Exploitation Tutorial: Patching VSFTPD Backdoor

Christopher Raley

Department of Computer Science, University of Virginia

6/3/2018

This document presents a tutorial for patching a known backdoor vulnerability on the Metasploitable 2 VM. There are step-by-step instructions on how to properly use OpenVAS to first identify the backdoor, then using it to install a patch to fix it. This tutorial assumes that you already have the Kali Attacker VM and Metasploitable VM installed on your machine. It is also required for the Kali Attacker VM to have OpenVAS installed already. This content has been provided for education purposes only.

Introduction

Recall from the previous tutorial where we scanned Metasploitable 2 for vulnerabilities and decided to exploit a certain vulnerability. In the end, we ended up gaining root access through a reverse shell from the Kali Attacker's machine. In this tutorial, we will work with a framework called OpenVAS (should have installed it in previous tutorial) and we will use it to find the backdoor vulnerability. Once we find this backdoor vulnerability within OpenVAS, we will find a solution that is suggested by OpenVAS in order to patch that specific version of VSFTPD so that the vulnerability does not exist anymore. In order to confirm that it is patched, we will run a scan in OpenVAS again.

Finding A Solution

We will log into OpenVAS and identify the backdoor we are trying to find a solution for.

1. Open up a terminal in Kali and start OpenVAS
    - Recall that you use “openvas-start”
    - Look at installation tutorial if errors come up

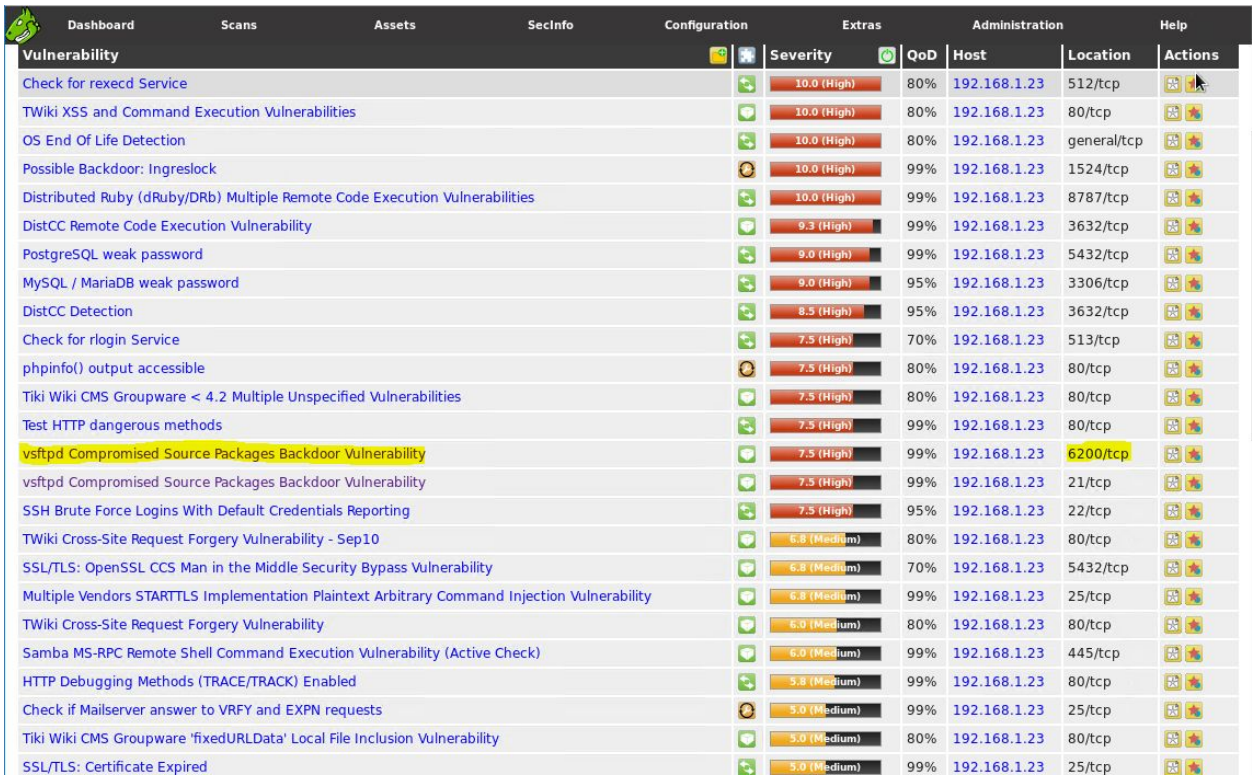
2. Log into OpenVAS with the proper credentials for “admin”

