Report on Vulnerability Analysis with OpenVAS on Metasploitable 2

* ZINEEDDINE BOUMRAR

1. Introduction :

This report presents a vulnerability analysis conducted with OpenVAS on Metasploitable 2. OpenVAS (Open Vulnerability Assessment System) is a powerful, open-source tool used to scan and identify security vulnerabilities in computer systems. Metasploitable 2, on the other hand, is a deliberately vulnerable virtual machine often used for security testing and training purposes.

1. Steps Followed :

After installing OpenVAS, we started the vulnerability manager with the <<gvm start>> command. To access the OpenVAS web interface, we used the command <<sudo openvasmd>>, which allows us to reach the interface typically at the address <<[http://localhost:9392](http://localhost:9392/)>>. This interface provides a user-friendly environment to configure and launch vulnerability scans, analyze the results, and take appropriate corrective actions.

1. Creating a target in OpenVAS

* Go to "Configuration"  in the top menu and select "Targets".
* Create new target with a name "Metasploitable2".
* The target IP host which is the IP address for our Metasploitable 2 lab machine.

1. Creating a Scanning task

* Navigate to the "Scans" section.
* Click on "Tasks".
* Select "Create Task".
* Task name let’s say “MetaX2”
* Make sure that the Metasploitable2 target we’ve created earlier is selected.

1. Running the OpenVAS vulnerability scan

* Click on "Start".

1. Viewing the Results

* Now that the vulnerability scan is finished we can browse to ‘Scans -> Reports’ in the top menu. On the reports page we can find the report for the completed scanning task.

1. Vulnerabilities :

* vsftpd 2.3.4 - Backdoor Vulnerability :
  + Unauthorized remote code execution via backdoor.
  + Solution:
    - Install a secure version of vsftpd.
* Weak MySQL Passwords :
  + Weak or default passwords detected.
  + Examples:

|  |  |
| --- | --- |
| **Username** | **password** |
| user | user |
| postgres | postgres |
| msfadmin | msfadmin |

* + Solution:
    - Change to strong, unique passwords.