following objectives:

- Identify and prioritize vulnerabilities found on the DVWA server.
- Research and recommend mitigation strategies.

Background / Scenario

Your pentesting team scanned the server at 10.6.6.13 with Nikto and determined that vulnerabilities exist on the server. It is your responsibility to further investigate the findings and determine which mitigation recommendations need to be included in the pentest report.

Required Resources

- Kali VM customized for the Ethical Hacker course
- Internet access

Instructions

Part 1: Identify and Prioritize Vulnerabilities Found on the DVWA Server

Step 1: Scan a vulnerable host with Nikto and create a report.

Run a quick scan of the DVWA server using Nikto and output the results to an HTM file. A number of vulnerabilities were discovered.

```
┌──(kali㉿Kali)-[~]
└─$ nikto -h 10.6.6.13 -o pentest.htm
```

You can use this report to investigate vulnerabilities that were found on the target.

Step 2: Perform a detail scan using GVM to further investigate the vulnerabilities on the server.

a. Start the GVM Dashboard to scan the DVWA server.

```
┌──(kali㉿Kali)-[/home/kali]
└─# sudo gvm-start
```

b. When the Firefox browser opens, login with the username **admin** and the password of **kali**.
c. Start a new task using the **Task Wizard** by clicking **Scans** from the menu bar and then selecting the **Task Wizard** from the magic wand icon on the top left of the scan window.

d. Enter the IP address **10.6.6.13** in the IP address or hostname field. Click **Start Scan**. The scan may take a few minutes, the status bar next to the scan name indicates the percent completed.

Step 3: Research the risks associated with each vulnerability.

a. When the GVM scan completes, go to the **Scans** menu and select **Reports**. You should see the report for your last scan listed there.
b. Click the date and time entry for the task to view the report. Click the **Results** tab to view the results of your scan.
c. Click each vulnerability that was found to display the detailed information about the risks associated with the vulnerability.
d. Open the Nikto pentest.htm scan report file that was created in Step 1.
e. Use internet resources to further research the vulnerabilities that were discovered using Nikto and GVM. Fill in the table with the information that you found. Based on your research, assign a priority to mitigation efforts.

- Priority 1 vulnerabilities should be fixed immediately.
- Priority 2 vulnerabilities should be fixed but are less likely or more difficult to exploit.
- Priority 3 vulnerabilities are low risk and unlikely to be exploited.

Priority	Vulnerability	Impact	Severity
Answer Area <!----><!---->	The anti-clickjacking X-Frame-Options header is not present.	Answer Area <!----><!---->	Answer Area <!----><!---->
Answer Area <!----><!---->	The X-Content-Type-Options header is not set.	Answer Area <!----><!---->	Answer Area <!----><!---->
Answer Area <!----><!---->	Directory indexing found.	Answer Area <!----><!---->	Answer Area <!----><!---->
Answer Area <!----><!---->	Operating System End-of-Life	Answer Area <!----><!---->	Answer Area <!----><!---->
Answer Area <!----><!---->	Missing “HttpOnly” Cookie Attribute (HTTP)	Answer Area <!----><!---->	Answer Area <!----><!---->
Answer Area <!----><!---->	Cleartext Transmission of Sensitive Information via HTTP	Answer Area <!----><!---->	Answer Area <!----><!---->

Priority	Vulnerability	Impact	Severity
Answer Area <!----><!---->	TCP timestamps	Answer Area <!----><!---->	Answer Area <!----><!---->
Answer Area <!----><!---->	ICMP Timestamp Reply Information Disclosure	Answer Area <!----><!---->	Answer Area <!----><!---->

Part 2: Research and Recommend Mitigation Strategies

At the end of a penetration testing project, a report or series of reports are created to inform the stakeholders of the test results. One of the main components of the report is the suggested fixes to mitigate, or work-around, the identified vulnerabilities. In this part, you will research each of the critical vulnerabilities and identify the necessary remediation.

For each of the listed vulnerabilities, describe a suggested fix or mitigation strategy.

What is your suggested fix for the **Operating System End-of-Life** vulnerability?

Answer Area
<!----><!---->

What is your suggested fix for the **Directory indexing found** vulnerability?

Answer Area
<!----><!---->

What is your suggested fix for the **Cleartext Transmission of Sensitive Information via HTTP** vulnerability?

Answer Area
<!----><!---->

What is your suggested fix for the **Missing “HttpOnly” Cookie Attribute (HTTP)** vulnerability?

Answer Area
<!----><!---->

What is your suggested fix for the **anti-clickjacking X-Frame-Options header is not present** vulnerability?

Answer Area

<!----><!---->

Reflection

Why is it important to use multiple methods to find vulnerabilities and misconfigurations in web servers?

Answer Area

<!----><!---->