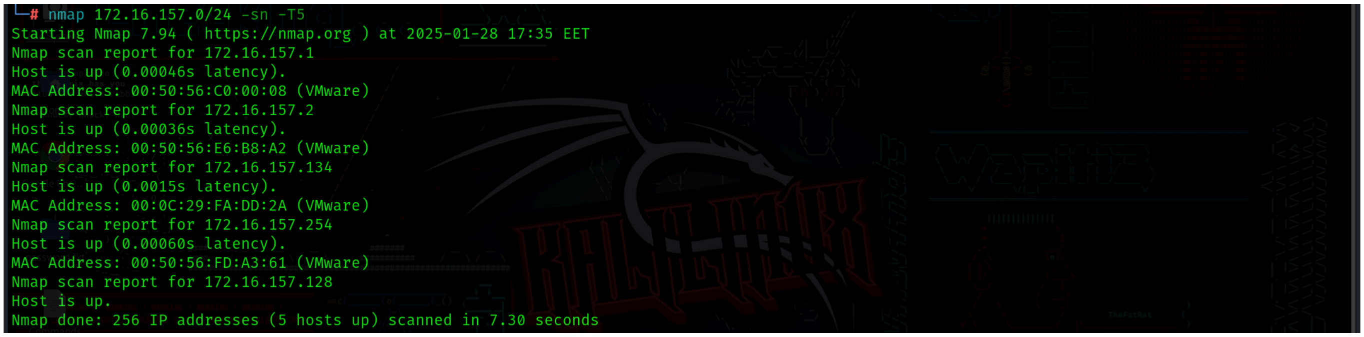
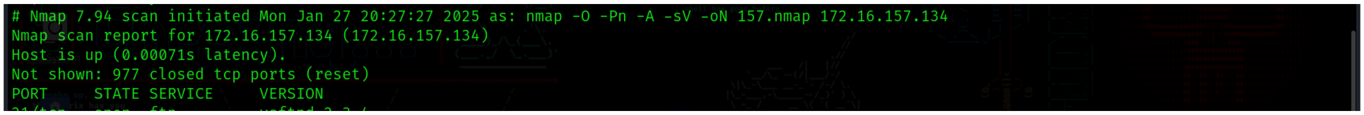
First we are using -sn to discover our target



```
└─# nmap 172.16.157.0/24 -sn -T5
Starting Nmap 7.94 ( https://nmap.org ) at 2025-01-28 17:35 EET
Nmap scan report for 172.16.157.1
Host is up (0.00046s latency).
MAC Address: 00:50:56:C0:00:08 (VMware)
Nmap scan report for 172.16.157.2
Host is up (0.00036s latency).
MAC Address: 00:50:56:E6:B8:A2 (VMware)
Nmap scan report for 172.16.157.134
Host is up (0.0015s latency).
MAC Address: 00:0C:29:FA:DD:2A (VMware)
Nmap scan report for 172.16.157.254
Host is up (0.00060s latency).
MAC Address: 00:50:56:FD:A3:61 (VMware)
Nmap scan report for 172.16.157.128
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 7.30 seconds
```

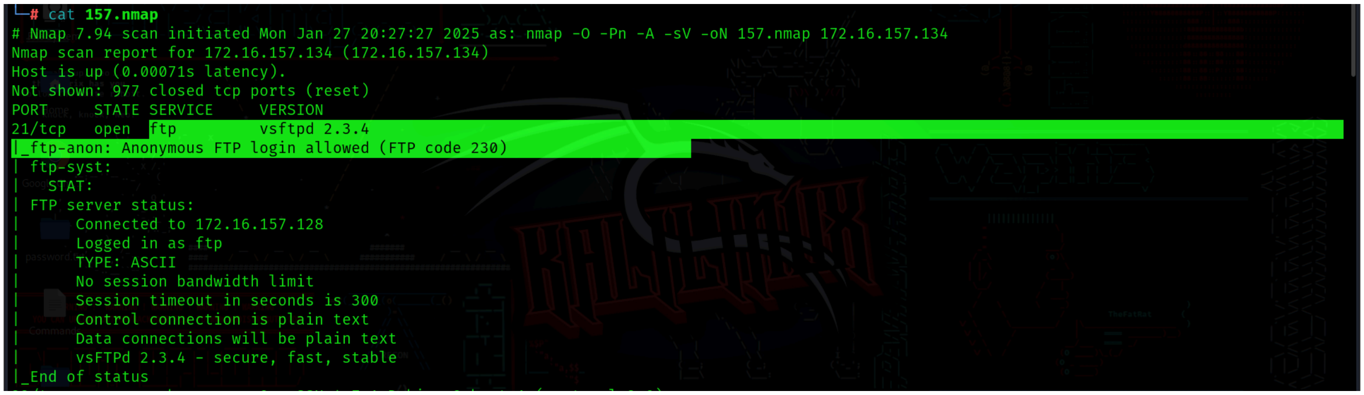
And here we go, we reaching out our traget "172.16.157.134"

