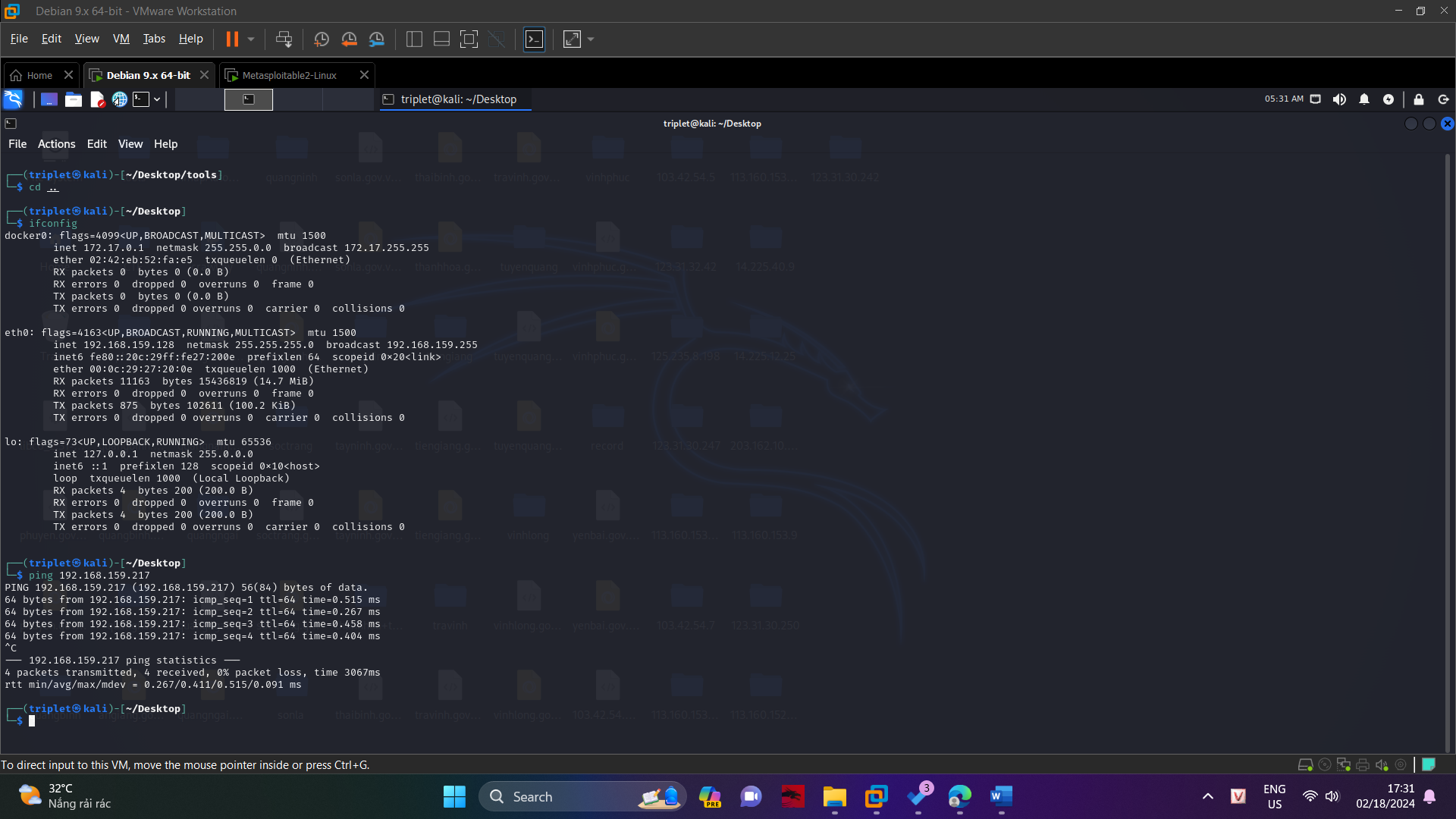
Họ và tên: Trần Minh Triết

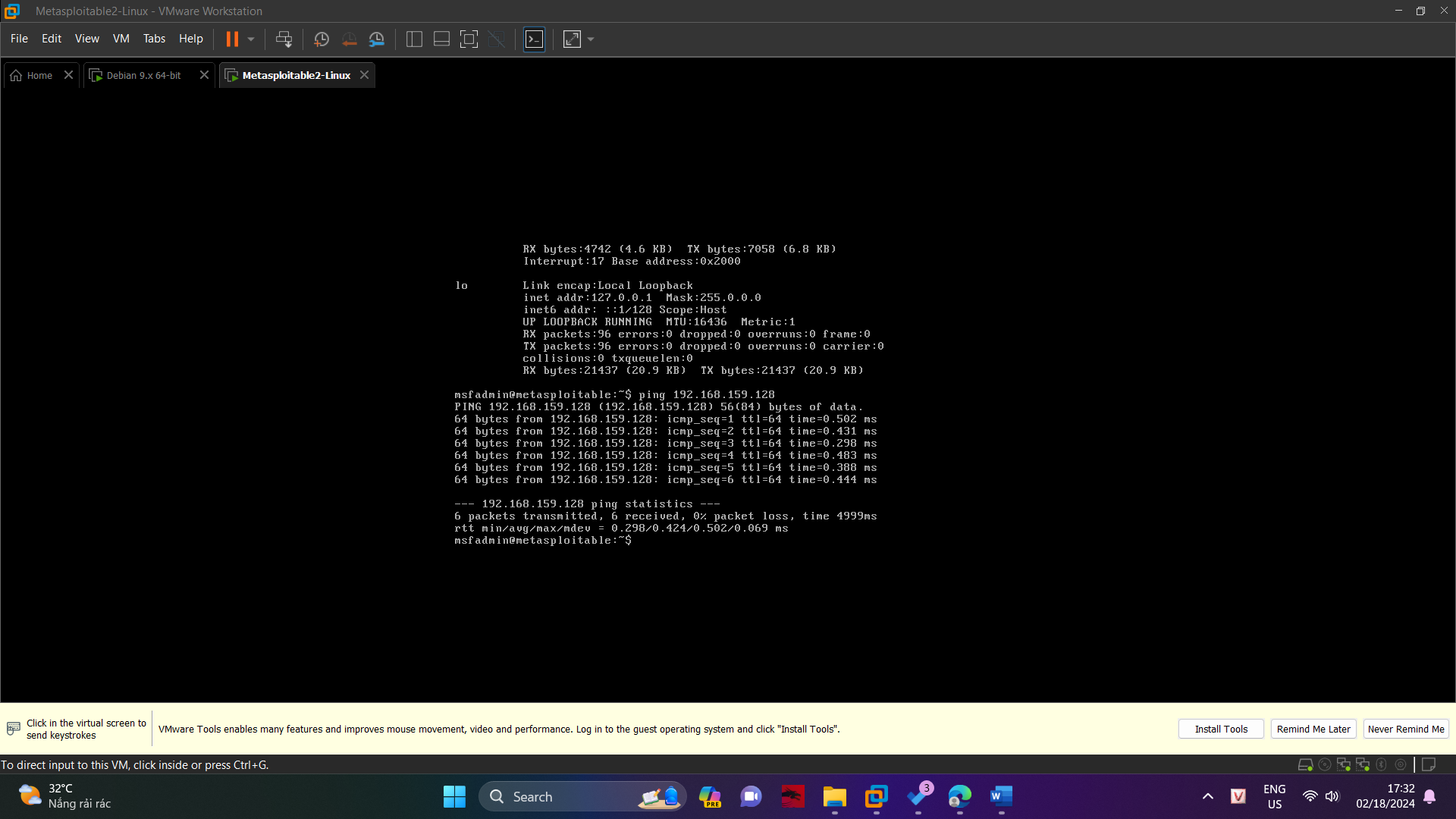
MSSV: SE172241

Class: IA1702

