**SMTP Enumeration**

SMTP (Simple Mail Transfer Protocol) is a TCP/IP protocol for transmitting email over networks. It operates as a push protocol, initiating the sending of emails from a client to a server or between servers.

SMTP enumeration is a technique that is used to interact with mail systems that rely on the Simple Mail Transfer Protocol (SMTP) for sending emails, on the other hand, POP3 and IMAP handle email retrieval. SMTP communicates with mail exchange (MX) servers, which route emails based on DNS (Domain Name System) records.

SMTP primarily uses port 25, but port 2525 can be an alternative, and port 587 is used for encrypted, authenticated submissions. Three key SMTP commands used for enumeration are:

1. **VRFY Command**: Checks if an email address exists on the server.
2. **EXPN Command**: Shows specific email addresses in a distribution list
3. **RCPT TO Command**: Tells the recipient of the email message

**SMTP Enumeration Tools**

1. **smtp-user-enum:** The smtp-user-enum tool is designed to identify operating system-level user accounts on systems by leveraging the SMTP protocol, typically implemented by the sendmail service. This tool looks at how servers respond to specific SMTP commands such as VRFY, EXPN, and RCPT TO.

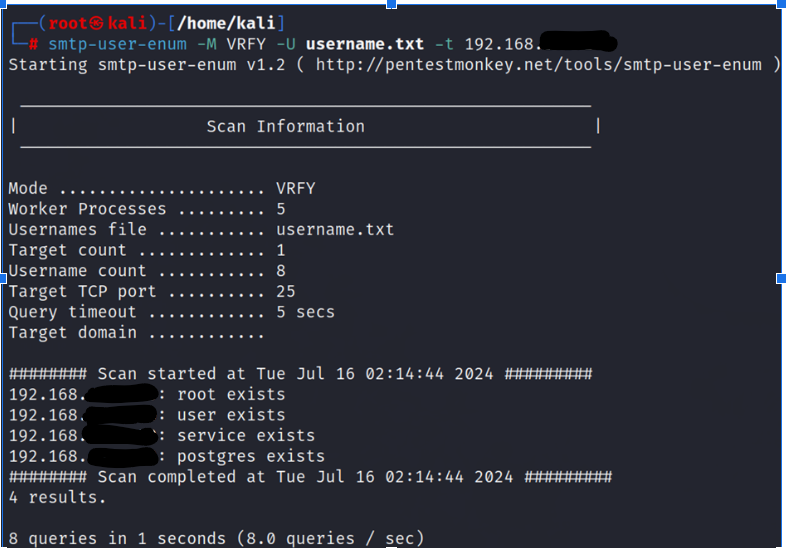
To make good use of this tool, you need to give it a list of usernames and at least one target host that's running an SMTP service.

### **Command-Line Options for smtp-user-enum:**

* **-D dom: Appends a domain to the provided list of usernames to create email addresses.**
* **-U file: Specifies a file with the list of usernames to check.**
* **-t host: Defines the SMTP server to be queried.**
* **-T file: Chooses a file that lists hostnames of SMTP servers to query.**
* **-p port: Sets the TCP port for the SMTP service (default port no. is 25).**
* **-d: Turns on debugging output for detailed process info.**
* **-t n: Sets a timeout in seconds for server response (default is 5 seconds).**
* **-v: Enables verbose output for detailed information during operation.**
* **-h: Shows a help screen that tells you how to use the command.**

### **Additional Options:**

* **-m n: Sets the highest number of processes running at once(default is 5).**
* **-M mode: Selects the SMTP command to guess usernames (EXPN, VRFY, or RCPT TO; default is VRFY).**
* **-u user: Checks if a specific user exists on the remote system you are checking.**
* **-f addr: Specifies the email address for the "RCPT TO" command (** [**user@example.com**](mailto:user@example.com) **is the default).**



1. **SMTP Enumeration using Metasploit Framework**

Metasploit offers two SMTP auxiliary Modules: **smtp\_enum** and **smtp\_version**, which are designed to assist in the enumeration of SMTP servers by providing detailed information.