Now we are going to do some scanning techniques for OS and Version detection

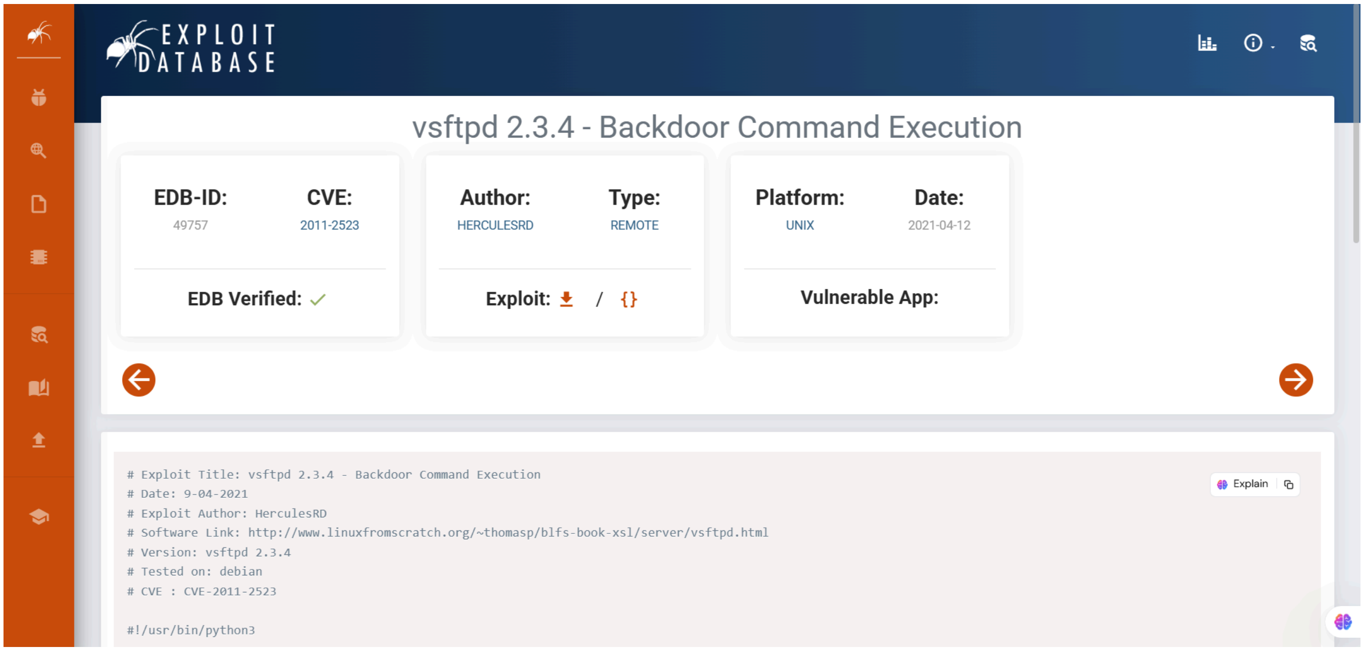


```
# Nmap 7.94 scan initiated Mon Jan 27 20:27:27 2025 as: nmap -O -Pn -A -sV -oN 157.nmap 172.16.157.134
Nmap scan report for 172.16.157.134 (172.16.157.134)
Host is up (0.00071s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
```