**Lab 8: Metasploit v Linux**

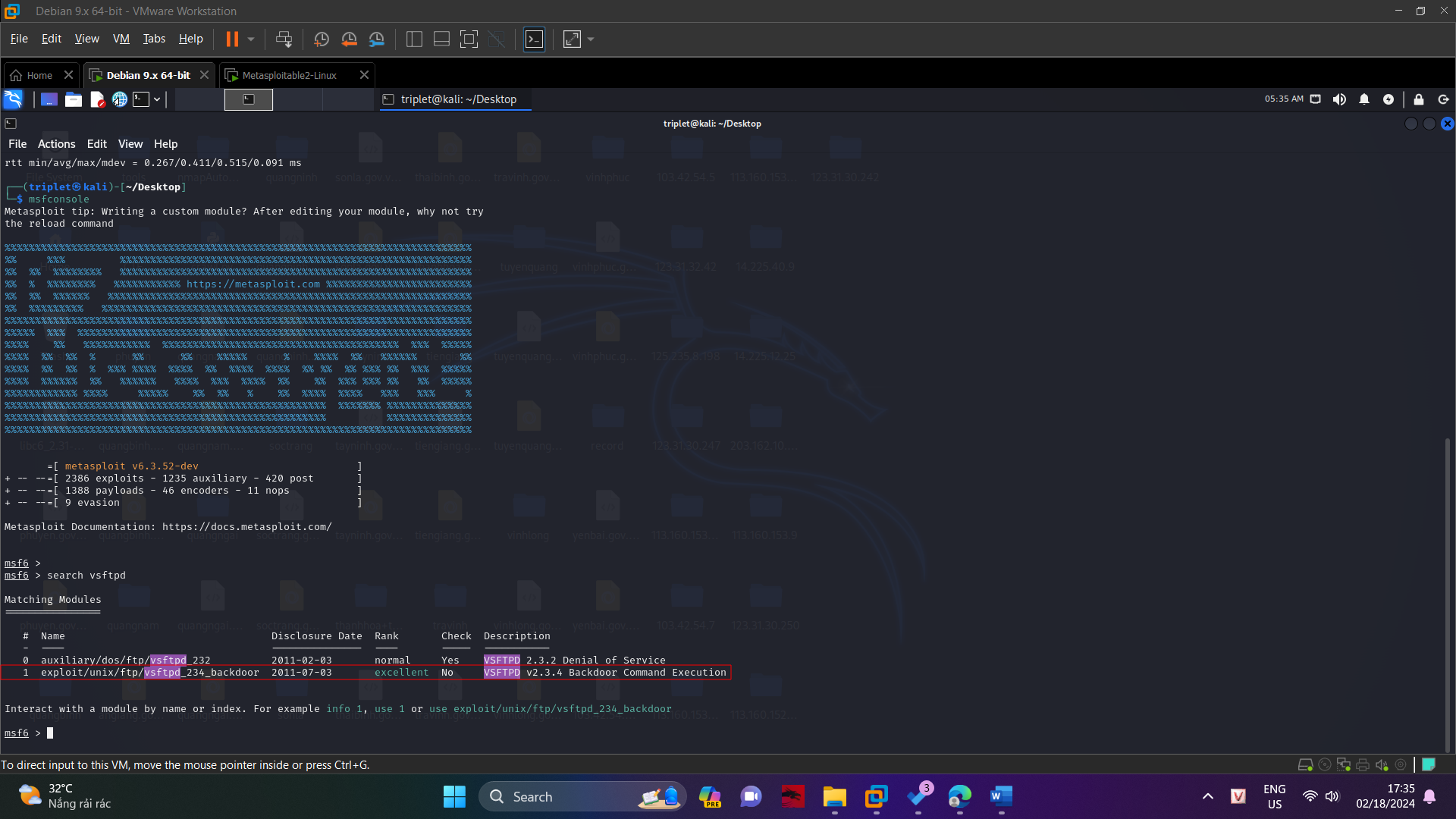
**Task 1: Exploiting vsftpd**





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.

