

LAB 3

Fuzzing - Reverse Engineering - Cryptography

Họ tên và MSSV: Nguyễn Thiên Tính - 0950080144

Link youtube: <https://www.youtube.com/@TinhNguyenThien-dp8iq/videos>

- *Các sinh viên bị phát hiện sao chép bài của nhau sẽ nhận 0đ cho TẤT CẢ các bài thực hành của môn này.*
- *Bài nộp phải ở dạng PDF, hình minh họa phải rõ ràng chi tiết. Hình minh họa chỉ cần chụp ở nội dung thực hiện, không chụp toàn màn hình.*

- Trình bày chi tiết từng bước 1

- ***Quay lại quá trình làm bài***, đưa video vào youtube và add link youtube vào trong file word, không gửi qua google drive, sv không có video sẽ không được chấm bài.

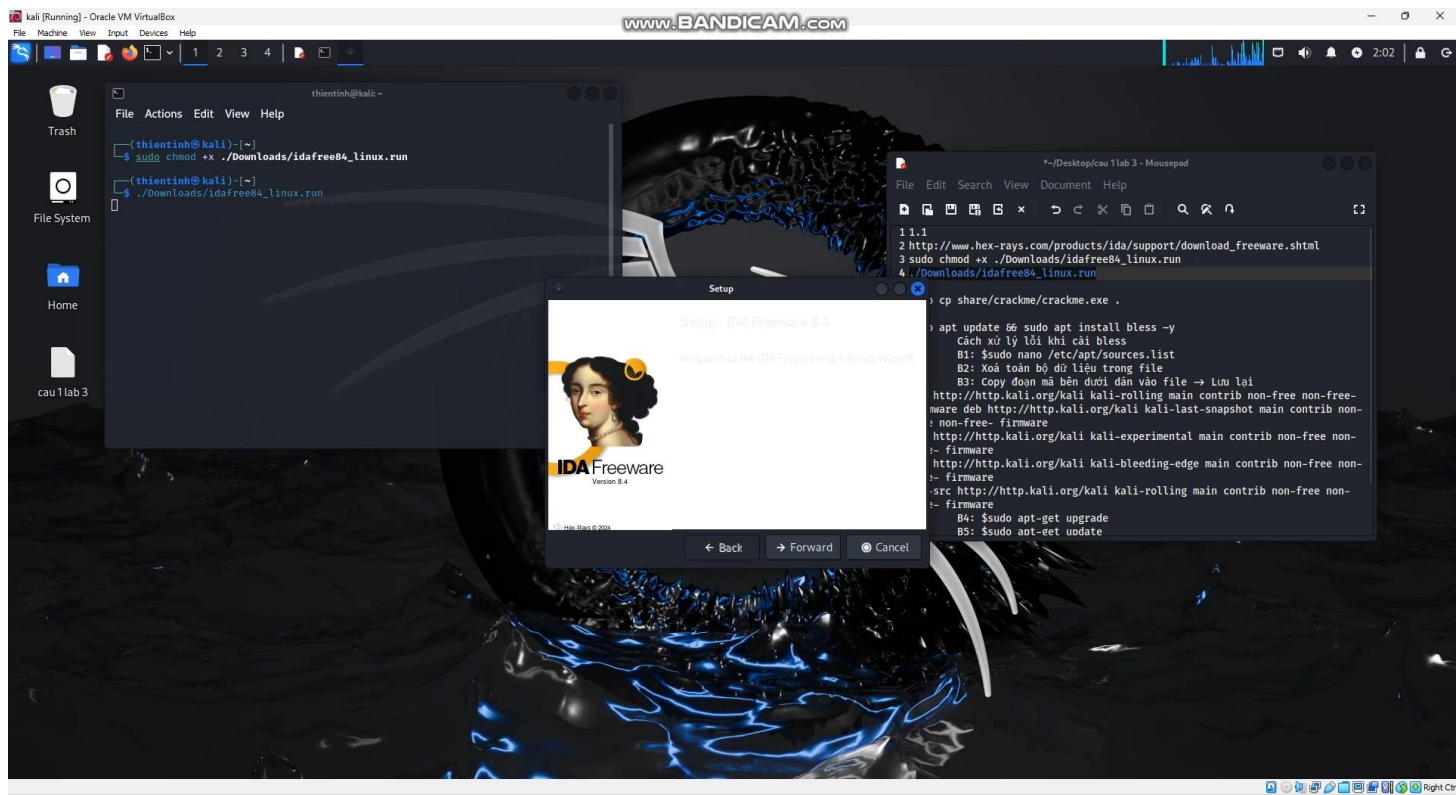
Lưu ý: sử dụng tài khoản là mã số sinh viên (đã tạo ở Câu 1.4 - Lab01) để thực hiện tất cả các câu trong bài thực hành. Tất cả các câu trong bài thực hành này được thực hiện trên Kali Linux

Câu 1: Thực hiện kỹ thuật Reverse Engineering với công cụ IDA Free

1.1. Cài đặt [IDA Free](#) vào Kali Linux. Tải file cài đặt (ví dụ: idafree83_linux.run):

```
$sudo chmod +x ./Downloads/idafree84_linux.run
```

```
$/Downloads/idafree84_linux.run
```



Tài và cài đặt IDA

- Thực hiện các bước theo yêu cầu. IDA Free sẽ được cài đặt ở thư mục cá nhân của người dùng.



1.2. Trên máy Windows, tải file Lab03.zip. Giải nén sẽ được thư mục crackme chứa 02 file crackme.exe

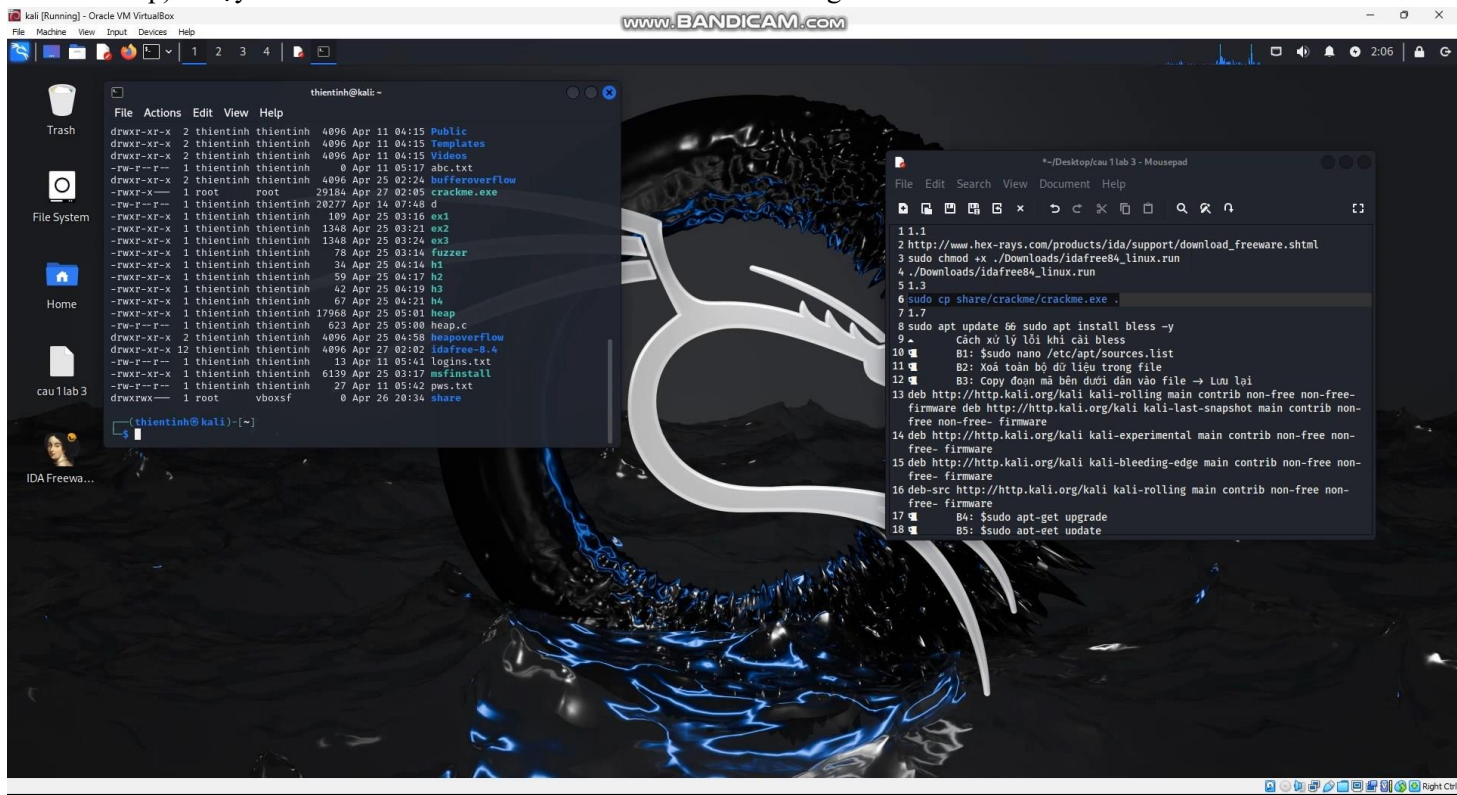
và msvcrt100d.dll. Chạy file crackme.exe ở môi trường CMD với vài giá trị đầu vào khác nhau và xem kết quả.

```
C:\Users\Admin\Downloads\Compressed\Lab03\crackme>crackme.exe .
Fail!

C:\Users\Admin\Downloads\Compressed\Lab03\crackme>crackme.exe . abc
Usage: game3.exe password

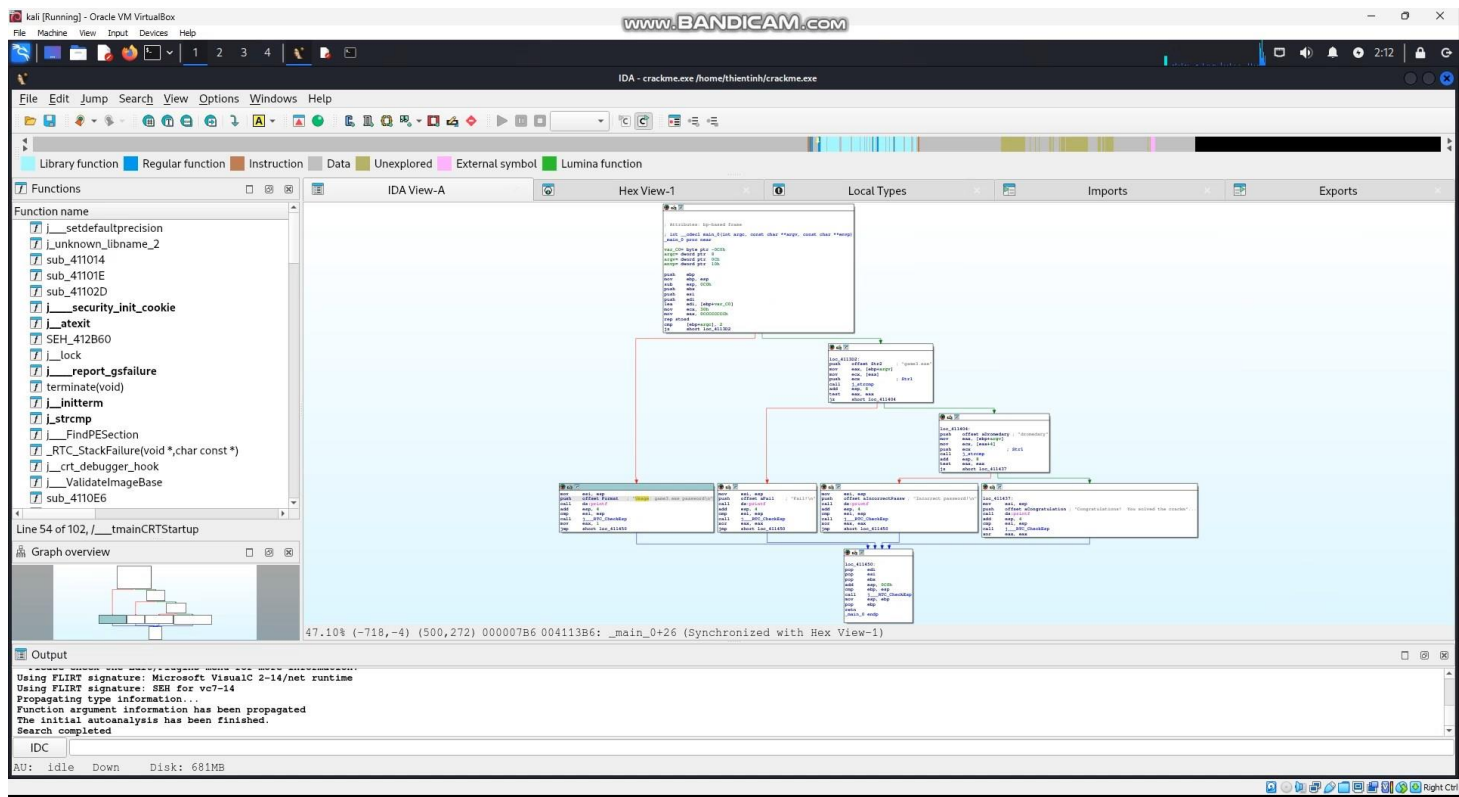
C:\Users\Admin\Downloads\Compressed\Lab03\crackme>
```

1.3. Di chuyển file crackme.exe vào máy ảo Kali Linux (sử dụng chức năng Shared Folders hoặc Drag and Drop). Chạy IDA Free và mở file crackme.exe trên môi trường IDA Free.



Dùng lệnh để copy file: `$sudo cp share/crackme/crackme.exe .`

1.4. Trên thanh menu, sử dụng chức năng “Search, Text” tìm kiếm với từ khóa “usage”. Trên cửa sổ “IDA - View A” chọn “Fit window”. Chọn “Text view” hoặc “Graph view” để xem mã Assembly của chương trình.



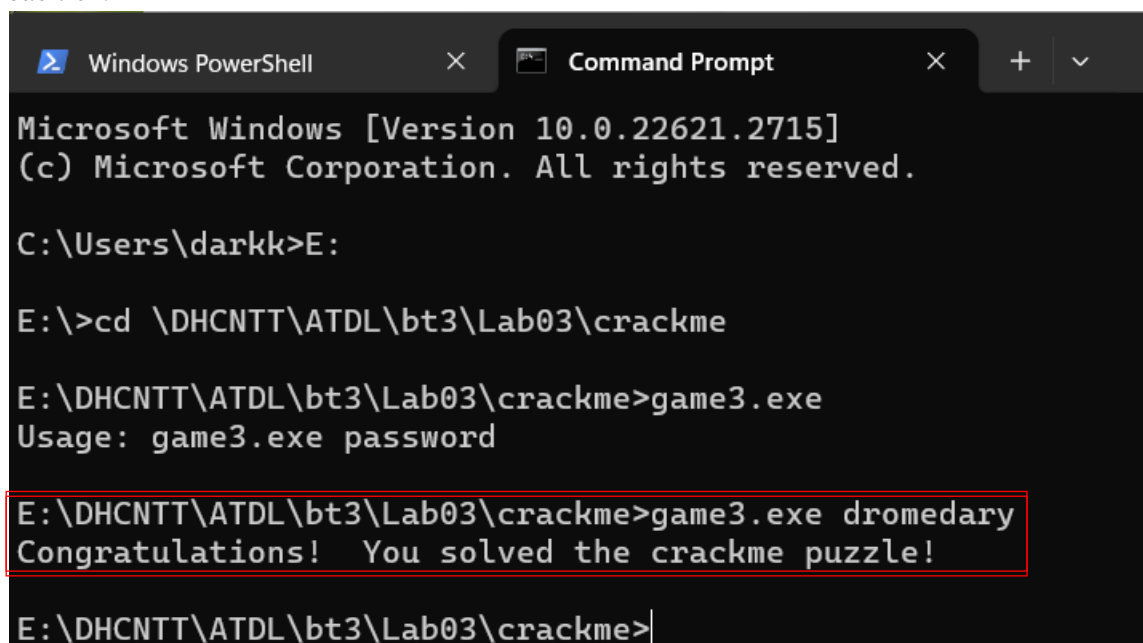
1.5 Trên thanh menu, sử dụng chức năng “View, Sub view, Generate pseudo code” (F5) để sinh mã giả của crackme.exe. Trên cửa sổ “Pseudocode - A”, sử dụng chức năng “Synchronize with” để đồng bộ với “IDA - View A” và “Hex - View 1”.

```

1 int __cdecl main_0(int argc, const char **argv, const char **envp)
2 {
3     if ( argc == 2 )
4     {
5         if ( !_j_strcmp(*argv, "game3.exe") )
6         {
7             if ( !_j_strcmp(argv[1], "dromedary") )
8                 printf("Congratulations! You solved the crackme puzzle!\n");
9             else
10                printf("Incorrect password!\n");
11            return 0;
12        }
13    }
14    else
15    {
16        printf("Fail!\n");
17        return 0;
18    }
19    else
20    {
21        printf("Usage: game3.exe password\n");
22        return 1;
23    }
24 }

