4 ways to SMTP Enumeration

posted in PENETRATION TESTING on SEPTEMBER 25, 2017 by RAJ CHANDEL SHARE

We can also find out **version** and **valid user** of SMTP server **using telnet**. Execute following command and find out its version and valid user.

Telnet

telnet 192.168.1.107 25

From given image you can observe that it has successfully shown "220 mail.ignite.lab ESMTP Postfix" has been installed on target machine.

You can guess for valid user account through following command and if you receive response code 550 it means unknown user account:

vrfy raj@mail.lab.ignite

If you received message **code 250,251,252** which means server has accept the request and user account is valid.

But if you received message **code 550** it means invalid user account as shown in given image

vrfy admin@mail.ignite.lab

```
root@kali:~# telnet 192.168.1.107 25
Trying 192.168.1.107...
Connected to 192.168.1.107.
Escape character is '^]'.
220 #myhostname ESMTP Postfix (Ubuntu)
vrfy raj@mail.ignite.lab
252 2.0.0 raj@mail.ignite.lab
vrfy admin@mail.ignite.lab
550 5.1.1 <admin@mail.ignite.lab>: Recipient address rejected: User unknown in l
ocal recipient table
421 4.4.2 mail.ignite.lab Error: timeout exceeded
Connection closed by foreign host.
```


Metasploit

The SMTP service has two internal commands that allow the enumeration of users: VRFY (confirming the names of valid users) and EXPN (which reveals the actual address of user's aliases and lists of e-mail (mailing lists)). Through the implementation of these SMTP commands can reveal a list of valid users.

use auxiliary/scanner/smtp/smtp_enum

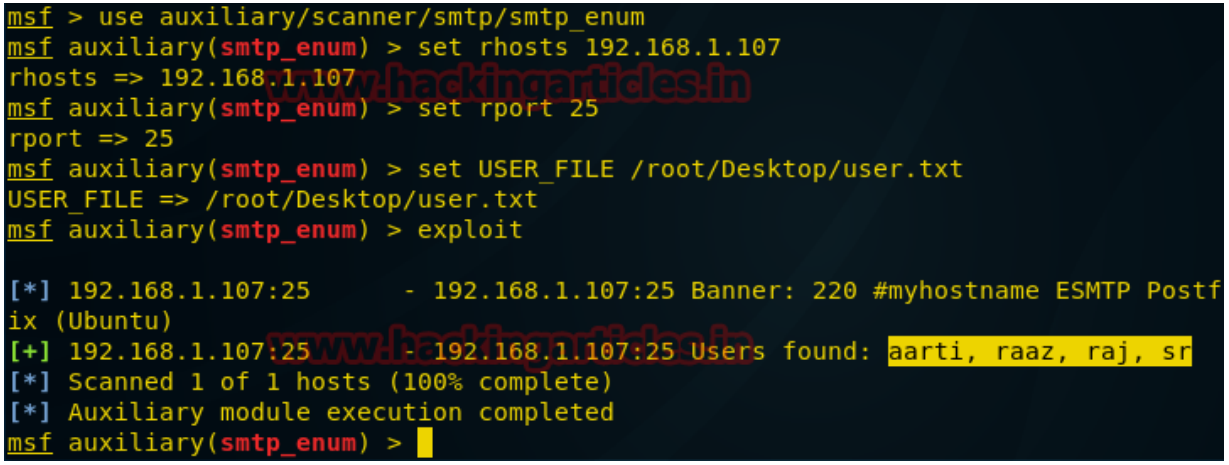
msf auxiliary(smtp_enum) > set rhosts 192.168.1.107

msf auxiliary(smtp_enum) > set rport 25

msf auxiliary(smtp_enum) > set USER_FILE /root/Desktop/user.txt

msf auxiliary(smtp_enum) > exploit

From given image you can read the valid username found in targeted server as well as it also grab SMTP banner.



smtp-user-enum

smtp-user-enum is a tool for enumerating OS-level user accounts on Solaris via the SMTP service (sendmail). Enumeration is performed by inspecting the responses to VRFY, EXPN and RCPT TO commands. It could be adapted to work against other vulnerable SMTP daemons, but this hasn't been done as of v1.0.