### **Search for SMTP Modules**

To find SMTP-related modules in Metasploit, use the search command:

search smtp

This command will display a list of SMTP modules. Two useful modules for enumeration are:

* auxiliary/scanner/smtp/smtp\_version
* auxiliary/scanner/smtp/smtp\_enum

**smtp\_enum**

**Use SMTP Enumeration Module:** To enumerate valid email addresses:

1. use the smtp\_enum module.

use auxiliary/scanner/smtp/smtp\_enum

1. Set the target address.

set RHOSTS <target\_ip>

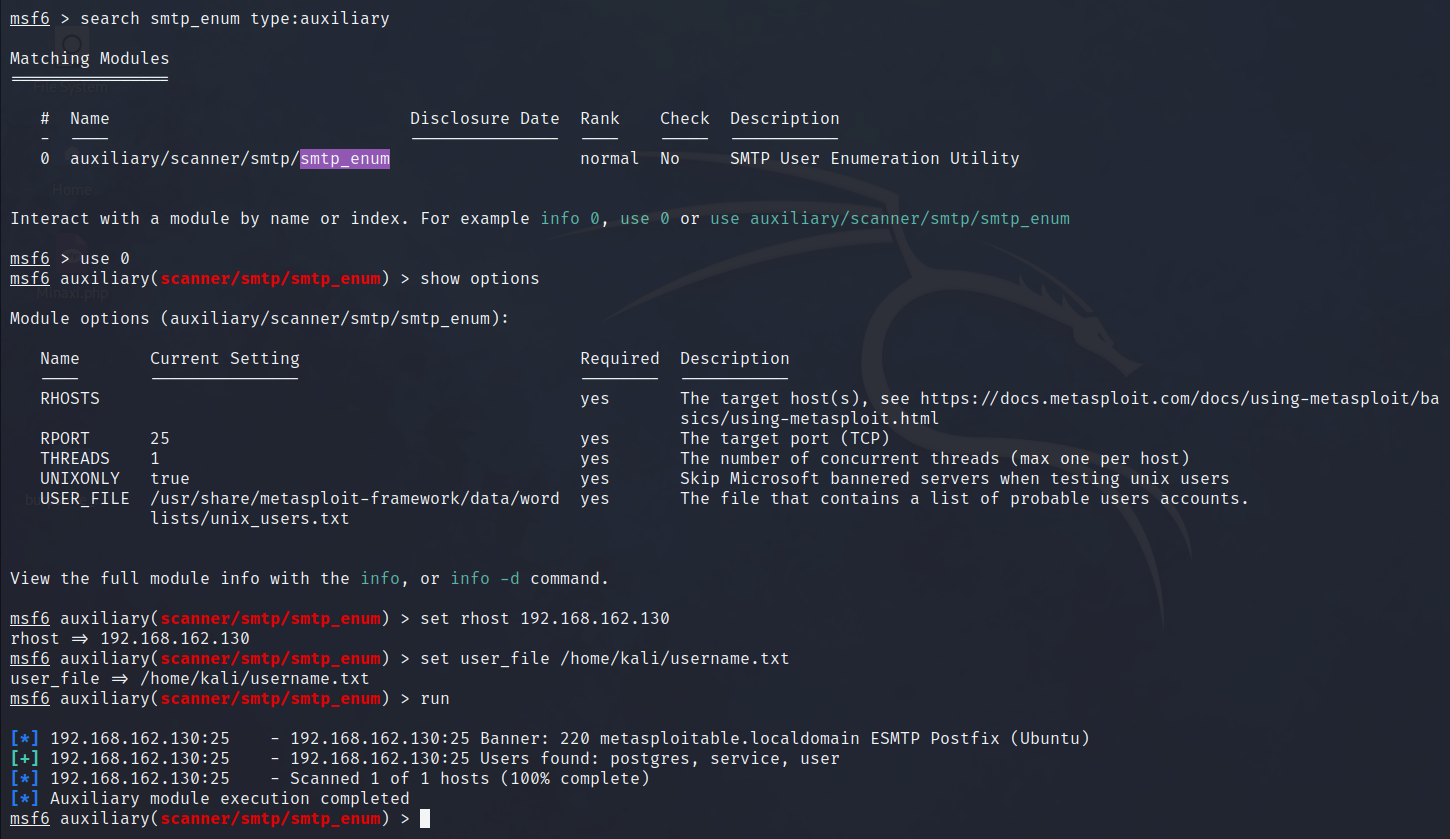
1. Set the user file containing a list of usernames to enumerate.

set USER\_FILE /path/to/usernames.txt

1. Run the module.

run

The module will attempt to enumerate valid email addresses based on the list provided.