```

1.6 Phân tích mã giả của crackme.exe để có thể chạy chương trình in ra thông báo "Congratulations! You solved the crackme puzzle!". Chạy file crackme.exe ở môi trường CMD của máy Windows in ra thông báo trên.



```

Microsoft Windows [Version 10.0.22621.2715]
(c) Microsoft Corporation. All rights reserved.

C:\Users\darkkk>E:

E:\>cd \DHCNTT\ATDL\bt3\Lab03\crackme

E:\DHCNTT\ATDL\bt3\Lab03\crackme>game3.exe
Usage: game3.exe password

E:\DHCNTT\ATDL\bt3\Lab03\crackme>game3.exe dromedary
Congratulations! You solved the crackme puzzle!

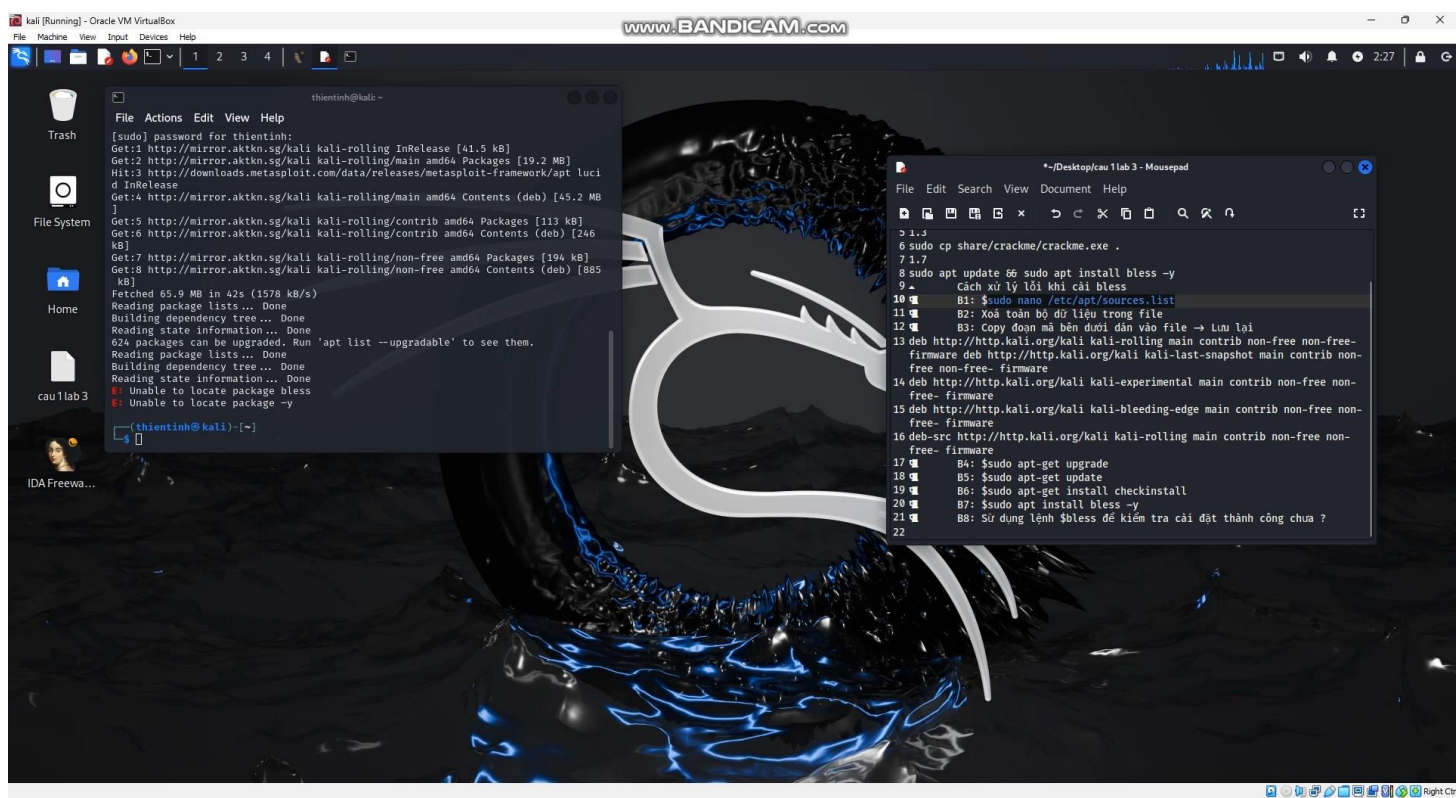
E:\DHCNTT\ATDL\bt3\Lab03\crackme>

```

1.7. Cài đặt công cụ Bless hex editor vào Kali Linux:

- Cài đặt Bless

\$ sudo apt update && sudo apt install bless -y

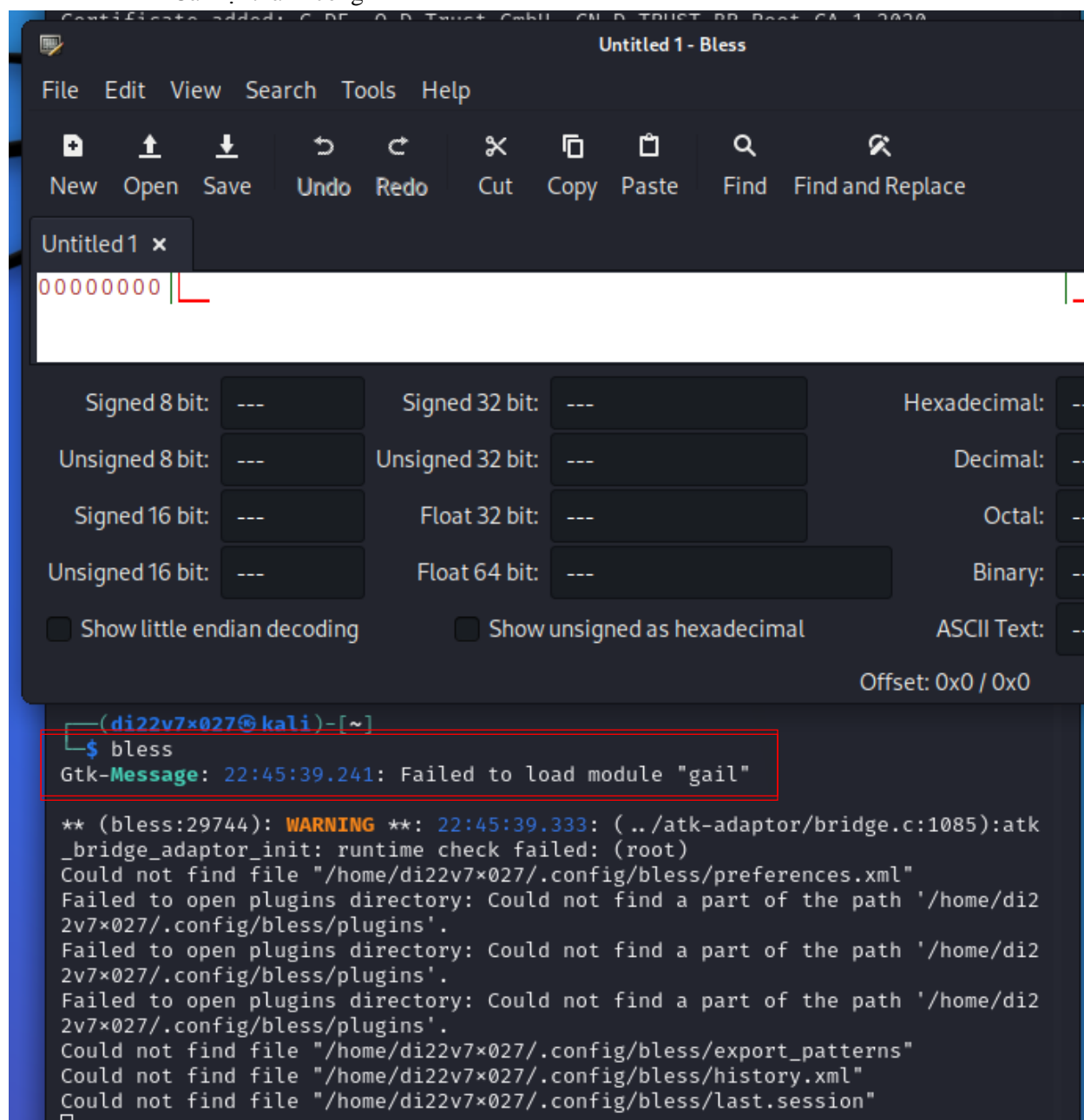


Nếu trong quá trình cài đặt bless xảy ra lỗi như hình bên dưới thì làm như sau

- Cách xử lý lỗi khi cài bless

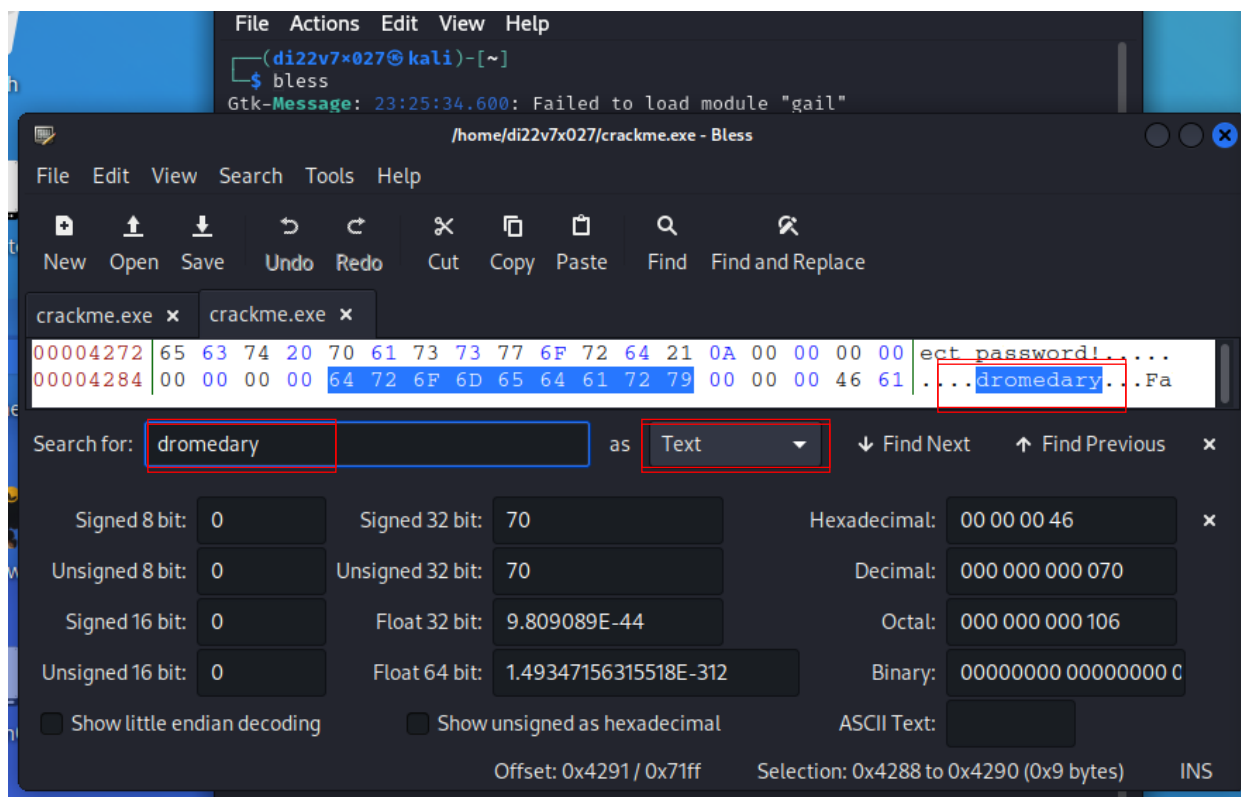
- ✓ B1: **\$sudo nano /etc/apt/sources.list**
- ✓ B2: Xóa toàn bộ dữ liệu trong file
- ✓ B3: Copy đoạn mã bên dưới dán vào file -> Lưu lại
deb http://http.kali.org/kali kali-rolling main contrib non-free non-free-firmware
deb http://http.kali.org/kali kali-last-snapshot main contrib non-free non-free-firmware
deb http://http.kali.org/kali kali-experimental main contrib non-free non-free-firmware
deb http://http.kali.org/kali kali-bleeding-edge main contrib non-free non-free-firmware
deb-src http://http.kali.org/kali kali-rolling main contrib non-free non-free-firmware
- ✓ B4: **\$sudo apt-get upgrade**
- ✓ B5: **\$sudo apt-get update**
- ✓ B6: **\$sudo apt-get install checkinstall**
- ✓ B7: **\$sudo apt install bless -y**
- ✓ B8: Sử dụng lệnh **\$bless** để kiểm tra cài đặt thành công chưa ?

➤ Cài đặt thành công

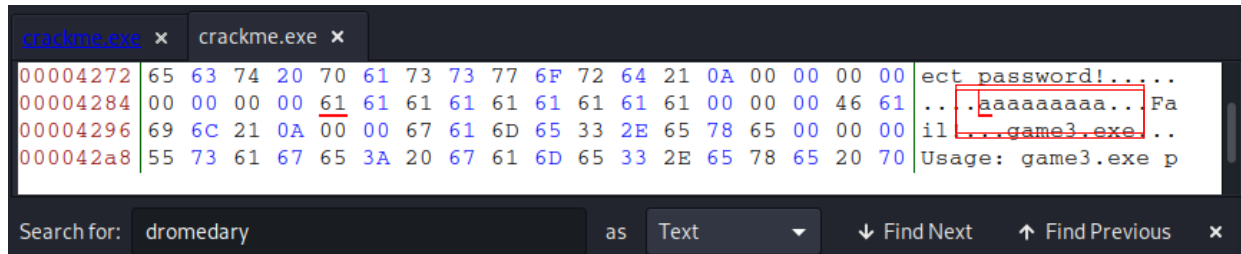


1.8. Sử dụng công cụ Bless hex editor để thay đổi giá trị password cần nhập cho crackme.exe thành “aaaaaaaa”. Di chuyển file crackme.exe từ Kali Linux qua máy Windows. Chạy file crackme.exe ở môi trường CMD của máy Windows in ra thông báo trên “Congratulations! You solved the crackme puzzle!”

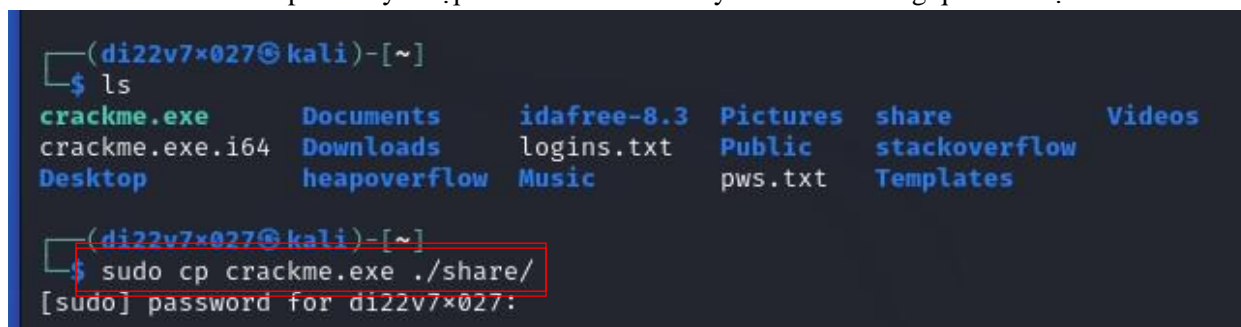
- Gõ lệnh: **\$bless** để mở công cụ chỉnh sửa
- Tiếp theo vào **Open** mở file **crackme**
- **Search -> Find ->** tìm kiếm từ **dromedary** chọn **as Text**



- Thay đổi mật khẩu từ **dromedary** bằng **aaaaaaaa** -> **Save** - > tắt công cụ **bless**



- Sao chép di chuyển tập tin **crackme** vào máy **Windows** thông qua thư mục **share**



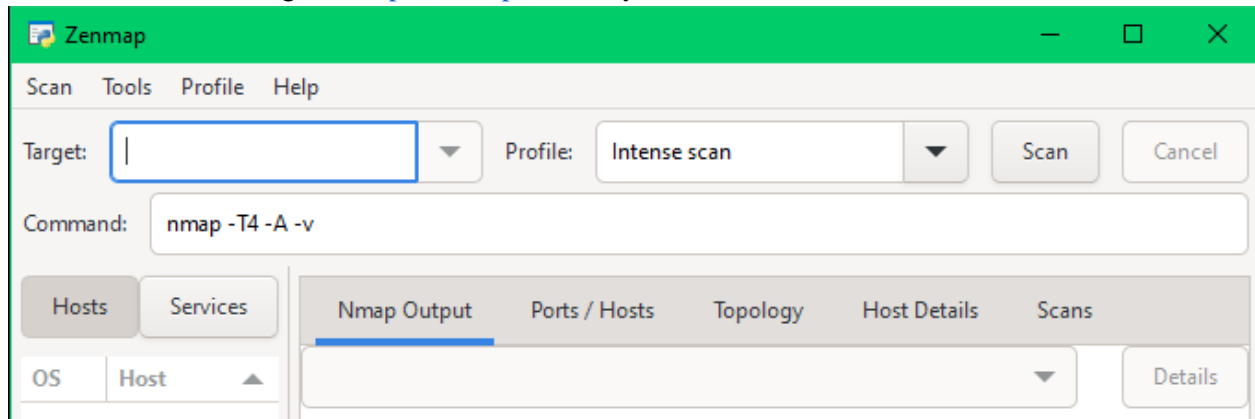
- Vào thư mục **crackme** trong máy Windows xóa file **game3 cũ**
- Copy file **crackme** vào thư mục **crackme** và đổi tên thành **game3**
- Mở CMD của Windows và thực thi file **game3.exe** với mật khẩu là **aaaaaaaa**

```
E:\DATA\CAU_HAI\STUDY\ATHT\bt3\Lab03\crackme>game3.exe aaaaaaaaaa
Congratulations! You solved the crackme puzzle!

E:\DATA\CAU_HAI\STUDY\ATHT\bt3\Lab03\crackme>_
```

Câu 2: Thực hiện kỹ thuật Fuzzing với công cụ Spike

- Cài đặt công cụ [nmap \(Zenmap\)](#) trên máy Windows.



- Tắt tường lửa trên máy Windows

Customize settings for each type of network

You can modify the firewall settings for each type of network that you use.