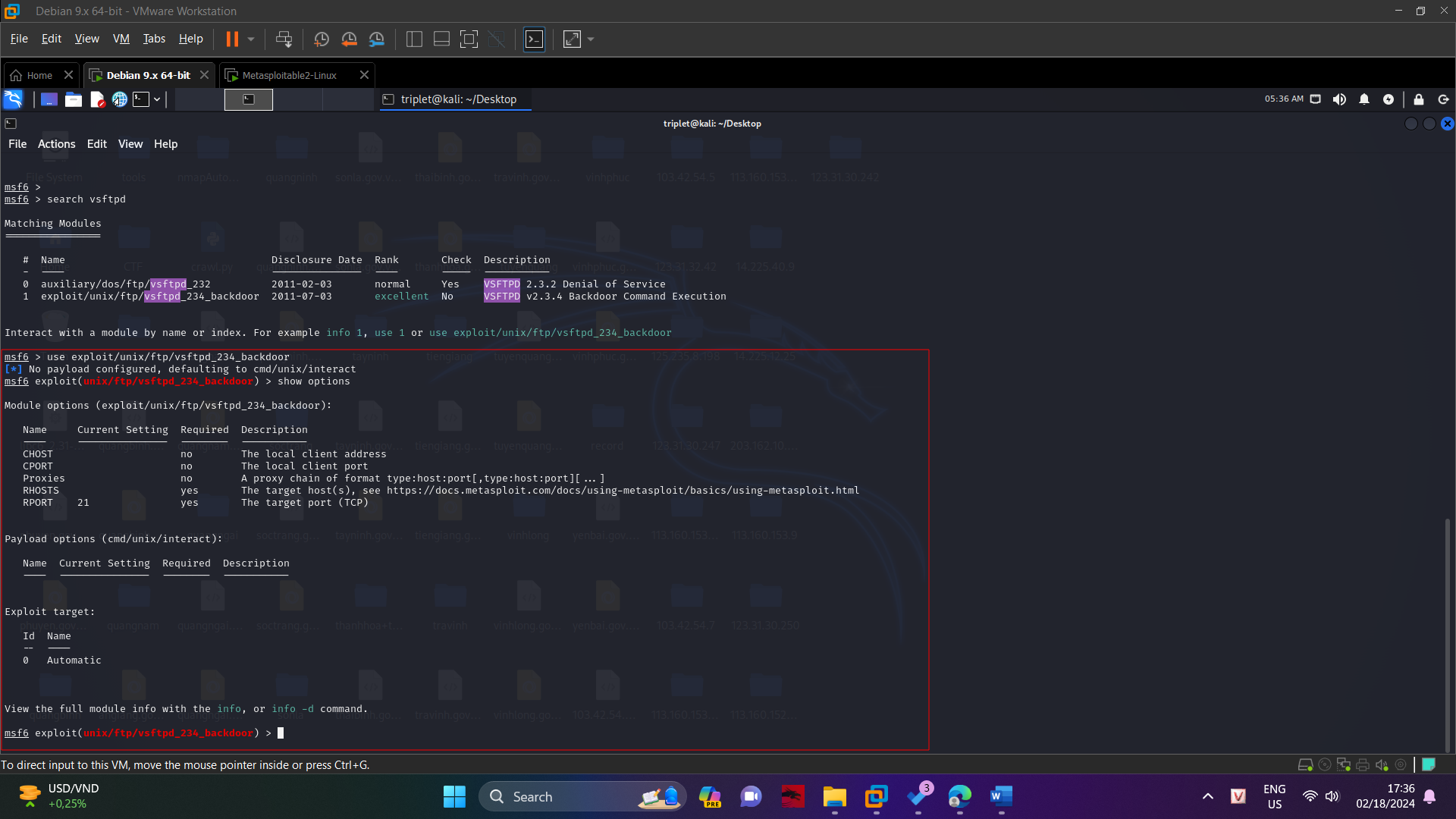


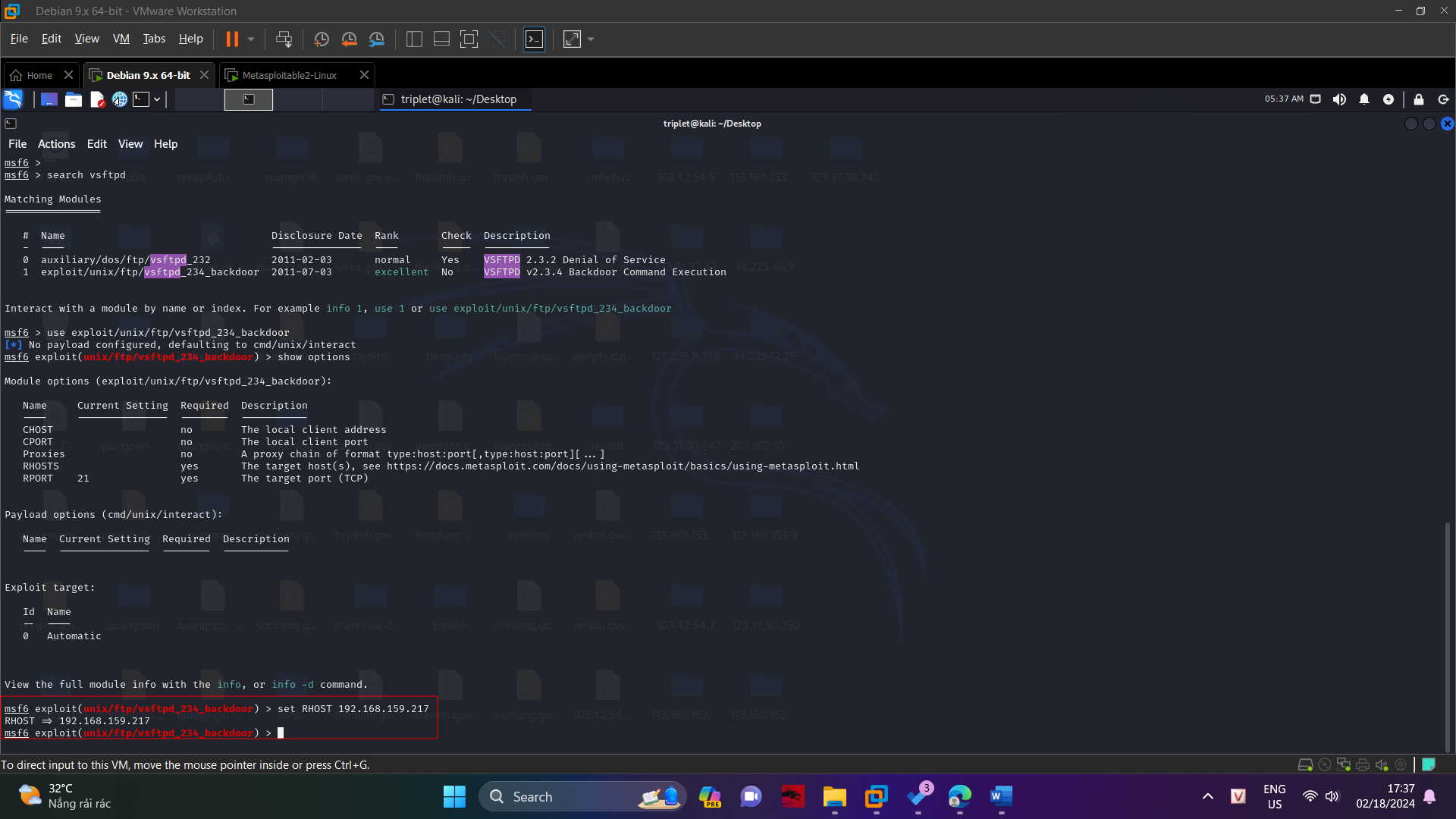
Execute these commands:

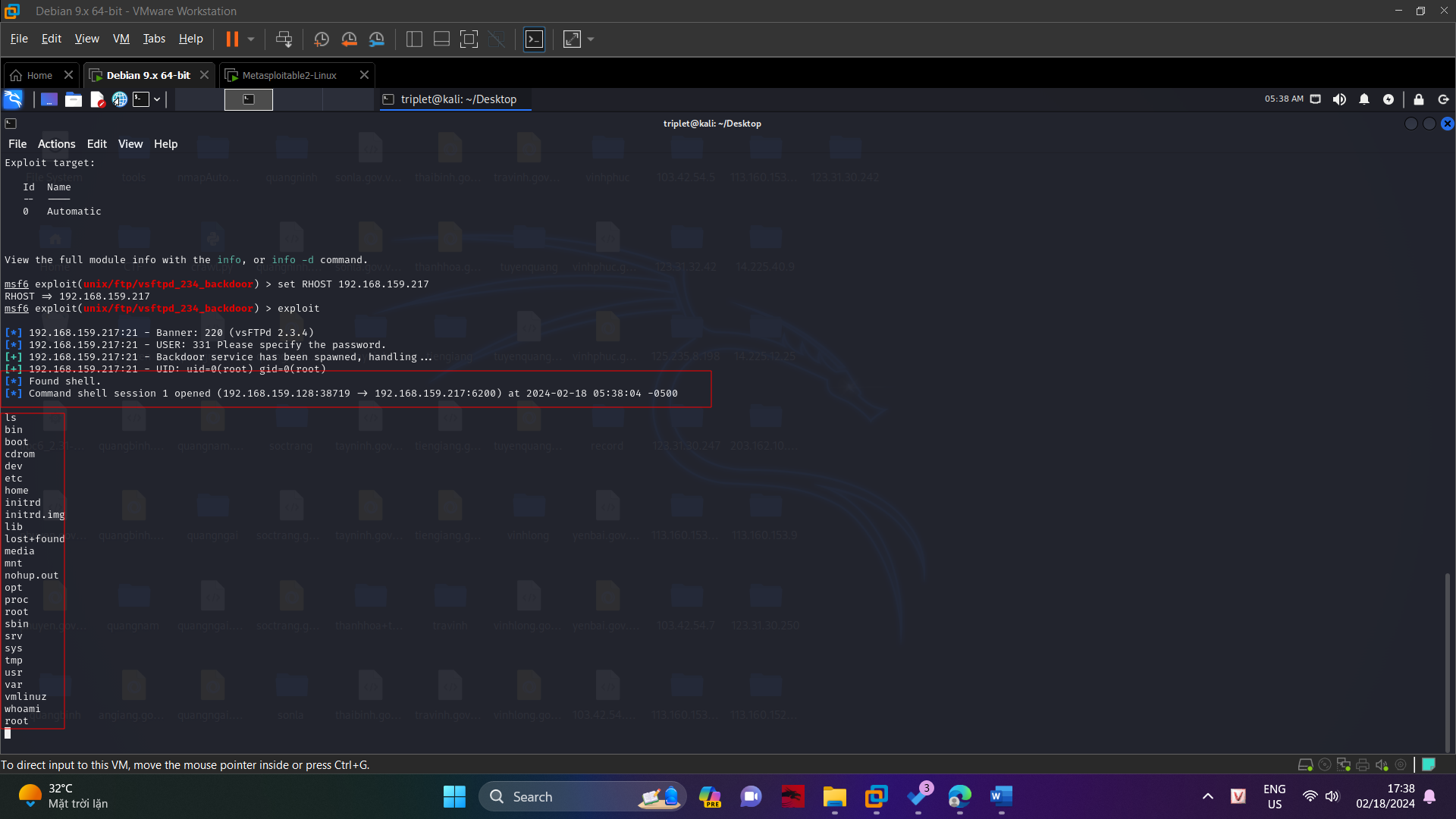
use exploit/unix/ftp/vsftpd\_234\_backdoor