3. Go to the results of the scans and look for the scan that we did for the installation tutorial for OpenVAS

Date	Status	Task	Severity	Scan Results					Actions
				High	Medium	Low	Log	False Pos.	
Thu May 31 06:37:51 2018	Done	Scan Metasploitable 2	10.0 (High)	16	28	3	75	0	

vApply to page contents

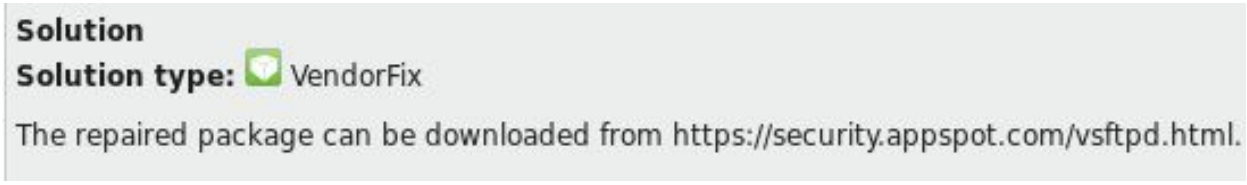
4. Look through the list of vulnerabilities until you find “vsftpd Compromised Source Packages Backdoor Vulnerability” where the location is “6200/tcp” and click on it



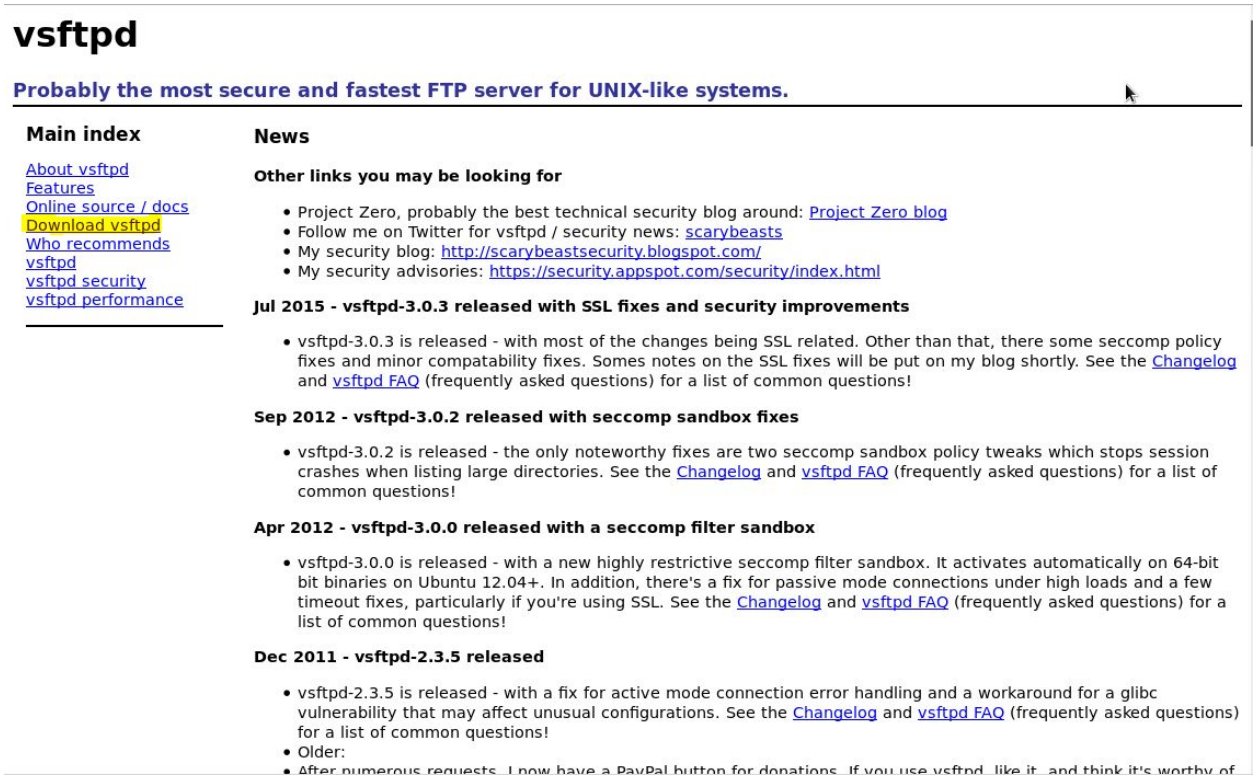
Dashboard | Scans | Assets | SecInfo | Configuration | Extras | Administration | Help

