

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

KHOA AN TOÀN THÔNG TIN



MÔN HỌC: PHÂN TÍCH MÃ ĐỘC

BÁO CÁO THỰC HÀNH BÀI 3

Giảng viên: PGS.TS. Đỗ Xuân Chợt

Sinh viên: Hoàng Trung Kiên – B20DCAT098

Hà Nội – 5/2023

Mục lục

1. Tìm hiểu về Ghidra.....	3
a, Mục đích.	3
b, Lý thuyết.....	3
2. Thực hành.	4
Nhiệm vụ 1: Sử dụng công cụ Ghidra.	4
Nhiệm vụ 2: Tạo project và nhập chương trình cadet01.....	5
Nhiệm vụ 3: Tìm cổng mạng của dịch vụ.	9
Nhiệm vụ 4: Tìm “Easter egg”.....	11
Nhiệm vụ 5: Làm gián đoạn dịch vụ.	12
3. Checkwork.....	13

1. Tìm hiểu về Ghidra.

a, Mục đích.

Bài thực hành này giới thiệu công cụ Ghidra của *ghidra-sre.org*. Sinh viên sẽ sử dụng Ghidra để phân tích một tập tin thực thi nhằm xác định một số thuộc tính của nó.

b, Lý thuyết.

Ghidra là một công cụ phân tích ngược mã máy mã nguồn mở được phát triển bởi Cơ quan An ninh Quốc gia Hoa Kỳ (NSA) và được công bố công khai vào tháng 3 năm 2019. Nó cung cấp một môi trường phân tích mạnh mẽ cho việc phân tích và giải mã các chương trình máy tính.

Ghidra có các tính năng chính sau:

1. Dịch mã máy: Ghidra cho phép người dùng dịch mã máy từ các tệp nhị phân và hiển thị mã hợp ngữ tương ứng. Nó có khả năng hỗ trợ nhiều kiến trúc vi xử lý khác nhau, bao gồm x86, ARM, MIPS, PowerPC và nhiều kiến trúc khác.
2. Phân tích động và tĩnh: Ghidra cung cấp các công cụ phân tích động và tĩnh để giúp người dùng hiểu cấu trúc và hoạt động của chương trình. Bằng cách theo dõi luồng điều khiển, các hàm và biến, người dùng có thể tìm hiểu cách chương trình hoạt động và cách các thành phần tương tác với nhau.
3. Hiển thị biểu đồ và tương tác: Ghidra cho phép người dùng xem và tương tác với các biểu đồ lưu đồ luồng điều khiển, biểu đồ phụ thuộc dữ liệu và các biểu đồ liên quan khác. Điều này giúp người dùng có cái nhìn tổng quan về cấu trúc của chương trình và tìm hiểu cách các thành phần tương tác với nhau.
4. Phân tích mã độc: Ghidra cung cấp các công cụ hỗ trợ phân tích mã độc và tìm kiếm lỗ hổng bảo mật. Nó cho phép người dùng tìm kiếm các mẫu và dấu hiệu của mã độc, như các lỗi tràn bộ đệm, lỗi truy cập không hợp lệ và các hành vi không an toàn khác.
5. Tích hợp scripting: Ghidra hỗ trợ việc viết và thực thi các script bằng nhiều ngôn ngữ, bao gồm Python và Java. Điều này cho phép người dùng mở rộng và tùy chỉnh các tính năng của Ghidra để phù hợp với nhu cầu của họ.

Ghidra là một công cụ mạnh mẽ và linh hoạt được sử dụng rộng rãi trong cộng đồng phân tích ngược và nghiên cứu bảo mật. Nó cung cấp một môi trường phân tích toàn diện và hỗ trợ cho việc tìm hiểu và phân tích mã máy.

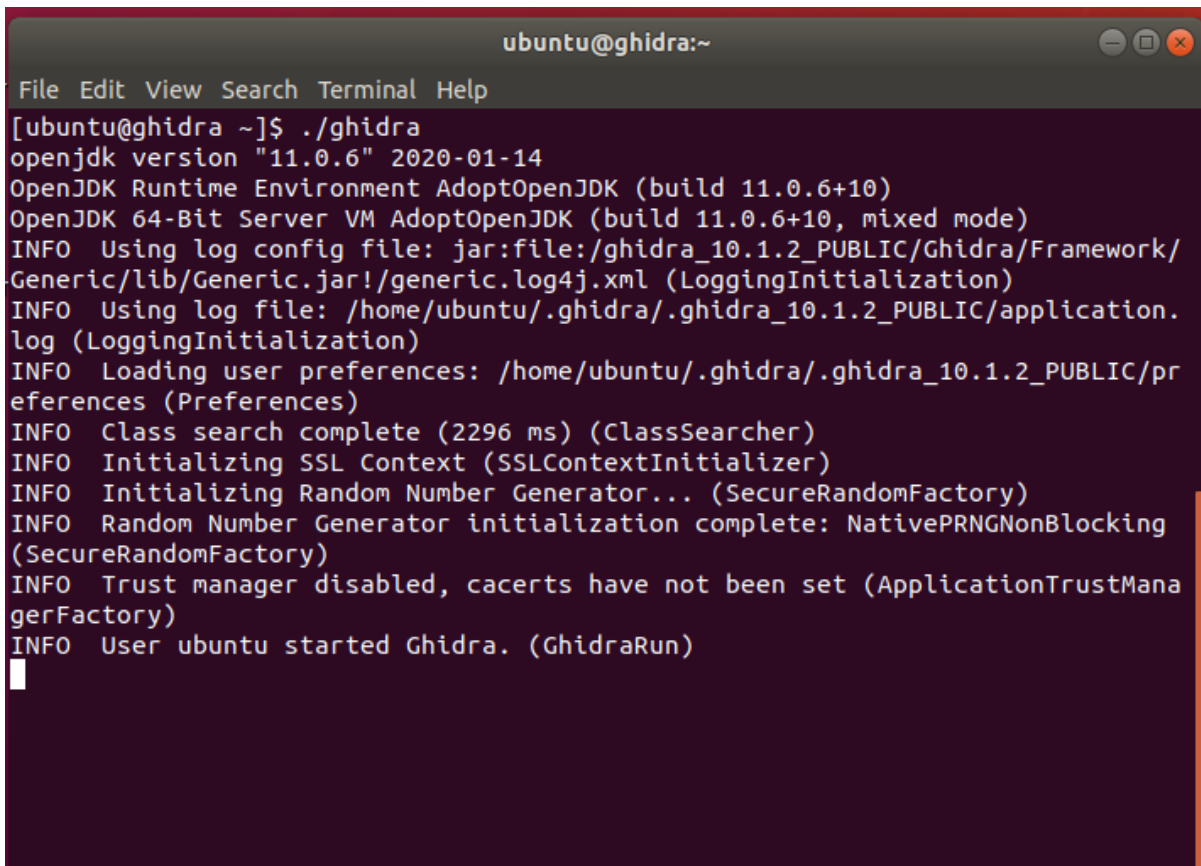
2. Thực hành.