show options

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







**Task 2: Exploiting Unreal IRCd**

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

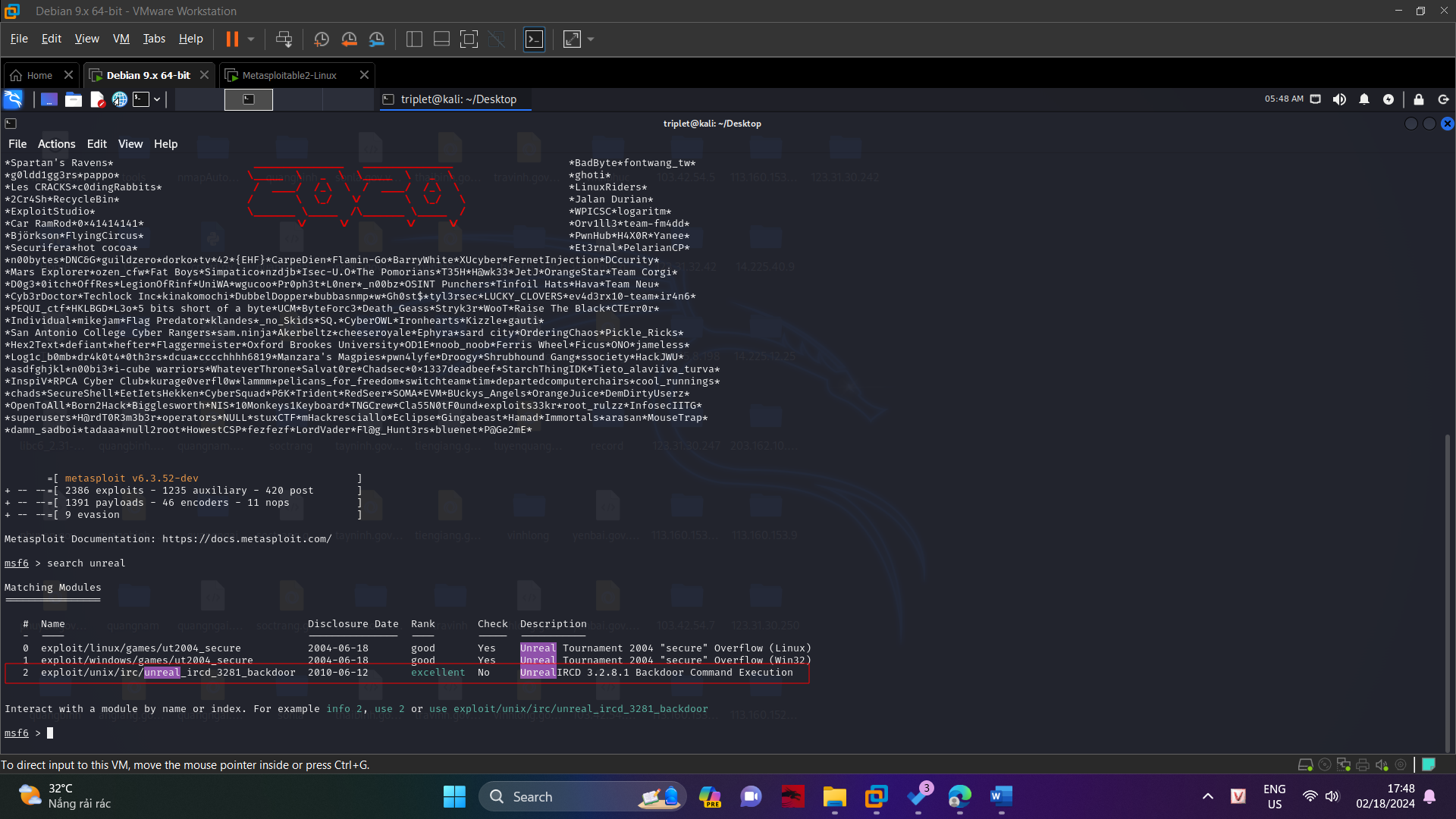
In Kali, execute this command to open Metasploit.