After scanning we found out some vulnerable ports



```
└─# cat 157.nmap
# Nmap 7.94 scan initiated Mon Jan 27 20:27:27 2025 as: nmap -O -Pn -A -sV -oN 157.nmap 172.16.157.134
Nmap scan report for 172.16.157.134 (172.16.157.134)
Host is up (0.00071s latency).
Not shown: 977 closed tcp ports (reset)
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 172.16.157.128
|      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
```



vsftpd 2.3.4 - Backdoor Command Execution

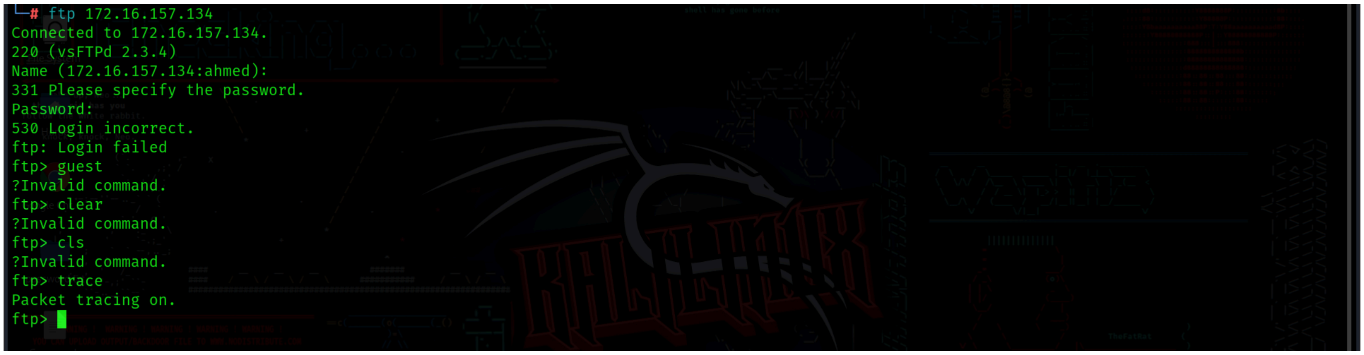
EDB-ID:	CVE:	Author:	Type:	Platform:	Date:
49757	2011-2523	HERCULESRD	REMOTE	UNIX	2021-04-12

EDB Verified: ✓

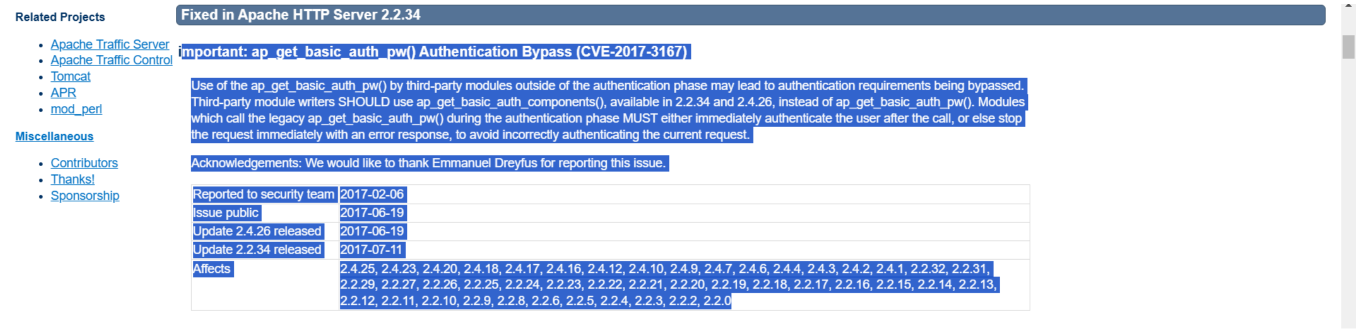
Exploit: / {}

Vulnerable App:

```
# Exploit Title: vsftpd 2.3.4 - Backdoor Command Execution
# Date: 9-04-2021
# Exploit Author: HerculesRD
# Software Link: http://www.linuxfromscratch.org/~thomasp/blfs-book-xsl/server/vsftpd.html
# Version: vsftpd 2.3.4
# Tested on: debian
# CVE : CVE-2011-2523

#!/usr/bin/python3
```



```
└─# ftp 172.16.157.134
Connected to 172.16.157.134.
220 (vsFTPd 2.3.4)
Name (172.16.157.134:ahmed):
331 Please specify the password.
Password:
530 Login incorrect.
ftp: Login failed
ftp> guest
?Invalid command.
ftp> clear
?Invalid command.
ftp> cls
?Invalid command.
ftp> trace
Packet tracing on.
ftp> 
```



