SMTP User Enumeration

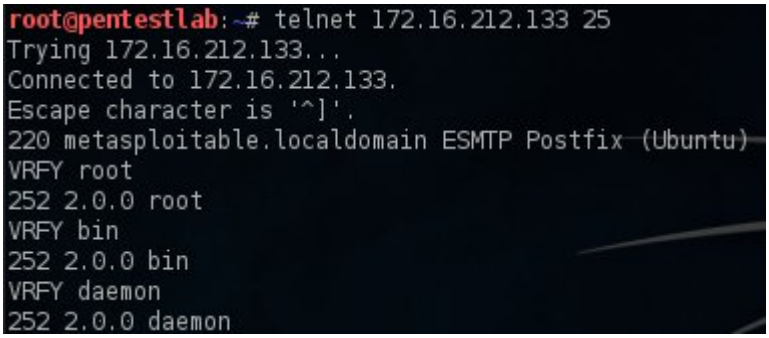
pentestlab.blog/category/information-gathering/page/5

November 20, 2012

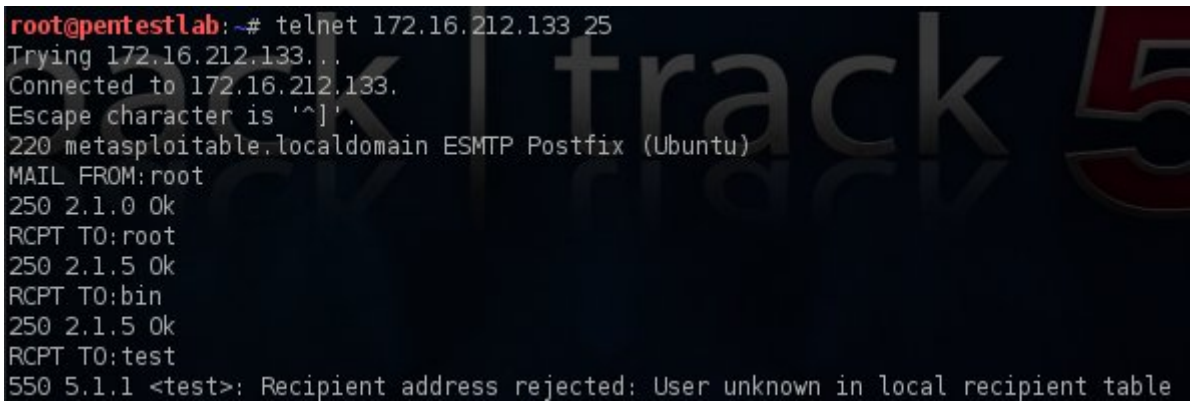
SMTP is a service that can be found in most infrastructure penetration tests.This service can help the penetration tester to perform username enumeration via the EXPN and VRFY commands if these commands have not been disabled by the system administrator.There are a number of ways which this enumeration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



Enumerating SMTP Users – Telnet



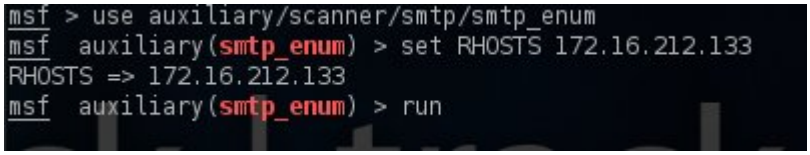
Enumerating Users with the RCPT command

Metasploit

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

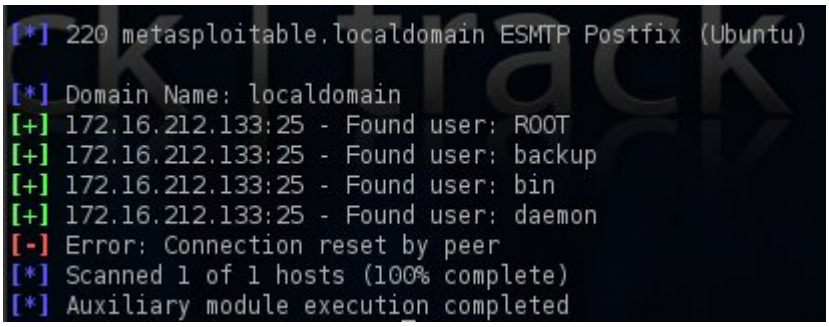
auxiliary/scanner/smtp/smtp_enum

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.