Private network settings

- ☒ Turn on Windows Defender Firewall
 - ☐ Block all incoming connections, including those in the list of allowed apps
 - ☐ Notify me when Windows Defender Firewall blocks a new app

- ☒ Turn off Windows Defender Firewall (not recommended)

Public network settings

- ☒ Turn on Windows Defender Firewall
 - ☐ Block all incoming connections, including those in the list of allowed apps
 - ☐ Notify me when Windows Defender Firewall blocks a new app

- ☒ Turn off Windows Defender Firewall (not recommended)

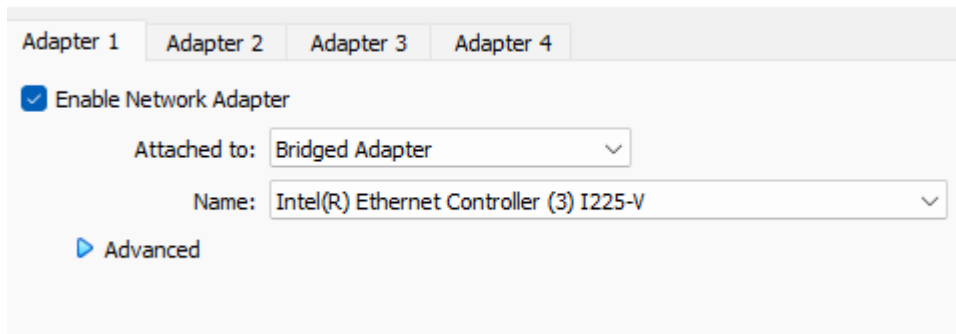
- Thực hiện dịch vụ Netcat ở môi trường CMD của máy Windows:

Gõ lệnh: **>ncat -vklp 9000**

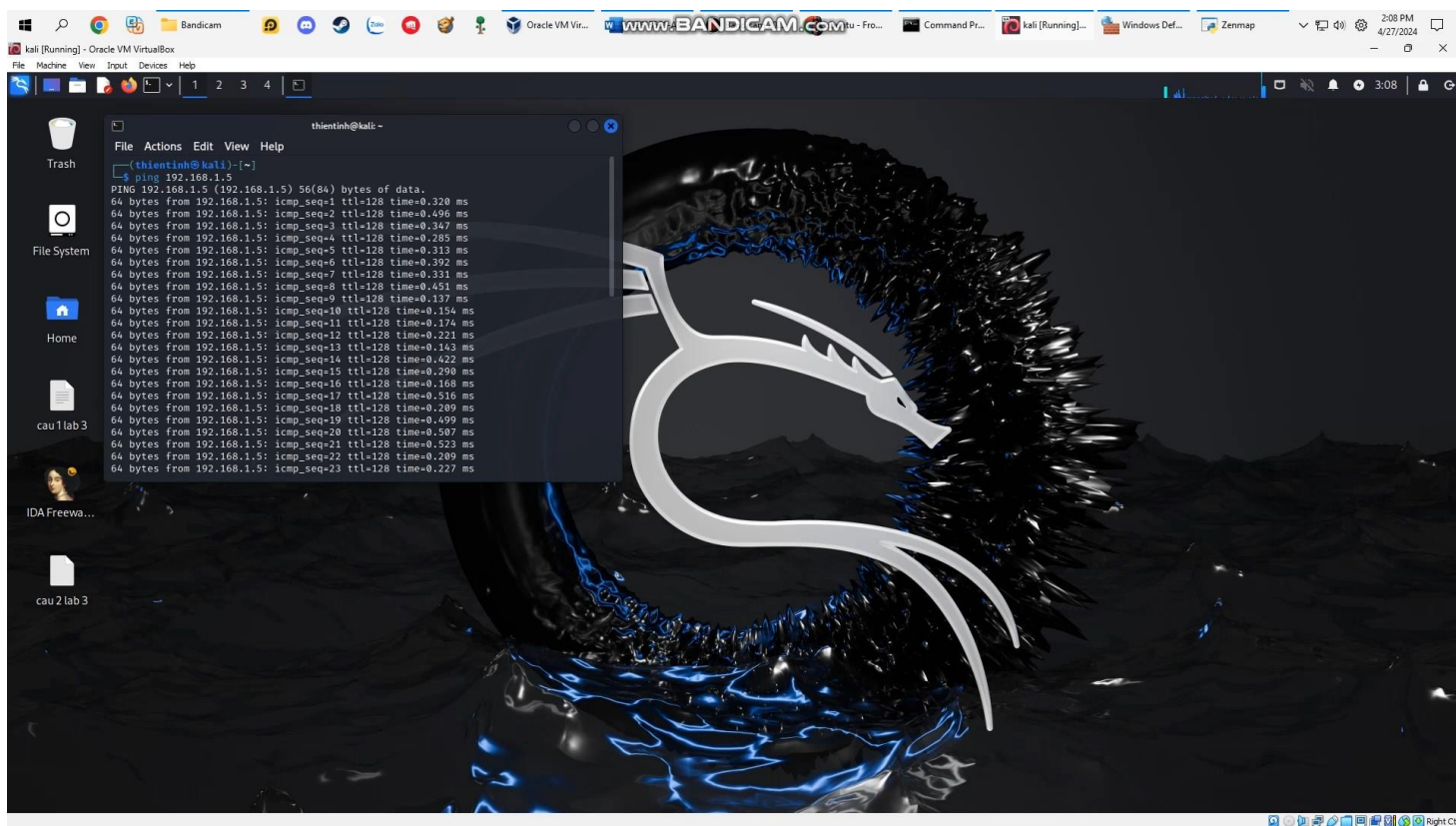
```
Command Prompt - ncat -vklp 9000
Microsoft Windows [Version 10.0.22631.3447]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Admin>ncat -vklp 9000
ncat: Version 7.95 ( https://nmap.org/ncat )
ncat: Listening on [::]:9000
ncat: Listening on 0.0.0.0:9000
```

- Thay đổi cấu hình mạng của máy ảo Kali Linux sao cho có thể giao tiếp mạng tới máy Windows (Sử dụng mạng Internet được chia sẻ từ điện thoại)

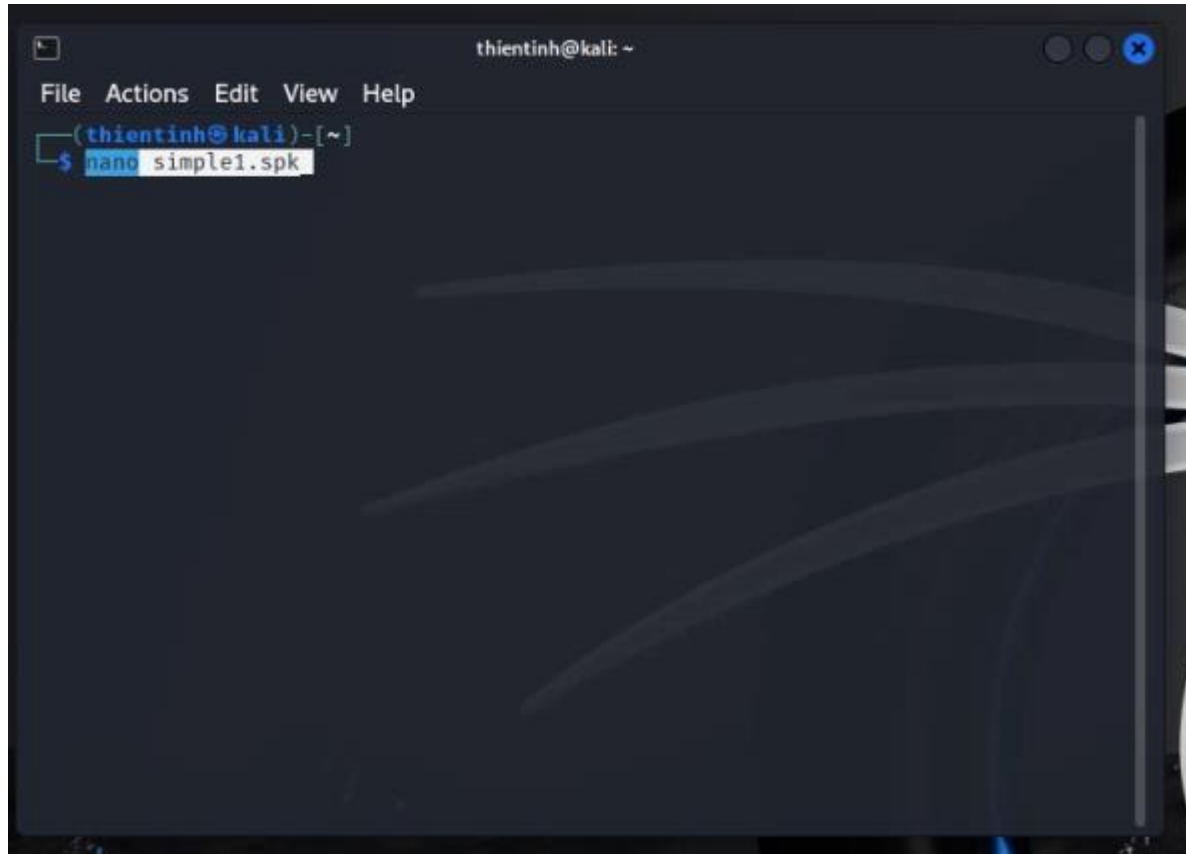


- IPv4 Address. : 192.168.1.5
- IP của máy Windows 192.168.1.5



Kiểm tra ping 192.168.1.5 (Tuỳ theo từng máy)

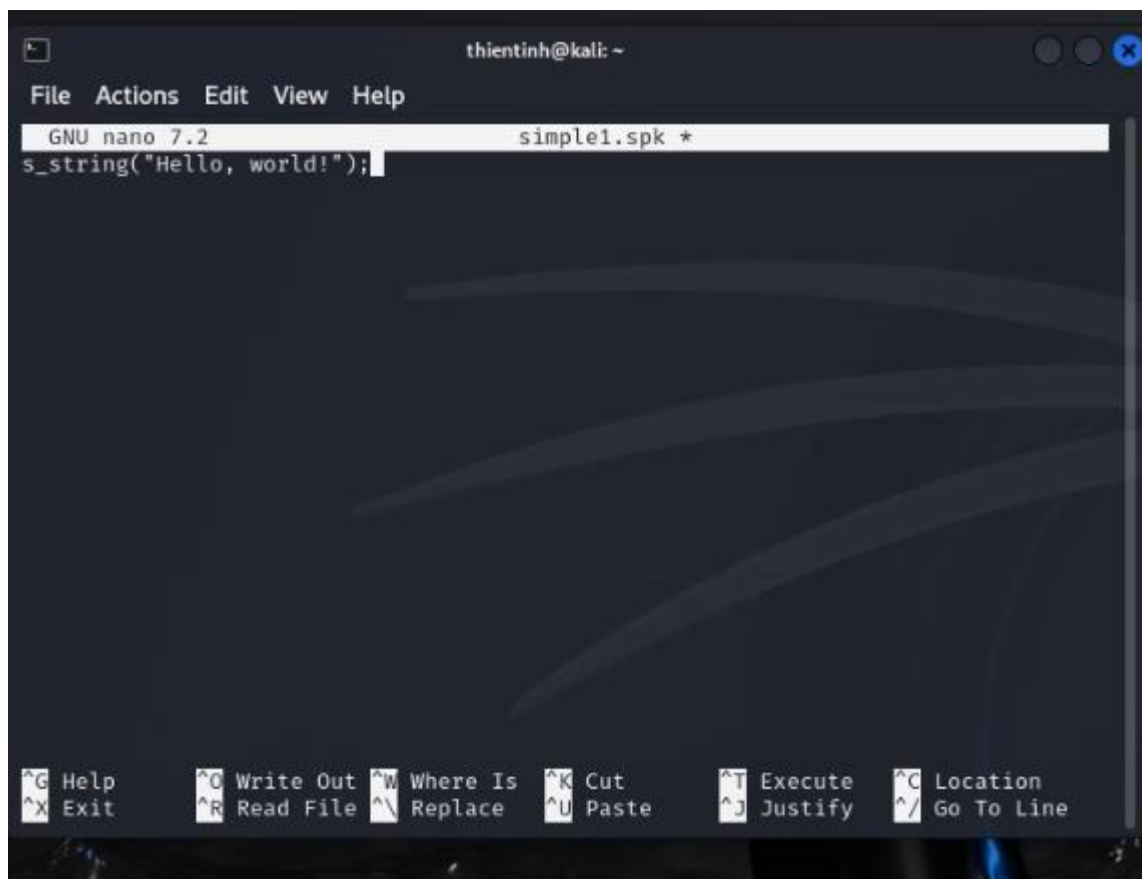
- Tạo file `simple1.spk` với nội dung bên dưới:

A terminal window titled 'thientinh@kali: ~' with a menu bar containing 'File', 'Actions', 'Edit', 'View', and 'Help'. The prompt is '(thientinh@kali)-[~]' and the command '\$ nano simple1.spk' is entered. The terminal has a dark background with light blue and white text. A vertical scrollbar is visible on the right side of the terminal window.

```
thientinh@kali: ~  
File Actions Edit View Help  
(thientinh@kali)-[~]  
$ nano simple1.spk
```

\$nano simple1.spk

- Nội dung file
`s_string("Hello, world!");`



```
thientinh@kali: ~
GNU nano 7.2 simple1.spk *
s_string("Hello, world!");

^G Help    ^O Write Out  ^W Where Is  ^K Cut       ^T Execute   ^C Location
^X Exit    ^R Read File  ^N Replace   ^U Paste     ^J Justify   ^_ Go To Line
```

- Thực hiện lệnh sau để fuzzing dịch vụ Netcat. Quan sát kết quả dịch vụ Netcat nhận được.

```
thientinh@kali: ~  
File Actions Edit View Help  
(thientinh@kali)-[~]  
$ nano simple1.spk  
  
(thientinh@kali)-[~]  
$ generic_send_tcp 192.168.1.5 9000 simple1.spk 0 0  
Total Number of Strings is 681  
Fuzzing  
Fuzzing Variable 0:0  
Fuzzing Variable 0:1  
Fuzzing Variable 0:2  
Fuzzing Variable 0:3  
Fuzzing Variable 0:4  
Fuzzing Variable 0:5  
Fuzzing Variable 0:6  
Fuzzing Variable 0:7
```

192.168.1.5 9000 simple1.spk 0 0

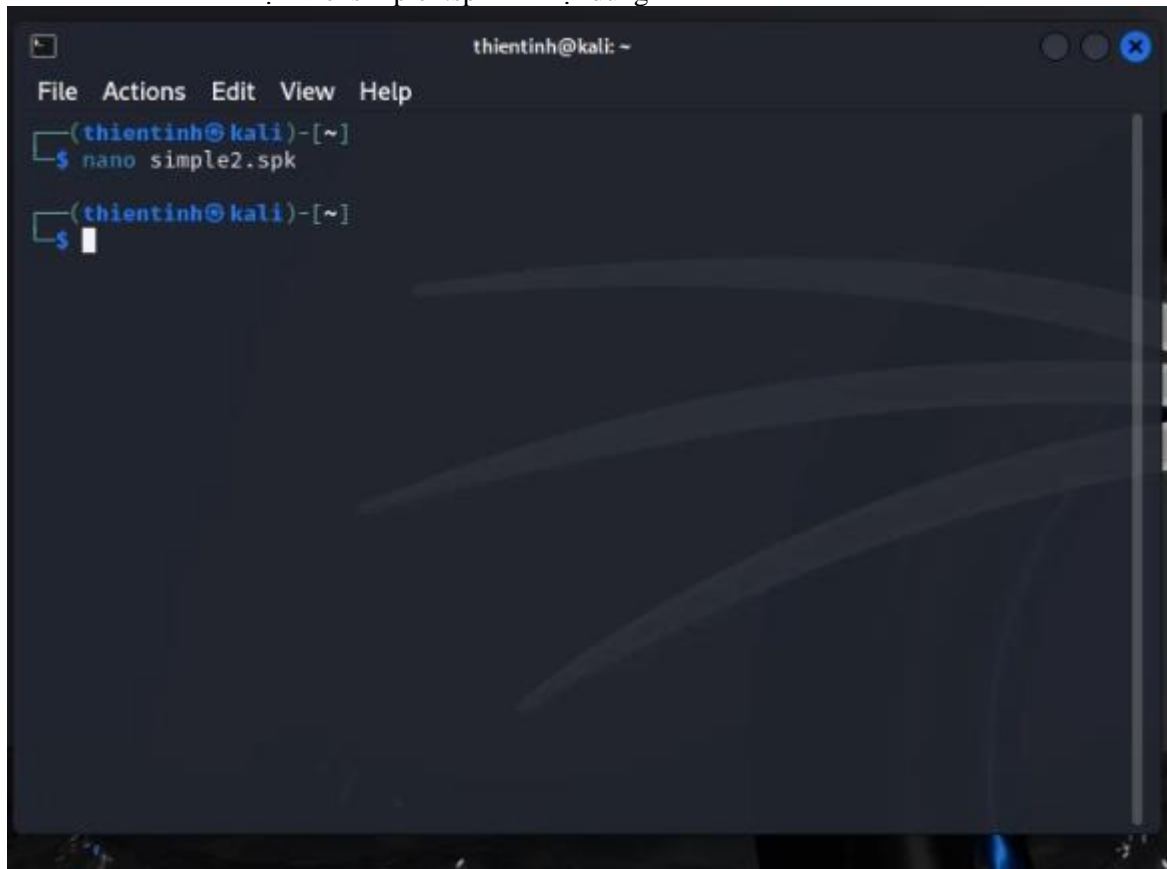
\$ generic_send_tcp

```
Command Prompt - ncat -vklp 9000  
Hello, world!Ncat: Connection from 192.168.1.8:46190.  
Hello, world!Ncat: Connection from 192.168.1.8:46192.  
Hello, world!Ncat: Connection from 192.168.1.8:46202.  
Hello, world!Ncat: Connection from 192.168.1.8:46206.  
Hello, world!Ncat: Connection from 192.168.1.8:46214.  
Hello, world!Ncat: Connection from 192.168.1.8:46228.  
Hello, world!Ncat: Connection from 192.168.1.8:46232.  
Hello, world!Ncat: Connection from 192.168.1.8:46244.  
Hello, world!Ncat: Connection from 192.168.1.8:46258.  
Hello, world!Ncat: Connection from 192.168.1.8:46272.  
Hello, world!Ncat: Connection from 192.168.1.8:46280.  
Hello, world!Ncat: Connection from 192.168.1.8:46286.  
Hello, world!Ncat: Connection from 192.168.1.8:46302.  
Hello, world!Ncat: Connection from 192.168.1.8:46316.  
Hello, world!Ncat: Connection from 192.168.1.8:46330.  
Hello, world!Ncat: Connection from 192.168.1.8:46346.  
Hello, world!Ncat: Connection from 192.168.1.8:46360.  
Hello, world!Ncat: Connection from 192.168.1.8:46374.  
Hello, world!Ncat: Connection from 192.168.1.8:46378.  
Hello, world!Ncat: Connection from 192.168.1.8:46390.  
Hello, world!Ncat: Connection from 192.168.1.8:46392.  
Hello, world!Ncat: Connection from 192.168.1.8:46402.  
Hello, world!Ncat: Connection from 192.168.1.8:46414.  
Hello, world!Ncat: Connection from 192.168.1.8:46416.  
Hello, world!Ncat: Connection from 192.168.1.8:46430.  
Hello, world!Ncat: Connection from 192.168.1.8:46446.  
Hello, world!Ncat: Connection from 192.168.1.8:46460.  
Hello, world!clear  
clear  
no trun.spk
```

Kết quả dịch vụ Netcat

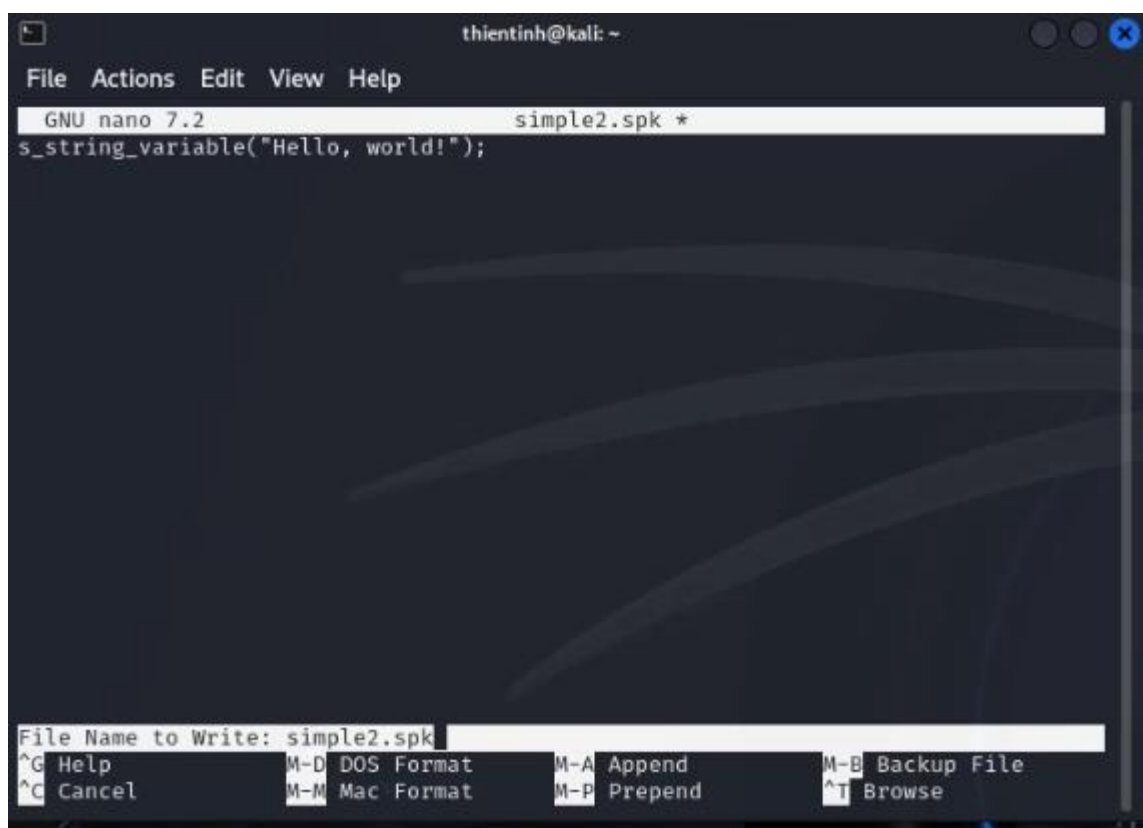
cleqr

- Tạo file `simple2.spk` với nội dung bên dưới:

A screenshot of a terminal window titled 'thientinh@kali: ~'. The window has a menu bar with 'File', 'Actions', 'Edit', 'View', and 'Help'. The terminal shows the prompt '(thientinh@kali)-[~]' followed by the command '\$ nano simple2.spk'. The prompt returns to '(thientinh@kali)-[~]' with a cursor on a new line. The terminal has a dark background with light blue text. A vertical scrollbar is visible on the right side of the terminal window.