Related Projects

- Apache Traffic Server
- Apache Traffic Control
- Tomcat
- APR
- mod_perl

Miscellaneous

- Contributors
- Thanks!
- Sponsorship

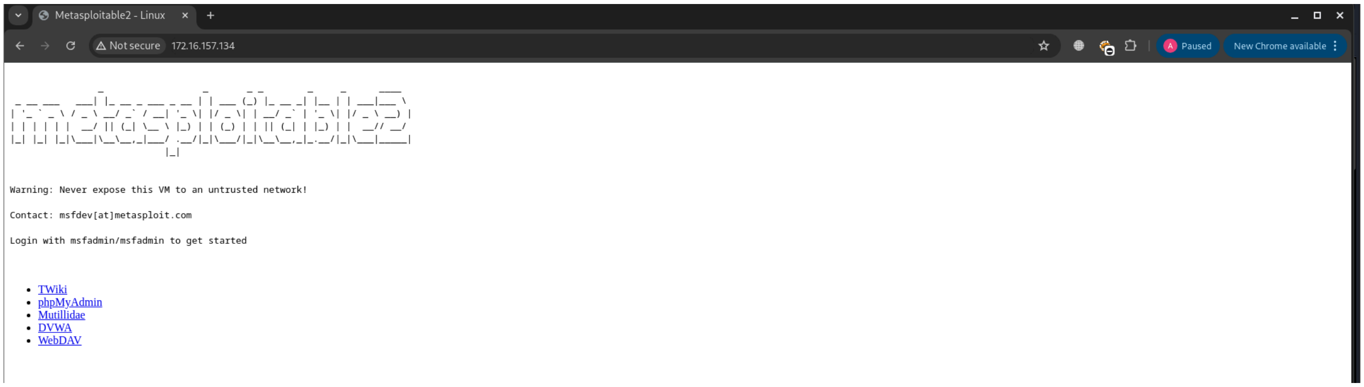
Fixed in Apache HTTP Server 2.2.34

important: ap_get_basic_auth_pw() Authentication Bypass (CVE-2017-3167)

Use of the ap_get_basic_auth_pw() by third-party modules outside of the authentication phase may lead to authentication requirements being bypassed. Third-party module writers SHOULD use ap_get_basic_auth_components(), available in 2.2.34 and 2.4.26, instead of ap_get_basic_auth_pw(). Modules which call the legacy ap_get_basic_auth_pw() during the authentication phase MUST either immediately authenticate the user after the call, or else stop the request immediately with an error response, to avoid incorrectly authenticating the current request.

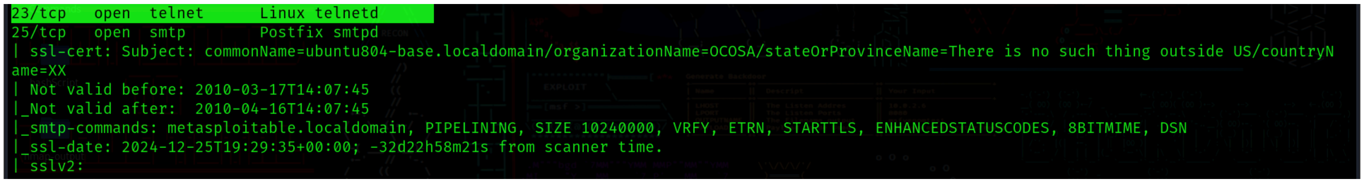
Acknowledgements: We would like to thank Emmanuel Dreyfus for reporting this issue.

Reported to security team	2017-02-06
Issue public	2017-06-19
Update 2.4.26 released	2017-06-19
Update 2.2.34 released	2017-07-11
Affects	2.4.25, 2.4.23, 2.4.20, 2.4.18, 2.4.17, 2.4.16, 2.4.12, 2.4.10, 2.4.9, 2.4.7, 2.4.6, 2.4.4, 2.4.3, 2.4.2, 2.4.1, 2.2.32, 2.2.31, 2.2.29, 2.2.27, 2.2.26, 2.2.25, 2.2.24, 2.2.23, 2.2.22, 2.2.21, 2.2.20, 2.2.19, 2.2.18, 2.2.17, 2.2.16, 2.2.15, 2.2.14, 2.2.13, 2.2.12, 2.2.11, 2.2.10, 2.2.9, 2.2.8, 2.2.6, 2.2.5, 2.2.4, 2.2.3, 2.2.2, 2.2.0

