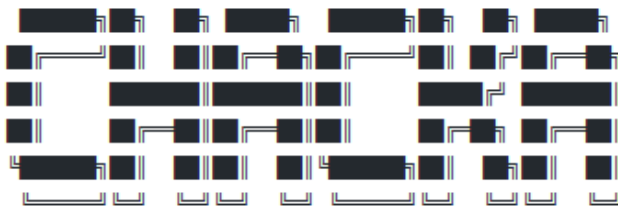




Colombia Hack Agent (CHackA)



### Colombia Hack Agent (CHackA)

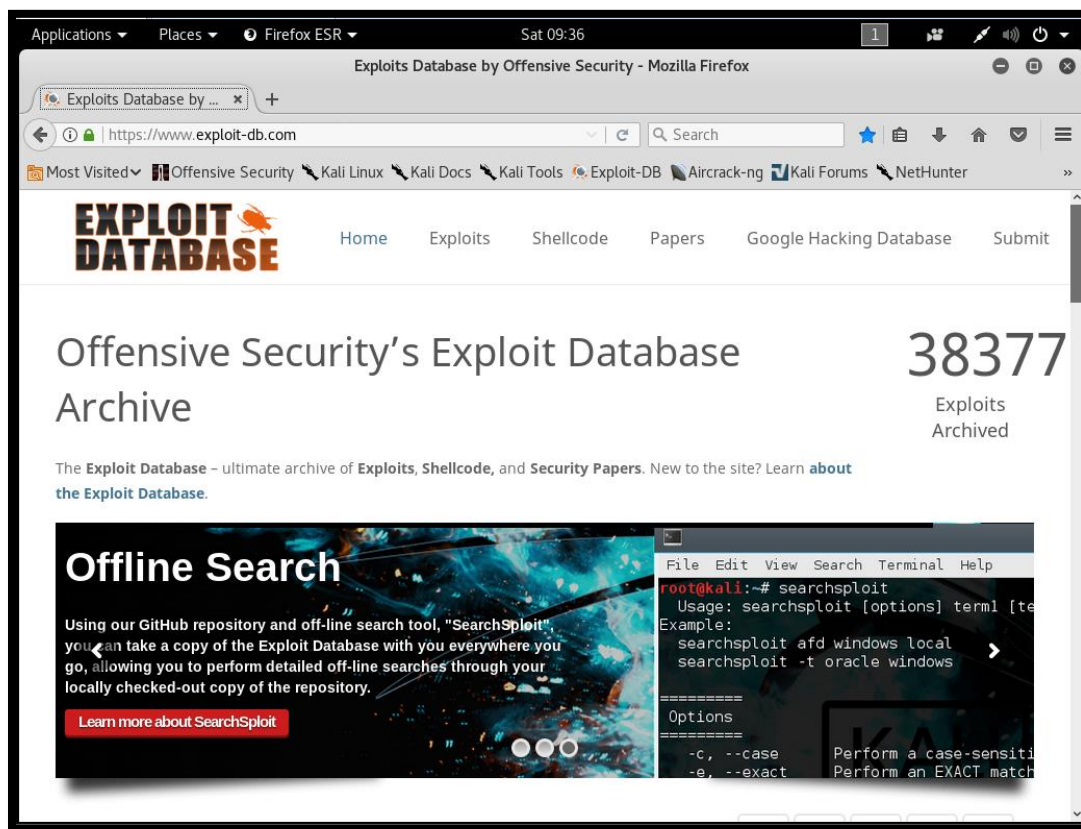
```
[...] Developer:      Jairo A. García H.      [...]
[...] Version:       1.0.                    [...]
[...] Codename:      HACKLAB PARA ADICIONAR EXPLOIT EN MSF [...]
[...] Report to:     chacka0101 @ gmail.com  [...]
[...] Homepage:      https://github.com/chacka0101/HACKLABS [...]
[...] Publication Date: 16/Dec/2017          [...]
```

## HACKLAB PARA ADICIONAR UN EXPLOIT EN METASPLOIT FRAMEWORK

Resumen: Realizaremos la adición de un nuevo exploit en el framework de metasploit.

Aplica para sistemas operativos: **DEBIAN (Distro KALI LINUX)**.

1. Buscamos en la página de "EXPLOIT DATABASE" el "exploit" nuevo que queremos adicionar, no necesariamente debe ser de esta página, puedes adicionar un exploit acondicionado para "Metasploit Framework", es importante aclarar que no cualquier exploit puede ser utilizado desde el "Metasploit Framework", es por esto que explicaremos que debe tener el exploit.