\$nano simple2.spk

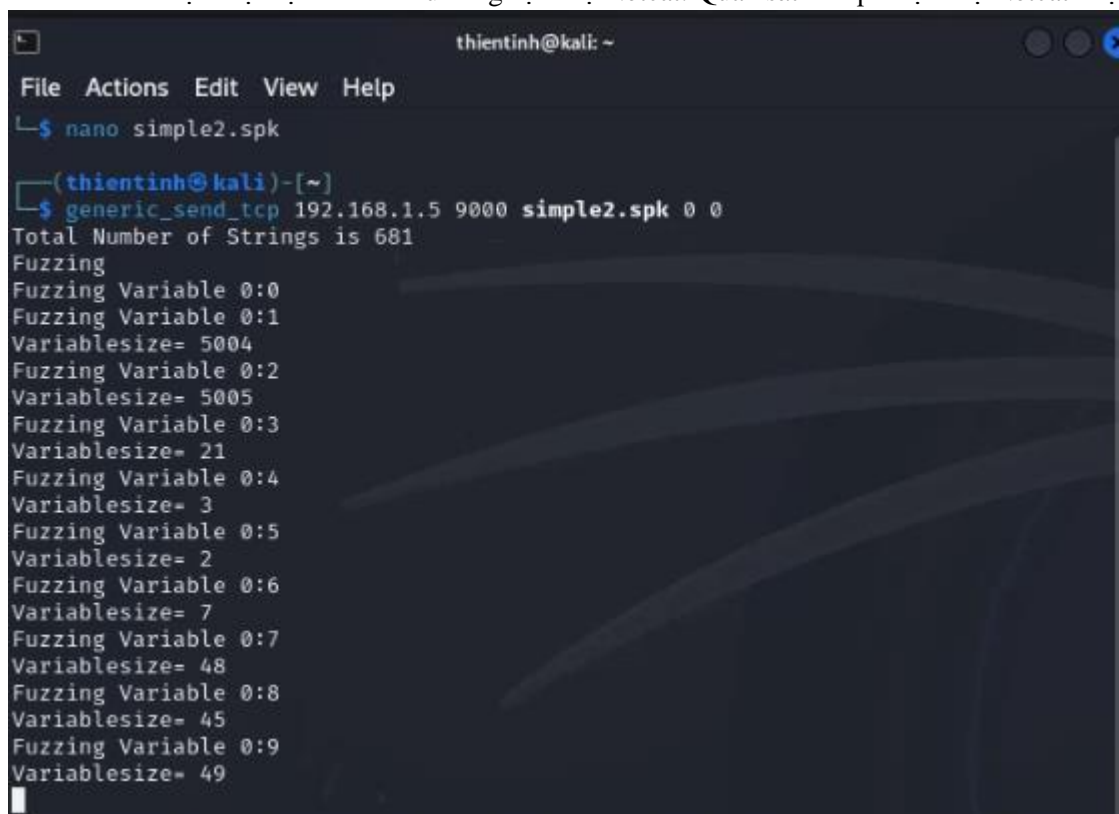
- # Nội dung file
`s_string_variable("Hello, world!");`



```
thientinh@kali: ~
File Actions Edit View Help
GNU nano 7.2 simple2.spk *
s_string_variable("Hello, world!");

File Name to Write: simple2.spk
^G Help      M-D DOS Format  M-A Append     M-B Backup File
^C Cancel    M-M Mac Format  M-P Prepend     ^T Browse
```

- Thực hiện lệnh sau để fuzzing dịch vụ Netcat. Quan sát kết quả dịch vụ Netcat nhận được.



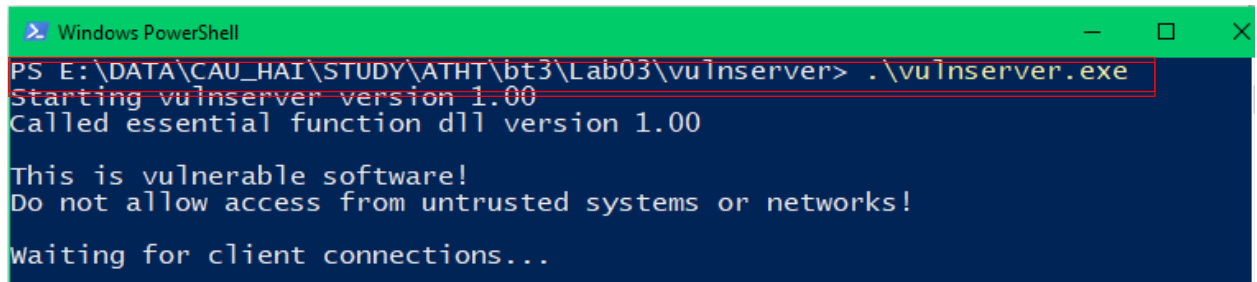
```
thientinh@kali: ~
File Actions Edit View Help
$ nano simple2.spk
(thientinh@kali)-[~]
$ generic_send_tcp 192.168.1.5 9000 simple2.spk 0 0
Total Number of Strings is 681
Fuzzing
Fuzzing Variable 0:0
Fuzzing Variable 0:1
Variablesize= 5004
Fuzzing Variable 0:2
Variablesize= 5005
Fuzzing Variable 0:3
Variablesize= 21
Fuzzing Variable 0:4
Variablesize= 3
Fuzzing Variable 0:5
Variablesize= 2
Fuzzing Variable 0:6
Variablesize= 7
Fuzzing Variable 0:7
Variablesize= 48
Fuzzing Variable 0:8
Variablesize= 45
Fuzzing Variable 0:9
Variablesize= 49
```

\$ generic_send_tcp 192.168.188.177 9000 simple2.spk 0 0


```
Command Prompt - ncat -vklp 9000
ncat: Connection from 192.168.1.8:43622.
ncat: Connection from 192.168.1.8:43630.
ncat: Connection from 192.168.1.8:43632.
```

Kết quả dịch vụ Netcat

- Tải và giải nén file Lab03.zip được thư mục vulnserver. Thực thi file vulnserver.exe ở môi trường CMD của máy Windows.



```
Windows PowerShell
PS E:\DATA\CAU_HAI\STUDY\ATHT\bt3\Lab03\vulnserver> .\vulnserver.exe
Starting vulnserver version 1.00
Called essential function dll version 1.00

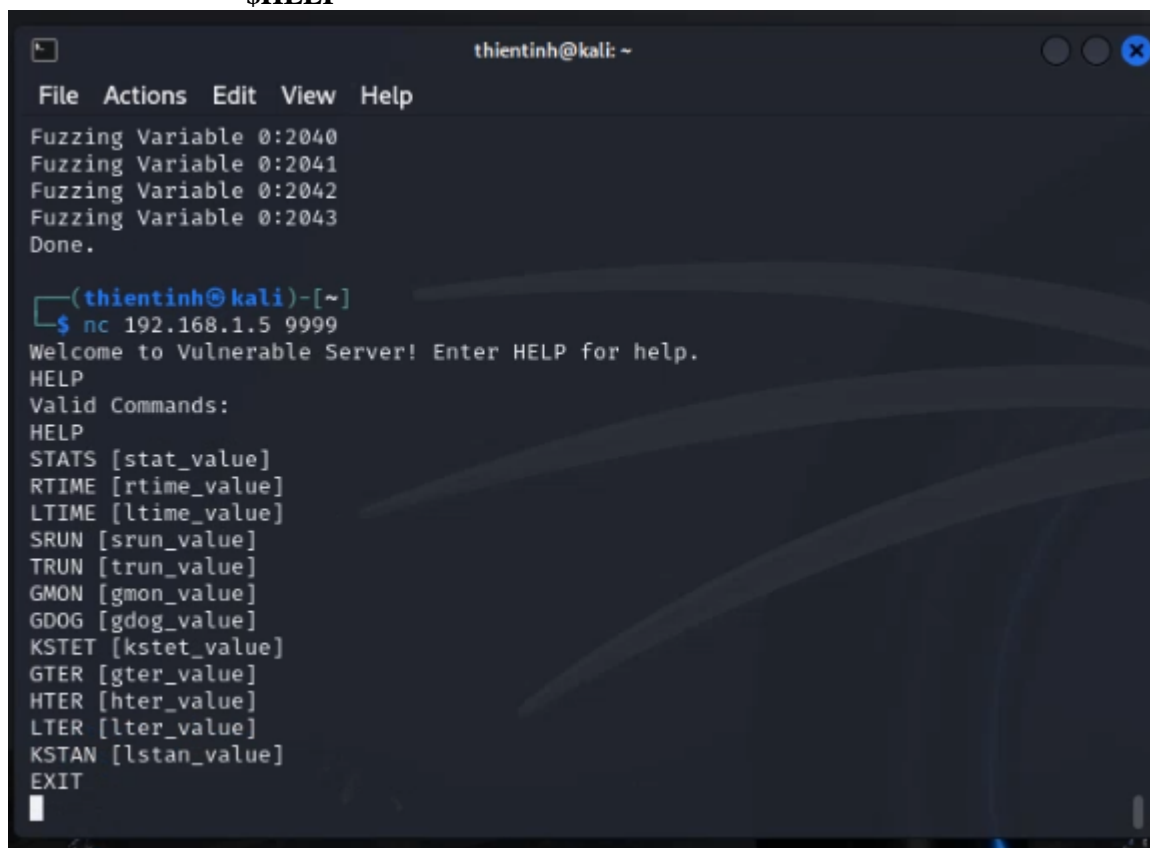
This is vulnerable software!
Do not allow access from untrusted systems or networks!

Waiting for client connections...
```

- Trên máy Kali Linux, nối kết vulnserver trên máy Windows:

\$nc 192.168.188.177 9999

\$HELP

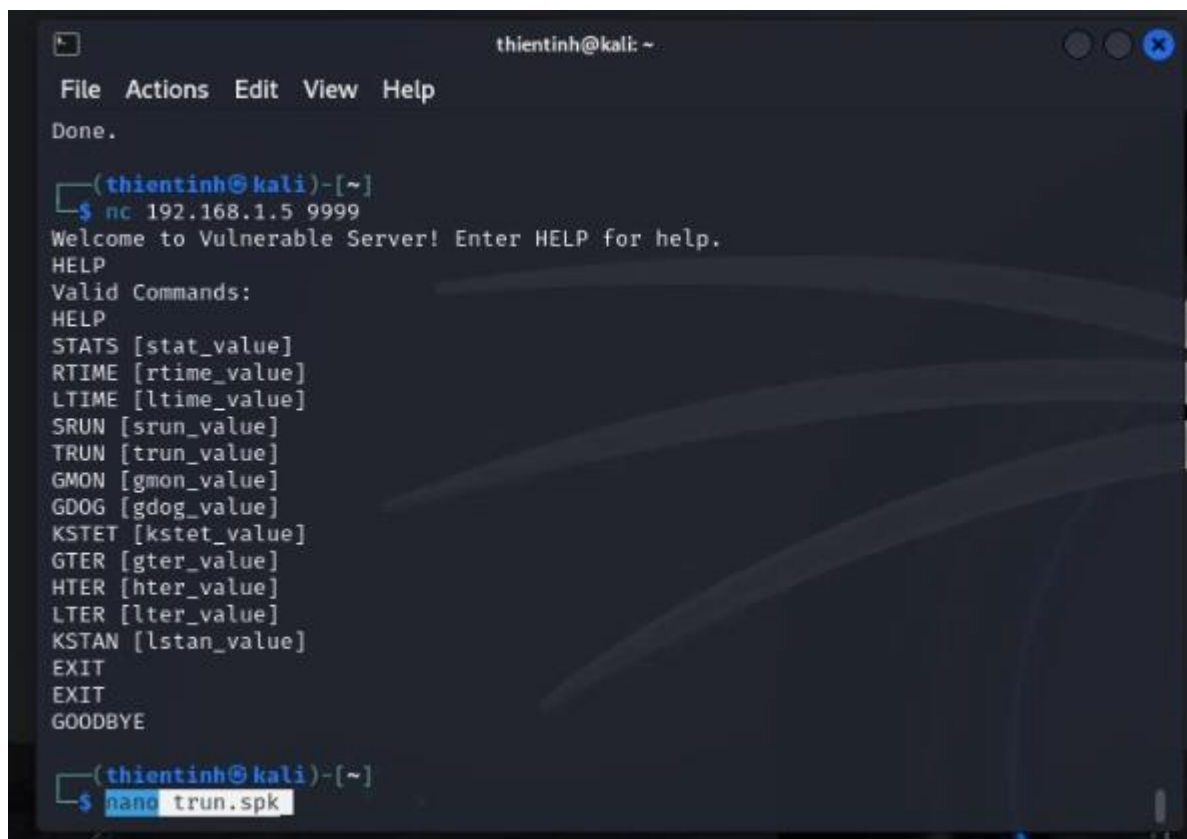


```
thientinh@kali: ~
File Actions Edit View Help
Fuzzing Variable 0:2040
Fuzzing Variable 0:2041
Fuzzing Variable 0:2042
Fuzzing Variable 0:2043
Done.

(thientinh@kali)-[~]
$ nc 192.168.1.5 9999
Welcome to Vulnerable Server! Enter HELP for help.
HELP
Valid Commands:
HELP
STATS [stat_value]
RTIME [rtime_value]
LTIME [ltime_value]
SRUN [srun_value]
TRUN [trun_value]
GMON [gmon_value]
GDOG [gdog_value]
KSTET [kstet_value]
GTER [gter_value]
HTER [hter_value]
LTER [lter_value]
KSTAN [lstan_value]
EXIT
```

\$EXIT

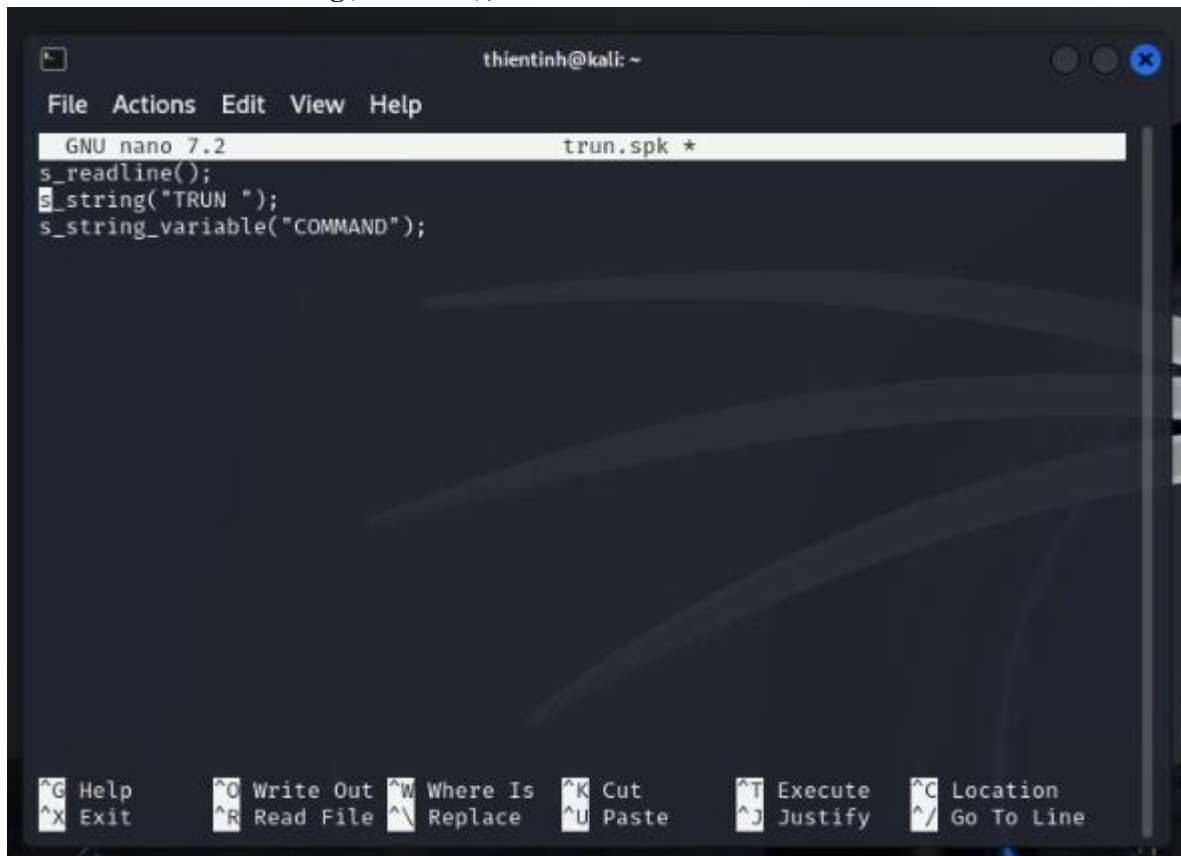
- Tạo file trun.spk với nội dung bên dưới:



```
thientinh@kali: ~  
File Actions Edit View Help  
Done.  
  
(thientinh@kali)-[~]  
$ nc 192.168.1.5 9999  
Welcome to Vulnerable Server! Enter HELP for help.  
HELP  
Valid Commands:  
HELP  
STATS [stat_value]  
RTIME [rtime_value]  
LTIME [ltime_value]  
SRUN [srun_value]  
TRUN [trun_value]  
GMON [gmon_value]  
GDOG [gdog_value]  
KSTET [kstet_value]  
GTER [gter_value]  
HTER [hter_value]  
LTER [lter_value]  
KSTAN [lstan_value]  
EXIT  
EXIT  
GOODBYE  
  
(thientinh@kali)-[~]  
$ nano trun.spk
```