Type following command to enumerate username using dictionary of usernames:

smtp-user-enum -M VRFY -U /root/Desktop/user.txt -t 192.168.1.107

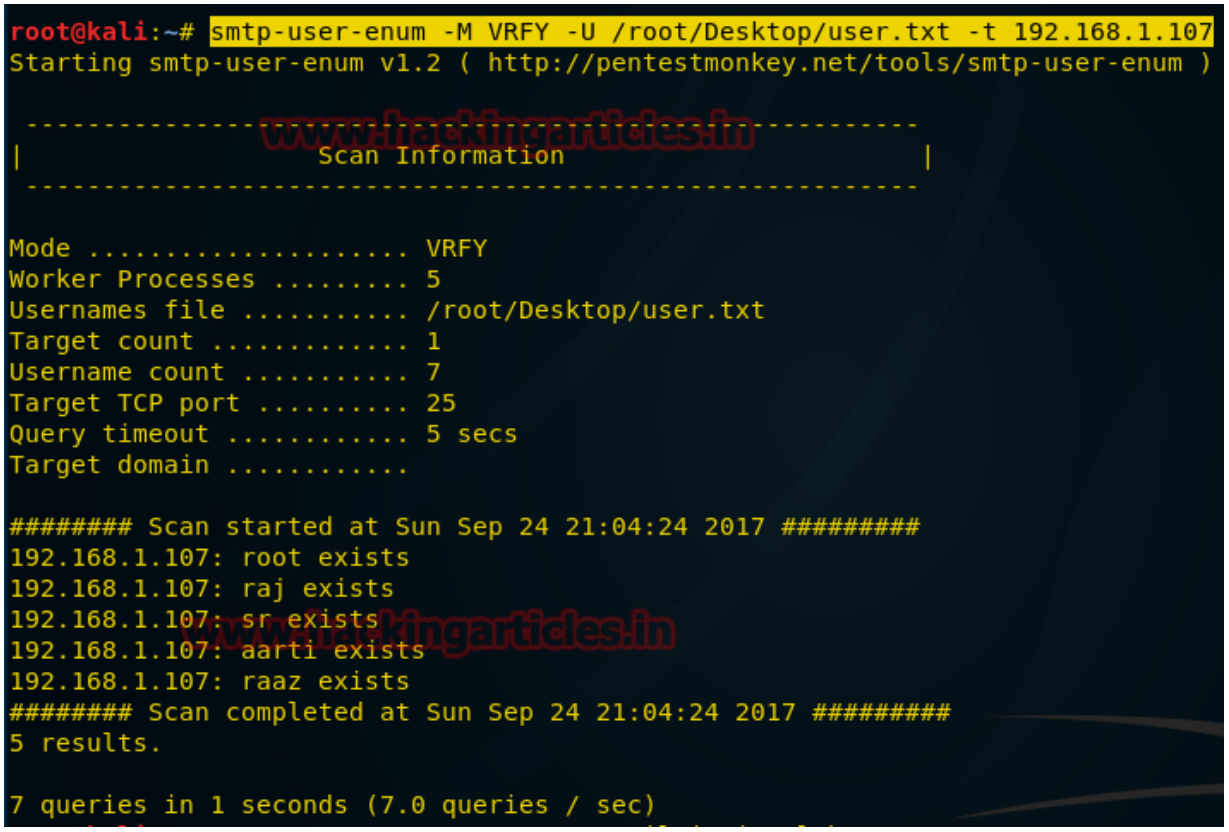
-M: mode Method to use for username guessing EXPN, VRFY or RCPT

-U: file File of usernames to check via smtp service
-t: host Server host running smtp service

Categories

- BackTrack 5 Tutorials
- Best of Hacking
- Browser Hacking
- Cryptography & Stegnography
- CTF Challenges
- Cyber Forensics
- Database Hacking
- Domain Hacking
- Email Hacking
- Footprinting
- Hacking Tools
- Kali Linux
- Nmap
- Others
- Penetration Testing
- Social Engineering Toolkit
- Trojans & Backdoors
- Website Hacking
- Window Password Hacking
- Windows Hacking Tricks
- Wireless Hacking
- Youtube Hacking

From given image you can see out of total 7 queries only 5 names are valid and exist in smtp server.



Type following command to verify user email address on mail server:

smtp-user-enum -M VRFY -D mail.ignite.lab -u raj -t 192.168.1.107

-D: dom Domain to append to supplied user list to make email addresses; Use this option when you want to guess valid email addresses instead of just usernames.

