



Colombia Hack Agent (CHackA)

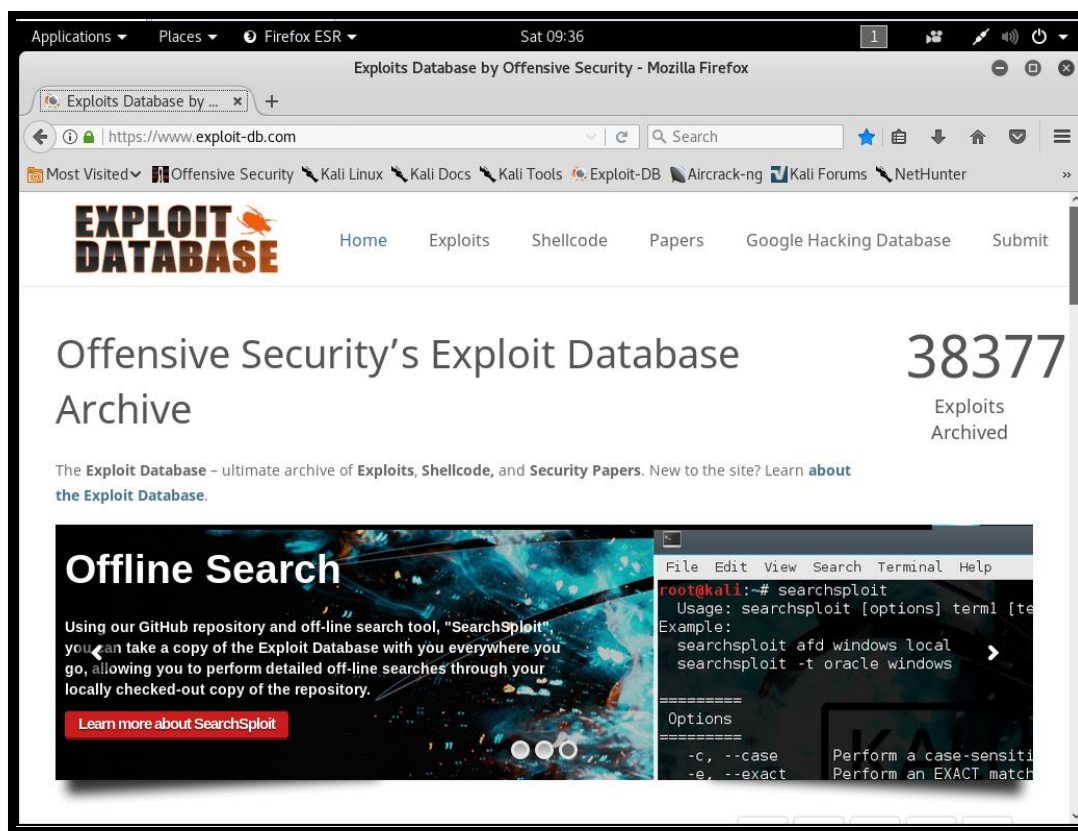
```
[...] Developer:      Jairo A. García H.      [...]
[...] Version:       1.0.                    [...]
[...] Codename:      HACKLAB PARA ADICIONAR EXPLOIT EN MSF [...]
[...] Report to:     chacka0101 @ gmail.com  [...]
[...] Homepage:      https://github.com/chacka0101/HACKLABS [...]
[...] Publication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