Vulnerability	Severity	QoD	Host	Location	Actions
Check for rexecd Service	10.0 (High)	80%	192.168.1.23	512/tcp	
TWiki XSS and Command Execution Vulnerabilities	10.0 (High)	80%	192.168.1.23	80/tcp	
OS End Of Life Detection	10.0 (High)	80%	192.168.1.23	general/tcp	
Possible Backdoor: Ingreslock	10.0 (High)	99%	192.168.1.23	1524/tcp	
Distributed Ruby (dRuby/DRb) Multiple Remote Code Execution Vulnerabilities	10.0 (High)	99%	192.168.1.23	8787/tcp	
DistCC Remote Code Execution Vulnerability	9.3 (High)	99%	192.168.1.23	3632/tcp	
PostgreSQL weak password	9.0 (High)	99%	192.168.1.23	5432/tcp	
MySQL / MariaDB weak password	9.0 (High)	95%	192.168.1.23	3306/tcp	
DistCC Detection	8.5 (High)	95%	192.168.1.23	3632/tcp	
Check for rlogin Service	7.5 (High)	70%	192.168.1.23	513/tcp	
phpinfo() output accessible	7.5 (High)	80%	192.168.1.23	80/tcp	
Tiki Wiki CMS Groupware < 4.2 Multiple Unspecified Vulnerabilities	7.5 (High)	80%	192.168.1.23	80/tcp	
Test HTTP dangerous methods	7.5 (High)	99%	192.168.1.23	80/tcp	
vsftpd Compromised Source Packages Backdoor Vulnerability	7.5 (High)	99%	192.168.1.23	6200/tcp	
vsftpd Compromised Source Packages Backdoor Vulnerability	7.5 (High)	99%	192.168.1.23	21/tcp	
SSH Brute Force Logins With Default Credentials Reporting	7.5 (High)	95%	192.168.1.23	22/tcp	
TWiki Cross-Site Request Forgery Vulnerability - Sep10	6.8 (Medium)	80%	192.168.1.23	80/tcp	
SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability	6.8 (Medium)	70%	192.168.1.23	5432/tcp	
Multiple Vendors STARTTLS Implementation Plaintext Arbitrary Command Injection Vulnerability	6.8 (Medium)	99%	192.168.1.23	25/tcp	
TWiki Cross-Site Request Forgery Vulnerability	6.0 (Medium)	80%	192.168.1.23	80/tcp	
Samba MS-RPC Remote Shell Command Execution Vulnerability (Active Check)	6.0 (Medium)	99%	192.168.1.23	445/tcp	
HTTP Debugging Methods (TRACE/TRACK) Enabled	5.8 (Medium)	99%	192.168.1.23	80/tcp	
Check if Mailserver answer to VRFY and EXPN requests	5.0 (Medium)	99%	192.168.1.23	25/tcp	
Tiki Wiki CMS Groupware 'fixedURLData' Local File Inclusion Vulnerability	5.0 (Medium)	80%	192.168.1.23	80/tcp	
SSL/TLS: Certificate Expired	5.0 (Medium)	99%	192.168.1.23	25/tcp	