2. Dentro del código del exploit debe decir "This module requires Metasploit:", es decir que, para que se pueda ejecutar es necesario utilizarlo desde el "Metasploit Framework":

Tomcat - Remote Code Execution via JSP Upload Bypass (Metasploit) - Mozilla Firefox

Tomcat - Remote Cod... x +

https://www.exploit-db.com/exploits/43008/ Search

Most Visited Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng Kali Forums NetHunter

**EXPLOIT DATABASE** Home Exploits Shellcode Papers Google Hacking Database Submit

## Tomcat - Remote Code Execution via JSP Upload Bypass (Metasploit)

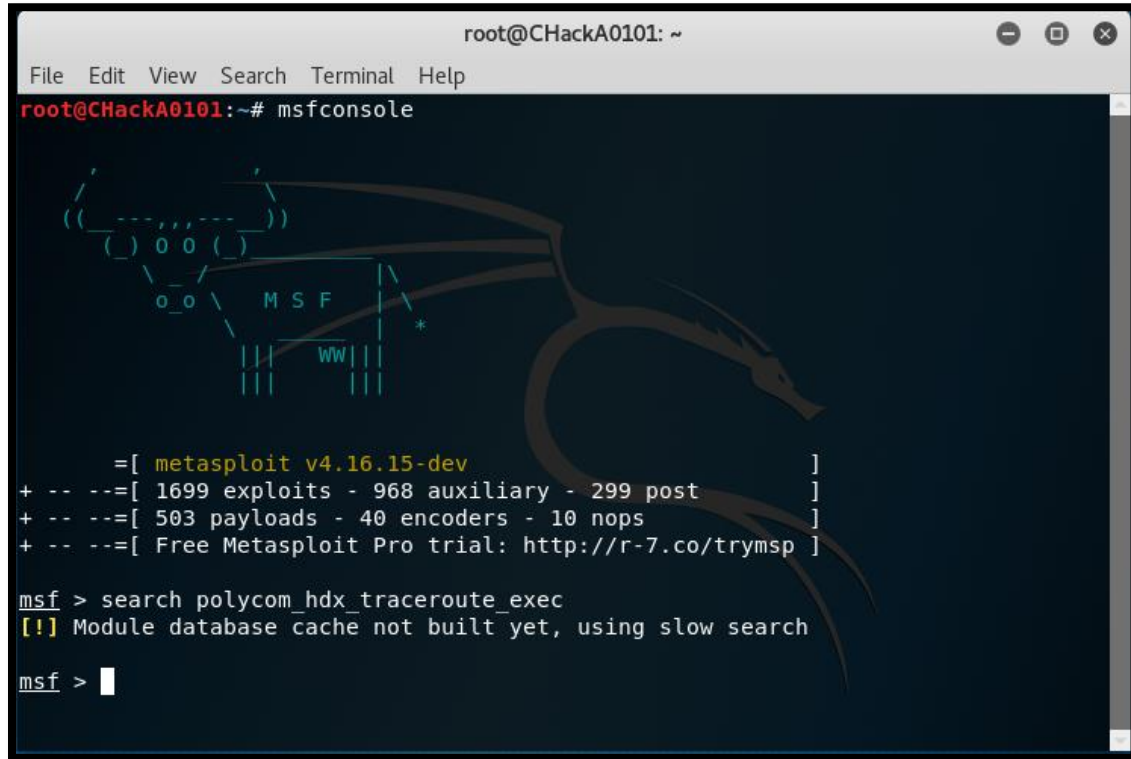
EDB-ID: 43008	Author: <a href="#">Metasploit</a>	Published: 2017-10-17
CVE: <a href="#">CVE-2017-12617</a>	Type: <a href="#">Remote</a>	Platform: <a href="#">Java</a>
Aliases: N/A	Advisory/Source: <a href="#">Link</a>	Tags: Metasploit Framework (MSF)
E-DB Verified:	Exploit: <a href="#">Download</a> / <a href="#">View Raw</a>	Vulnerable App: N/A

