

SMTP User Enumeration

SMTP is a service that can be found in most infrastructure penetration tests. This service can help the penetration tester to perform username enumeration via the EXPN and VRFY commands if these commands have not been disabled by the system administrator. There are a number of ways which this enumeration through the SMTP can be achieved and there will be explained in this article.

The role of the EXPN command is to reveal the actual address of users aliases and lists of email and VRFY which can confirm the existence of names of valid users.

The SMTP enumeration can be performed manually through utilities like telnet and netcat or automatically via a variety of tools like metasploit, nmap and smtp-user-enum. The following 2 screenshots are showing how we can enumerate users with the VRFY and RCPT commands by using the telnet service.

```
root@pentestlab:~# telnet 172.16.212.133 25
Trying 172.16.212.133...
Connected to 172.16.212.133.
Escape character is '^]'.
220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
VRFY root
252 2.0.0 root
VRFY bin
252 2.0.0 bin
VRFY daemon
252 2.0.0 daemon
```

Enumerating SMTP Users – Telnet

```
root@pentestlab:~# telnet 172.16.212.133 25
Trying 172.16.212.133...
Connected to 172.16.212.133.
Escape character is '^]'.
220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
MAIL FROM:root
250 2.1.0 Ok
RCPT TO:root
250 2.1.5 Ok
RCPT TO:bin
250 2.1.5 Ok
RCPT TO:test
550 5.1.1 <test>: Recipient address rejected: User unknown in local recipient table
```

Enumerating Users with the RCPT command

Metasploit

The module that can perform user enumeration via SMTP in Metasploit Framework is the following:

auxiliary/scanner/smtp/smtp_enum

The only thing that this module requires is to enter the IP address of the remote host and to execute it with the run command as the other options have been filled automatically from metasploit.

```
msf > use auxiliary/scanner/smtp/smtp_enum
msf auxiliary(smtp_enum) > set RHOSTS 172.16.212.133
RHOSTS => 172.16.212.133
msf auxiliary(smtp_enum) > run
```

Metasploit SMTP Enumeration Module – Configuration

We can see the results of the metasploit in the next image:

```
[*] 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
[*] Domain Name: localdomain
[+] 172.16.212.133:25 - Found user: ROOT
[+] 172.16.212.133:25 - Found user: backup
[+] 172.16.212.133:25 - Found user: bin
[+] 172.16.212.133:25 - Found user: daemon
[-] Error: Connection reset by peer
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Metasploit SMTP Enumeration Results

smtp-user-enum

Another tool that can be used is the **smtp-user-enum** which provides 3 methods of user enumeration. The commands that this tool is using in order to verify usernames are the EXPN, VRFY and RCPT. It can also support single username enumeration and multiple by checking through a .txt list. So in order to use this tool effectively you will need to have a good list of usernames. Below is an example of a scan with the VRFY command which discovered the following usernames.

```

root@pentestlab:/pentest/enumeration/smtp/smtp-user-enum# perl smtp-user-enum.pl -M VRFY -U
users.txt -t 172.16.212.133
Starting smtp-user-enum v1.2 ( http://pentestmonkey.net/tools/smtp-user-enum )

-----
|                               |
|             Scan Information             |
|                               |
|-----|
Mode ..... VRFY
Worker Processes ..... 5
Usernames file ..... users.txt
Target count ..... 1
Username count ..... 12
Target TCP port ..... 25
Query timeout ..... 5 secs
Target domain .....

##### Scan started at Fri Nov 16 10:50:58 2012 #####
172.16.212.133: lp exists
172.16.212.133: daemon exists
172.16.212.133: bin exists
172.16.212.133: sync exists
172.16.212.133: root exists
172.16.212.133: mail exists
172.16.212.133: backup exists
172.16.212.133: news exists
##### Scan completed at Fri Nov 16 10:50:58 2012 #####
8 results.

12 queries in 1 seconds (12.0 queries / sec)

```

SMTP User Enumeration via smtp-user-enum

Also smtp-user-enum can be used for discovery valid email addresses instead of usernames. The next image indicates this usage.

```

root@pentestlab:/pentest/enumeration/smtp/smtp-user-enum# perl smtp-user-enum.pl -M VRFY -D
metasploitable.localdomain -U users.txt -t 172.16.212.133
Starting smtp-user-enum v1.2 ( http://pentestmonkey.net/tools/smtp-user-enum )

-----
|                               |
|             Scan Information             |
|                               |
|-----|
Mode ..... VRFY
Worker Processes ..... 5
Usernames file ..... users.txt
Target count ..... 1
Username count ..... 12
Target TCP port ..... 25
Query timeout ..... 5 secs
Target domain ..... metasploitable.localdomain

##### Scan started at Fri Nov 16 11:20:06 2012 #####
172.16.212.133: daemon@metasploitable.localdomain exists
172.16.212.133: root@metasploitable.localdomain exists
172.16.212.133: bin@metasploitable.localdomain exists
172.16.212.133: sync@metasploitable.localdomain exists
172.16.212.133: mail@metasploitable.localdomain exists
172.16.212.133: backup@metasploitable.localdomain exists
172.16.212.133: lp@metasploitable.localdomain exists
##### Scan completed at Fri Nov 16 11:20:09 2012 #####
7 results.

12 queries in 3 seconds (4.0 queries / sec)

```

Discover Email addresses via smtp-user-enum

Nmap

SMTP enumeration can be implemented through the Nmap as well. There is a script in the NSE (Nmap Scripting Engine) that can be used for SMTP user enumeration. The generic usage of the script is the following:

nmap --script smtp-enum-users.nse 172.16.212.133

```
root@pentestlab:~# nmap --script smtp-enum-users.nse 172.16.212.133

Starting Nmap 6.01 ( http://nmap.org ) at 2012-11-16 13:13 GMT
Nmap scan report for 172.16.212.133
Host is up (0.00032s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
| smtp-enum-users:
|_ Method RCPT returned a unhandled status code.
53/tcp    open  domain
80/tcp    open  http
```

SMTP Username Enumeration via Nmap

As we can see from the above image the enumeration didn't succeed in this case.

Conclusion

SMTP is a common service that can be found in every network. Administrators need to properly configured the mail servers by disallowing the execution of the commands **EXPN**, **VRFY** and **RCPT** in order to avoid this leakage. From the other side penetration testers can use the usernames that have been obtained from this enumeration to conduct further attacks on other systems.