LAB

12

Vulnerability Assessment

By the end of this section, you should be able to:

- Identify services offered on a server.
- Find vulnerability and exploit the vulnerability on a server.

12.1 Introduction to Vulnerability Assessment

A Vulnerability Assessment (VA) is intended to identify threats and the risks a server or web application poses that eventually exposes them to cyber-attacks. Typically VA involves the use of automated testing tools, such as network security scanners, whose results are listed in a vulnerability assessment report.

Organizations of any size, or even individuals who face an increased risk of cyberattacks, can benefit from some form of vulnerability assessment, but large enterprises and other types of organizations that are subject to ongoing attacks will benefit most from vulnerability analysis.

Because security vulnerabilities can enable hackers to access IT systems and applications, it is essential for enterprises to identify and remediate weaknesses before they can be exploited. A

comprehensive vulnerability assessment along with a management program can help companies improve the security of their systems.

A vulnerability assessment is a crucial part in every penetration test and is the process of identifying and assessing vulnerabilities on a target system. In this part of this Lab Tutorial we will be assessing the vulnerabilities available on the network side of the Metasploitable 2 virtual machine

The Lab Tutorial will manually search for exploits by using scanning tools like Nmap and we will look at the use of automated vulnerability scanners like Open-Vas. Each scanning technique and method has its own advantages and disadvantages

12.1.1 ZenMAP

1. This tutorial needs :-
    a. Kali Virtual Machine that is set to NAT network
    b. Metasploitable 2 (M2) Virtual Machine that is set to NAT network
2. Make sure both VM kali and VM M2 are connected in the same network by testing the network connection using PING
3. Open Zenmap in kali | type in VM M2 IP address and start scanning.
4. Investigate the output and find the vulnerabilities of VM M2 by referring to CVE MITRE Website. List the vulnerability of VM M2

12.1.2 VSFTPD VA

1. To determine if the FTP service contains a backdoor without actually gaining a shell we can use an Nmap script.
2. Nmap script ftp-vsftpd-backdoor tests the VSFTPD v2.3.4 installation for the backdoor.
3. Open a Terminal in VM kali and type in the command below

   nmap –script ftp-vsftpd-backdoor –p 21 [target host]
4. Report the output of the NMAP

12.1.1.3 Unreal ircd VA

1. Using NMAP scan the Port that offer ircd service

   nmap –A –p 6667 [target host]
2. Report the output of the NMAP

12.2 Automated VA using OPENVAS

OpenVAS is an advanced open source vulnerability scanner and manager and can save you a lot of time when performing a vulnerability analysis and assessment. Using an automated up-to-date vulnerability scanner in penetration test often helps you to find vulnerabilities which can be easily overlooked during a manual assessment. The OpenVAS scanner uses more than 47.000 Network Vulnerability Tests (NVTs) as of June 2016.

12.2.1 Installing OPENVAS in Kali

1. installing OpenVAS and run the following commands in a terminal session to download and install OpenVAS:

```
apt-get install openvas
openvas-setup
```

2. When the installation process is finished you will be presented a long password on the last line of the console. This password is used to login to the OpenVAS web interface so you need to save it somewhere and change it after the first login.
3. When the OpenVAS setup process is finished the OpenVAS manager, scanner and services are listening on port 9390, 9391, 9392 and on port 80. You can use the following netstat command to check if these services are listening:

```
netstat –antp
```

4. if the OpenVAS services are not running than use the following command to start these services:

```
openvas-start
```

5. Than connect to the web interface using a browser and point it to:

```
https://127.0.0.1:9392
```

6. Accept the self-signed SSL certificate and sign in with user ‘admin’ and the password generated during the setup process.

7. Once login you can start scanning your target
8. Starting a scan with OpenVAS is very easy and straightforward. Just enter the target’s hostname or IP address in the quick start field and press the ‘Start Scan’ button