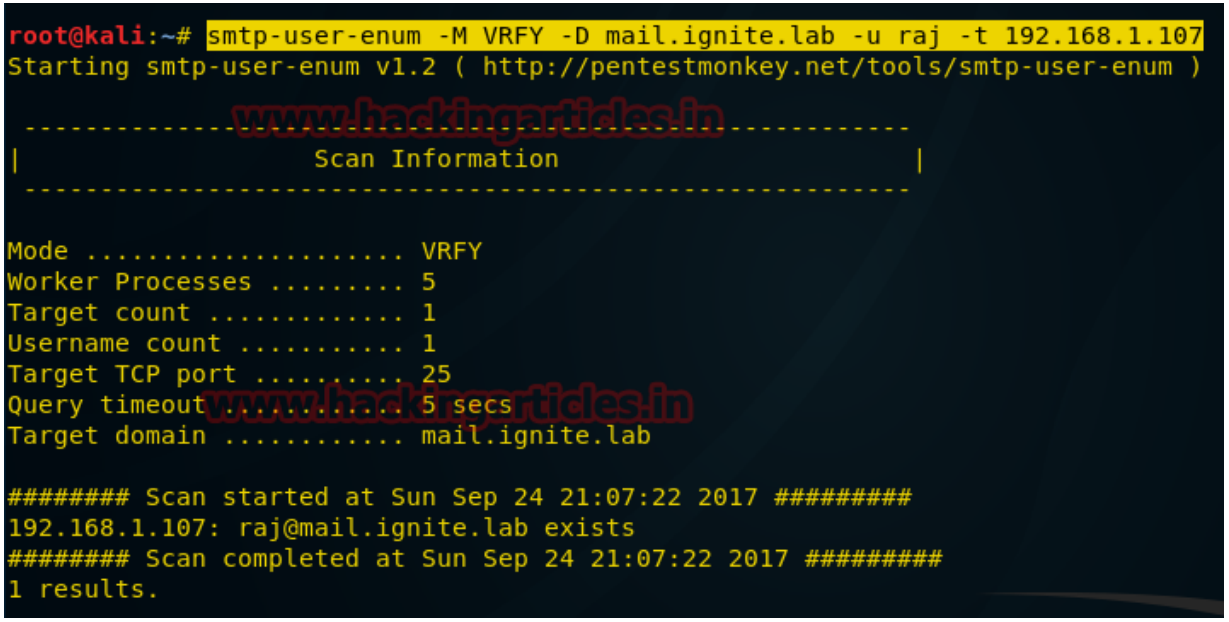
From given image you can see it has shown raj@mail.ignite.lab is valid email ID for user raj.

Articles

Select Month

Facebook Page

Be the first of your friends to like this



iSMTP

iSMTP is the kali Linux toolw which is use for testing SMTP user enumeration (RCPT TO and VRFY), internal spoofing, and relay.

Type following command to enumerate valid email ID of targeted server:

ismtp -h 192.168.1.107:25 -e /root/Desktop/email.txt

-h <host> The target IP and port (IP:port)

-e <file> Enable SMTP user enumeration testing and imports email list.

From given image you can see blue color text refer to valid email account and red color text refer to invalid account.

```
root@kali:~# ismtp -h 192.168.1.107:25 -e /root/Desktop/email.txt

------------------------------------------------------------------------
 iSMTP v1.6 - SMTP Server Tester, Alton Johnson (alton.jx@gmail.com)
------------------------------------------------------------------------

Testing SMTP server [user enumeration]: 192.168.1.107:25
Emails provided for testing: 7

Performing SMTP VRFY test...

Error: 2.0.0 root.

Performing SMTP RCPT TO test...

[+] root@mail.ignite.lab --- [ valid ]
[-] toor@mail.ignite.lab --- [ invalid ]
[-] admin@mail.ignite.lab -- [ invalid ]
[+] raj@mail.ignite.lab ---- [ valid ]
[+] sr@mail.ignite.lab ----- [ valid ]
[+] aarti@mail.ignite.lab -- [ valid ]
[+] raaz@mail.ignite.lab --- [ valid ]

Completed SMTP user enumeration test.
```

Author: Sanjeet Kumar is a Information Security Analyst | Pentester | Researcher
Contact Here

Share this:

Like this:

Loading...

ABOUT THE AUTHOR

RAJ CHANDEL

Raj Chandel is a Skilled and Passionate IT Professional especially in IT-Hacking Industry. At present other than his name he can also be called as An Ethical Hacker, A Cyber Security Expert, A Penetration Tester. With years of quality Experience in IT and software industry

PREVIOUS POST

← PENETRATION TESTING ON TELNET (PORT 23)

NEXT POST

HACK THE PRIMER VM (CTF CHALLENGE) →

1 Comment → 4 WAYS TO SMTP ENUMERATION

HRISHI February 8, 2018 at 2:18 pm

Hi there,
Command : “smtp-user-enum -M VRFY -p 25 -U /root/n.txt -t 10.11.1.22”
When i tried the below command, it shows zero results.

But when i tired using nectar or telnet, i am able to VRFY user.

Can you help or figure out why i am unable to get results using smtp-user-enum.

REPLY ↓

Leave a Reply

Your email address will not be published. Required fields are marked *

Comment

Name *

Email *

Website

Save my name, email, and website in this browser for the next time I comment.

POST COMMENT

Notify me of follow-up comments by email.

Notify me of new posts by email.