Metasploit SMTP Enumeration Module – Configuration

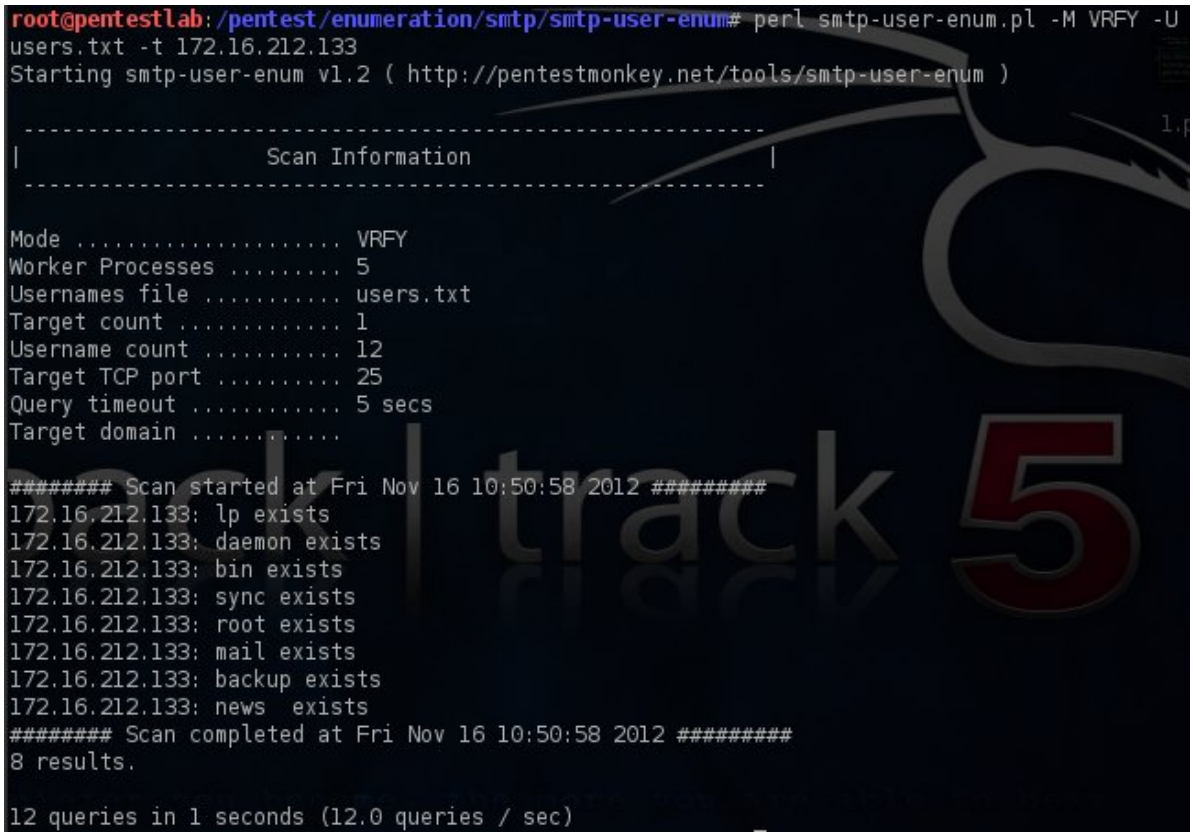
We can see the results of the metasploit in the next image:



Metasploit SMTP Enumeration Results

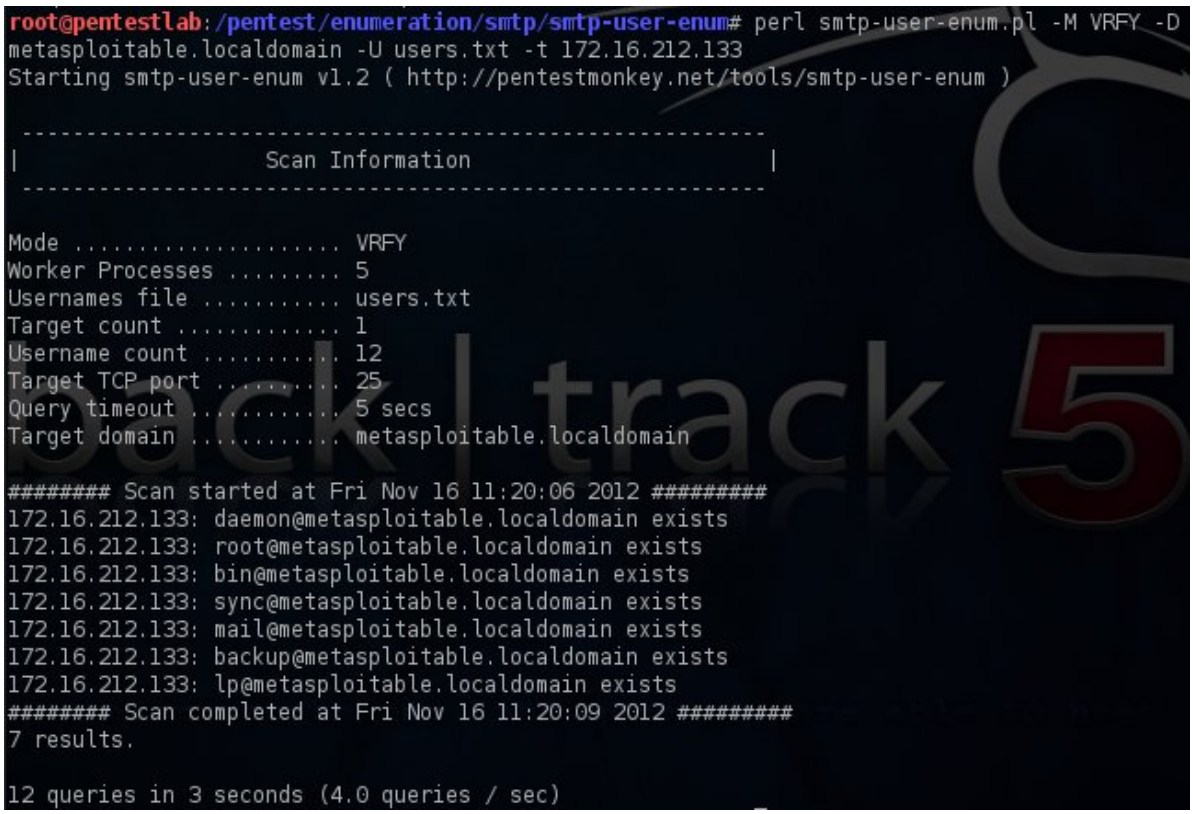
smtp-user-enum

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.



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.

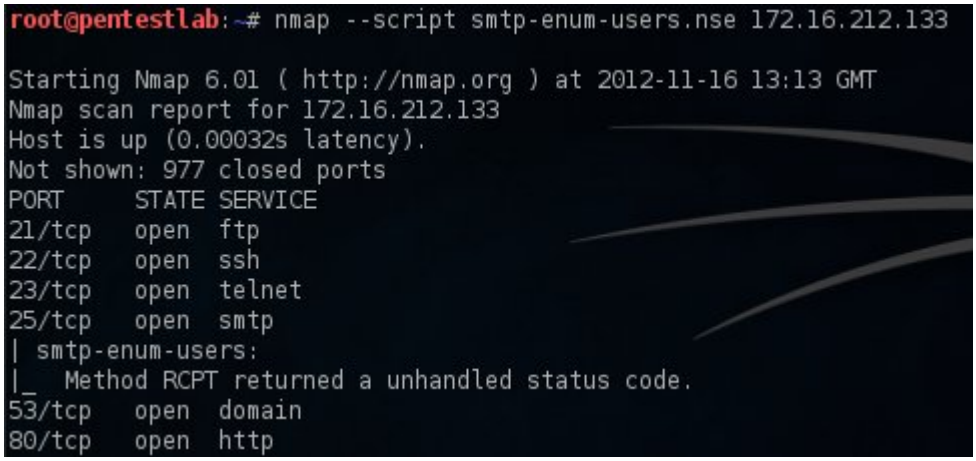


Discover Email addresses via smtp-user-enum

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



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.