\$nano trun.spk

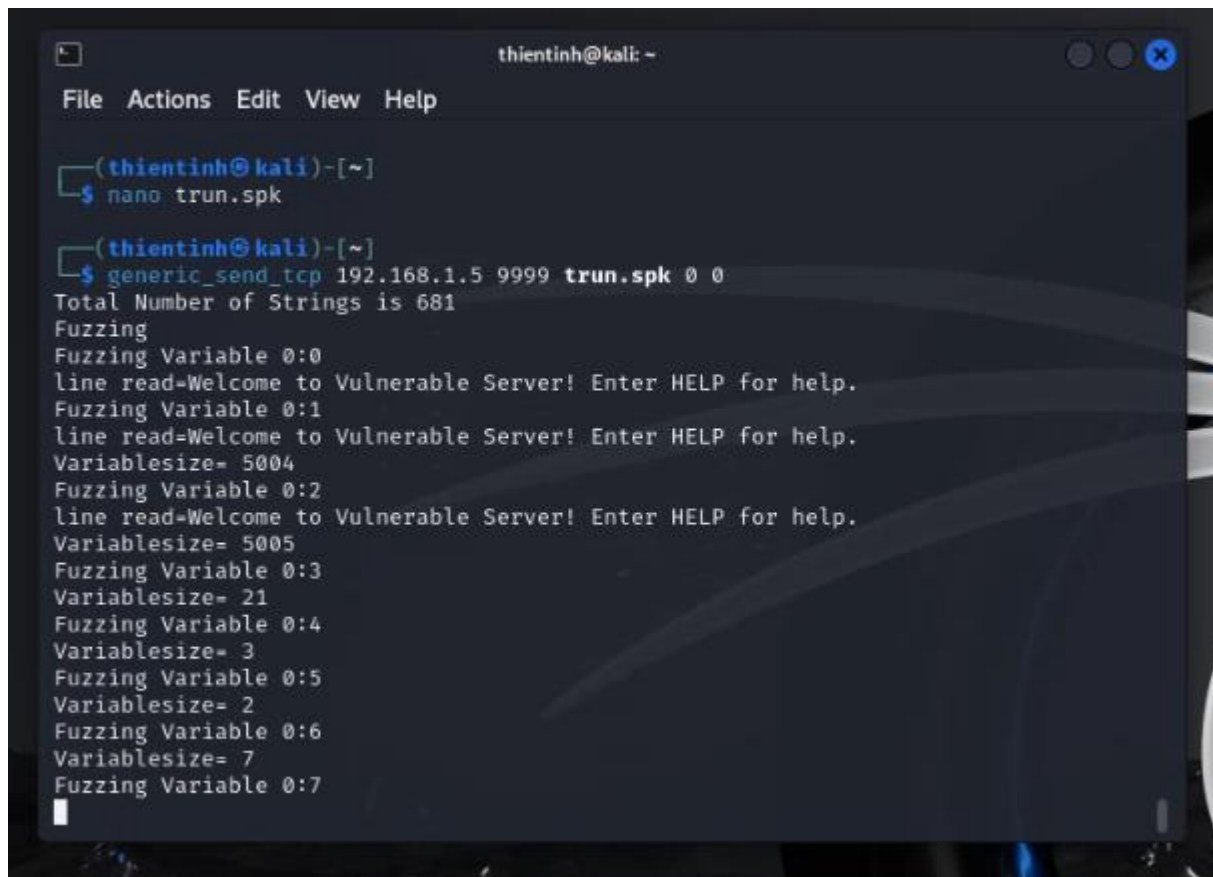
- Nội dung file
`s_readline();`
`s_string("TRUN ");`



```
thientinh@kali: ~  
File Actions Edit View Help  
GNU nano 7.2 trun.spk *  
s_readline();  
s_string("TRUN ");  
s_string_variable("COMMAND");  
  
^G Help    ^O Write Out  ^W Where Is  ^K Cut      ^T Execute   ^C Location  
^X Exit    ^R Read File  ^\ Replace   ^U Paste    ^J Justify   ^_ Go To Line
```

`s_string_variable("COMMAND");`

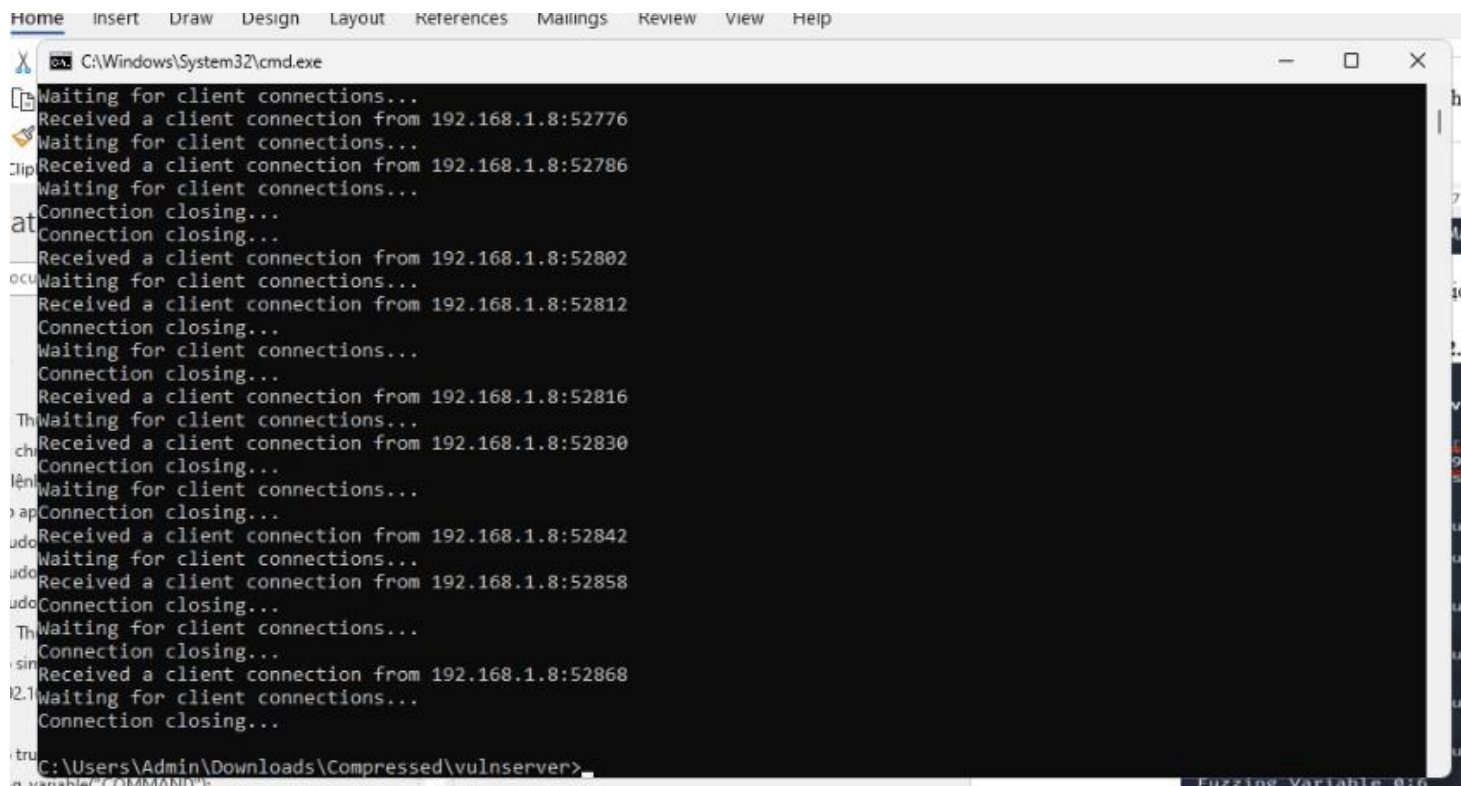
- Thực hiện lệnh sau để fuzzing dịch vụ vulnserver. Quan sát kết quả sẽ thấy vulnserver dừng hoạt động sau một thời gian ngắn:



```
thientinh@kali: ~  
File Actions Edit View Help  
(thientinh@kali)~  
$ nano trun.spk  
(thientinh@kali)~  
$ generic_send_tcp 192.168.1.5 9999 trun.spk 0 0  
Total Number of Strings is 681  
Fuzzing  
Fuzzing Variable 0:0  
line read-Welcome to Vulnerable Server! Enter HELP for help.  
Fuzzing Variable 0:1  
line read-Welcome to Vulnerable Server! Enter HELP for help.  
Variablesized= 5004  
Fuzzing Variable 0:2  
line read-Welcome to Vulnerable Server! Enter HELP for help.  
Variablesized= 5005  
Fuzzing Variable 0:3  
Variablesized= 21  
Fuzzing Variable 0:4  
Variablesized= 3  
Fuzzing Variable 0:5  
Variablesized= 2  
Fuzzing Variable 0:6  
Variablesized= 7  
Fuzzing Variable 0:7
```

\$ generic_send_tcp 192.168.1.5 9999 trun.spk 0 0

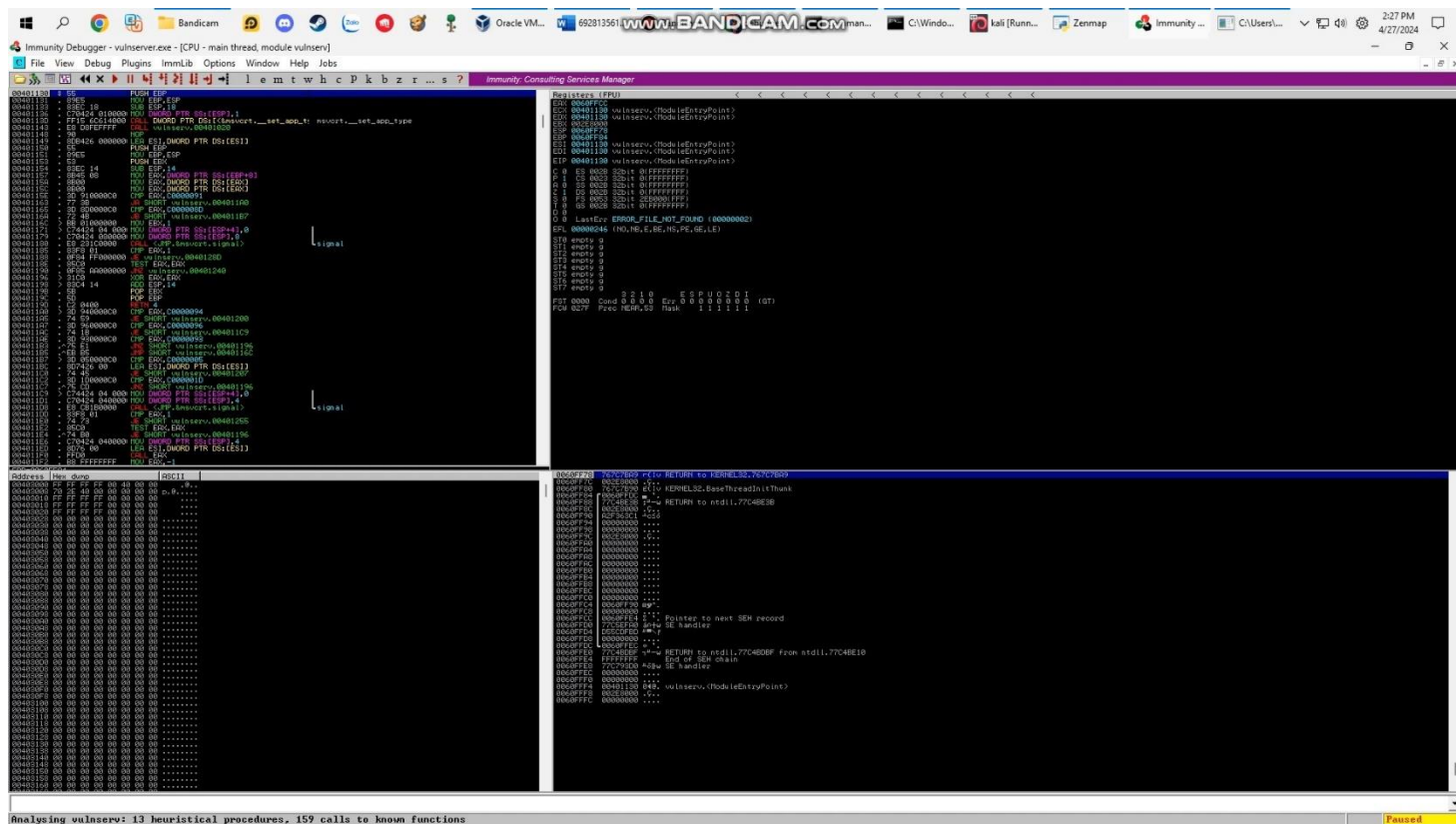
➤ Kết quả dịch vụ vulnserver



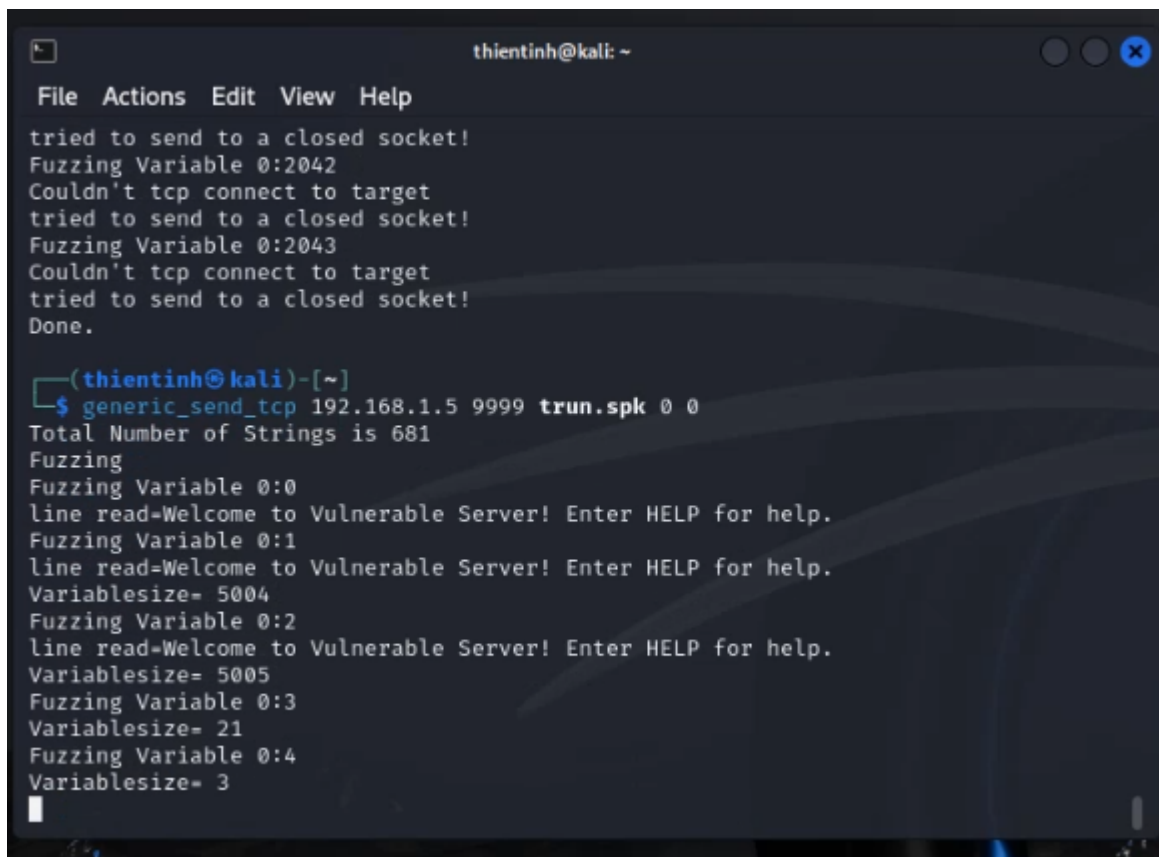
```
Home Insert Draw Design Layout References Mailings Review View Help
C:\Windows\System32\cmd.exe
Waiting for client connections...
Received a client connection from 192.168.1.8:52776
Waiting for client connections...
Received a client connection from 192.168.1.8:52786
Waiting for client connections...
Connection closing...
Connection closing...
Received a client connection from 192.168.1.8:52802
Waiting for client connections...
Received a client connection from 192.168.1.8:52812
Connection closing...
Waiting for client connections...
Connection closing...
Received a client connection from 192.168.1.8:52816
Waiting for client connections...
Received a client connection from 192.168.1.8:52830
Connection closing...
Waiting for client connections...
Connection closing...
Received a client connection from 192.168.1.8:52842
Waiting for client connections...
Received a client connection from 192.168.1.8:52858
Connection closing...
Waiting for client connections...
Connection closing...
Received a client connection from 192.168.1.8:52868
Waiting for client connections...
Connection closing...
C:\Users\Admin\Downloads\Compressed\vulnserver>
```

Cài đặt công cụ [Immunity Debugger](#) vào máy Windows. Sử dụng công cụ để mở file và thực thi file vulnserver.exe. Tiếp tục fuzzing dịch vụ vulnserver. Quan sát giao diện để thấy thanh ghi EIP chứa giá trị “41414141” (có lỗi buffer overflow).

