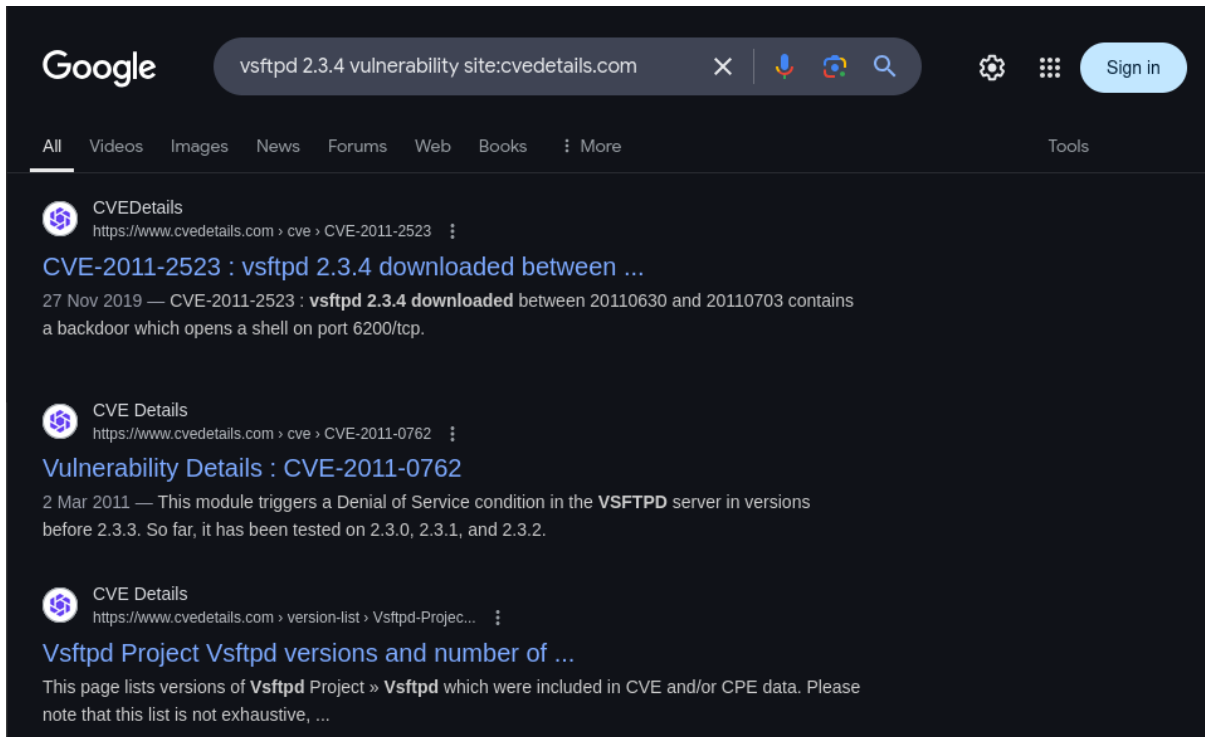


## Task 2: Vulnerability Research with Google Dorking

1. Find vulnerabilities related the port using its version. We found this using the ‘-sC -sV’ flags with nmap.



This screenshot shows the Google search interface with the query 'vsftpd 2.3.4 vulnerability site:cvedetails.com'. The search results are filtered to show only pages from cvedetails.com. The top result is 'CVE-2011-2523 : vsftpd 2.3.4 downloaded between ...' dated 27 Nov 2019, describing a backdoor on port 6200/tcp. The second result is 'Vulnerability Details : CVE-2011-0762' dated 2 Mar 2011, describing a Denial of Service condition. The third result is 'Vsftpd Project Vsftpd versions and number of ...' which lists versions included in CVE and CPE data.