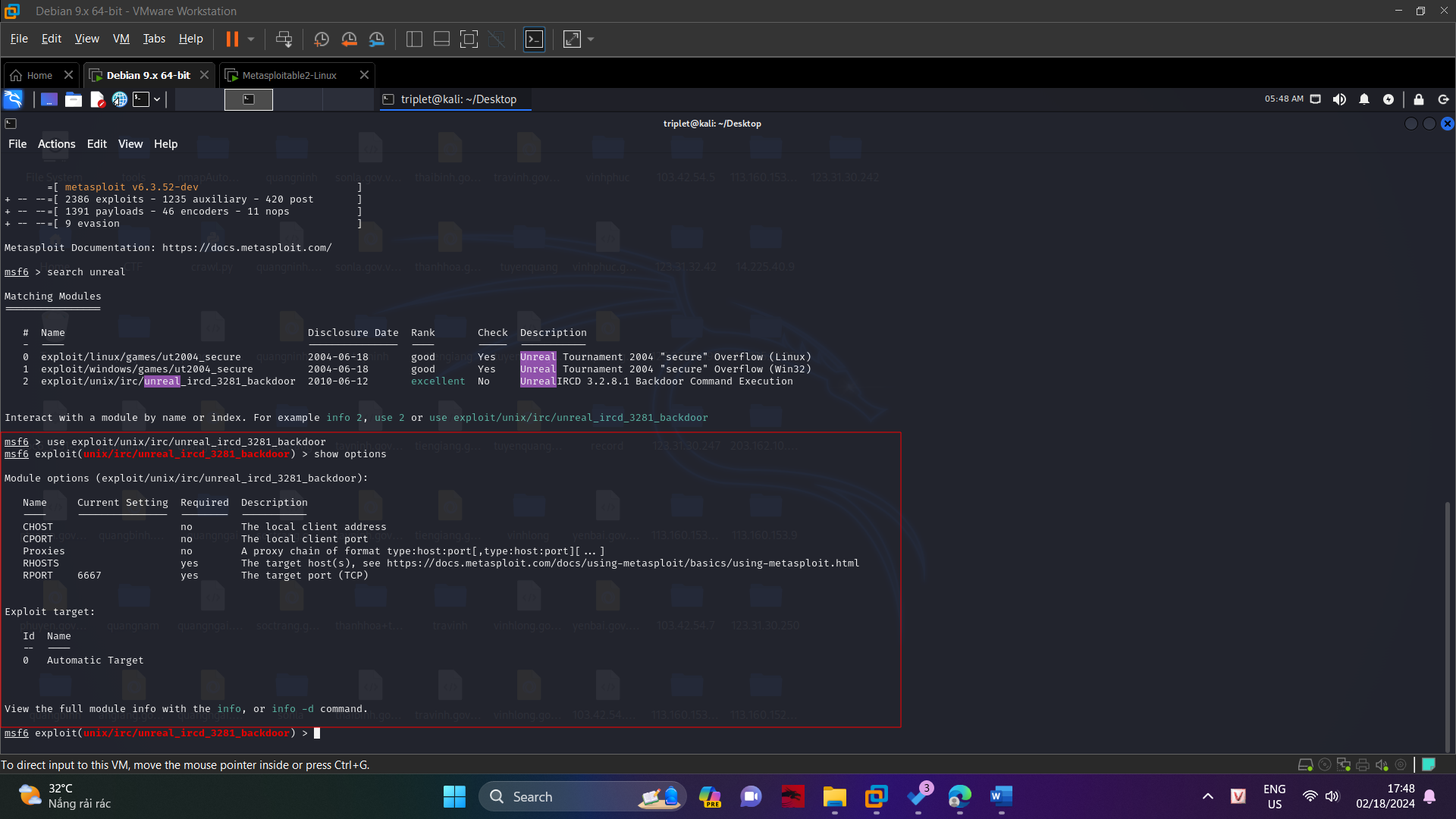
msfconsole

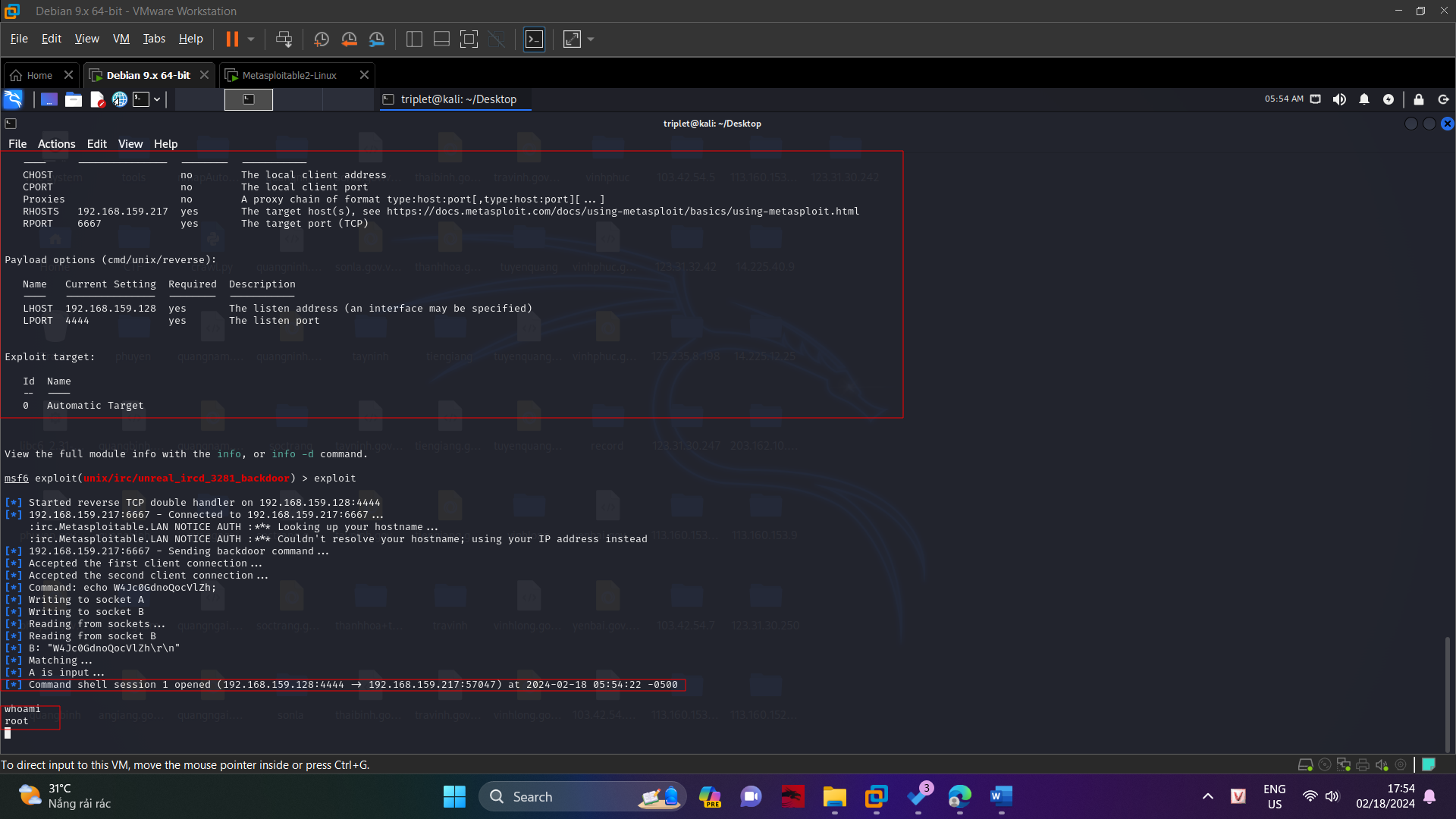
At the "msf>" prompt, execute this command.