« Previous Exploit Next Exploit »

```

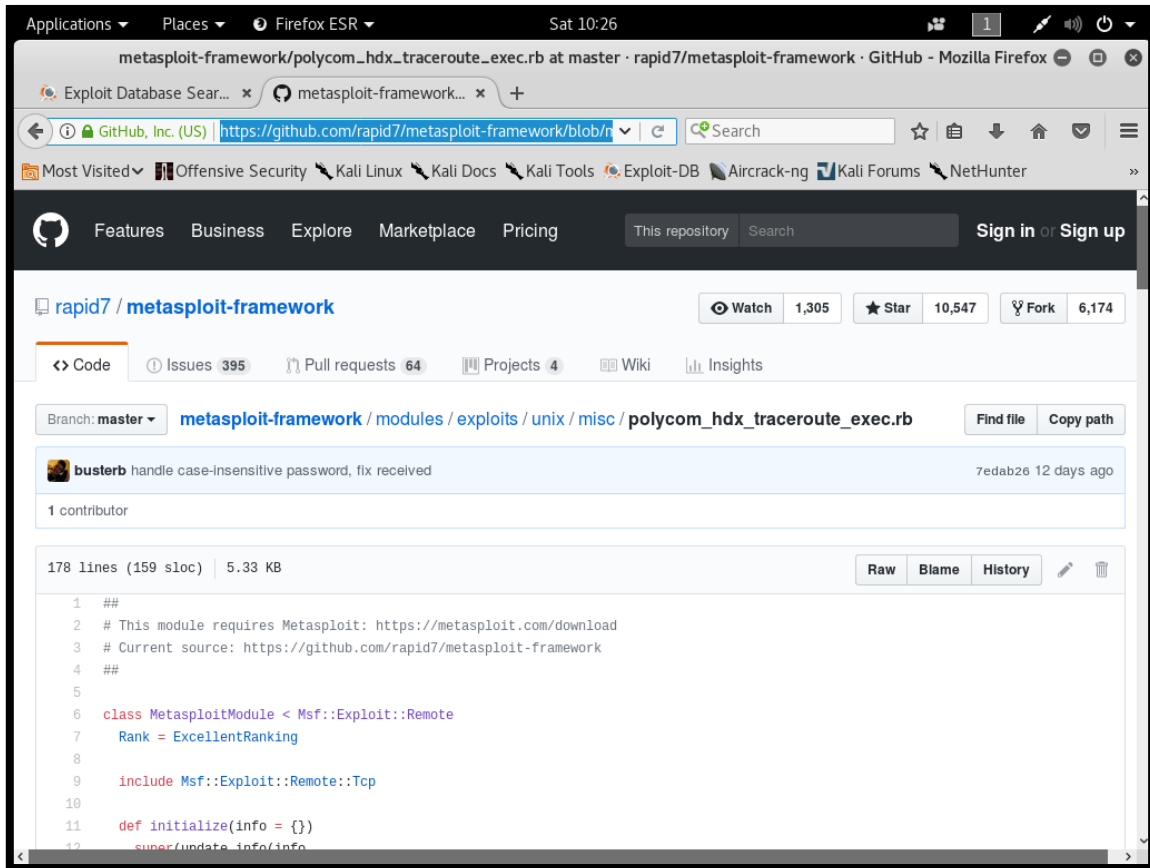
1  ##
2  # This module requires Metasploit: http://metasploit.com/download
3  # Current source: https://github.com/rapid7/metasploit-framework
4  ##
5
6  class MetasploitModule < Msf::Exploit::Remote
7
8      Rank = ExcellentRanking
  
```

Buscamos el exploit "polycom\_hdx\_traceroute\_exec" para comprobar utilizamos el comando "search":



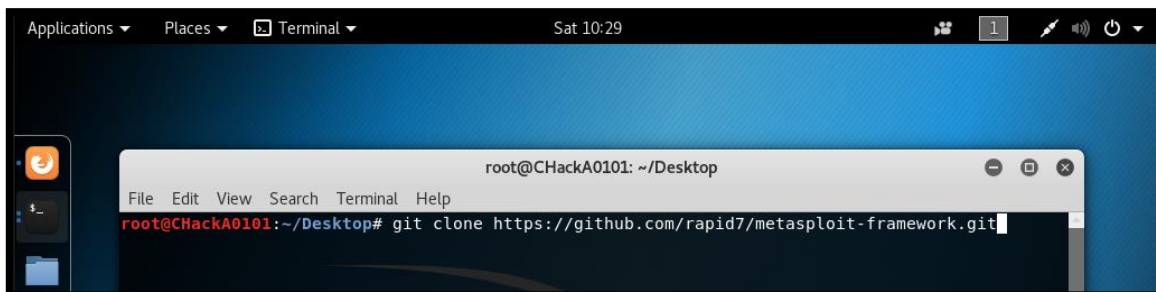
4. Buscamos el exploit en Git Hub, más exactamente de una fuente confiable "Rapid7":

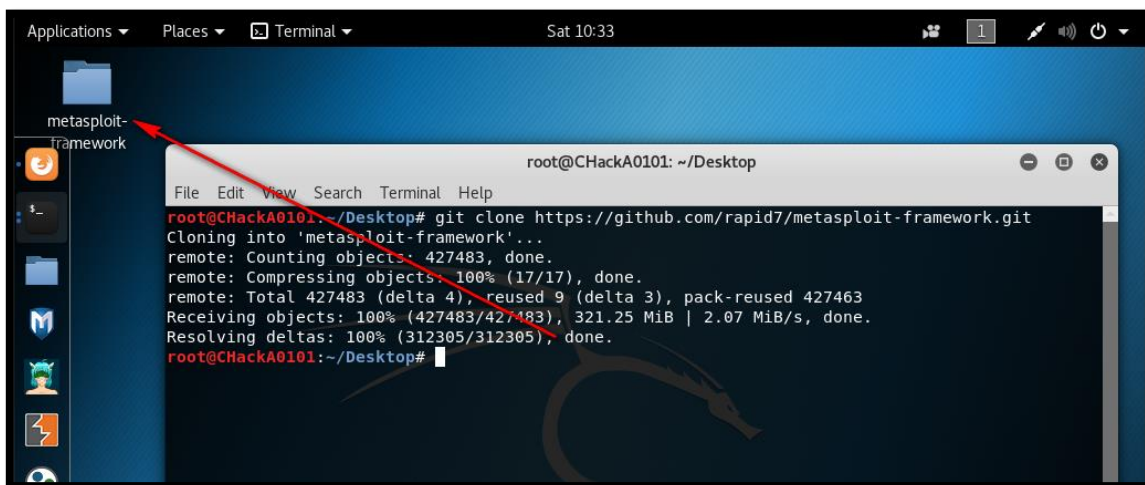
[https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/misc/polycom\\_hdl\\_traceroute\\_exec.rb](https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/misc/polycom_hdl_traceroute_exec.rb)