Google

vsftpd 2.3.4 vulnerability site:cvedetails.com

All Videos Images News Forums Web Books More Tools

**CVEDetails**  
https://www.cvedetails.com › cve › CVE-2011-2523

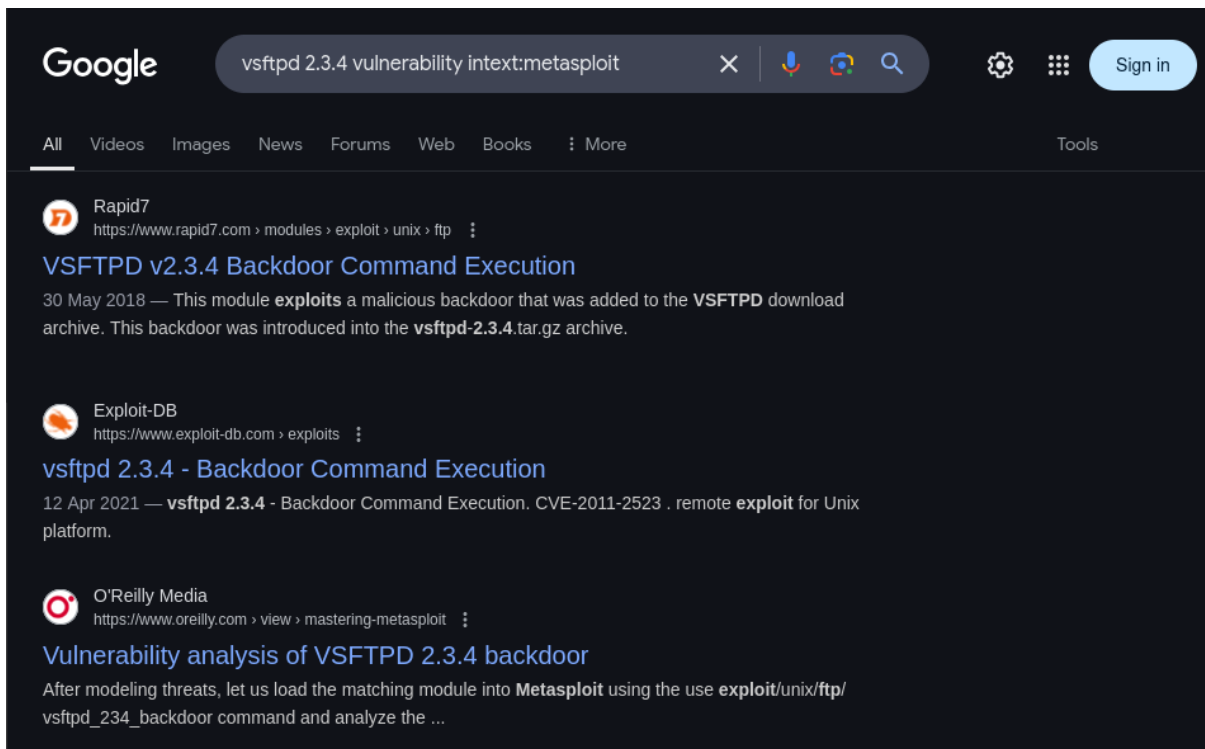
**CVE-2011-2523 : vsftpd 2.3.4 downloaded between ...**  
27 Nov 2019 — CVE-2011-2523 : **vsftpd 2.3.4 downloaded** between 20110630 and 20110703 contains a backdoor which opens a shell on port 6200/tcp.

**CVE Details**  
https://www.cvedetails.com › cve › CVE-2011-0762

**Vulnerability Details : CVE-2011-0762**  
2 Mar 2011 — This module triggers a Denial of Service condition in the **VSFTPD** server in versions before 2.3.3. So far, it has been tested on 2.3.0, 2.3.1, and 2.3.2.

**CVE Details**  
https://www.cvedetails.com › version-list › Vsftpd-Projec...

**Vsftpd Project Vsftpd versions and number of ...**  
This page lists versions of **Vsftpd** Project » **Vsftpd** which were included in CVE and/or CPE data. Please note that this list is not exhaustive, ...



This screenshot shows the Google search interface with the query 'vsftpd 2.3.4 vulnerability intext:metasploit'. The search results are filtered to show only pages containing the word 'metasploit'. The top result is 'VSFTPD v2.3.4 Backdoor Command Execution' from Rapid7, dated 30 May 2018, describing a malicious backdoor. The second result is 'vsftpd 2.3.4 - Backdoor Command Execution' from Exploit-DB, dated 12 Apr 2021, describing a remote exploit for Unix. The third result is 'Vulnerability analysis of VSFTPD 2.3.4 backdoor' from O'Reilly Media, which discusses loading the module into Metasploit.