- Nhiệm vụ: Một bản sao của phần mềm dịch vụ có trong máy ghidra có tên là cadet011 trong thư mục Home. Chương trình này đang chạy trên máy chủ. Mục tiêu của bạn là kết nối đến dịch vụ; khiến nó hiển thị “easter egg”; và sau đó làm chương trình bị lỗi. Sinh viên sử dụng Ghidra để phân tích chương trình cadet01 nhằm đạt được các mục tiêu trên.

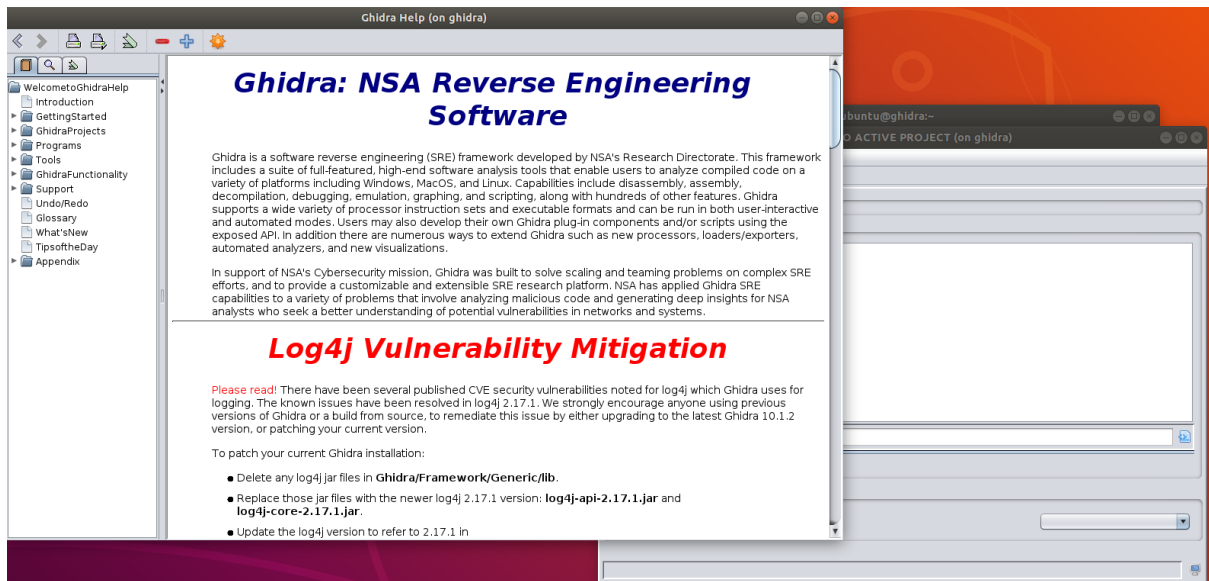
Nhiệm vụ 1: Sử dụng công cụ Ghidra.