5. Descargamos el exploit, para esto debemos descargar el gihub completo de Metasploit-framework:

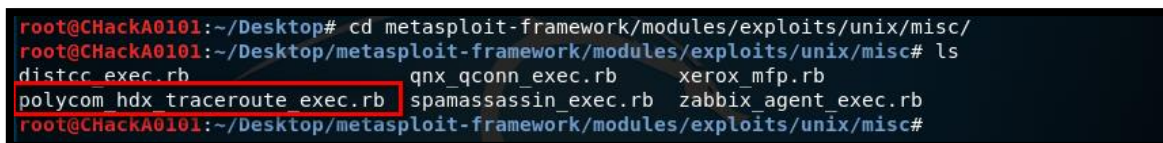
```
root@CHACKA0101:~/Desktop# git clone https://github.com/rapid7/metasploit-framework.git
```





6. Buscamos el exploit en el directorio:

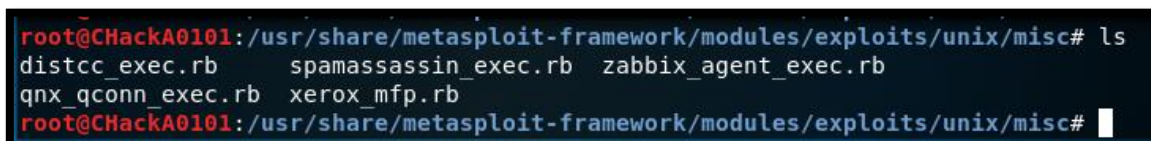
```
root@CHACKA0101:~/Desktop# cd metasploit-framework/modules/exploits/unix/misc/
```



7. Adicionamos el exploit "polycom\_hdx\_traceroute\_exec.rb" a la base de datos de los exploits del directorio del "metasploit-framework" del "Kali Linux".

Este es el directorio oficial del "metasploit-framework" del "Kali Linux":

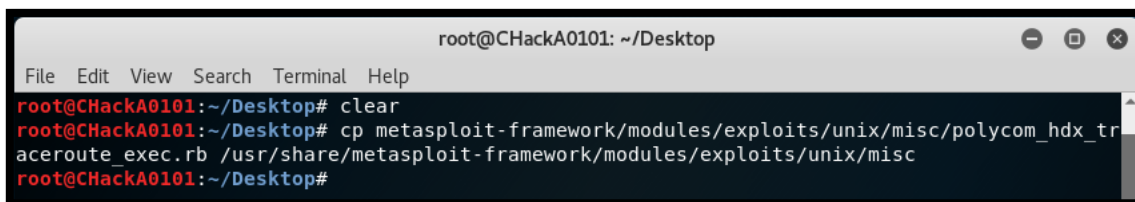
```
root@CHACKA0101: /usr/share/metasploit-framework/modules/exploits/unix/misc#
```



El exploit no está en este directorio.

Desde la ubicación de "Desktop", para adicionar el exploit el comando es el siguiente:

```
root@CHACKA0101:~/Desktop# cp metasploit-
framework/modules/exploits/unix/misc/polycom_hdx_traceroute_exec.rb
/usr/share/metasploit-framework/modules/exploits/unix/misc
```





Colombia Hack Agent (CHACKA)

8. Comprobamos que el exploit esté adicionado en el directorio:

```
root@CHACKA0101:~/Desktop# cd /usr/share/metasploit-framework/modules/exploits/unix/misc
root@CHACKA0101:/usr/share/metasploit-framework/modules/exploits/unix/misc#
root@CHACKA0101:/usr/share/metasploit-framework/modules/exploits/unix/misc# ls
distcc_exec.rb          qnx_qconn_exec.rb      xerox_mfp.rb
polycom_hdx_traceroute_exec.rb  spamassassin_exec.rb  zabbix_agent_exec.rb
root@CHACKA0101:/usr/share/metasploit-framework/modules/exploits/unix/misc#
```