Google

vsftpd 2.3.4 vulnerability intext:metasploit

All Videos Images News Forums Web Books More Tools

**Rapid7**  
https://www.rapid7.com › modules › exploit › unix › ftp

**VSFTPD v2.3.4 Backdoor Command Execution**  
30 May 2018 — 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.

**Exploit-DB**  
https://www.exploit-db.com › exploits

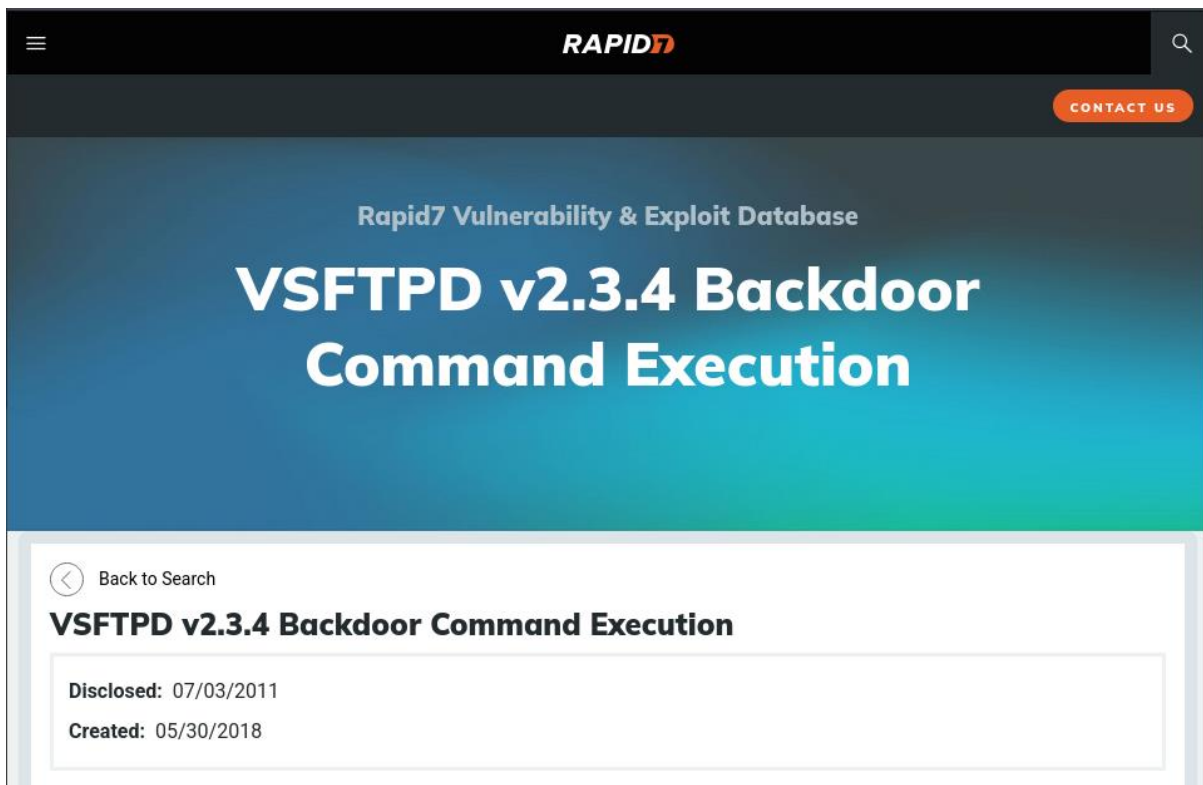
**vsftpd 2.3.4 - Backdoor Command Execution**  
12 Apr 2021 — **vsftpd 2.3.4** - Backdoor Command Execution. CVE-2011-2523 . remote **exploit** for Unix platform.

**O'Reilly Media**  
https://www.oreilly.com › view › mastering-metasploit

**Vulnerability analysis of VSFTPD 2.3.4 backdoor**  
After modeling threats, let us load the matching module into **Metasploit** using the use **exploit/unix/ftp/vsftpd\_234\_backdoor** command and analyze the ...