Khởi động Ghidra

Chạy lệnh `./ghidra` để khởi động chương trình

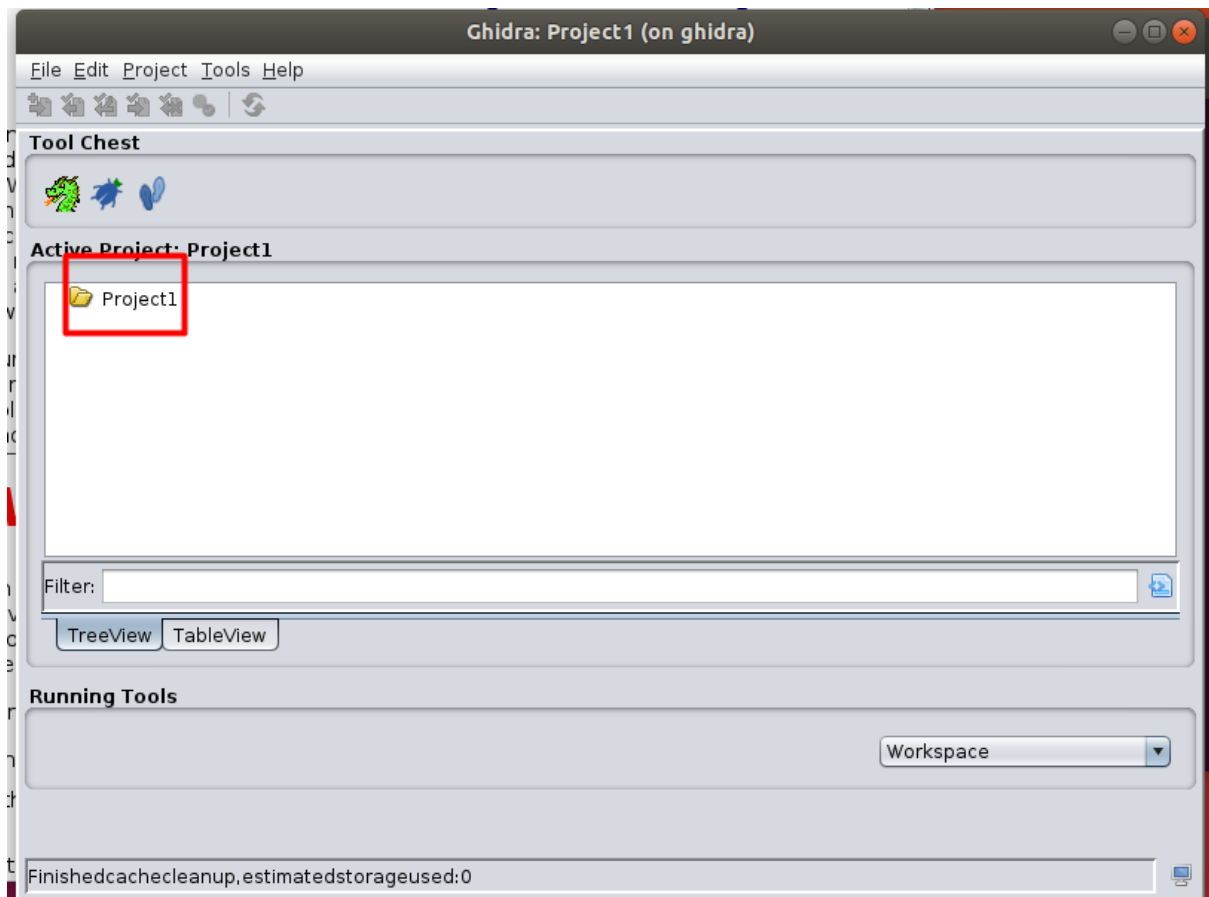


```
ubuntu@ghidra:~  
File Edit View Search Terminal Help  
[ubuntu@ghidra ~]$ ./ghidra  
openjdk version "11.0.6" 2020-01-14  
OpenJDK Runtime Environment AdoptOpenJDK (build 11.0.6+10)  
OpenJDK 64-Bit Server VM AdoptOpenJDK (build 11.0.6+10, mixed mode)  
INFO Using log config file: jar:file:/ghidra_10.1.2_PUBLIC/Ghidra/Framework/  
Generic/lib/Generic.jar!/generic.log4j.xml (LoggingInitialization)  
INFO Using log file: /home/ubuntu/.ghidra/.ghidra_10.1.2_PUBLIC/application.  
log (LoggingInitialization)  
INFO Loading user preferences: /home/ubuntu/.ghidra/.ghidra_10.1.2_PUBLIC/pr  
eferences (Preferences)  
INFO Class search complete (2296 ms) (ClassSearcher)  
INFO Initializing SSL Context (SSLContextInitializer)  
INFO Initializing Random Number Generator... (SecureRandomFactory)  
INFO Random Number Generator initialization complete: NativePRNGNonBlocking  
(SecureRandomFactory)  
INFO Trust manager disabled, cacerts have not been set (ApplicationTrustMana  
gerFactory)  
INFO User ubuntu started Ghidra. (GhidraRun)  
█
```