9. Es muy importante ahora revisar los privilegios que tiene el exploit, es muy importante porque los privilegios deben estar configurados de forma correcta, de esta forma podemos o no ejecutar el exploit:

```
root@CHACKA0101:~/usr/share/metasploit-framework/modules/exploits/unix/misc/#
chmod 644 polycom_hdx_traceroute_exec.rb
```

```
root@CHACKA0101:/usr/share/metasploit-framework/modules/exploits/unix/misc# ls -la
total 40
drwxr-xr-x  2 root root 4096 Dec 16 10:52 .
drwxr-xr-x 13 root root 4096 Dec  2 01:16 ..
-rw-r--r--  1 root root 3218 Nov  2 12:01 distcc_exec.rb
-rw-r--r--  1 root root 5455 Dec 16 10:52 polycom_hdx_traceroute_exec.rb
-rw-r--r--  1 root root 3055 Nov  2 12:01 qnx_qconn_exec.rb
-rw-r--r--  1 root root 1889 Nov  2 12:01 spamassassin_exec.rb
-rw-r--r--  1 root root 4350 Nov  2 12:01 xerox_mfp.rb
-rw-r--r--  1 root root 2443 Nov  2 12:01 zabbix_agent_exec.rb
root@CHACKA0101:/usr/share/metasploit-framework/modules/exploits/unix/misc#
```

Para calcular los privilegios nos podemos ayudar con: <https://chmod-calculator.com/>

The screenshot shows the Chmod Calculator website. The title is "Chmod Calculator" with the subtitle "An awesome Chmod Calculator to convert Linux file permissions between different formats." Below this, there are three columns: "Owner", "Group", and "Public". Each column has three rows: "Read" (checked), "Write" (checked), and "Execute" (unchecked). At the bottom, there is a section for "Linux Permissions" with two input fields: one containing "644" and another containing "rw-r--r--".





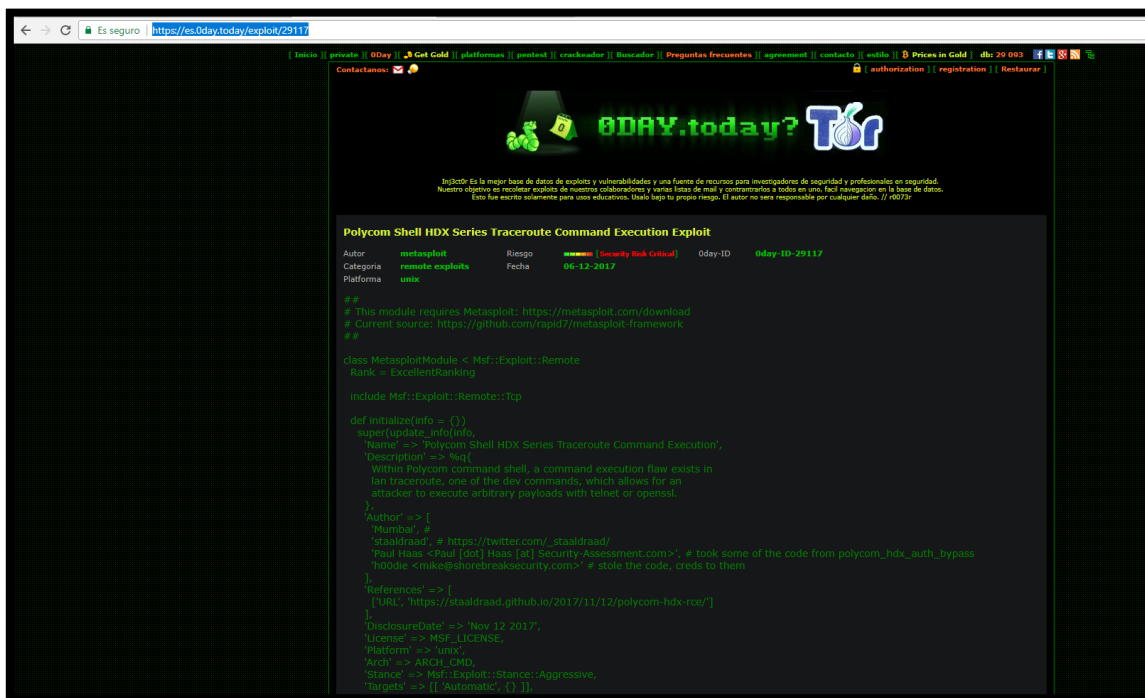


Colombia Hack Agent (CHACKA)

## SEGUNDO MÉTODO

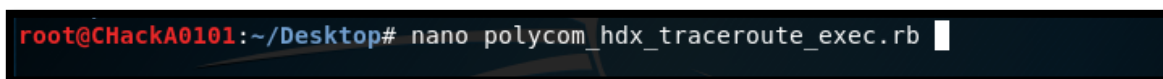
1. De igual forma existen varias formas de poderlo hacer, por ejemplo, en este segundo método, lo copiáramos desde otra fuente, por ejemplo, de;