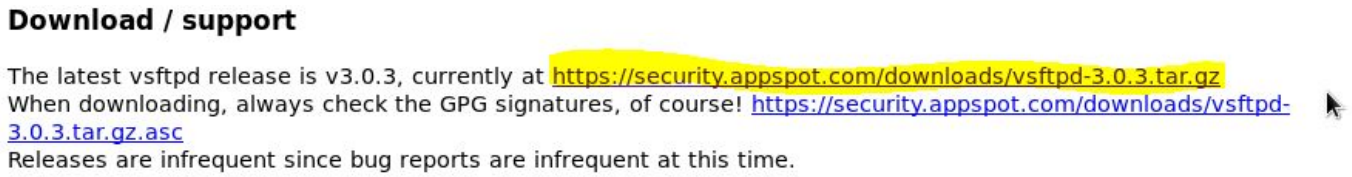
5. On that page you will find a section where a solution is presented. Go to the link that the solution says to go to in order to update vsftpd



6. You will end up on the main page for vsftpd. Click on the “Download vsftpd” tab on the left hand side



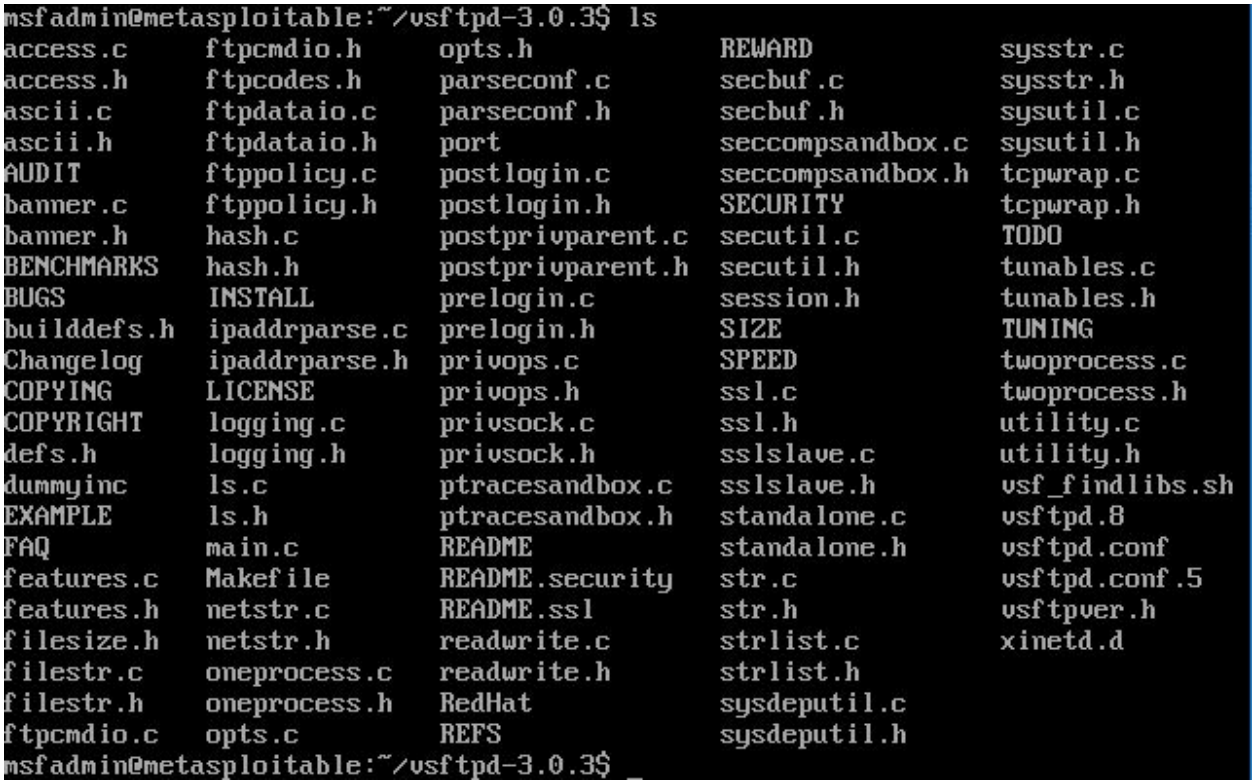
7. Take note of the download link for the tar file that holds the up-to-date version of vsftpd