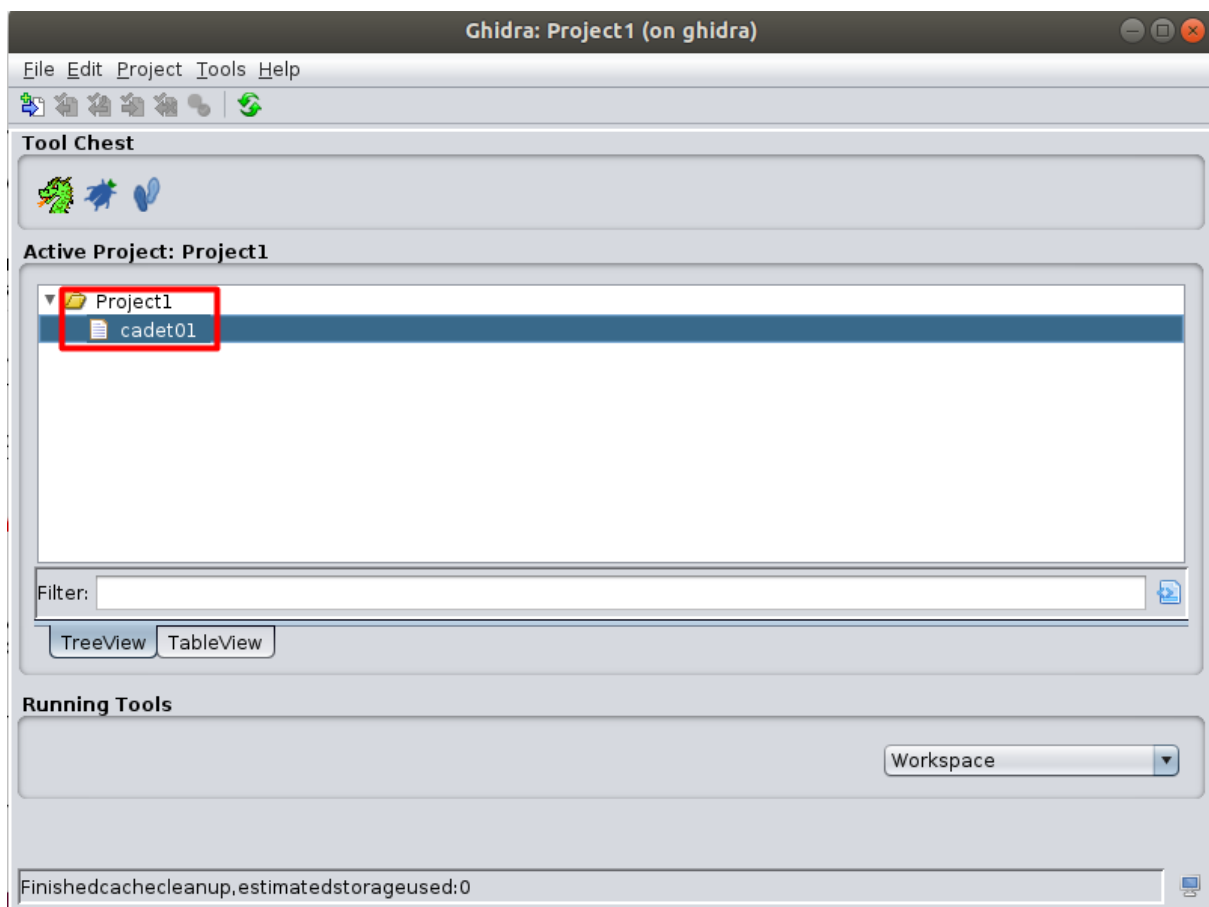
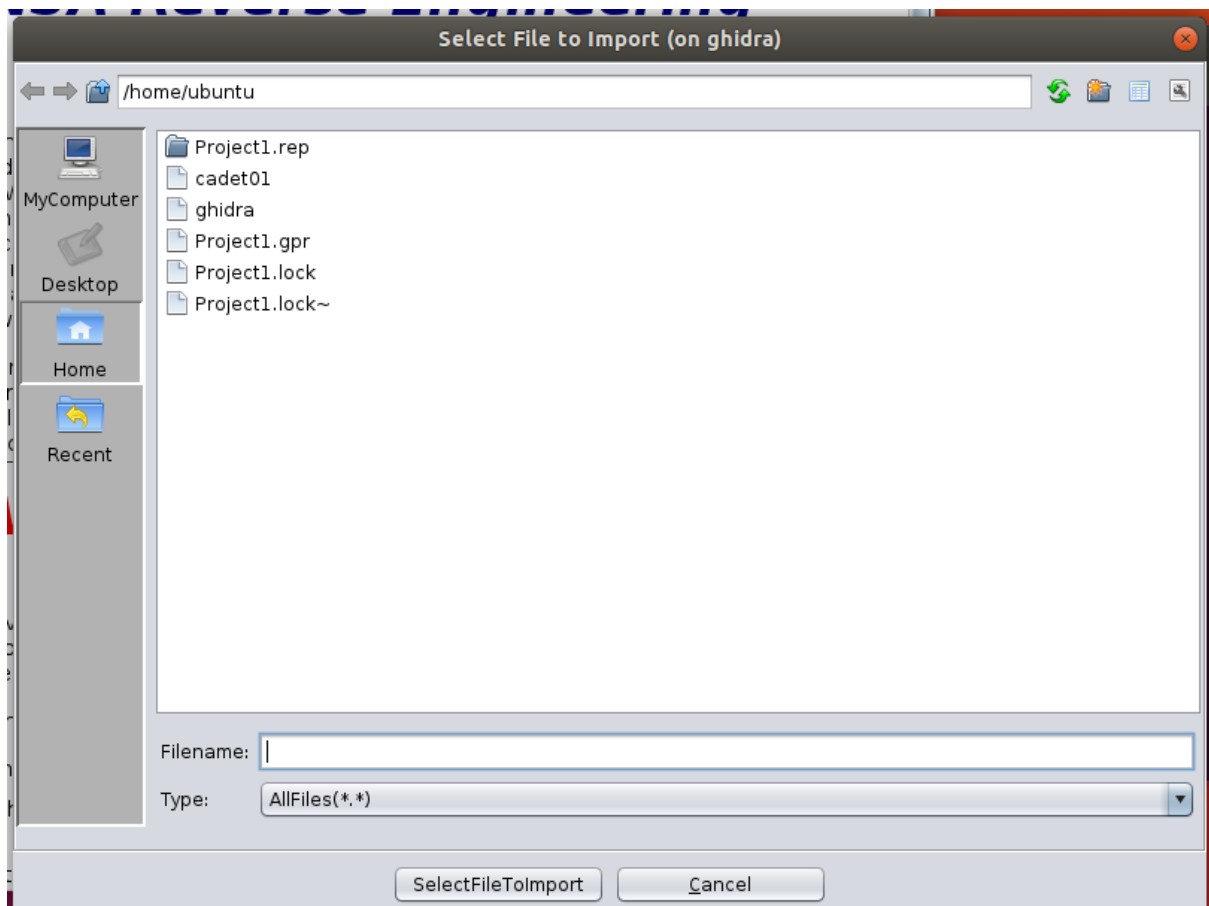


Nhiệm vụ 2: Tạo project và nhập chương trình cadet01.