<https://es.0day.today/exploit/29117>

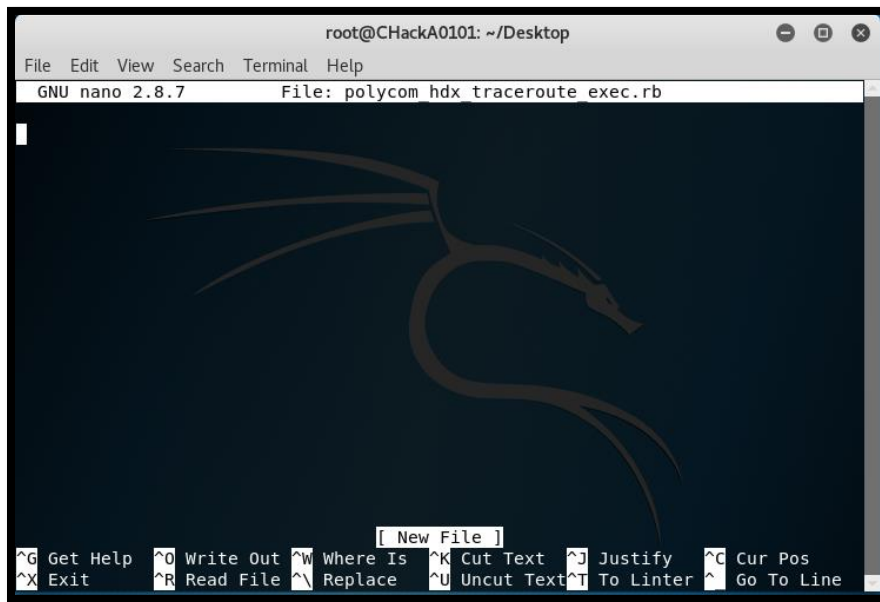


2. Creamos un archivo con el nombre del exploit y la extensión de Ruby:

```
root@CHACKA0101:~/Desktop# nano polycom_hdx_traceroute_exec.rb
```





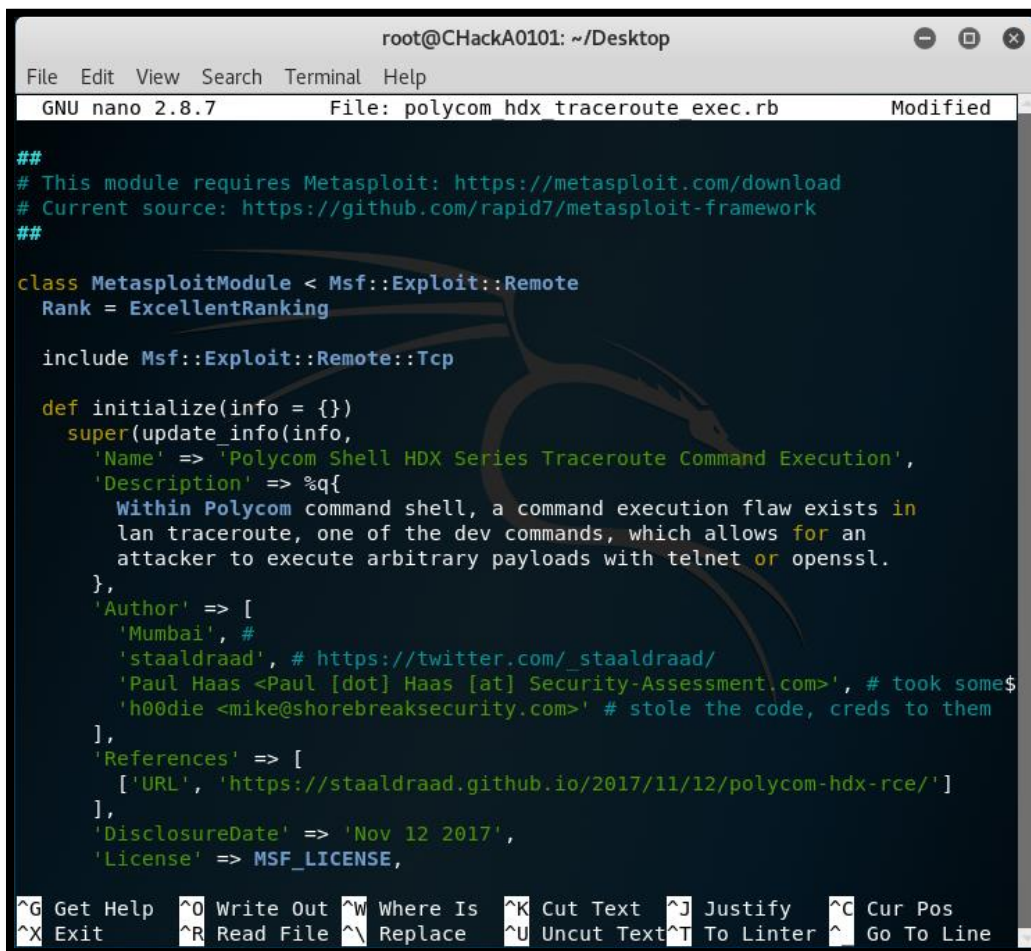


```

root@CHACKA0101: ~/Desktop
File Edit View Search Terminal Help
GNU nano 2.8.7 File: polycom_hdx_traceroute_exec.rb

[ New File ]
^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos
^X Exit ^R Read File ^\ Replace ^U Uncut Text ^T To Linter ^_ Go To Line
  
