

Sri Lanka Institute of Information Technology

VSFTPD VERSION 2.3.5 BACKDOOR

## SYSTEMS AND NETWORK PROGRAMMING

Individual Assignment

Submitted by:

## P M S T Rathnayake

IT19163314

CONTENT

1. Introduction to VSFTP Exploitation

2. Impacts from VSFTPD Exploits

3. What are the Exploiting techniques

4.How to check the exploitation

5.What is the techniques I used to exploits

6. References used to gather information

VSFTP (Introduction)

VSFTP is stands for “very secure FTP daeman”.This is an FTP server for Unix-like system , and also Linux. This is licensed under the GNU general public licensees VSFTP supports TPV6 and SSL.

This was firstly discovered in 2011 July, in the discovery It shows that VSFTPD version 2.3.4 can be downloaded from master site had been compromised also there is an issue of users logging in to a compromised VSFTPD 2.3.4. This is like someone had uploaded a different version of VSFTPD which contains with a backdoor. Exploit/Unix/ftp/vsftpd\_234-backdoor, This exploits a malicious backdoor that was added to the VSFTPS download archived.

And also, this backdoor was introduced into the VSFTPD 2.3.4.tar.gz archive. This was introduced between June 30th, 2011 and July 1st 2011 according to the most recent information.

So this metasploitable 1: VSFTPD 2.3.4 is an internationally vulnerable Linux server. We can also use this in the real world, when is sometimes necessary to employ stealth to evade detection from blue teams. This can be obtaining root-level(high Level) access to the metasploits.

This Nmap is a Network mapper and it was maintained by Gordan Lynon and this is used by many security professions .The utility of this network mapper works both in Linux and windows. The purpose of having Nmap server is ,that it allows for an administrator to quickly and thoroughly learn about the system on Network MAPPER or Nmap .In this case also we use Nmap because, it has an ability to quickly locate live hosts. And also scripting engine allows administrators to quickly create a script that can be used to discover any of vulnerability exit on a Networks.

Impacts from VSFTPD Exploits

VSFTPD might containing backdoor, this backdoor can be created using an intruder so this kind of backdoor can be identified and removed quickly by many developers .

FTP users many authenticate themselves with protocol, in this form a username and password , can connect anonymous if the server is allow it.The project will exploit a malicious backdoor that was added to the VSFTPD aerchive.so any OS which can exits though backdoor can remotely harm to another platform.

Exploiting techniques

Techniques no 01

In this case to exploits any user can use a venerable source code. So in below Screenshot you will be the source code which use for backdoor exiting. This kind of codes can be easily recognizes the next special thing want to say about this is.t hat the backdoor payload is initiate in response to a : ) character which is a combination in the username in this case I will show a sample code segment and describe about it.

In there if you check you could see that in line 37 and 38,the user input contains hexadecimal chars 0x3a followed by Ox29 which represent the Simile face : ) characters.

A screenshot of a cell phone

Description automatically generated

Techniques no 02

Let’s fake there is a port in risk and the port is 6200.

In this techniques we are going to explain how to exploits VSFTPD c2.3.4 backdoor manually.in this case we have to a connect to a Metasploitable 2 VSFTPD server and use a smiley as the username to authenticate.

In there we have to use command from attack box:

**telnet[Metasploitable IP]21;**

And also we can use these commands:

**USER user ; )**

**PASS pass :** )

Then you have to use escape characters ^] or wait few seconds when you have fire up Nmap and scan for port 6200,you will get to see a malicious code was executed and port 6200 is opened,

Then you have to connect to the relevant port 6200 by using a command]dt.

**telnet[Metasploitable IP]6200**

Techniques no 03

Let’s see how we can exploits this backdoor vulnerability by using the Metasploit framework.

This is much simple in here we have to use command:

**Msfconsole**

When msfconsole is running select the backdoor exploit using another command:

User exploit/unit/ftp/vsftpd\_234\_backdoor

Then you have to type a command to see what are the exploits option you have the command used is :

**Show options**

After checking the exploits option you need to supply a remote host Ip and port which we leave to port .Then you can type run exploit the target.

This is the method I have used to exploit my vulnerability.

How to check whether we an Exploitation.

AS you know nmap is a network mapper and it was maintained by Gordan Lyon and this is used by many security professions. The utility of this network mapper works in linux and windows also. The purpose of having a nmap server is,that it allows for an administrator to quickly and through learn about the system network.

It has an ability to quickly locate live hosts. And also scripting engine allows administrators to quickly create a script.

In very first what we have to knows is ,that we cannot hack what we don’t.t know so the simplest and the easy way to determine remotely what server is serving to do a port scan against it. This case we are using NMAP. Nmap is the application of choice for this task.

When you8 hit the Nmap commands,

You will display that there will be an anonymous logins which are permitted. Then we have to check to what is stored on the FTP server.

And also there will banner reveals which is specifying server is being used and its versions as :Vsftpd 2.3.4 and we should have a good research if this server has any unknown vulnerabilities.

In here of course I have used the way how we can exploit this backdoor vulnerability using Metasploit framework.

Lets see how I have done that

In first case we have to keep all thr required services , we have to run some codes in the terminal to active that services. In below picture it will show what are commands we have to run

A screenshot of a computer

Description automatically generated

So to remotely access to the metasploitable2 platform we have to take the relevant ip address which is relevant to natnetwork

A screenshot of a cell phone

Description automatically generated

In here the ip address is 10.0.2.5

We have to type msfconsole that is select the backdoor exploit using another command.A screenshot of a cell phone

Description automatically generated

A screenshot of a computer

Description automatically generated

Then we have to use another platform. In my case I have used kali linux.. in there we have to run some set commands:

Set RHOSTS<IP address>

A close up of a screen

Description automatically generated

Then we have to run this

After running this it will display something.

A close up of text on a black background

Description automatically generated

The out put will display as backdoor service has been spawned

While this is running we have to type id to check whether the backdoor has accessed to the relevant roots.

A close up of text on a black background

Description automatically generated

When we press the command cat /etc/shadow it will display the malicious set of code that can be also used to remotely controlled is metasploitable 2 server

A screenshot of a cell phone

Description automatically generated

Then we have to type sudo nano /etc/shadow command in the metasploitable 2 platform. And then we have to check whether the same outout will be displaying as in the kali linux version. Is it so then you have successfully exploited the VSFTPD version 2.3.4 backdoor which is used to control any platform remotely.

A screen shot of a computer

Description automatically generated

References used to take information

<https://www.cyberciti.biz/faq/cve-2015-0235-patch-ghost-on-debian-ubuntu-fedora-centos-rhel-linux/>

<https://www.acunetix.com/vulnerabilities/web/the-ghost-vulnerability/>

<https://www.cyberciti.biz/faq/cve-2015-0235-ghost-glibc-buffer-overflow-linux-test-program/>

<https://www.thegeekstuff.com/2012/08/lsof-command-examples/>

<https://ghost.org/docs/concepts/vulnerabilities/>