- 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: Metasploit	Published: 2017-10-17
CVE: CVE-2017-12617	Type: Remote	Platform: Java
Aliases: N/A	Advisory/Source: Link	Tags: Metasploit Framework (MSF)
E-DB Verified:	Exploit: Download / View Raw	Vulnerable App: N/A

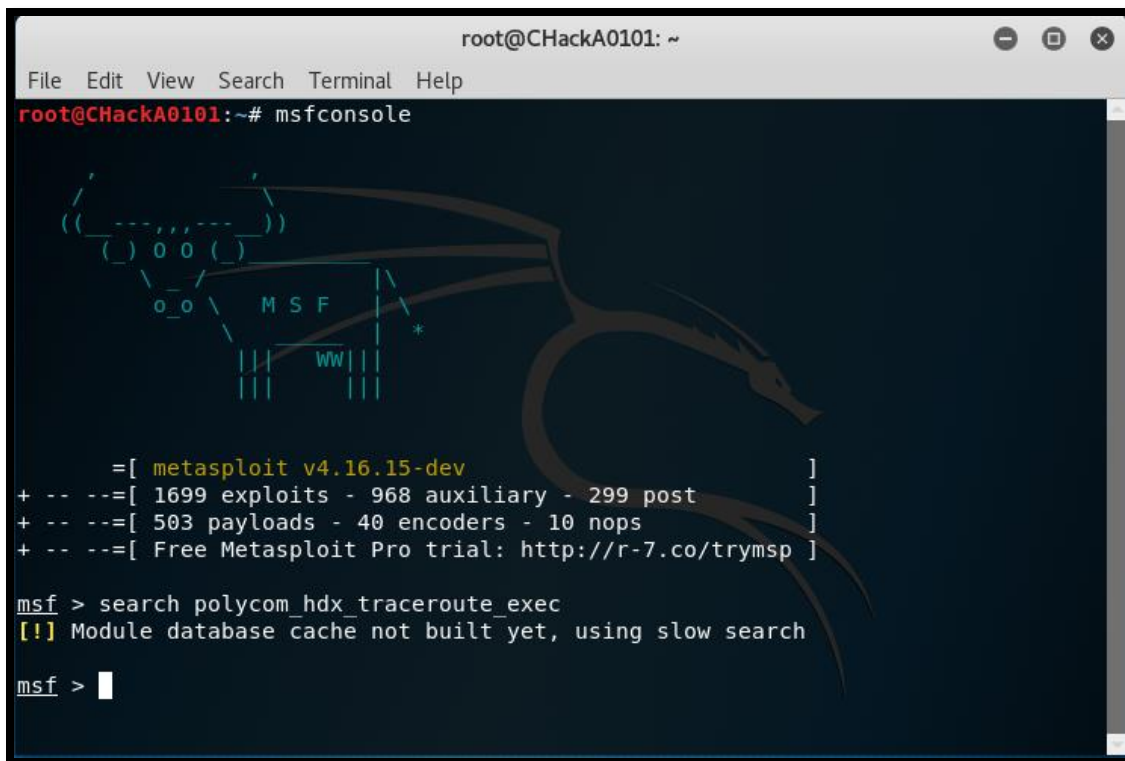
« Previous Exploit Next Exploit »

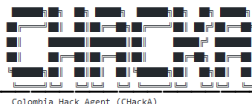
```