```

3. Copiamos el código del exploit y lo pegamos al archivo que creamos:



```

root@CHACKA0101: ~/Desktop
File Edit View Search Terminal Help
GNU nano 2.8.7 File: polycom_hdx_traceroute_exec.rb Modified

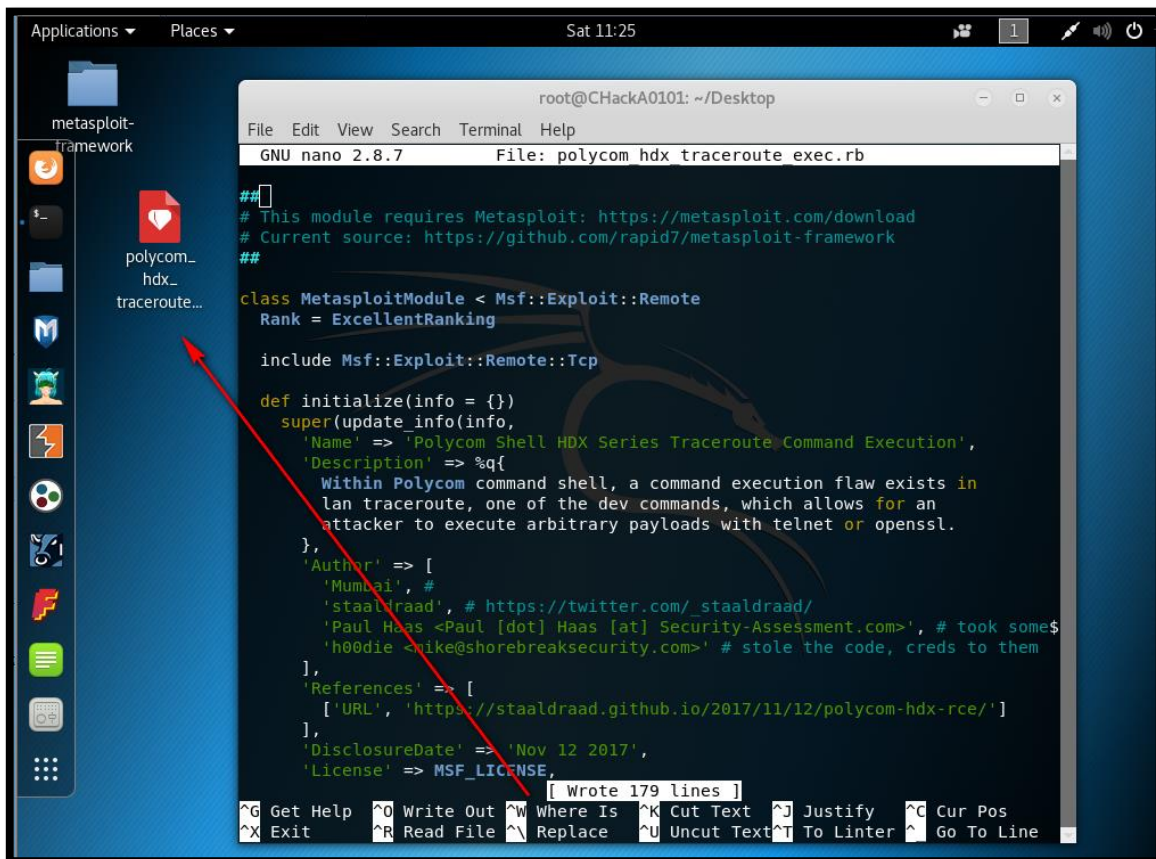
##
# This module requires Metasploit: https://metasploit.com/download
# Current source: https://github.com/rapid7/metasploit-framework
##

class MetasploitModule < Msf::Exploit::Remote
  Rank = ExcellentRanking

  include Msf::Exploit::Remote::Tcp

  def initialize(info = {})
    super(update_info(info,
      'Name' => 'Polycom Shell HDX Series Traceroute Command Execution',
      'Description' => %q{
        Within Polycom command shell, a command execution flaw exists in
        lan traceroute, one of the dev commands, which allows for an
        attacker to execute arbitrary payloads with telnet or openssl.
      },
      'Author' => [
        'Mumbai', #
        'staaldraad', # https://twitter.com/_staaldraad/
        'Paul Haas <Paul [dot] Haas [at] Security-Assessment.com>', # took some$
        'h00die <mike@shorebreaksecurity.com>' # stole the code, creds to them
      ],
      'References' => [
        ['URL', 'https://staaldraad.github.io/2017/11/12/polycom-hdx-rce/']
      ],
      'DisclosureDate' => 'Nov 12 2017',
      'License' => MSF_LICENSE,
    ))
  end
end
  