➤ Mở file vulnserver trên công cụ **Immunity Debugger**



- Tiếp tục `$generic_send_tcp 192.168.1.15 9999 trun.spk 0 0`



```
thientinh@kali: ~  
File Actions Edit View Help  
tried to send to a closed socket!  
Fuzzing Variable 0:2042  
Couldn't tcp connect to target  
tried to send to a closed socket!  
Fuzzing Variable 0:2043  
Couldn't tcp connect to target  
tried to send to a closed socket!  
Done.  
  
(thientinh@kali)-[~]  
$ generic_send_tcp 192.168.1.5 9999 trun.spk 0 0  
Total Number of Strings is 681  
Fuzzing  
Fuzzing Variable 0:0  
line read=Welcome to Vulnerable Server! Enter HELP for help.  
Fuzzing Variable 0:1  
line read=Welcome to Vulnerable Server! Enter HELP for help.  
Variablesized= 5004  
Fuzzing Variable 0:2  
line read=Welcome to Vulnerable Server! Enter HELP for help.  
Variablesized= 5005  
Fuzzing Variable 0:3  
Variablesized= 21  
Fuzzing Variable 0:4  
Variablesized= 3
```

- Kết quả dịch vụ **Immunity Debugger** thấy thanh ghi EIP chứa giá trị “77C56ADC” (có lỗi buffer overflow).

```

Registers (FPU)
EAX 00000000
ECX 00000000
EDX 00000000
EBX 770D0C00 ntdll.770D0C00
ESP 00000000
ESI 00000000
EDI 00000000
EIP 77C56ADC ntdll.77C56ADC
C 0 ES 0028 32bit 0(FFFFFFFF)
P 0 CS 0020 32bit 0(FFFFFFFF)
R 0 SS 0028 32bit 0(FFFFFFFF)
R 0 DS 0028 32bit 0(FFFFFFFF)
S 0 FS 0053 32bit 2EB000(FFF)
T 0 GS 0028 32bit 0(FFFFFFFF)
D 0
O 0
L 0 LastErr ERROR_SUCCESS (00000000)
EPL 00000202 (NO,HB,NE,A,NS,PO,GE,G)
ST0 empty q
ST1 empty q
ST2 empty q
ST3 empty q
ST4 empty q
ST5 empty q
ST6 empty q
ST7 empty q
FST 0000 Cond 0 0 0 0 Err 0 0 0 0 0 0 (GT)
FCW 057F Freq NEAR,64 Rask 1 1 1 1 1 1
0060FE10 77C56ADC jmp BFD0H to ntdll.77C563ED from ntdll.7615c9a1a5Process
    
```

- Khai thác lỗi buffer overflow trên vulnserver.exe theo [hướng dẫn](#). (Không bắt buộc thực hiện)

Câu 3: Giải thuật băm và tấn công mật khẩu

3.1. Tìm giá trị băm của chuỗi "@ntoanhethong_ct222" sử dụng giải thuật MD5 và SHA512 sử dụng công cụ md5sum và sha512sum:

```

thientinh@kali: ~
File Actions Edit View Help

(thientinh@kali)-[~]
$ echo -n "@ntoanhethong_ct222" | md5sum
cdf279ec13f76cb3c87ee5d362463f88 -

(thientinh@kali)-[~]
$
    
```

\$ echo -n "@ntoanhethong_ct222" | md5sum

```

(thientinh@kali)-[~]
$ echo -n "@ntoanhethong_ct222" | sha512sum
e6f3a3a5b5f8e1e4beaf185ed958839ec2c51e219ab0e69fa8aba23f626b4b894d4e362f98f5505cb
55d01a365f775630152f56be6032cdce5106c7f2d93d493 -

(thientinh@kali)-[~]
$
    
```

\$ echo -n "@ntoanhethong_ct222" | sha512sum

- Sử dụng một trang web online cho phép thực hiện giải thuật băm, ví dụ :<https://www.pelock.com/products/hash-calculator> để kiểm tra kết quả.

md5	16	CDF279EC13F76CB3C87EE5D362463F88	
sha512	64	E6F3A3A5B5FBE1E4BEAF185ED958839E	

3.2. Sử dụng công cụ john và hashcat để dịch ngược giá trị băm "b109f3bbbc244eb82441917ed06d618b9008dd09b3befd1b5e07394c706a8bb980b1d7785e5976ec049b46df5f1326af5a2ea6d103fd07c95385ffab0cacbc86"

Xác định giải thuật băm

- **\$ hashid**
"b109f3bbbc244eb82441917ed06d618b9008dd09b3befd1b5e07394c706a8bb980b1d7785e5976ec049b46df5f1326af5a2ea6d103fd07c95385ffab0cacbc86"

```
(thientinh@kali)-[~]  
$ hashid  
"b109f3bbbc244eb82441917ed06d618b9008dd09b3befd1b5e07394c706a8bb980b1d7 785e5976ec049b46df5f1326af5a2ea6d103fd07c95385ffab0cacbc86"
```

- **\$ echo -n**
"b109f3bbbc244eb82441917ed06d618b9008dd09b3befd1b5e07394c706a8bb980b1d7785e5976ec049b46df5f1326af5a2ea6d103fd07c95385ffab0cacbc86" > hash

```
(thientinh@kali)-[~]  
$ echo -n "b109f3bbbc244eb82441917ed06d618b9008dd09b3befd1b5e07394c706a8bb980b1d7 785e5976ec049b46df5f1326af5a2ea6d103fd07c95385ffab0cacbc86" > hash  
  
(thientinh@kali)-[~]
```

- **Hiển thị nội dung: \$ cat hash**

```
(thientinh@kali)-[~]  
$ cat hash  
b109f3bbbc244eb82441917ed06d618b9008dd09b3befd1b5e07394c706a8bb980b1d7 785e5976ec049b46df5f1326af5a2ea6d103fd07c95385ffab0cacbc86  
  
(thientinh@kali)-[~]
```


- # Sử dụng John the Ripper

\$john --format=raw-sha512 --wordlist=/usr/share/wordlists/metasploit/password.lst hash

```
(thientinh@kali)-[~]
$ john --format=raw-sha512 --wordlist=/usr/share/wordlists/metasploit/password
.lst hash
Created directory: /home/thientinh/.john
Using default input encoding: UTF-8
No password hashes loaded (see FAQ)
```

- # Sử dụng hashcat

\$hashcat -a 0 -m 1700 ./hash /usr/share/wordlists/metasploit/password.lst

```
(thientinh@kali)-[~]
$ hashcat -a 0 -m 1700 ./hash /usr/share/wordlists/metasploit/password.lst
hashcat (v6.2.6) starting

/usr/share/wordlists/metasploit/password.lst: No such file or directory

Started: Sat Apr 27 03:42:47 2024
Stopped: Sat Apr 27 03:42:48 2024
```

Không đủ dung lượng bộ nhớ cho hình thức tấn công này. Vì vậy ta tắt máy ảo và tăng dung lượng bộ nhớ RAM trên máy ảo lên. Sau đó chạy lại lệnh trên

```
b109f3bbbc244eb82441917ed06d618b9008dd09b3befd1b5e07394c706a8bb980b1d7785e5976
ec049b46df5f1326af5a2ea6d103fd07c95385ffab0cacbc86:password

Session.....: hashcat
Status.....: Cracked
Hash.Mode.....: 1700 (SHA2-512)
Hash.Target.....: b109f3bbbc244eb82441917ed06d618b9008dd09b3befd1b5e0 ... acbc8
6
Time.Started.....: Wed Nov 22 21:00:38 2023 (1 sec)
Time.Estimated ... : Wed Nov 22 21:00:39 2023 (0 secs)
Kernel.Feature ... : Pure Kernel
Guess.Base.....: File (/usr/share/wordlists/metasploit/password.lst)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 471.5 kH/s (0.12ms) @ Accel:256 Loops:1 Thr:1 Vec:4
Recovered.....: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.....: 57856/88397 (65.45%)
Rejected.....: 0/57856 (0.00%)
Restore.Point....: 57344/88397 (64.87%)
Restore.Sub.#1 ... : Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: passivity → pejorative
Hardware.Mon.#1..: Util: 46%

Started: Wed Nov 22 21:00:29 2023
Stopped: Wed Nov 22 21:00:40 2023

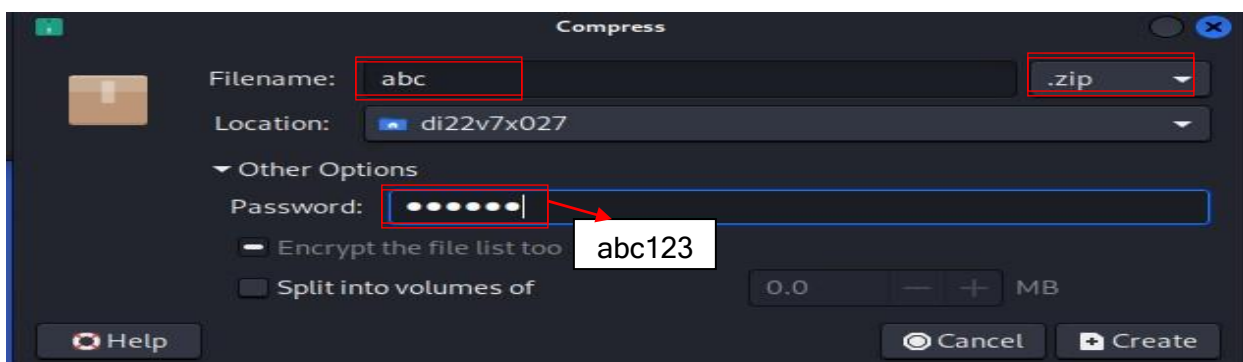
(di22v7x027@kali)-[~]
$
```

- Sử dụng một trang web cho phép dịch ngược giá trị băm, ví dụ: <https://crackstation.net/>, để kiểm tra kết quả.

Hash	Type	Result
b109f3bbbc244eb82441917ed06d618b9008dd09b3befd1b5e07394c706a8bb980b1d7785e5976ec049b46df5f1326af5a2ea6d103fd07c95385ffab0cacbc86	sha512	password

Color Codes: **Green**: Exact match, **Yellow**: Partial match, **Red**: Not found.

3.3. Tạo một file zip “abc.zip” với mật khẩu mở file là "abc123". Sử dụng john và hashcat để dò mật khẩu của file:



- Trích xuất giá băm của mật khẩu
\$ zip2john abc.zip > hash

```
(di22v7x027@kali)-[~]
$ ls
abc.zip      Downloads  Music      simple1.spk  Videos
crackme.exe  hash       Pictures    simple2.spk
crackme.exe.i64  heapoverflow Public      stackoverflow
Desktop      idafree-8.3 pws.txt    Templates
Documents    logins.txt  share      trun.spk

(di22v7x027@kali)-[~]
$ rm hash

(di22v7x027@kali)-[~]
$ zip2john abc.zip > hash

(di22v7x027@kali)-[~]
$ cat hash
abc.zip/hash:$zip2$*0*1*0*28209012be720f37*1012*55*82a99b1127da7ed8ce893276ea6
d27e4fe115ce3e9fd6187addd483a080b62a0ee2357df0e22b698cfd0c55644cb50c6dd70614ee
6506fb2cc52299941f55ca433a48d04bbafc919436d62f9fa35e67a4998087799*c8dea4a30a8a
4c3b7efb*$/zip2$:hash:abc.zip:abc.zip
```

- Dò mật khẩu:
\$ john --wordlist=/usr/share/wordlists/metasploit/password.lst hash

```
(di22v7x027@kali)-[~]
$ john --wordlist=/usr/share/wordlists/metasploit/password.lst hash
Using default input encoding: UTF-8
Loaded 1 password hash (ZIP, WinZip [PBKDF2-SHA1 256/256 AVX2 8x])
Cost 1 (HMAC size) is 85 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
abc123      (abc.zip/hash)
1g 0:00:00:00 DONE (2023-11-22 21:15) 8.333g/s 34133p/s 34133c/s 34133C/s !@#$
%..armoured
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Chỉnh sửa file hash cho phù hợp định dạng của hashcat

```
GNU nano 7.2 hash
$zip2$*0*1*0*28209012be720f37*1012*55*82a99b1127da7ed8ce893276ea6d27e4fe115ce>
```

Xoá đi đoạn đầu đoạn cuối trong file hash chỉ lấy "\$zip.....zip\$"

```
# hashcat -a 0 -m 13600 hash /usr/share/wordlists/metasploit/password.lst
```

```
$zip2$*0*1*0*28209012be720f37*1012*55*82a99b1127da7ed8ce893276ea6d27e4fe115ce3
e9fd6187addd483a080b62a0ee2357df0e22b698cfd0c55644cb50c6dd70614ee6506fb2cc5229
9941f55ca433a48d04bbafc919436d62f9fa35e67a4998087799*c8dea4a30a8a4c3b7efb*$/zi
p2$:abc123

Session.....: hashcat
Status.....: Cracked
Hash.Mode.....: 13600 (WinZip)
Hash.Target.....: $zip2$*0*1*0*28209012be720f37*1012*55*82a99b1127da7 ... /zip2
$
Time.Started.....: Wed Nov 22 21:21:40 2023 (1 sec)
Time.Estimated...: Wed Nov 22 21:21:41 2023 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.....: File (/usr/share/wordlists/metasploit/password.lst)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 859 H/s (20.74ms) @ Accel:256 Loops:999 Thr:1 Vec:8
Recovered.....: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.....: 512/88397 (0.58%)
Rejected.....: 0/512 (0.00%)
Restore.Point....: 0/88397 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-999
Candidate.Engine.: Device Generator
Candidates.#1....: !@#$% → abyssal
Hardware.Mon.#1..: Util: 51%

Started: Wed Nov 22 21:20:21 2023
Stopped: Wed Nov 22 21:21:42 2023

(di22v7x027@kali)-[~]
$
```

3.4. Sử dụng công cụ john dò mật khẩu người dùng:

- Tạo người dùng mới “newuser” với mật khẩu “qwerty”

```
$ sudo adduser newuser
```

```
(di22v7x027@kali)-[~]
$ sudo adduser newuser
[sudo] password for di22v7x027:
info: Adding user `newuser' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `newuser' (1002) ...
info: Adding new user `newuser' (1002) with group `newuser (1002)' ...
info: Creating home directory `/home/newuser' ...
info: Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for newuser
Enter the new value, or press ENTER for the default
    Full Name []: newuser
    Room Number []: user
    Work Phone []: no
    Home Phone []: no
    Other []: no
Is the information correct? [Y/n]
info: Adding new user `newuser' to supplemental / extra groups `users' ...
info: Adding user `newuser' to group `users' ...
```

- Trích xuất giá trị băm của mật khẩu người dùng
`$ sudo cat /etc/shadow | grep "newuser" > hash`

```
(di22v7@kali)-[~]  
$ sudo cat /etc/shadow | grep "newuser" > hash  
  
(di22v7@kali)-[~]  
$ cat hash  
newuser:$y$j9T$IiLXrerpw04ORhDX41tsX1$9s0EUTDVov.cqajm.m18il5bL5TPCxGxhwf0KTKp  
kG9:19684:0:99999:7:::
```

- Dò mật khẩu:
`$ john --format=crypt --wordlist=/usr/share/wordlists/metasploit/password.lst hash`

```
(di22v7@kali)-[~]  
$ john --format=crypt --wordlist=/usr/share/wordlists/metasploit/password.l  
t hash  
Using default input encoding: UTF-8  
Loaded 1 password hash (crypt, generic crypt(3) [?/64])  
Cost 1 (algorithm [1:descrypt 2:md5crypt 3:sunmd5 4:bcrypt 5:sha256crypt 6:sha  
512crypt]) is 0 for all loaded hashes  
Cost 2 (algorithm specific iterations) is 1 for all loaded hashes  
Will run 2 OpenMP threads  
Press 'q' or Ctrl-C to abort, almost any other key for status  
qwerty (newuser)  
1g 0:00:10:39 DONE (2023-11-22 21:54) 0.001564g/s 98.64p/s 98.64c/s 98.64C/s q  
uo..raciness  
Use the "--show" option to display all of the cracked passwords reliably  
Session completed.
```

Câu 4: Tìm hiểu giải thuật AES

- Cài và tạo môi trường ảo cho python:
 - `$ sudo apt update && sudo apt install python3-venv -y`

```
thientinh@kali: ~  
File Actions Edit View Help  
  
(thientinh@kali)-[~]  
$ sudo apt update && sudo apt install python3-venv -y  
[sudo] password for thientinh:  
Hit:1 http://http.kali.org/kali kali-rolling InRelease  
Hit:2 http://http.kali.org/kali kali-experimental InRelease  
Hit:3 http://http.kali.org/kali kali-bleeding-edge InRelease  
0% [Working]
```

- `$ python -m venv lab03_04`

```
Setting up python3 venv (3.11.0-2) in  
  
(thientinh@kali)-[~]  
$ python -m venv lab03_04  
  
(thientinh@kali)-[~]  
$
```


- Cài đặt module pycryptodome:

\$./lab03_04/bin/pip install pycryptodome

```
(thientinh@kali)-[~]
$ python -m venv lab03_04

(thientinh@kali)-[~]
$ ./lab03_04/bin/pip install pycryptodome
Collecting pycryptodome
  Downloading pycryptodome-3.20.0-cp35-abi3-manylinux_2_17_x86_64.manylinux2014_x86_64.whl.metadata (3.4 kB)
  Downloading pycryptodome-3.20.0-cp35-abi3-manylinux_2_17_x86_64.manylinux2014_x86_64.whl (2.1 MB)
    2.1/2.1 MB 11.6 MB/s eta 0:00:00
Installing collected packages: pycryptodome
Successfully installed pycryptodome-3.20.0

(thientinh@kali)-[~]
$
```

- Tải và giải nén file Lab03.zip được thư mục aes. Sử dụng lệnh bên dưới copy file
- **\$sudo cp -r ./share/aes ./**

```
(di22v7x027@kali)-[~]
$ sudo cp -r ./share/aes ./
```

\$ls-l lúc này quyền thuộc root

File	Actions	Edit	View	Help
drwxr-xr-x	2	thientinh	thientinh	4096 Apr 14 08:35 Pictures
drwxr-xr-x	2	thientinh	thientinh	4096 Apr 11 04:15 Public
drwxr-xr-x	2	thientinh	thientinh	4096 Apr 11 04:15 Templates
drwxr-xr-x	2	thientinh	thientinh	4096 Apr 11 04:15 Videos
-rw-r--r--	1	thientinh	thientinh	0 Apr 11 05:17 abc.txt
drwxr-xr-x	2	root	root	4096 Apr 27 04:22 aes
drwxr-xr-x	2	thientinh	thientinh	4096 Apr 25 02:24 bufferoverflow
-rwxr-xr-x	1	thientinh	thientinh	29184 Apr 27 02:05 crackme.exe
-rw-r--r--	1	thientinh	thientinh	303104 Apr 27 02:10 crackme.exe.id0
-rw-r--r--	1	thientinh	thientinh	106496 Apr 27 02:10 crackme.exe.id1
-rw-r--r--	1	thientinh	thientinh	5209 Apr 27 02:10 crackme.exe.id2
-rw-r--r--	1	thientinh	thientinh	16384 Apr 27 02:10 crackme.exe.nam
-rw-r--r--	1	thientinh	thientinh	156 Apr 27 02:10 crackme.exe.til
-rw-r--r--	1	thientinh	thientinh	20277 Apr 14 07:48 d

- Chuyển quyền cho người dùng user: **\$sudo chown -R thientinh aes**