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
9  
```



3. Para este ejemplo, debemos buscar un exploit que no esté dentro de la base de datos de "Metasploit Framework" con el fin de adicionarlo. Para este ejemplo vamos a adicionar el exploit llamado "polycom hdx traceroute exec".

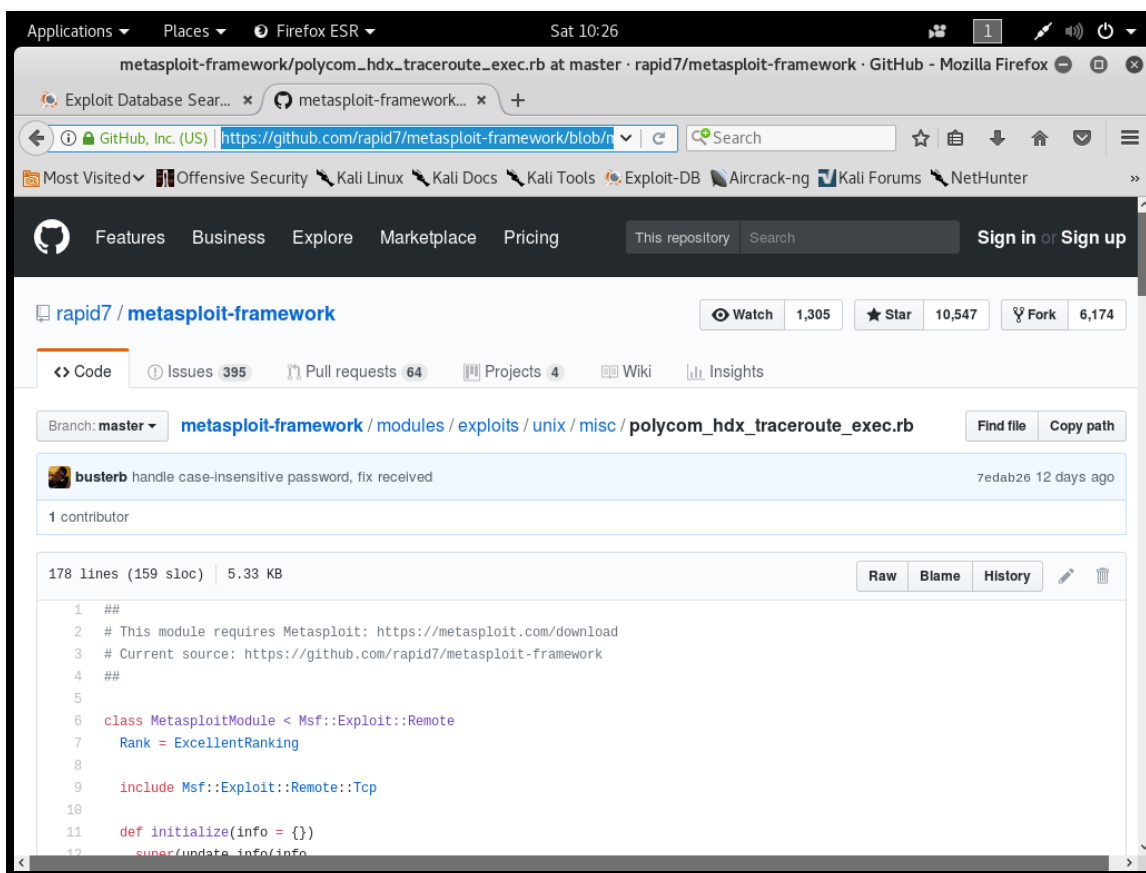




Colombia Hack Agent (CHACKA)

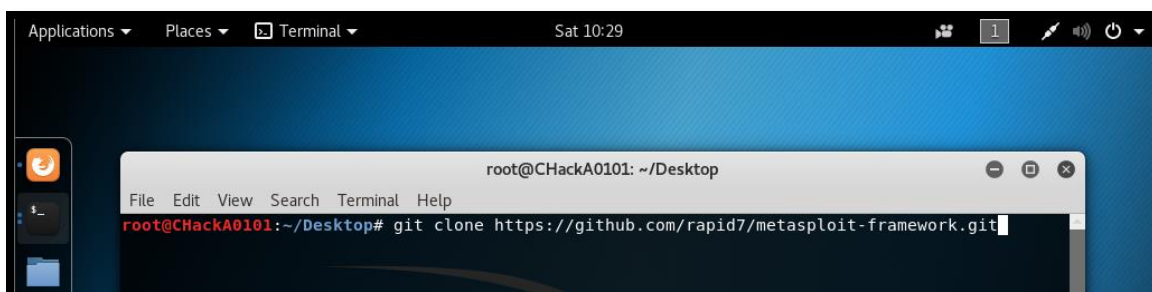
4. Buscamos el exploit en Git Hub, más exactamente de una fuente confiable "Rapid7":

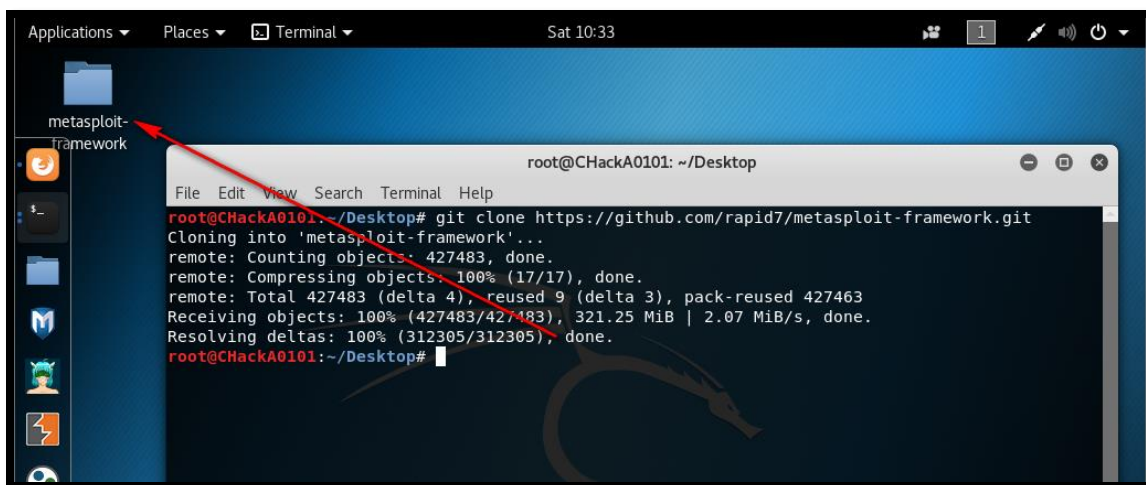