```

4. Lo guardamos y lo visualizamos:



```

root@CHackA0101: ~/Desktop
File Edit View Search Terminal Help
GNU nano 2.8.7 File: polycom_hdx_traceroute_exec.rb

##
# This module requires Metasploit: https://metasploit.com/download
# Current source: https://github.com/rapid7/metasploit-framework
##

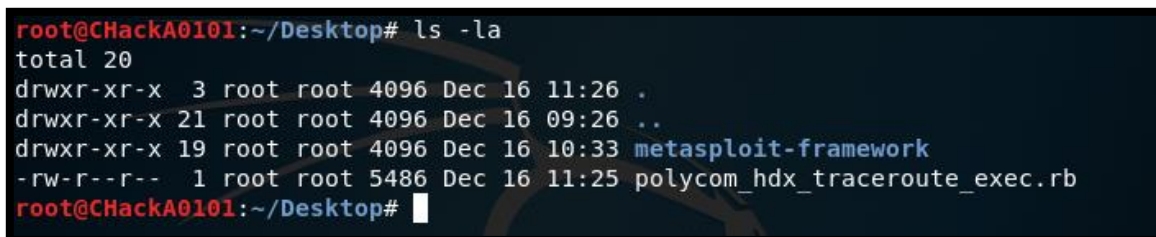
class MetasploitModule < Msf::Exploit::Remote
  Rank = ExcellentRanking

  include Msf::Exploit::Remote::Tcp

  def initialize(info = {})
    super(update_info(info,
      'Name' => 'Polycom Shell HDX Series Traceroute Command Execution',
      'Description' => %q{
        Within Polycom command shell, a command execution flaw exists in
        lan traceroute, one of the dev commands, which allows for an
        attacker to execute arbitrary payloads with telnet or openssl.
      },
      'Author' => [
        'Mumbai', #
        'staal draad', # https://twitter.com/_staal draad/
        'Paul Haas <Paul [dot] Haas [at] Security-Assessment.com>', # took some$
        'h00die <mike@shorebreaksecurity.com>' # stole the code, creds to them
      ],
      'References' => [
        ['URL', 'https://staal draad.github.io/2017/11/12/polycom-hdx-rce/']
      ],
      'DisclosureDate' => 'Nov 12 2017',
      'License' => MSF_LICENSE,
    ])
  end

  def execute
    # ... (code continues)
  end
end

```



```

root@CHackA0101:~/Desktop# ls -la
total 20
drwxr-xr-x  3 root root 4096 Dec 16 11:26 .
drwxr-xr-x 21 root root 4096 Dec 16 09:26 ..
drwxr-xr-x 19 root root 4096 Dec 16 10:33 metasploit-framework
-rw-r--r--  1 root root 5486 Dec 16 11:25 polycom_hdx_traceroute_exec.rb
root@CHackA0101:~/Desktop#

```

Copiamos el exploit creado al directorio de "Metasploit Framework" y eso ustedes ya lo saben hacer.



Colombia Hack Agent (CheckA)

Un paso impórtate para finalizar es el de actualizar la base de datos de los módulos del metasploit framework, para esto hacemos lo siguiente:

msf > **reload\_all**

```
msf > reload_all
[*] Reloading modules from all module paths...
[-] WARNING! The following modules could not be loaded!
[-] N:/usr/share/metasploit-framework/modules/exploits/linux/smtp/haraka.rb: Errno::ENOENT No such file or directory @ rb_sysopen
[-] /usr/share/metasploit-framework/modules/exploits/windows/smb/ms17_010_eternalblue_win8.rb: Errno::ENOENT No such file or
eternalblue_win8.rb
Configuración del idioma
Terminal Help
e-Doublepulsar-Metasploit.git
Cloning into 'Eternalblue-Doublepulsar-Ma
root@kali: /usr/share/meta
e_c/Python34/Lib/test/tracedmodules/_pycact
e_c/Python34/Lib/test/tracedmodules/testmod
re/metasploit-framework/modules/exploits/wa
asploit-framework/modules/exploits/windows
re/metasploit-framework/modules/exploits/wa
asploit-framework/modules/exploits/windows
games license motorola oracle smb
http local mssql pop3 smtp
iis lotus mysql postgres ssh
imap lpd nfs proxy ssl
isapi misc nntp scada telnet
ldap mmsp novell sip tftp
asploit-framework/modules/exploits/windows
asploit-framework/modules/exploits/windows
on.rb ms08_067_netapi.rb
ms09_050_smb2_negotiate_func_index.rb
ms10_046_shortcut_icon_dllloader.rb
ms10_061_spoolss.rb
ms15_020_shortcut_icon_dllloader.rb
ms17_010_eternalblue.rb
```

Agradecimientos a:

0day.today - <http://0day.today/>  
Rapid7 - <https://www.rapid7.com/>  
Kali Linux - <https://www.kali.org/>

-END-