```
(thientinh@kali)-[~]
$ sudo chown -R thientinh aes

(thientinh@kali)-[~]
```

Tạo tập tin aes_ecb.py để mã hóa tập tin tux.bmp theo giải thuật AES-ECB. Thực thi aes_ecb.py:

```
(thientinh@kali)-[~]
$ nano ./aes_ecb.py
```

- Tạo tập tin **\$nano ./aes_ecb.py**

➤ `$/lab03_04/bin/python aes_ecb.py`

```
from Crypto.Cipher import AES
key = b"aaaabbbbccccdddd"
cipher = AES.new(key, AES.MODE_ECB)

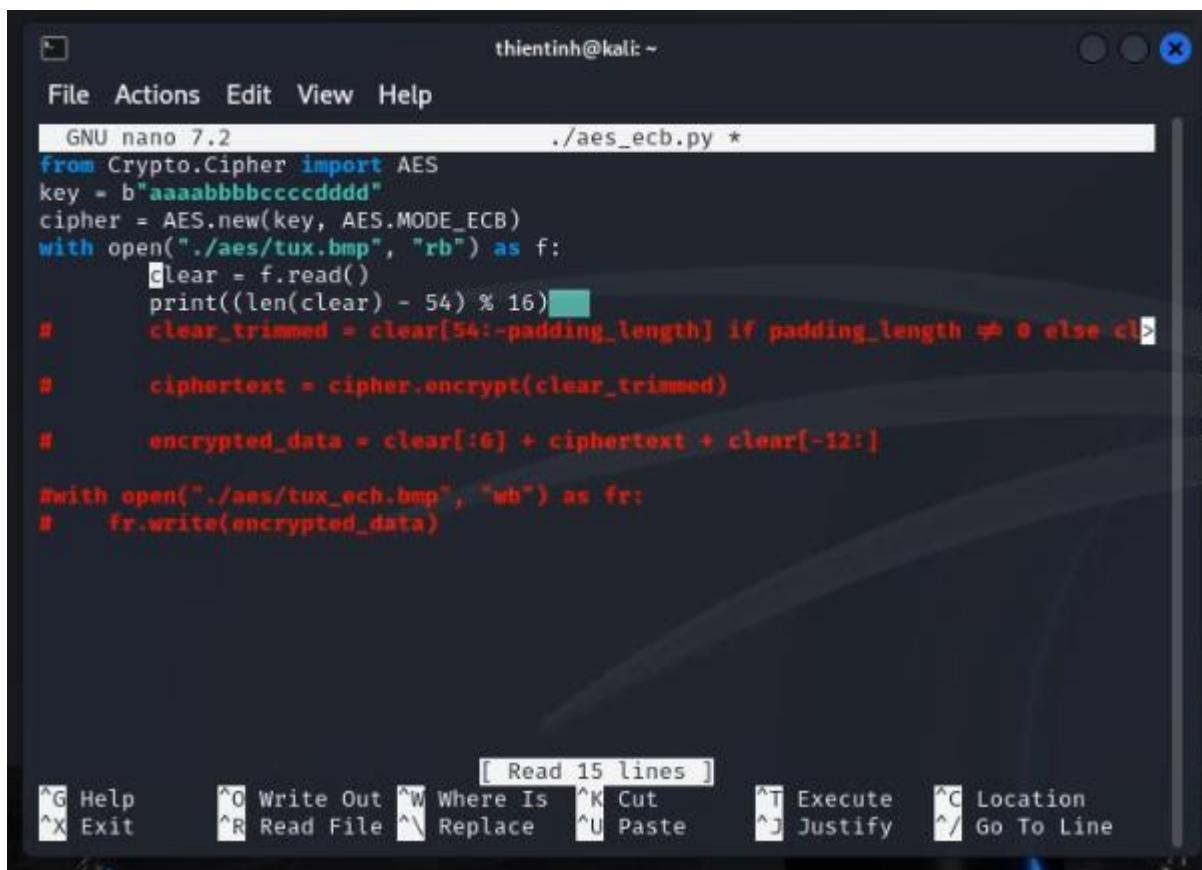
with open("./aes/tux.bmp", "rb") as f:
```

```
clear = f.read()
clear_trimmed = clear[54:-12]
ciphertext = cipher.encrypt(clear_trimmed)
ciphertext = clear[0:54] + ciphertext + clear[-12:]
with open("./aes/tux_ecb.bmp", "wb") as f:
    f.write(ciphertext)
```

- Kiểm tra chiều dài tập tin mã hoá

```
(thientinh@kali)-[~]
$ ./lab03_04/bin/python aes_ecb.py
12
```

- Thực hiện chỉnh sửa code mã hoá tập tin

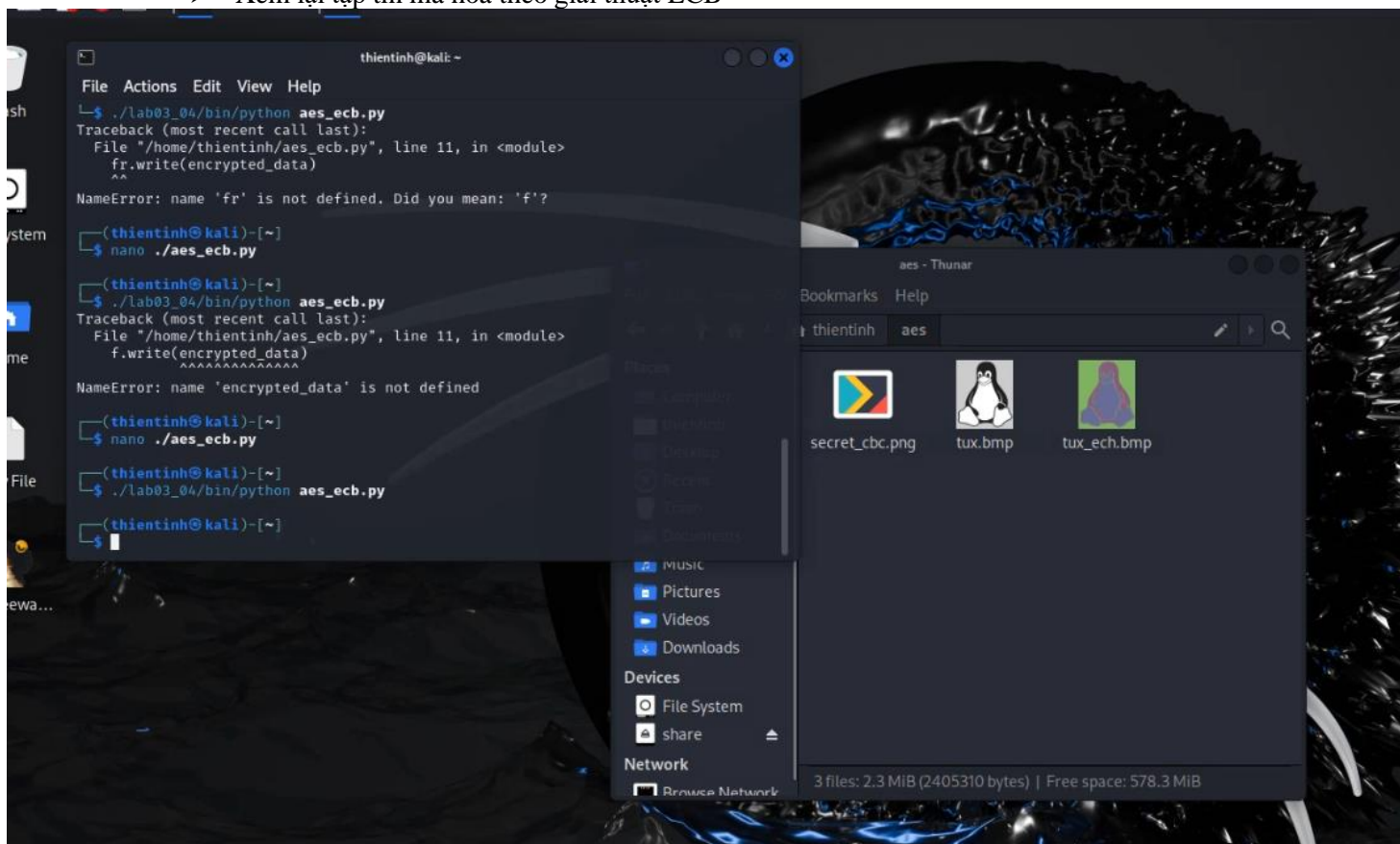


```
thientinh@kali: ~
File Actions Edit View Help
GNU nano 7.2 ./aes_ecb.py *
from Crypto.Cipher import AES
key = b"aaaabbbbccccdddd"
cipher = AES.new(key, AES.MODE_ECB)
with open("./aes/tux.bmp", "rb") as f:
    clear = f.read()
    print((len(clear) - 54) % 16)
# clear_trimmed = clear[54:-padding_length] if padding_length != 0 else cl>
# ciphertext = cipher.encrypt(clear_trimmed)
# encrypted_data = clear[:6] + ciphertext + clear[-12:]
# with open("./aes/tux_ecb.bmp", "wb") as fr:
#     fr.write(encrypted_data)
[ Read 15 lines ]
^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute   ^C Location
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify   ^/ Go To Line
```

```
(thientinh@kali)-[~]
$ ./lab03_04/bin/python aes_ecb.py
```

Gõ lệnh thực thi chương trình mã hoá tập tin

- Xem lại tập tin mã hoá theo giải thuật ECB



Tạo tập tin aes_cbc.py để mã hóa tập tin tux.bmp theo giải thuật AES-CBC. Thực thi aes_cbc.py:

- Tạo tập tin: **\$nano aes_cbc.py**

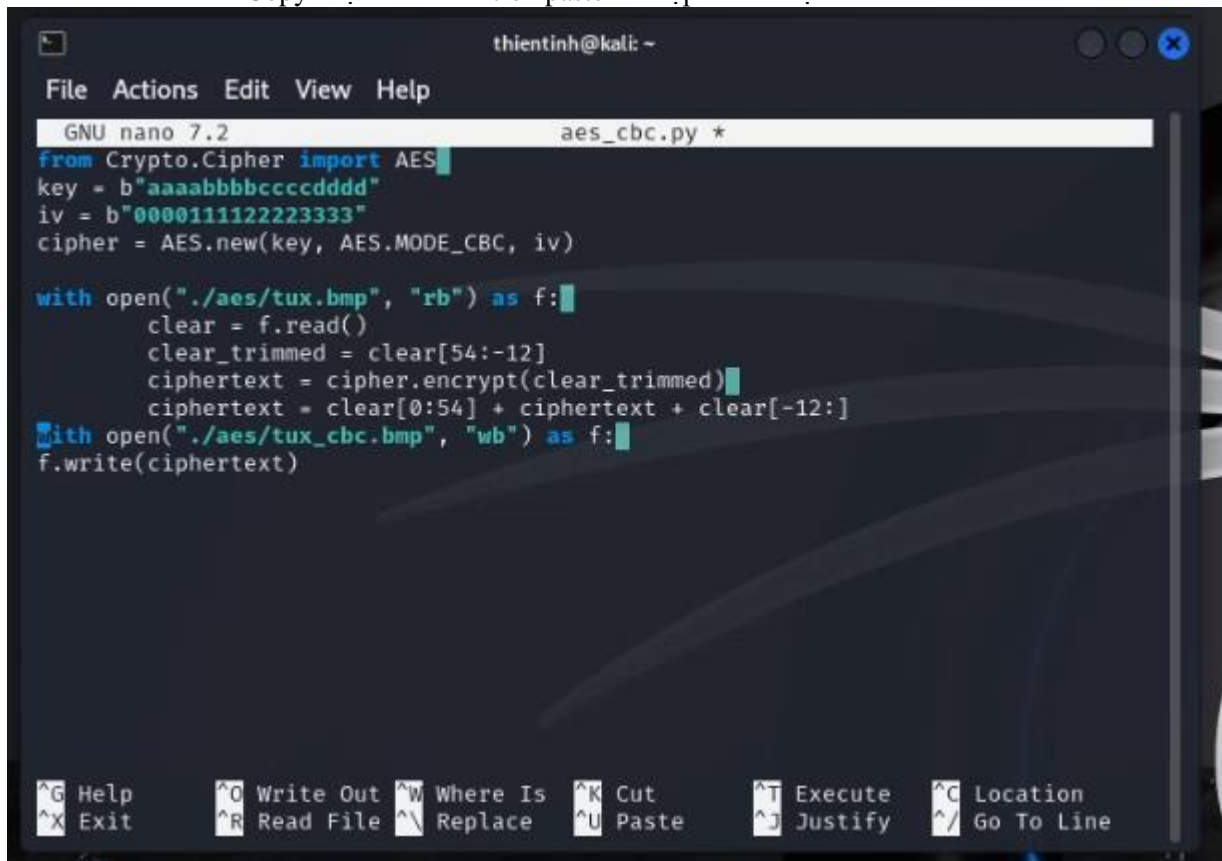
```
(thientinh@kali)-[~]
$ nano aes_cbc.py
```

```
from Crypto.Cipher import AES
key = b"aaaabbbbccccdddd"
iv = b"0000111122223333"
cipher = AES.new(key, AES.MODE_CBC, iv)

with open("./aes/tux.bmp", "rb") as f:
    clear = f.read()
    clear_trimmed = clear[54:-12]
    ciphertext = cipher.encrypt(clear_trimmed)
    ciphertext = clear[0:54] + ciphertext + clear[-12:]

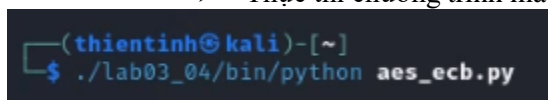
with open("./aes/tux_cbc.bmp", "wb") as f:
    f.write(ciphertext)
```

- Copy đoạn code bên trên paste vào tập tin vừa tạo



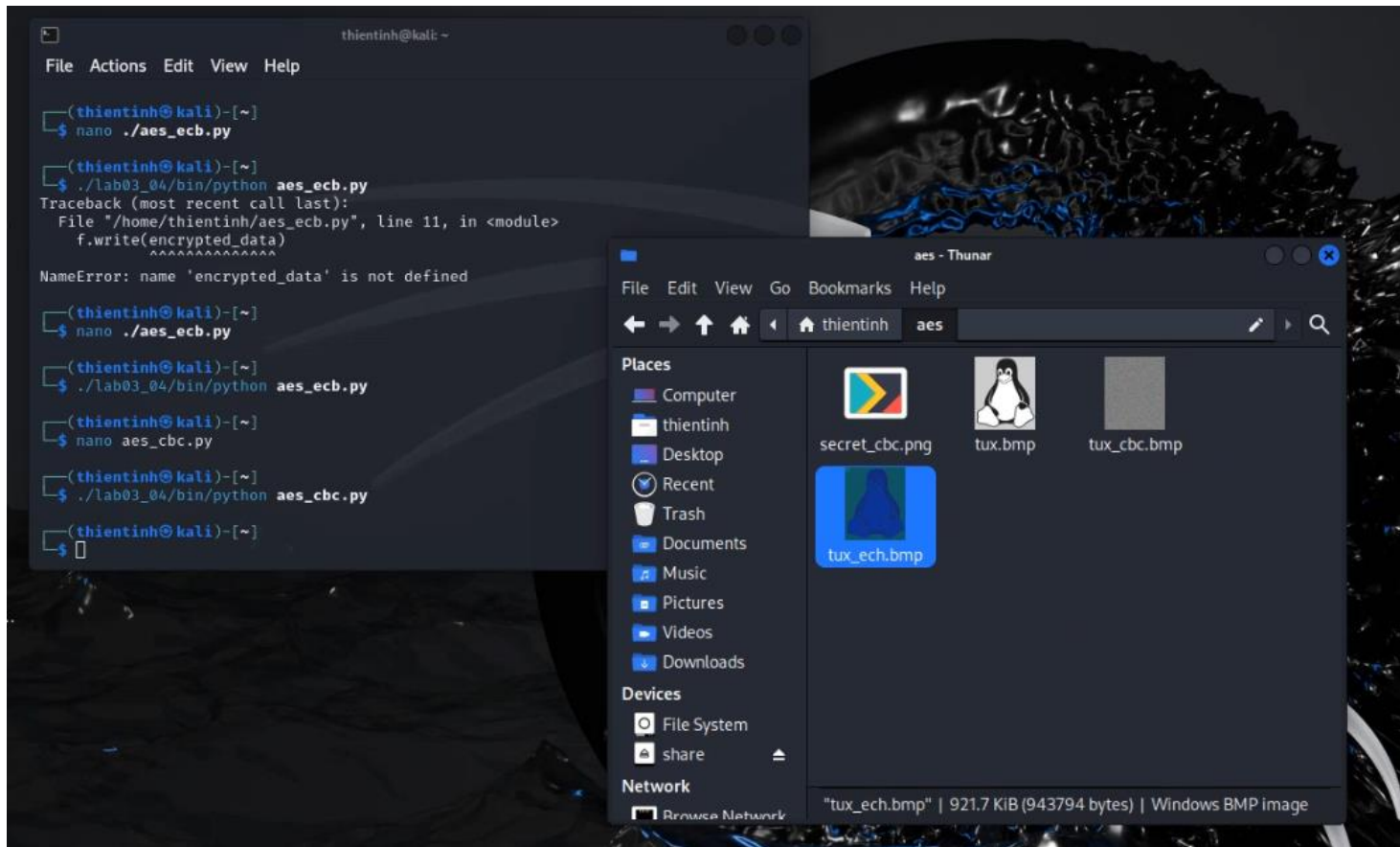
```
thientinh@kali: ~  
File Actions Edit View Help  
GNU nano 7.2 aes_cbc.py *  
from Crypto.Cipher import AES  
key = b"aaaabbbbccccdddd"  
iv = b"0000111122223333"  
cipher = AES.new(key, AES.MODE_CBC, iv)  
  
with open("./aes/tux.bmp", "rb") as f:  
    clear = f.read()  
    clear_trimmed = clear[54:-12]  
    ciphertext = cipher.encrypt(clear_trimmed)  
    ciphertext = clear[0:54] + ciphertext + clear[-12:]  
with open("./aes/tux_cbc.bmp", "wb") as f:  
    f.write(ciphertext)  
  