https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/misc/polycom_hdx_traceroute_exec.rb



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:

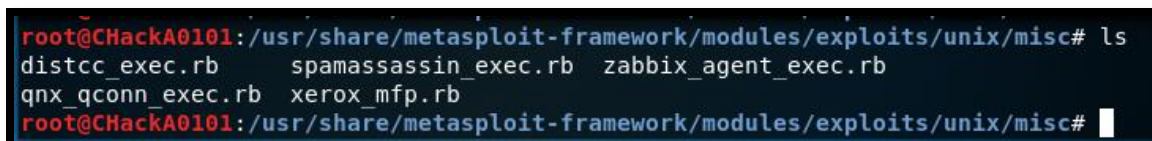
```
root@CHACKA0101:~/Desktop# cd metasploit-framework/modules/exploits/unix/misc/
```



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":

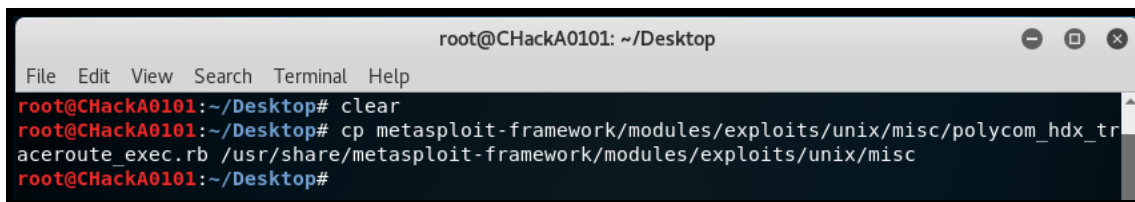
```
root@CHACKA0101: /usr/share/metasploit-framework/modules/exploits/unix/misc#
```



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# 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#
```