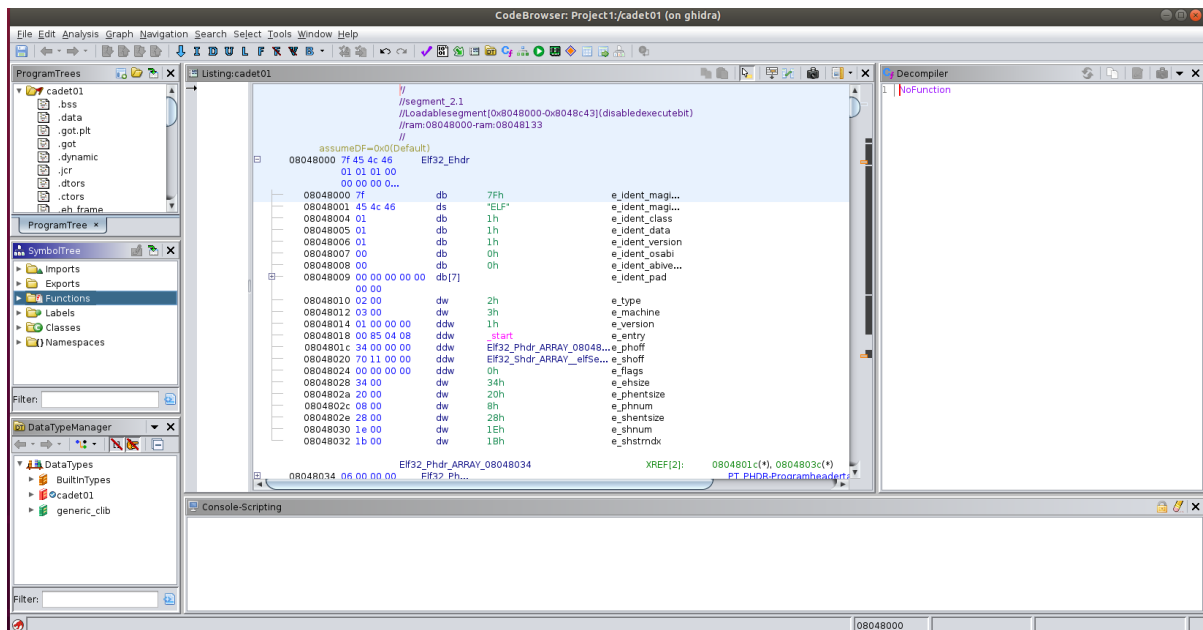
Sử dụng menu File/New project trên cửa sổ chính của Ghidra để tạo một dự án mới.



Sau đó sử dụng menu File/Import file để nhập chương trình cadet01.



Khi yêu cầu phân tích, hãy chọn Yes và chấp nhận các phân tích mặc định.



```
INFO Using log config file: jar:file:/ghidra_10.1.2_PUBLIC/Ghidra/Framework/Generic/lib/Generic.jar
!/generic.log4j.xml (LoggingInitialization)
INFO Using log file: /home/ubuntu/.ghidra/.ghidra_10.1.2_PUBLIC/application.log (LoggingInitializat
ion)
INFO Loading user preferences: /home/ubuntu/.ghidra/.ghidra_10.1.2_PUBLIC/preferences (Preferences)

INFO Class search complete (2355 ms) (ClassSearcher)
INFO Initializing SSL Context (SSLContextInitializer)
INFO Initializing Random Number Generator... (SecureRandomFactory)
INFO Random Number Generator initialization complete: NativePRNGNonBlocking (SecureRandomFactory)
INFO Trust manager disabled, cacerts have not been set (ApplicationTrustManagerFactory)
INFO User ubuntu started Ghidra. (GhidraRun)
INFO Creating project: /home/ubuntu/Lab (DefaultProject)
INFO Starting cache cleanup: /tmp/ubuntu-Ghidra/fscache2 (FileCacheMaintenanceDaemon)
INFO Finished cache cleanup, estimated storage used: 0 (FileCacheMaintenanceDaemon)
INFO DWARF external debug information found: ExternalDebugInfo [filename=null, crc=0, hash=8c87d2da
398575d5eea5daf0ae5e9e21b4cfb06a] (ExternalDebugFilesService)
INFO Unable to find DWARF information, skipping DWARF analysis (DWARFAnalyzer)
INFO hit non-returning function, restarting decompiler switch analyzer later (DecompilersSwitchAnaly
zer)
INFO Packed database cache: /tmp/ubuntu-Ghidra/packed-db-cache (PackedDatabaseCache)
```

```

ubuntu@ghidra:~
File Edit View Search Terminal Help
)
INFO Packed database cache: /tmp/ubuntu-Ghidra/packed-db-cache (PackedDatabaseCache)
INFO -----
ASCII Strings                                0.583 secs
Apply Data Archives                          0.650 secs
Call Convention ID                           0.086 secs
Call-Fixup Installer                         0.009 secs
Create Address Tables                        0.012 secs
Create Function                             0.023 secs
DWARF                                         0.020 secs
Data Reference                              0.008 secs
Decompiler Switch Analysis                   0.116 secs
Decompiler Switch Analysis - One Time        0.256 secs
Demangler GNU                               0.029 secs
Disassemble Entry Points                    0.235 secs
ELF Scalar Operand References                0.022 secs
Embedded Media                              0.020 secs
External Entry References                    0.005 secs
Function ID                                 0.153 secs
Function Start Search                       0.022 secs
GCC Exception Handlers                      0.029 secs
Non-Returning Functions - Discovered          0.019 secs
Non-Returning Functions - Known              0.011 secs
Reference                                   0.029 secs
Shared Return Calls                         0.002 secs
Stack                                        0.266 secs
Subroutine References                       0.024 secs
X86 Function Callee Purge                     0.005 secs
x86 Constant Reference Analyzer              0.152 secs
-----
Total Time 2 secs
-----
(AutoAnalysisManager)