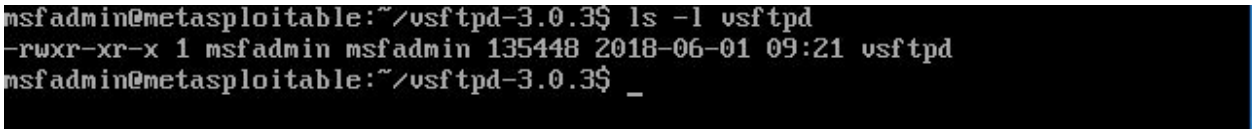
8. Switch to your Metasploitable 2 VM and type the following command to download the file: “wget https://security.appspot.com/downloads/vsftpd-3.0.3.tar.gz --no-check-certifcate”
    - Wget is a command used to download files via terminal

9. In the same directory as where you downloaded the tar file, use the following command to extract the files within it: “tar -xvf vsftpd-3.0.3.tar.gz”

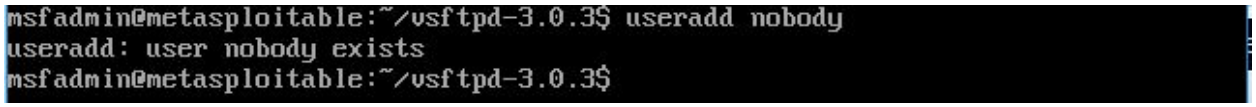
10. You can now change into the directory “vsftpd-3.0.3” where you can read the “INSTALL” file on how to install the new version, however, we will take you through this process in the tutorial



11. Type the following (assuming you’re in the directory): “make” which should create a vsftpd binary file
    - You can make sure that the file was indeed created by using the following command: “ls -l vsftpd”



12. It is required for the user “nobody” to exist within the system so to ensure that it has been created use “useradd nobody”



13. The installation also requires an empty directory at /usr/share/empty, so to ensure that has been created use “mkdir /usr/share/empty”

```
msfadmin@metasploitable:~/vsftpd-3.0.3$ mkdir /usr/share/empty/
mkdir: cannot create directory `/usr/share/empty/': File exists
msfadmin@metasploitable:~/vsftpd-3.0.3$
```

14. We will also need the user “ftp” to exist, so use the following:
    - Sudo mkdir /var/ftp/
    - Sudo useradd -d /var/ftp ftp
    - Sudo chown root.root /var/ftp
    - Sudo chmod og-w /var/ftp

```
msfadmin@metasploitable:~/vsftpd-3.0.3$ sudo mkdir /var/ftp
mkdir: cannot create directory `/var/ftp': File exists
msfadmin@metasploitable:~/vsftpd-3.0.3$ sudo useradd -d /var/ftp ftp
useradd: user ftp exists
msfadmin@metasploitable:~/vsftpd-3.0.3$ sudo chown root.root /var/ftp
msfadmin@metasploitable:~/vsftpd-3.0.3$ sudo chmod og-w /var/ftp
msfadmin@metasploitable:~/vsftpd-3.0.3$ _
```