10. Se recomienda cerrar el metasploit framework en caso que lo tenga abierto y volvemos a buscar el exploit que adicionamos:

```
root@CHACKA0101: ~
File Edit View Search Terminal Help

  RECON

o o o
o o
o
PAYLOAD
| (e) (e) * * * * | (e) (e) * * | (e)
=====

  LOOT

=====
[ ]
[ ]
[ ]
[ ]

[ metasploit v4.16.15-dev ]
+ -- --[ 1700 exploits - 968 auxiliary - 299 post ]
+ -- --[ 503 payloads - 40 encoders - 10 nops ]
+ -- --[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > search polycom_hdx traceroute exec
[!] Module database cache not built yet, using slow search

Matching Modules
=====

  Name                                     Disclosure Date  Rank      Description
  ----                                     -
  exploit/unix/misc/polycom_hdx_traceroute_exec  2017-11-12      excellent  Polycom Shell HDX Ser
ies Traceroute Command Execution

msf >
```

Adicionamos el exploit y podemos utilizarlo.

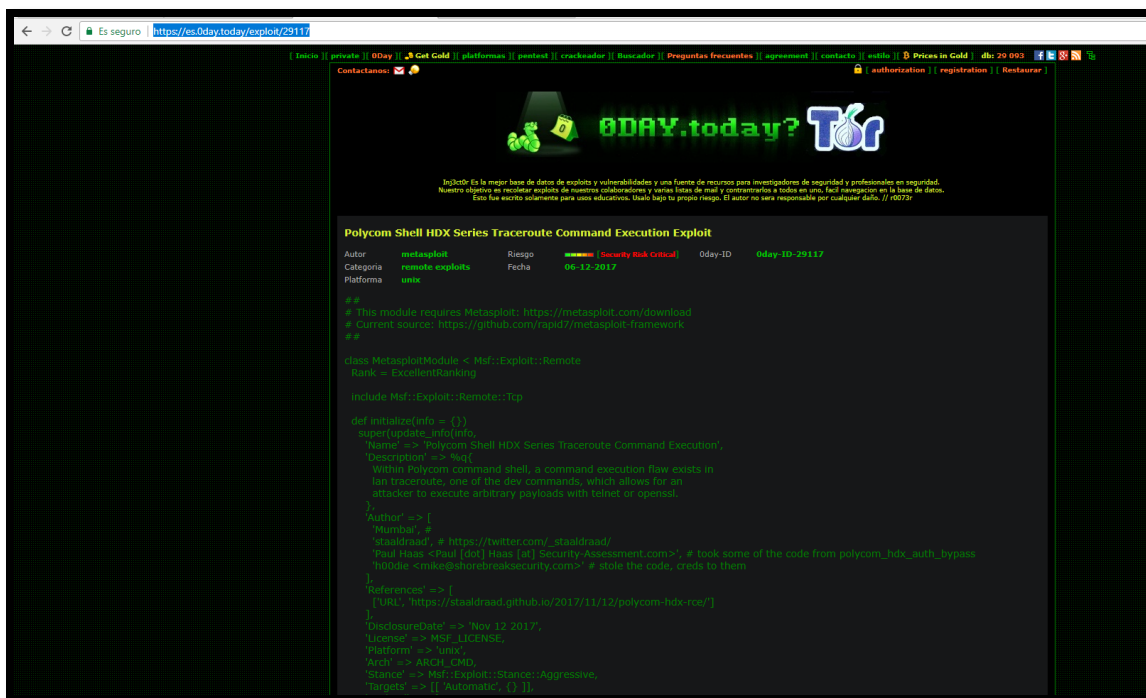


Colombia Hack Agent (CHACKA)

SEGUNDO MÉTODO

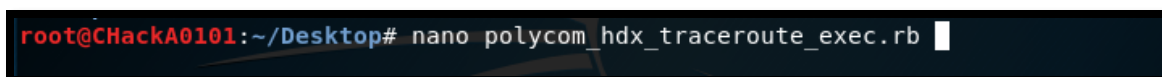
1. De igual forma existen varias formas de poderlo hacer, por ejemplo, en este segundo método, lo copiáramos desde otra fuente, por ejemplo, de;