```

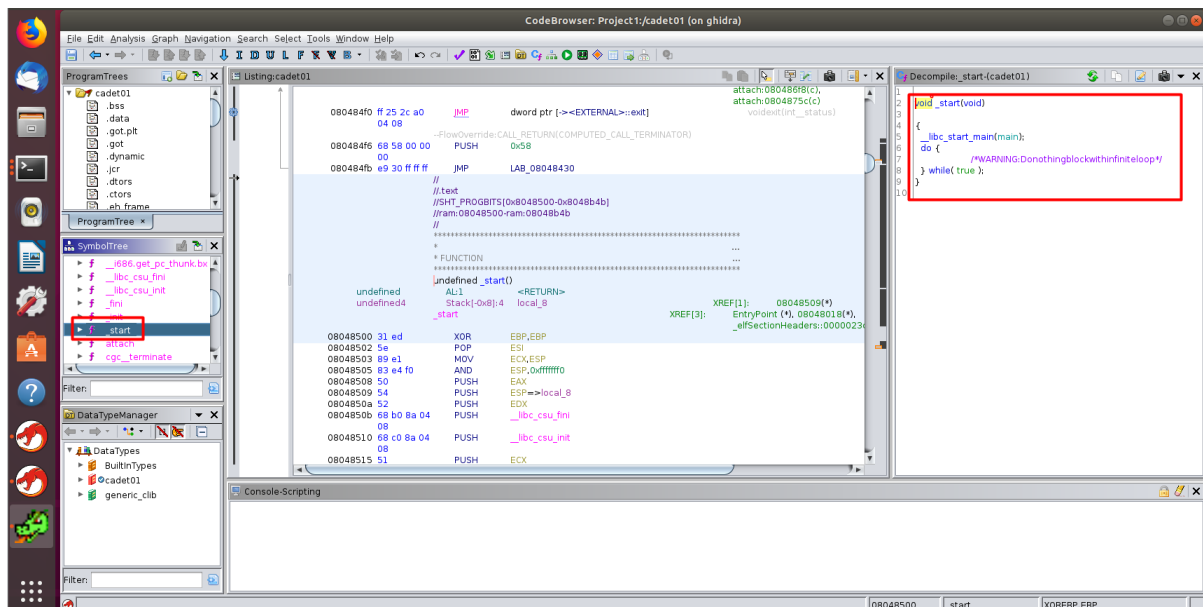
Các hàm gọi bởi hàm chính

Hàm được gọi bởi hàm main là: `cgc_terminate()`, `cgc_transmit_all()`, `cgc_check()`,

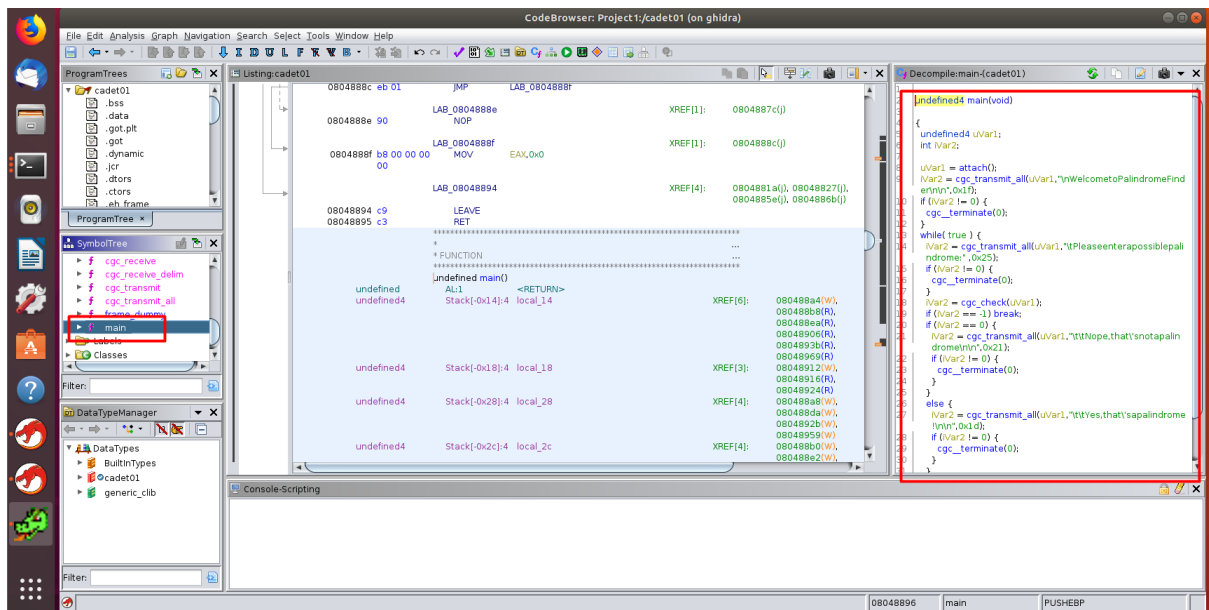
Hàm `cgc_transmit_all()` gọi hàm `cgc_transmit()`

Hàm `cgc_terminate()` gọi hàm `exit(1)`

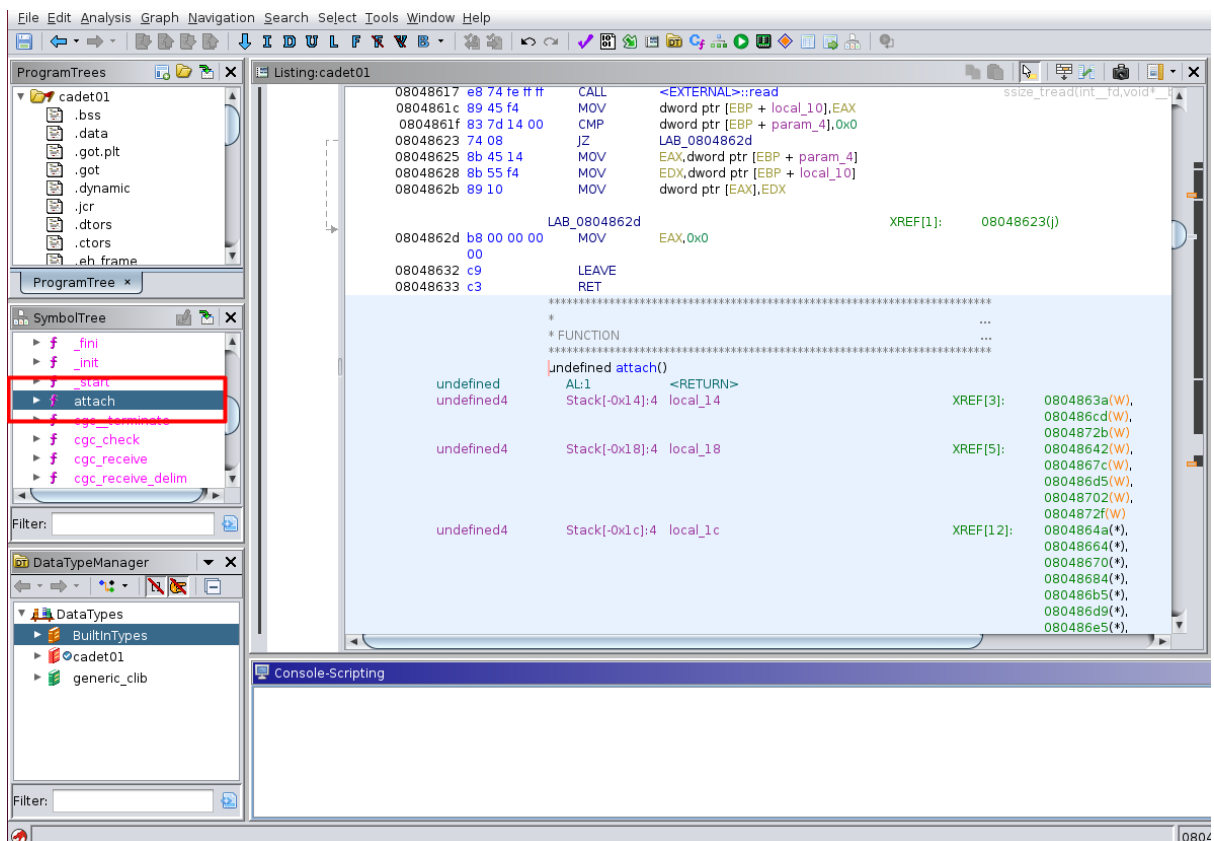
Hàm `cgc_check()` gọi hàm `cgc_receive_delim()`, `cgc_transmit_all()`, `cgc_terminate()`