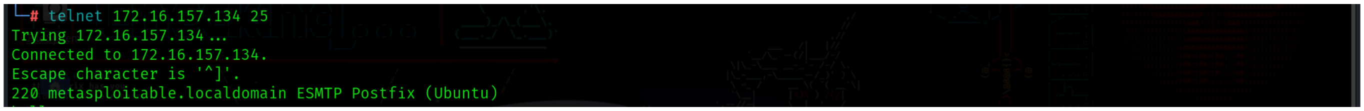


```
                _                  _       _ _        _     _      ____  
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \ 
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/ 
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|                                          


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started
```

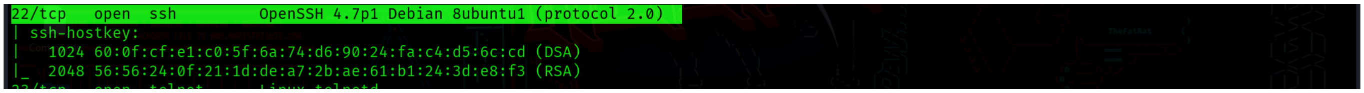
- TWiki
- phpMyAdmin
- Mutillidae
- DVWA
- WebDAV



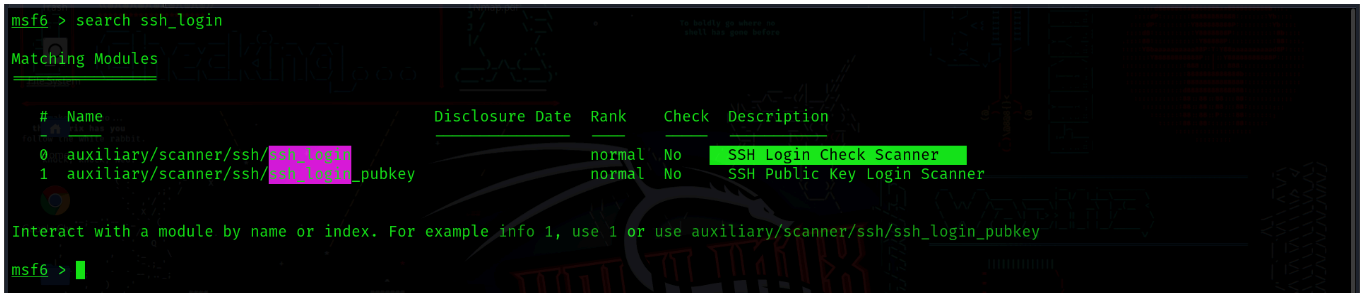
```
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryN
ame=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
|_ssl-date: 2024-12-25T19:29:35+00:00; -32d22h58m21s from scanner time.
| sslv2:
```



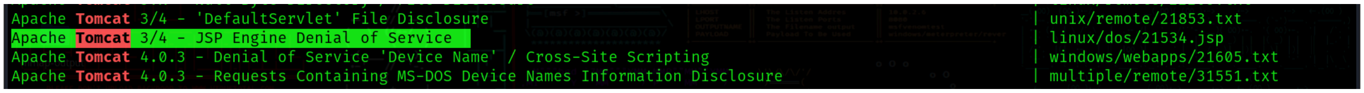
```
└─# telnet 172.16.157.134 25
Trying 172.16.157.134 ...
Connected to 172.16.157.134.
Escape character is '^]'.
220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
```



```
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp   open  telnet      Linux telnetd
```



```
msf6 > search ssh_login

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

   #  Name                                        Disclosure Date  Rank    Check  Description
   -  ----                                        ---------------  ----    -----  -----------
   0  auxiliary/scanner/ssh/ssh_login                              normal  No     SSH Login Check Scanner
   1  auxiliary/scanner/ssh/ssh_login_pubkey                       normal  No     SSH Public Key Login Scanner


Interact with a module by name or index. For example info 1, use 1 or use auxiliary/scanner/ssh/ssh_login_pubkey

msf6 >
```



```
Apache Tomcat 3/4 - 'DefaultServlet' File Disclosure                                                 | unix/remote/21853.txt
Apache Tomcat 3/4 - JSP Engine Denial of Service                                                     | linux/dos/21534.jsp
Apache Tomcat 4.0.3 - Denial of Service 'Device Name' / Cross-Site Scripting                         | windows/webapps/21605.txt
Apache Tomcat 4.0.3 - Requests Containing MS-DOS Device Names Information Disclosure                 | multiple/remote/31551.txt
```