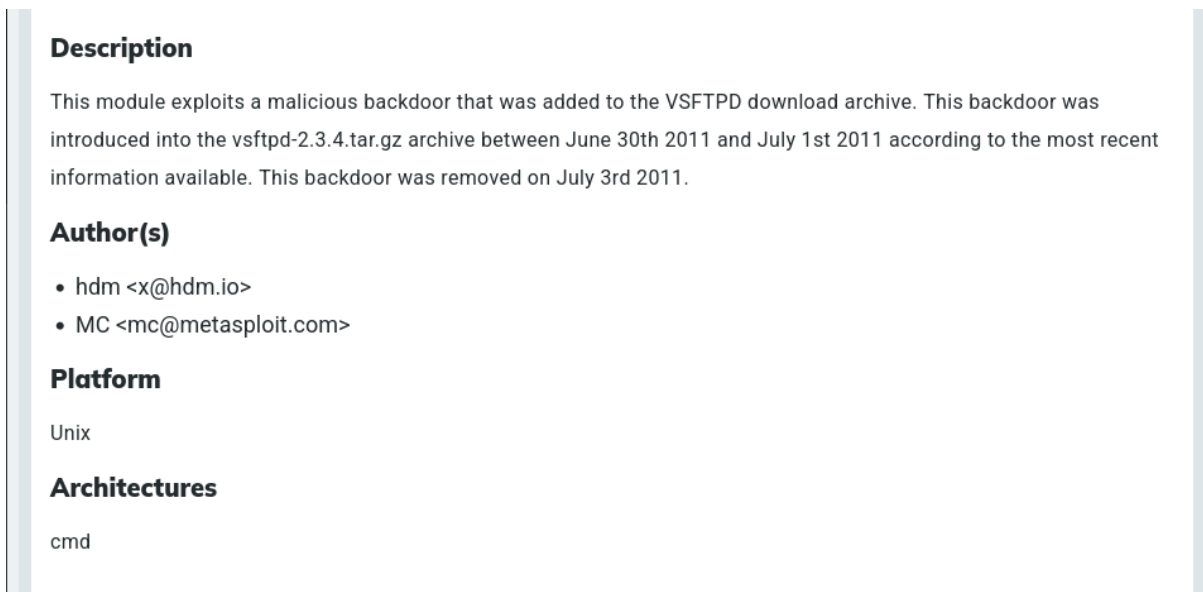
NOTE: Using 'site' we can force the search engine to return websites from cvedetails.com only. There is also 'filetype' (specify the filetype) and 'intext' (filters searches that use the specified word).

2. Using the search results display what you have learned



The screenshot shows the Rapid7 Vulnerability & Exploit Database interface. At the top, there is a navigation bar with the Rapid7 logo and a search icon. Below the navigation bar, the text "Rapid7 Vulnerability & Exploit Database" is displayed. The main heading is "VSFTPD v2.3.4 Backdoor Command Execution". Below the heading, there is a section with a "Back to Search" link and the title "VSFTPD v2.3.4 Backdoor Command Execution". Underneath, the "Disclosed" date is "07/03/2011" and the "Created" date is "05/30/2018".

NOTE: We can see that VSFTPD has been disclosed in 2011. It is very old and potentially outdated.



The screenshot shows the detailed view of the exploit entry. The "Description" section states: "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 "Author(s)" section lists two authors: "hdm <x@hdm.io>" and "MC <mc@metasploit.com>". The "Platform" section lists "Unix". The "Architectures" section lists "cmd".

NOTE: Scrolling down we can see a description for a exploit for this model, the authors involved, platform and what architectures are used.

## Module Options

To display the available options, load the module within the Metasploit console and run the commands 'show options' or 'show advanced':

```
1 msf > use exploit/unix/ftp/vsftpd_234_backdoor
2 msf exploit(vsftpd_234_backdoor) > show targets
3     ...targets...
4 msf exploit(vsftpd_234_backdoor) > set TARGET < target-id >
5 msf exploit(vsftpd_234_backdoor) > show options
6     ...show and set options...
7 msf exploit(vsftpd_234_backdoor) > exploit
```

NOTE: Finally, we can see that a Metasploit module exists for this vulnerability, and it includes the steps to use it.

NOTE: Exploit DB is another website that provides a vulnerability database. It includes the backend code of an exploit that takes advantage of the service version. This can be used to do manual exploitation if the Metasploit module doesn't work.

Conclusion:

- Sites like exploit.db and rapid7 are powerful tools when it comes to vulnerability research
- Google Dorking is an effective way to enhance searching capabilities