15. Finally complete the installation by using following commands:
    - Sudo cp vsftpd /usr/local/sbin/vsftpd
    - Sudo cp vsftpd.conf.5 /usr/local/man/man5
    - Sudo cp vsftpd.8 /usr/local/man/man8
    - Sudo cp vsftpd.conf /etc

```
msfadmin@metasploitable:~/vsftpd-3.0.3$ sudo cp vsftpd /usr/local/sbin/vsftpd
msfadmin@metasploitable:~/vsftpd-3.0.3$ sudo cp vsftpd.conf.5 /usr/local/man/man
5
msfadmin@metasploitable:~/vsftpd-3.0.3$ sudo cp vsftpd.8 /usr/local/man/man8
msfadmin@metasploitable:~/vsftpd-3.0.3$ sudo cp vsftpd.conf /etc/
msfadmin@metasploitable:~/vsftpd-3.0.3$
```

Ensure Exploit Is Patched

1. On the Metasploitable machine type in the following to start the new vsftpd service: “/etc/init.d/xinetd stop”
2. Use “sudo vim /etc/vsftpd.conf” and make sure that listen=YES is commented out

```
# users to NOT chroot().
# (Warning! chroot'ing can be very dangerous. If using chroot, make sure that
# the user does not have write access to the top level directory within the
# chroot)
#chroot_local_user=YES
#chroot_list_enable=YES
# (default follows)
#chroot_list_file=/etc/vsftpd.chroot_list
#
# You may activate the "-R" option to the builtin ls. This is disabled by
# default to avoid remote users being able to cause excessive I/O on large
# sites. However, some broken FTP clients such as "ncftp" and "mirror" assume
# the presence of the "-R" option, so there is a strong case for enabling it.
#ls_recurse_enable=YES
#
# When "listen" directive is enabled, vsftpd runs in standalone mode and
# listens on IPv4 sockets. This directive cannot be used in conjunction
# with the listen_ipv6 directive.
#listen=YES
#
# This directive enables listening on IPv6 sockets. To listen on IPv4 and IPv6
# sockets, you must run two copies of vsftpd with two configuration files.
# Make sure, that one of the listen options is commented !!
#listen_ipv6=YES
```

3. Start the service by typing: “/usr/local/sbin/vsftpd &”

4. Switch back to the Kali machine and log back into OpenVAS. We will run the same scan that we did previously.

5. Once the scan has finished, view the results and we will see that there is no longer the vulnerability for vsftpd's backdoor.

Vulnerability	Severity	QoD	Host	Location
OS End Of Life Detection	10.0 (High)	80%	192.168.1.23	general/tcp
Check for rexecd Service	10.0 (High)	80%	192.168.1.23	512/tcp
TWiki XSS and Command Execution Vulnerabilities	10.0 (High)	80%	192.168.1.23	80/tcp
Distributed Ruby (dRuby/DRb) Multiple Remote Code Execution Vulnerabilities	10.0 (High)	99%	192.168.1.23	8787/tcp
Possible Backdoor: Ingreslock	10.0 (High)	99%	192.168.1.23	1524/tcp
DistCC Remote Code Execution Vulnerability	9.3 (High)	99%	192.168.1.23	3632/tcp
MySQL / MariaDB weak password	9.0 (High)	95%	192.168.1.23	3306/tcp
PostgreSQL weak password	9.0 (High)	99%	192.168.1.23	5432/tcp
DistCC Detection	8.5 (High)	95%	192.168.1.23	3632/tcp
Check for rlogin Service	7.5 (High)	70%	192.168.1.23	513/tcp
phpinfo() output accessible	7.5 (High)	80%	192.168.1.23	80/tcp
Tiki Wiki CMS Groupware < 4.2 Multiple Unspecified Vulnerabilities	7.5 (High)	80%	192.168.1.23	80/tcp
Test HTTP dangerous methods	7.5 (High)	99%	192.168.1.23	80/tcp
Check for Backdoor in UnrealIRCd	7.5 (High)	70%	192.168.1.23	6667/tcp
SSH Brute Force Logins With Default Credentials Reporting	7.5 (High)	95%	192.168.1.23	22/tcp