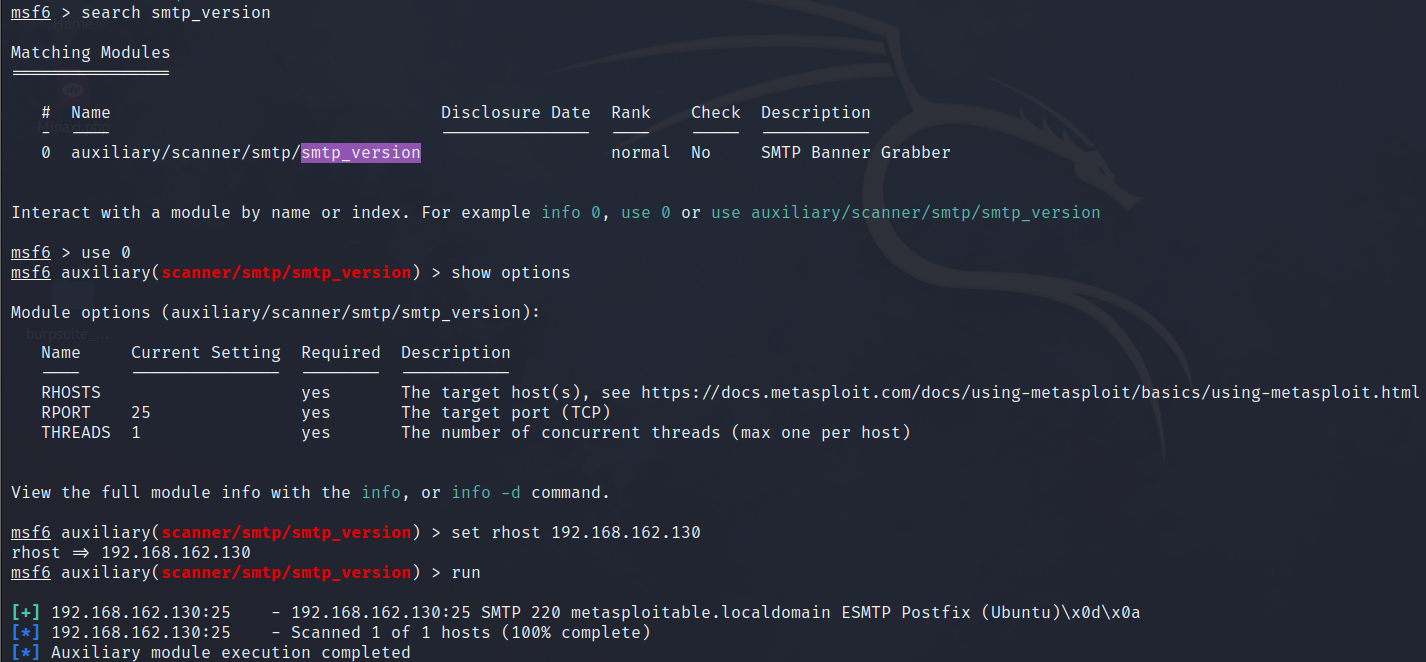
**smtp\_version**

### **Use the SMTP Version Scanner**

To identify the SMTP server version,

1. use the smtp\_version module.  
   use auxiliary/scanner/smtp/smtp\_version
2. Set the target address:  
   set RHOSTS <target\_ip>
3. Run the module:  
   run

This will provide information about the SMTP server version.



**3. SMTP Enumeration using iSMTP (Interactive SMTP)**

ISMTP is a tool that helps you verify whether certain email addresses exist on a server by "asking" the server in a way that’s similar to inquiring about people at a front desk.

It does this by sending different kinds of commands to the server to check if specific email addresses exist.

**ismtp -h 192.168.162.129:25 -e /home/kali/emails.txt**

**-h (host):** The victim’s IP and Port number (IP:Port)

**-e (file):**  Flag to specify the email addresses or username list file.

**/home/kali/emails.txt**: The path to the file that contains the list of email addresses to be tested against the SMTP server