^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute   ^C Location  
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify   ^_ Go To Line
```

- Thực thi chương trình mã hoá `./lab03_04/bin/python aes_cbc.py`



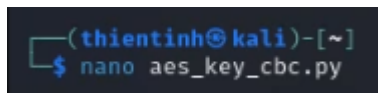
```
(thientinh@kali)-[~]  
$ ./lab03_04/bin/python aes_ecb.py
```

- Xem lại tập tin được mã hoá theo giải thuật CBC



Viết code giải mã tập tin secret.png đã được mã hóa theo giải thuật AES CBC. Biết key mã hóa là "aaaabbbbccccdddd" và IV là "0000111122223333". Lưu ý: phần header của tập tin không được mã hóa.

- Tạo tập tin giải mã: `$nano aes_key_cbc.py`




```
from Crypto.Cipher import AES

key = b"aaaabbbbccccdddd"
iv = b"0000111122223333"
cipher = AES.new(key, AES.MODE_CBC, iv)

with open("./aes/tux_cbc.bmp", "rb") as f:
    encrypted_data = f.read()

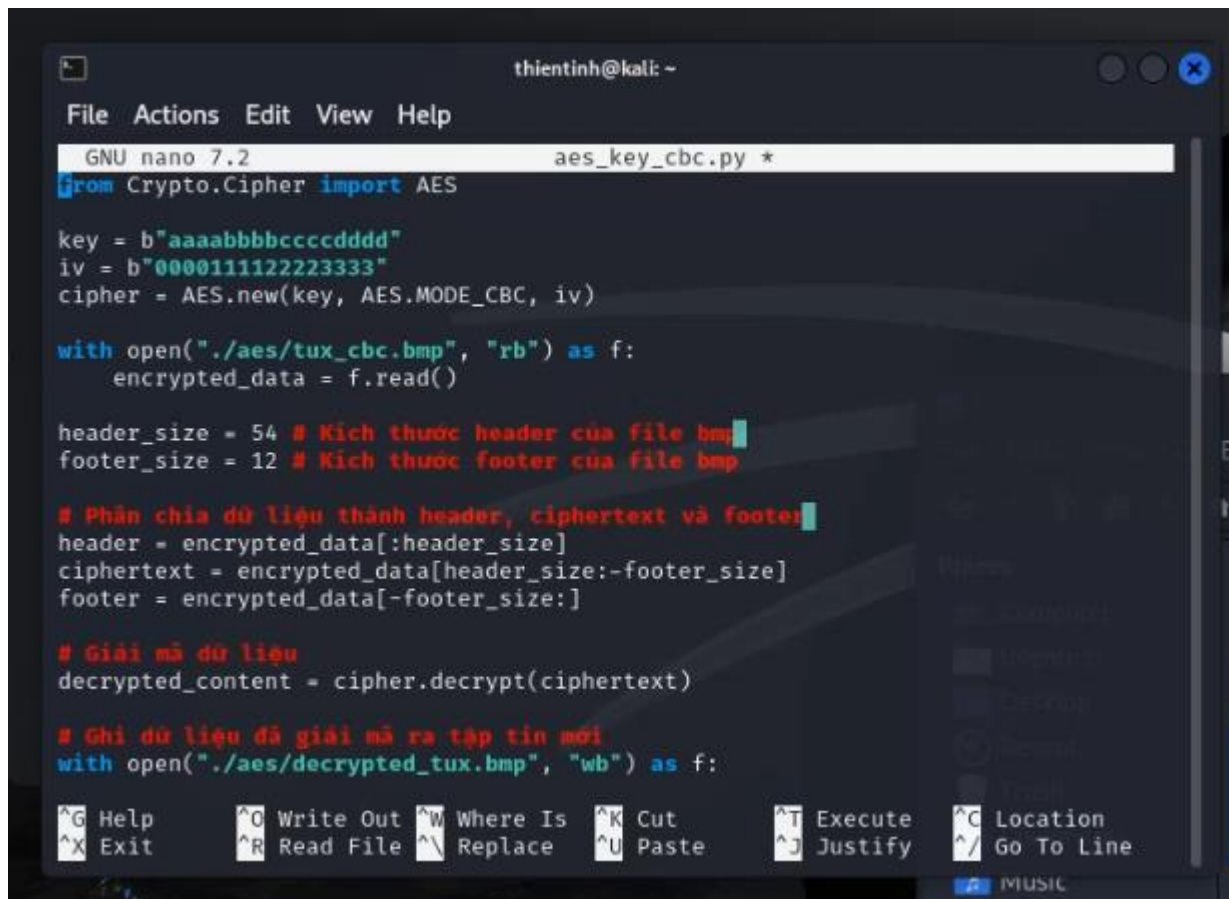
header_size = 54 # Kích thước header của file bmp
footer_size = 12 # Kích thước footer của file bmp

# Phân chia dữ liệu thành header, ciphertext và footer
header = encrypted_data[:header_size]
ciphertext = encrypted_data[header_size:-footer_size]
footer = encrypted_data[-footer_size:]

# Giải mã dữ liệu
decrypted_content = cipher.decrypt(ciphertext)

# Ghi dữ liệu đã giải mã ra tập tin mới
with open("./aes/decrypted_tux.bmp", "wb") as f:
    f.write(header + decrypted_content + footer)
```

- Copy đoạn code bên trên paste vào tập tin vừa tạo



The image shows a terminal window titled 'thientinh@kali: ~' with a menu bar (File, Actions, Edit, View, Help). The terminal is running GNU nano 7.2, editing a file named 'aes_key_cbc.py'. The script imports AES from Crypto.Cipher and defines a key and IV. It reads a BMP file 'tux_cbc.bmp', splits it into header, ciphertext, and footer, decrypts the ciphertext, and writes the result to 'decrypted_tux.bmp'. The script includes Vietnamese comments for each step. At the bottom, there is a table of nano editor shortcuts.

```
thientinh@kali: ~
File Actions Edit View Help
GNU nano 7.2 aes_key_cbc.py *
from Crypto.Cipher import AES

key = b"aaaaabbbccccddddd"
iv = b"0000111122223333"
cipher = AES.new(key, AES.MODE_CBC, iv)

with open("../aes/tux_cbc.bmp", "rb") as f:
    encrypted_data = f.read()

header_size = 54 # Kích thước header của file bmp
footer_size = 12 # Kích thước footer của file bmp

# Phân chia dữ liệu thành header, ciphertext và footer
header = encrypted_data[:header_size]
ciphertext = encrypted_data[header_size:-footer_size]
footer = encrypted_data[-footer_size:]

# Giải mã dữ liệu
decrypted_content = cipher.decrypt(ciphertext)

# Ghi dữ liệu đã giải mã ra tệp tin mới
with open("../aes/decrypted_tux.bmp", "wb") as f:
```

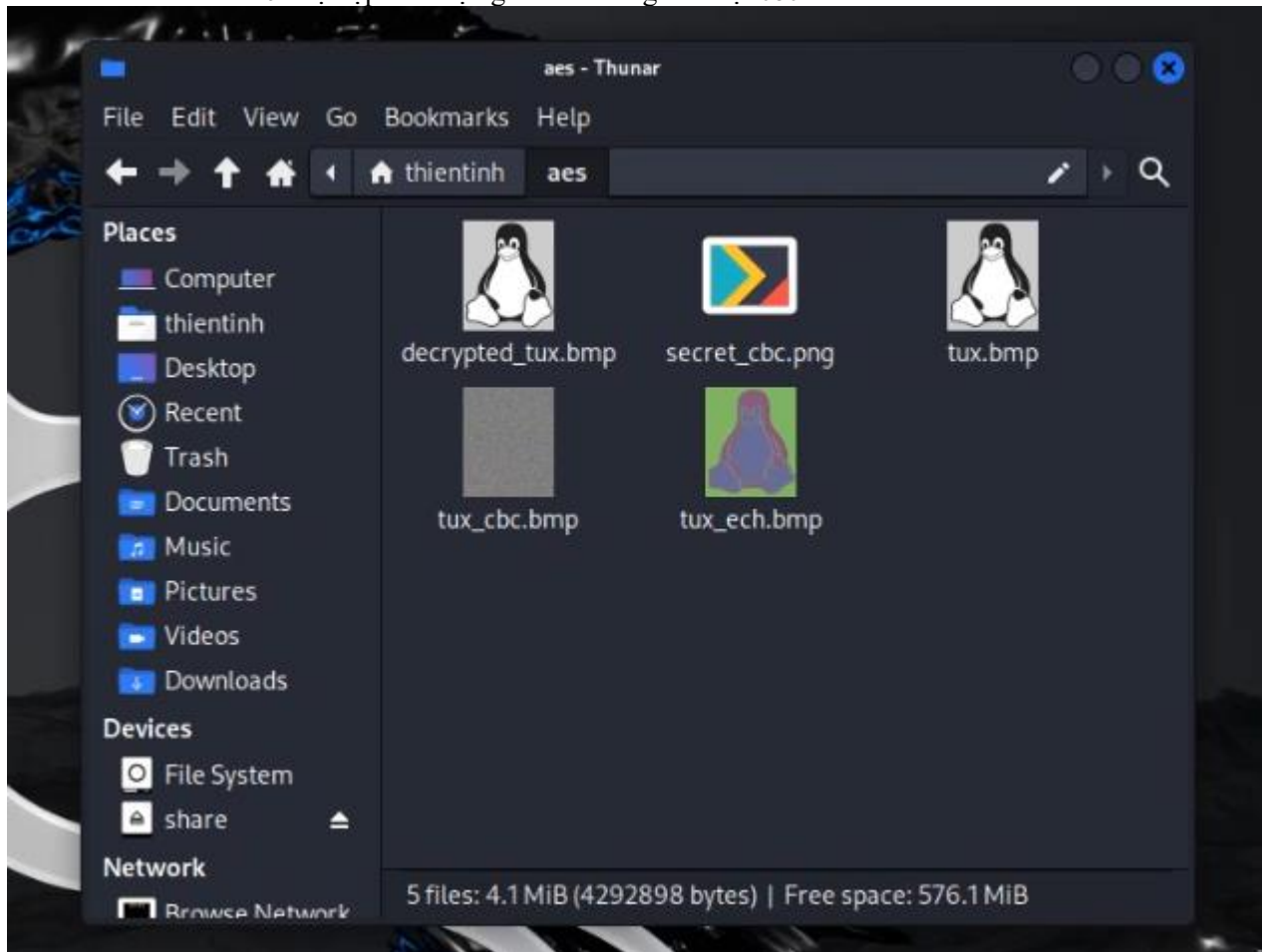
^G Help	^O Write Out	^W Where Is	^K Cut	^T Execute	^C Location
^X Exit	^R Read File	^\\ Replace	^U Paste	^J Justify	^_ Go To Line

MUSIC

- Thực thi chương trình mã hoá `$/lab03_04/bin/python aes_key_cbc.py`

```
(thientinh@kali)-[~]  
$ ./lab03_04/bin/python aes_key_cbc.py
```

- Xem lại tập tin được giải mã theo giải thuật cbc

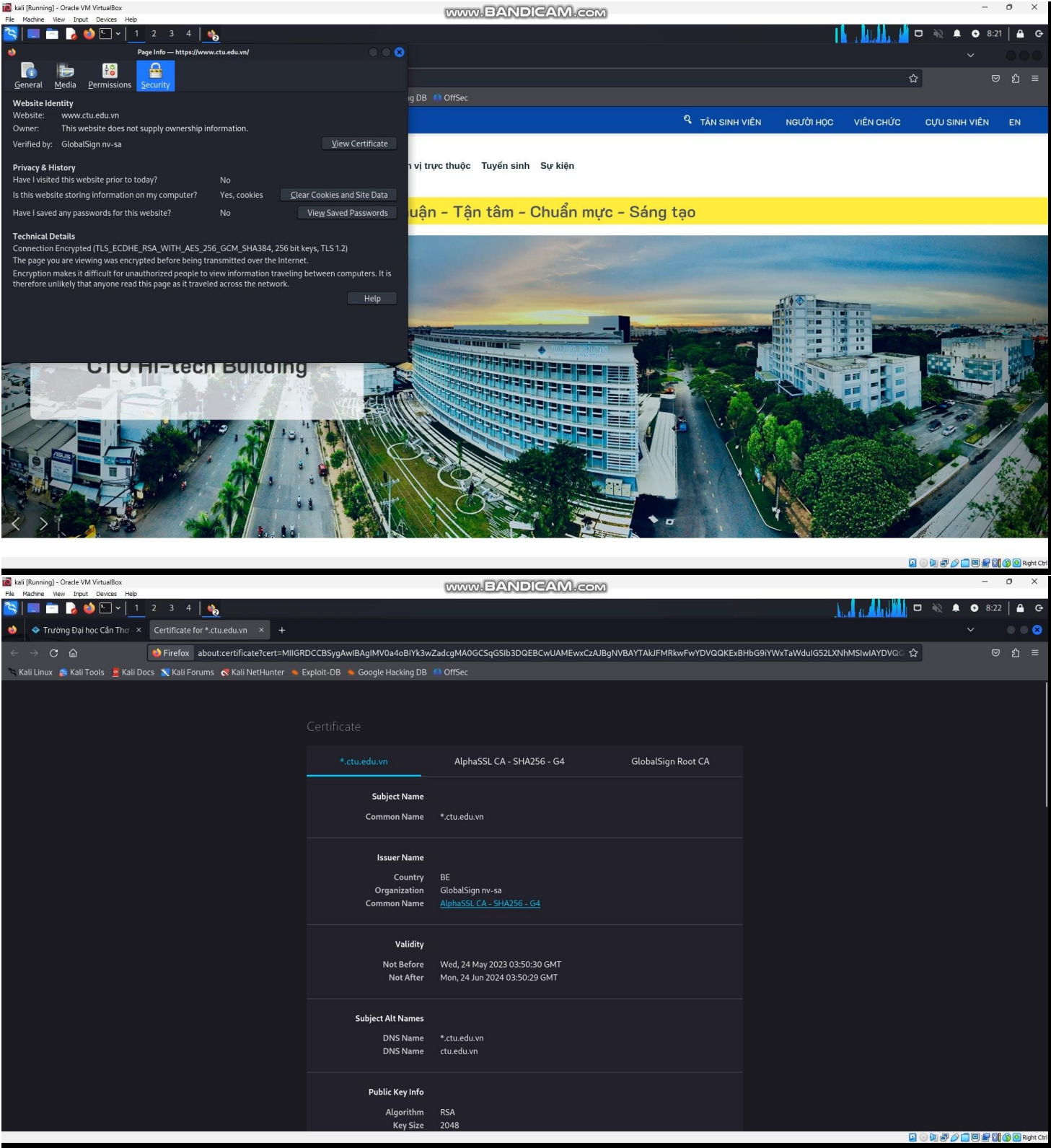


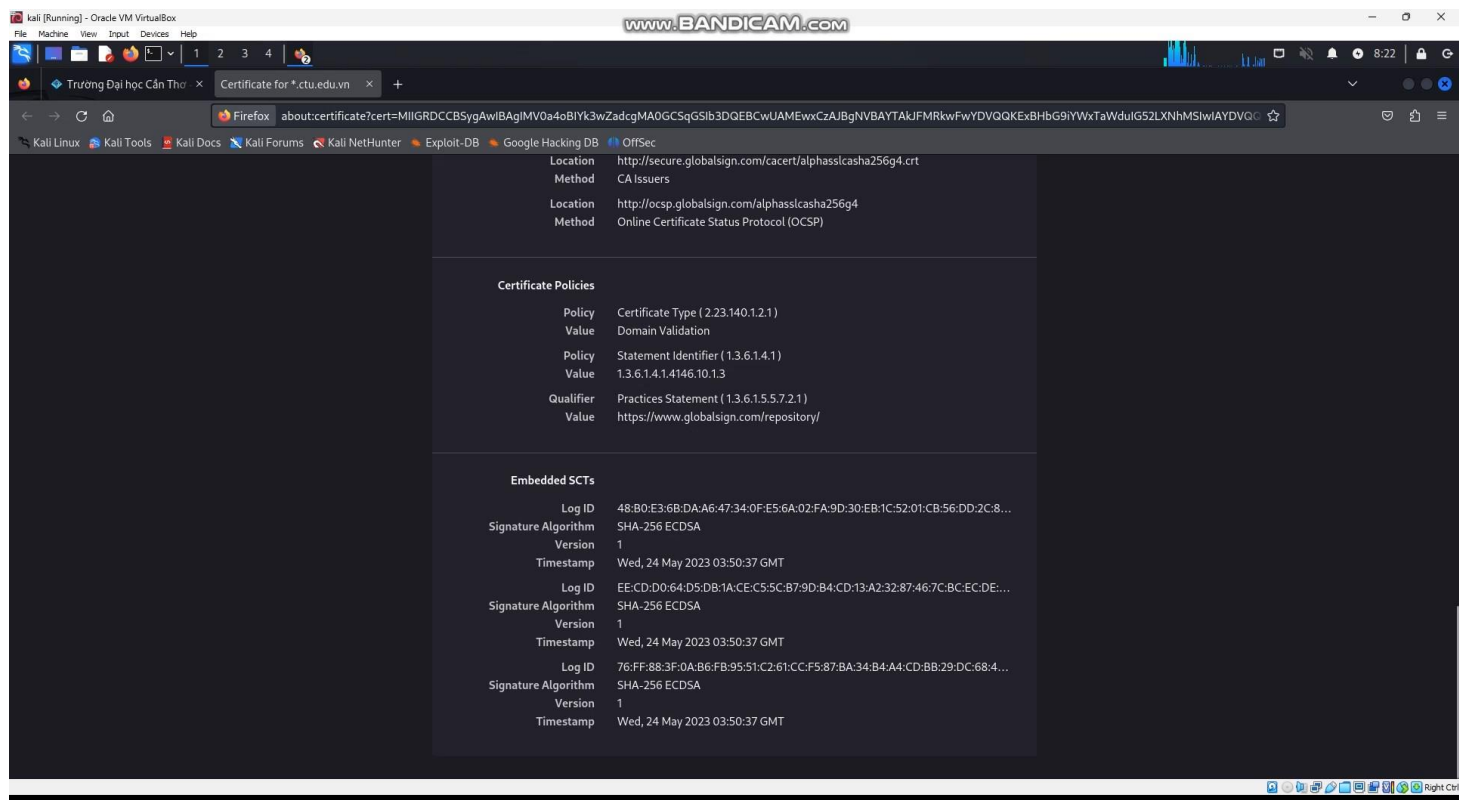
Câu 5: Chứng chỉ số

Sử dụng một trình duyệt web truy cập đến địa chỉ <https://www.ctu.edu.vn/>, sau đó tìm chứng chỉ số (SSL Server Certificate) của địa chỉ nói trên và trả lời các thông tin sau:

- Đơn vị phát hành chứng chỉ: AlphaSSL CA –SHA256 –G2
- Ngày hết hạn chứng chỉ: 29/05/2022
- Khóa công khai (public key) của chứng chỉ: RSA (2048 Bits)

An toàn hệ thống - Khoa CNTT





---HẾT---