search unreal

As shown below, one exploit is found



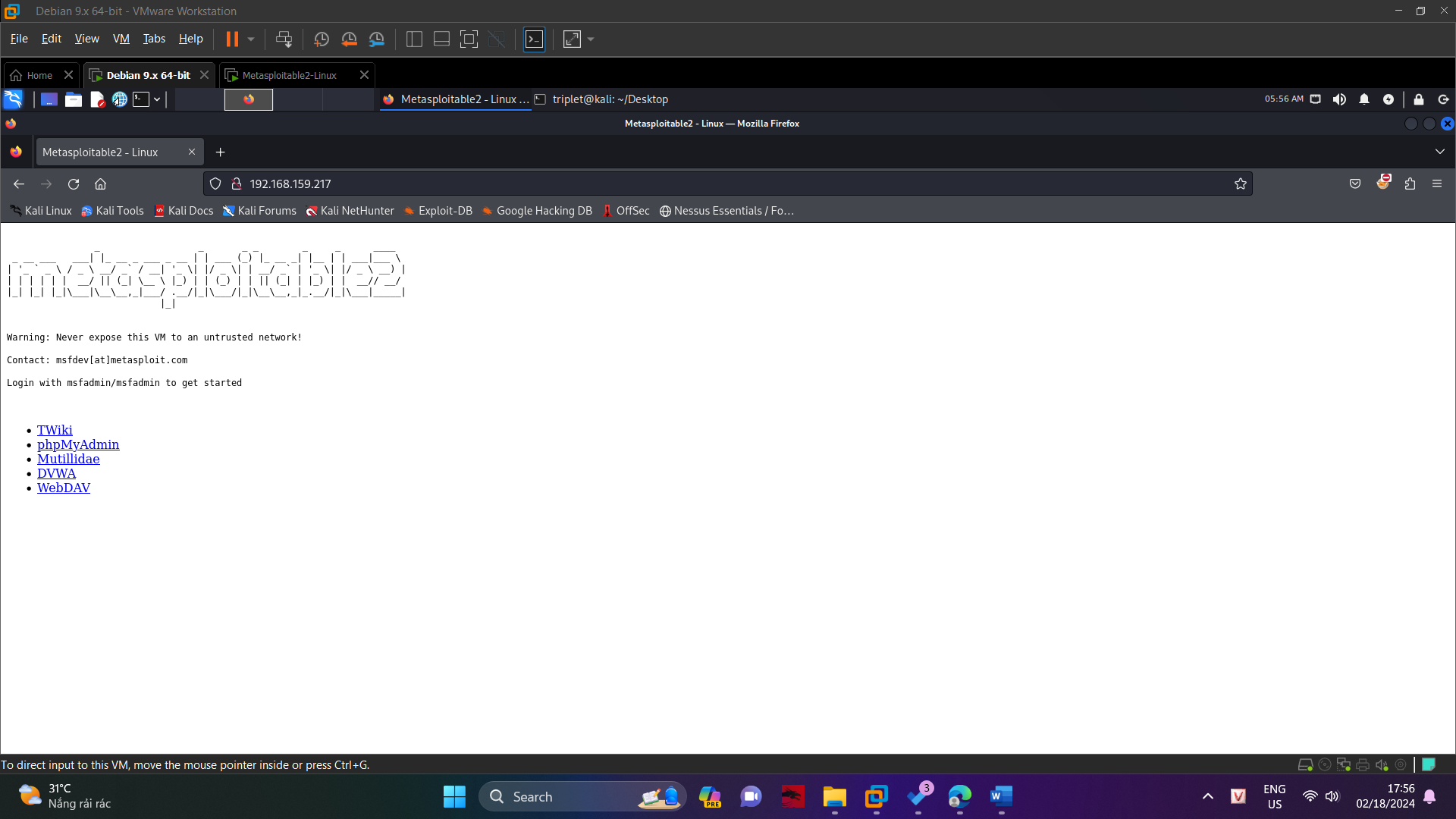


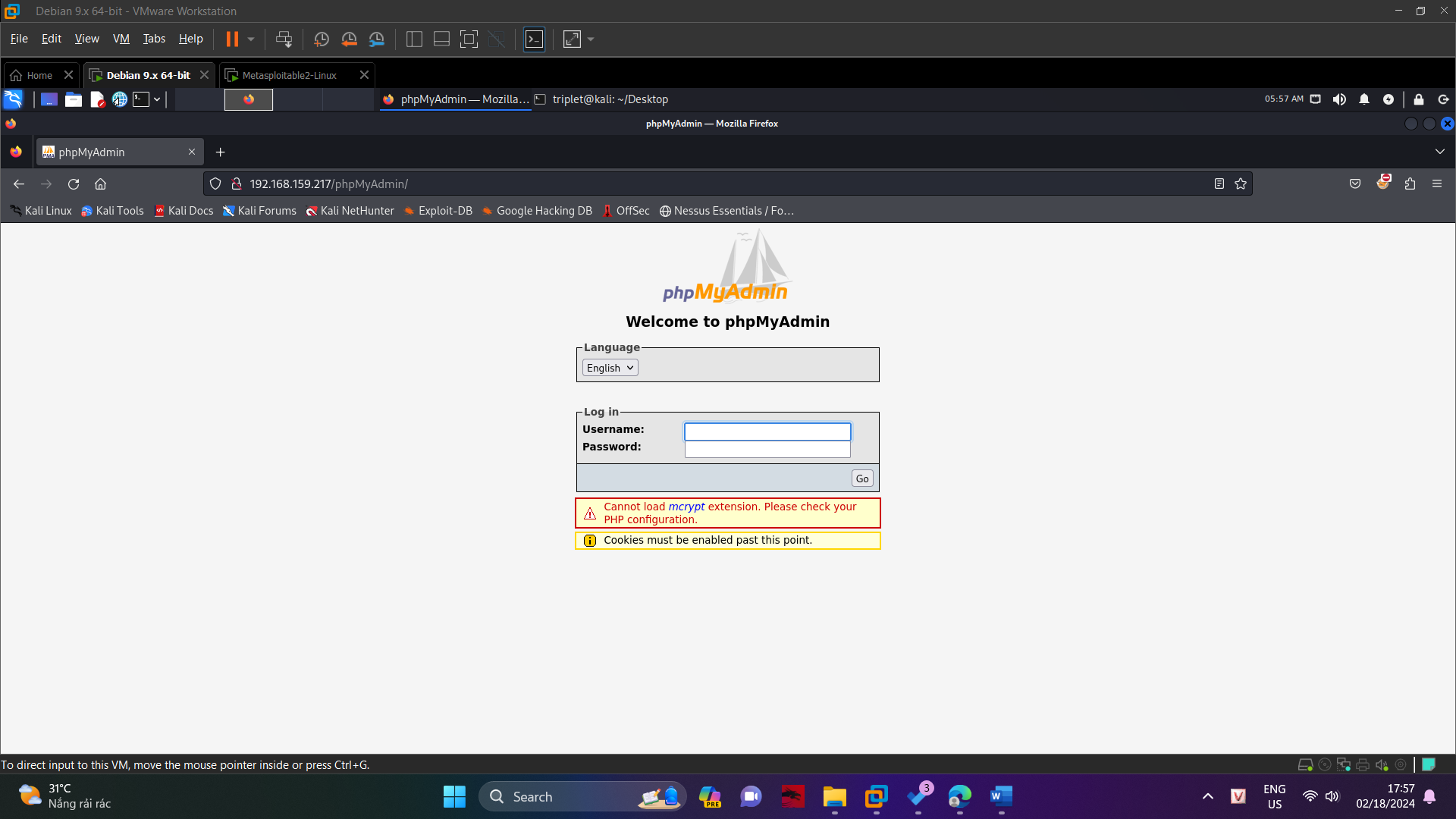


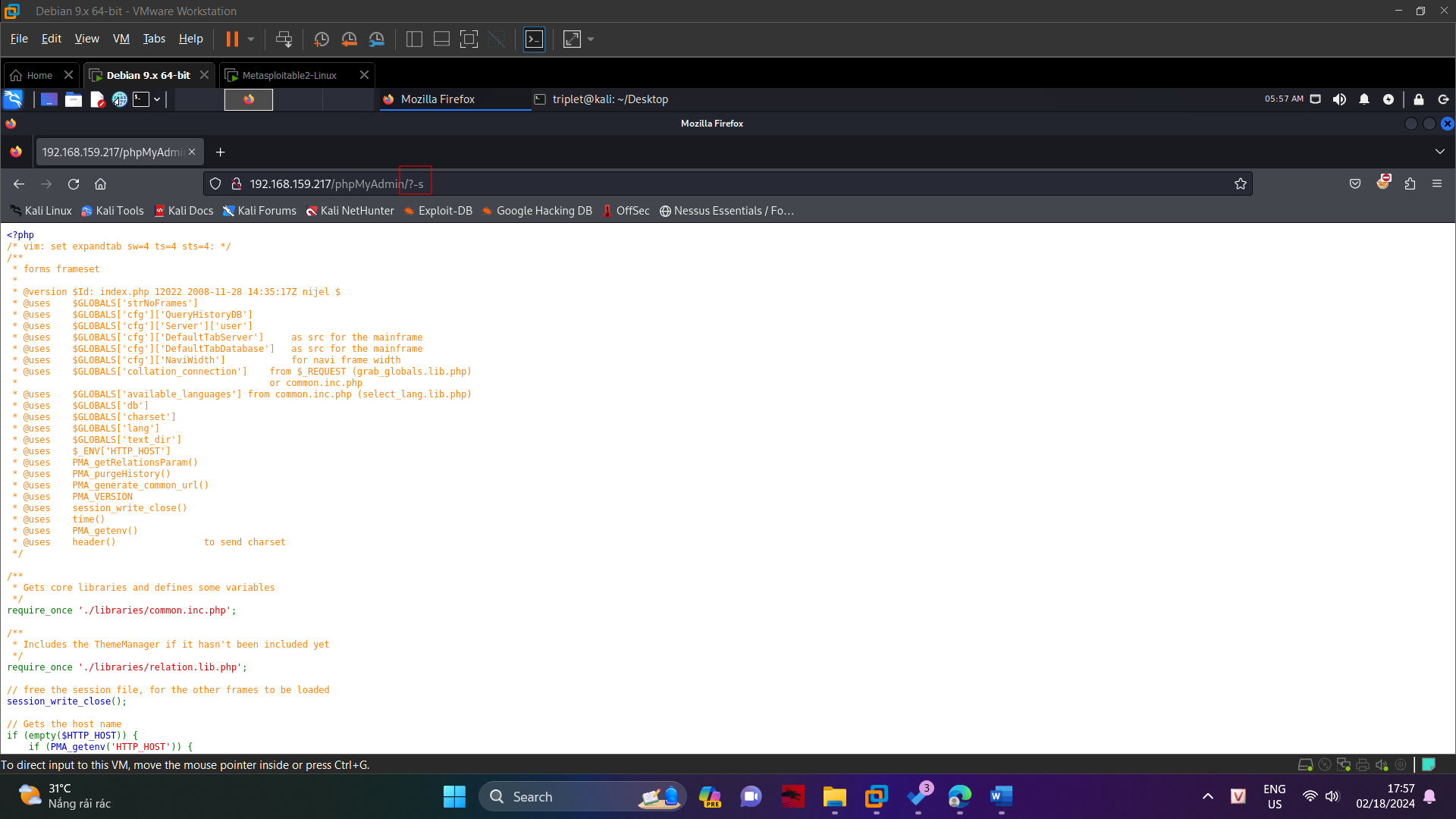
**Task 3: Exploiting PHP CGI Argument Injection**

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

A Web page opens, as shown below.







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.

