|  |  |
| --- | --- |
| **Name** : Muhammad Zain Ul Abideen | **Domain** : Cyber Security |
| **CID** : DEP6384 | **Task Instructor** : Noor Us Sama |
| **Topic** : Recommendation & Report | **Tools** : OpenVAS With Greenbone GVM |

**Vulnerability Report for IP 192.168.0.112**

*Summary:* The security scan on IP 192.168.0.112 revealed 2 high-risk vulnerabilities and 8 medium-risk vulnerabilities. These findings should be thoroughly investigated and confirmed for remediation.

*Recommendations:*

1. Investigate and address the 2 high-risk vulnerabilities promptly to prevent potential security breaches.
2. Pay attention to the 8 medium-risk vulnerabilities as they could serve as entry points for more severe attacks if left unattended.

**High Risk Vulnerabilities:**

* Host 192.168.0.112 has a high-risk vulnerability related to SQL injection techniques on CGI scripts. The vulnerability allows attackers to bypass authentication or take control of the remote database.

**Medium Risk Vulnerabilities:**

* Another medium-risk vulnerability on the same host is related to Microsoft ASP.NET Information Disclosure. This vulnerability could allow remote attackers to decrypt sensitive data encrypted by the server or read data from arbitrary files within an ASP.NET application.

**Recommendations:**

* It is crucial to address both the high and medium-risk vulnerabilities promptly to prevent potential security breaches. Implement the recommended solutions to mitigate these vulnerabilities effectively.

Solutions for the mentioned vulnerabilities:

**SQL Injection Vulnerability:**

* Modify the relevant CGIs to properly escape arguments to prevent SQL injection attacks.
* Refer to http://www.securiteam.com/securityreviews/5DP0N1P76E.html for additional information.

**Service Pack Vulnerability:**

* Ensure that the server is running the latest stable Service Pack to address the vulnerability.
* The remote IIS server may be at risk due to a lower patch level, potentially exposing it to security threats.

**Microsoft ASP.NET Information Disclosure Vulnerability:**

* Run Windows Update and apply the necessary hotfixes mentioned in Microsoft Bulletin MS10-070 to mitigate the vulnerability.
* The flaw in ASP.NET handling of cryptographic padding can allow remote attackers to decrypt sensitive data, emphasizing the importance of applying the security update.

Additional Solutions for These Errors

**1. Microsoft IIS Service Pack Vulnerability:**

* Ensure the server is updated with the latest stable Service Pack for Microsoft IIS to mitigate security risks.

**2. SQL Injection Vulnerability in CGI Scripts:**

* Modify the relevant CGIs to properly escape arguments and prevent attackers from exploiting SQL injection flaws.

**3. ASP.NET Information Disclosure Vulnerability:**

* Run Windows Update and apply the necessary hotfixes listed in Microsoft Bulletin MS10-070 to address the cryptographic padding error in ASP.NET.

**4. POODLE SSLv3 Protocol CBC Ciphers Vulnerability:**

* Disable SSL v3.0 to mitigate the information disclosure vulnerability in OpenSSL and prevent man-in-the-middle attacks.

**Summary of Vulnerabilities:**

* **High Risk:** 2
* **Medium Risk:** 8
* **Low Risk:** 0

**Scan Details:**

* Scan started: Wed Aug 7 12:51:47 2024 UTC
* Scan ended: Task: testasp.vulnweb.com

**Host Summary:**

* Host 192.168.0.112
* High Risk: 2
* Medium Risk: 8
* Low Risk: 0

**Security Issues for Host 192.168.0.112:**

* **High Risk (CVSS: 7.5):** SQL injection vulnerability detected with NVT: wpoison
* **Medium Risk (CVSS: 5.0):** Microsoft ASP.NET Information Disclosure Vulnerability detected

**Recommendations:**

* Investigate and confirm HIGH and MEDIUM risk vulnerabilities for remediation.
* Address SQL injection vulnerabilities by modifying relevant CGIs to properly escape arguments.
* Update critical security patches for Microsoft ASP.NET to prevent information disclosure.