Nhiệm vụ 3: Tìm cổng mạng của dịch vụ.



Ta mở đến hàm attach



Ở bên phải ta thấy đoạn chương trình của hàm attach và thấy biến “portno=0x135b”, ta đổi sang mã nhị phân là 4955 => cổng là 4955

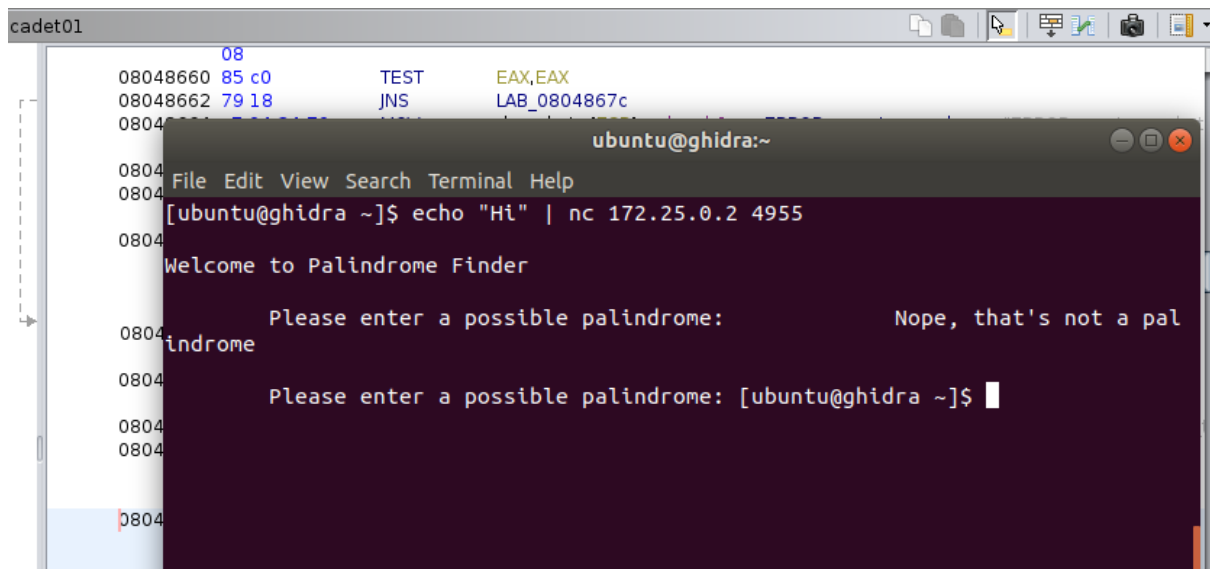
```
Decompile:attach-(cadet01)
1
2 int attach(void)
3
4 {
5     int iVar1;
6
7     sockfd = socket(2,1,0);
8     if (sockfd < 0) {
9         perror("ERRORopeningsocket" );
10        /*WARNING:Subroutinedoesnotreturn*/
11        exit(1);
12    }
13    bzero(serv_addr,0x10);
14    portno = 0x135b;
15    serv_addr._0_2_ = 2;
16    serv_addr._4_4_ = 0;
17    serv_addr._2_2_ = htons(0x135b);
18    iVar1 = bind(sockfd,(sockaddr *)serv_addr,0x10);
19    if (iVar1 < 0) {
20        perror("ERRORonbinding" );
21        /*WARNING:Subroutinedoesnotreturn*/
22        exit(1);
23    }
24    listen(sockfd,5);
25    clilen = 0x10;
26    newsockfd = accept(sockfd,(sockaddr *)cli_addr,&clilen);
27    if (newsockfd < 0) {
28        perror("ERRORonaccept" );
29        /*WARNING:Subroutinedoesnotreturn*/
30        exit(1);
31    }
32    return newsockfd;
33 }
34
```

Xem qua các hàm của chương trình cadet01 để tìm số cổng mạng được sử dụng khi gắn kết với socket mạng. Sau khi đã tìm được số cổng, hãy sử dụng nó để kết nối đến server, sử dụng câu lệnh:

```
echo "Hi" | nc 172.25.0.2 <port number>
```

<port number>: số cổng tìm được là 4955. Sau khi kết nối thành công sinh viên sẽ nhận được phản hồi từ server.