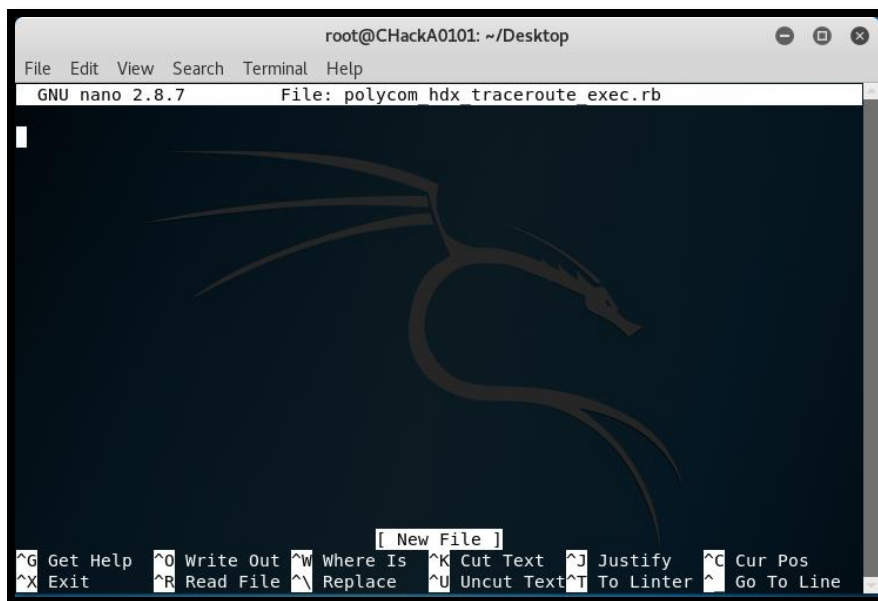
<https://es.0day.today/exploit/29117>



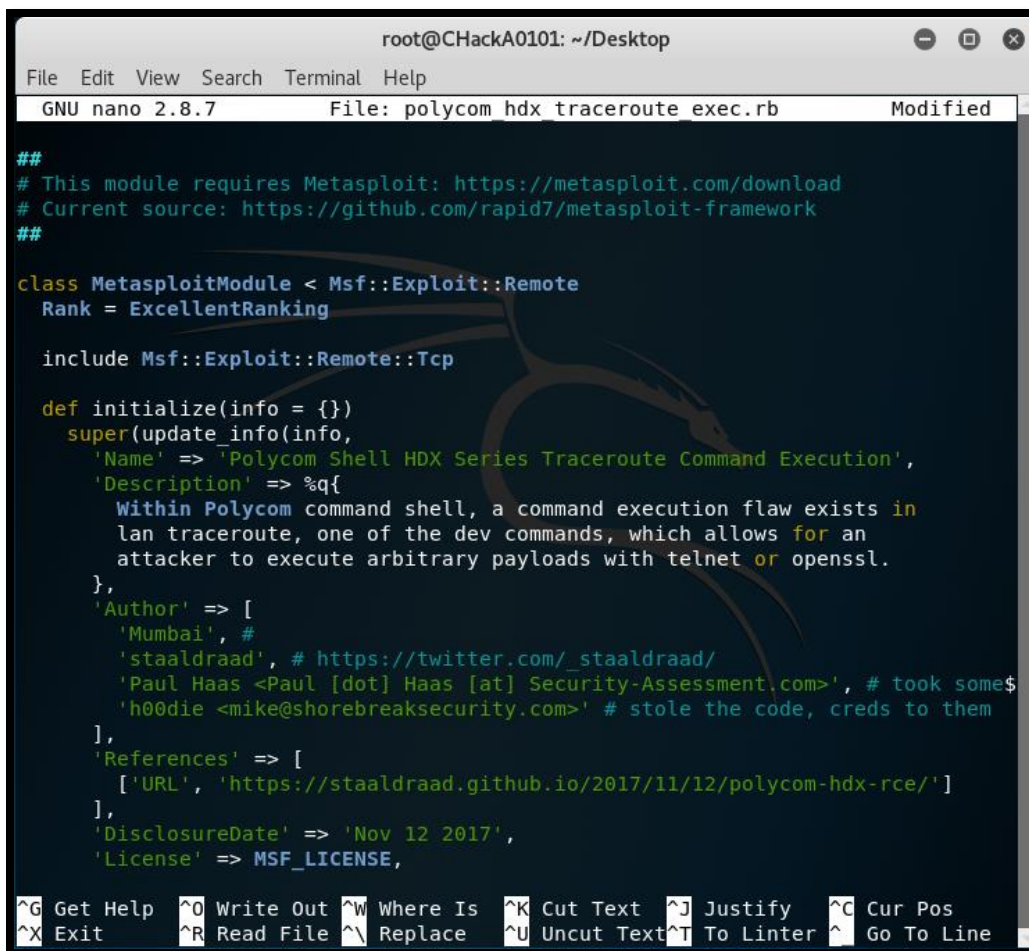
2. Creamos un archivo con el nombre del exploit y la extensión de Ruby:

```
root@CHackA0101:~/Desktop# nano polycom_hdx_traceroute_exec.rb
```





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



```
##
# 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
end
```




Colombia Hack Agent (CHACKA)

4. Lo guardamos y lo visualizamos:

The screenshot shows a Kali Linux desktop environment. On the left, a file manager window displays the desktop contents, including a folder named 'metasploit-framework' and a file named 'polycom_hdx_traceroute...'. A red arrow points from this file to the nano editor window. The nano editor window, titled 'root@CHACKA0101: ~/Desktop', shows the content of the file 'polycom_hdx_traceroute_exec.rb'. The file is a Metasploit module with the following code:

```
##
# 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
end
```

The screenshot shows a terminal window with the command 'ls -la' and its output:

```
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#
```

Yá para finalizar, copiamos el exploit creado al directorio de "Metasploit Framework" y eso ustedes yá lo saben hacer.

Agradecimientos a:

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

-END-