Kết nối thành công



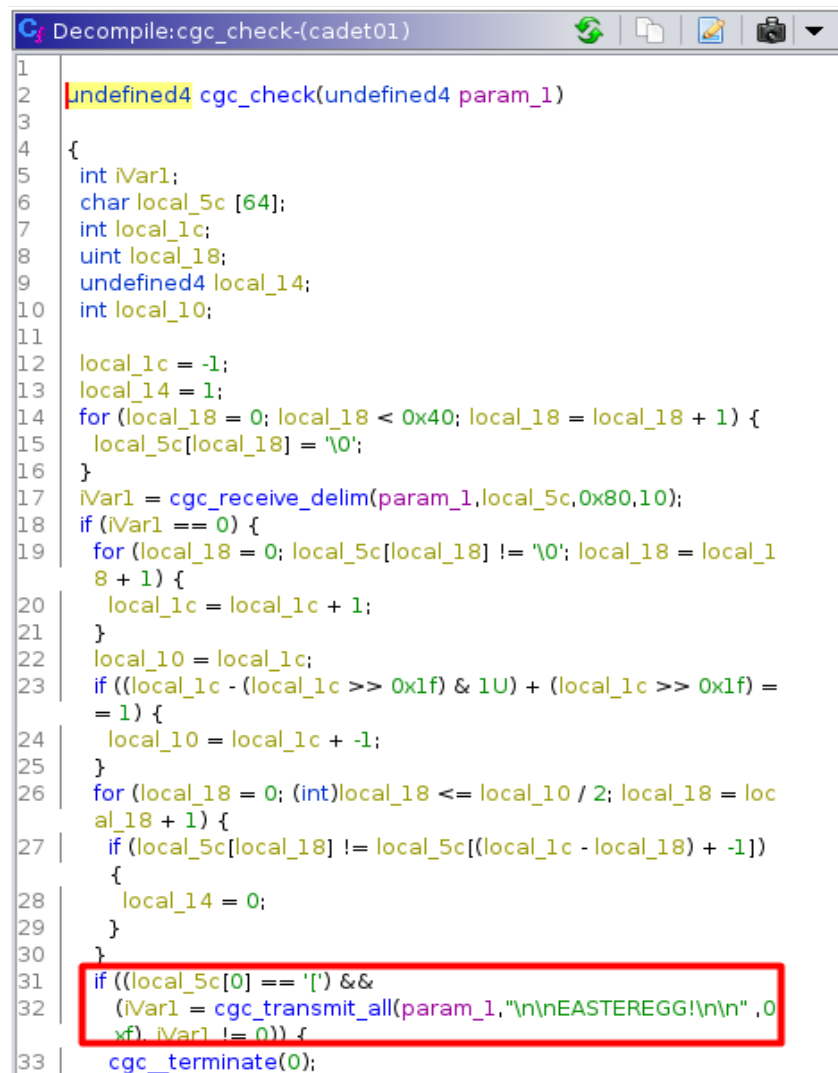
The screenshot shows a debugger window with assembly code on the left and a terminal window on the right. The assembly code includes instructions like `TEST EAX,EAX` and `JNS LAB_0804867c`. The terminal window, titled `ubuntu@ghidra:~`, shows the command `[ubuntu@ghidra ~]$ echo "Hi" | nc 172.25.0.2 4955` being executed. The output of the program in the terminal is:

```
Welcome to Palindrome Finder

Please enter a possible palindrome: Nope, that's not a pal
indrome

Please enter a possible palindrome: [ubuntu@ghidra ~]$
```

Nhiệm vụ 4: Tìm “Easter egg”.



The screenshot shows the decompiled code for the function `cgc_check`. The code includes several local variables and a loop that checks for a specific string in memory. A red box highlights the final conditional statement:

```
1  undefined4 cgc_check(undefined4 param_1)
2
3
4  {
5      int iVar1;
6      char local_5c [64];
7      int local_1c;
8      uint local_18;
9      undefined4 local_14;
10     int local_10;
11
12     local_1c = -1;
13     local_14 = 1;
14     for (local_18 = 0; local_18 < 0x40; local_18 = local_18 + 1) {
15         local_5c[local_18] = '\0';
16     }
17     iVar1 = cgc_receive_delim(param_1,local_5c,0x80,10);
18     if (iVar1 == 0) {
19         for (local_18 = 0; local_5c[local_18] != '\0'; local_18 = local_1
20             8 + 1) {
21             local_1c = local_1c + 1;
22         }
23         local_10 = local_1c;
24         if (((local_1c - (local_1c >> 0x1f) & 1U) + (local_1c >> 0x1f) =
25             = 1) {
26             local_10 = local_1c + -1;
27         }
28         for (local_18 = 0; (int)local_18 <= local_10 / 2; local_18 = loc
29             al_18 + 1) {
30             if (local_5c[local_18] != local_5c[(local_1c - local_18) + -1])
31             {
32                 local_14 = 0;
33             }
34         }
35         if ((local_5c[0] == '[') &&
36             (iVar1 = cgc_transmit_all(param_1,"\\n\\nEASTEREGG!\\n\\n",0
37                 xf), iVar1 != 0)) {
38             cgc_terminate(0);
39         }
40     }
```

```
echo "[" | nc 172.25.0.2 4955
```

```

ubuntu@ghidra:~
File Edit View Search Terminal Help

Welcome to Palindrome Finder

Please enter a possible palindrome: Nope, that's not a palindrome

Please enter a possible palindrome: [ubuntu@ghidra ~]$
[ubuntu@ghidra ~]$ echo "Hi" | nc 172.25.0.2 4955

Welcome to Palindrome Finder

Please enter a possible palindrome: Nope, that's not a palindrome

Please enter a possible palindrome: [ubuntu@ghidra ~]$ EASTER EGG!
-bash: EASTER: command not found
[ubuntu@ghidra ~]$ echo "[" | nc 172.25.0.2 4955

Welcome to Palindrome Finder

Please enter a possible palindrome:

EASTER EGG!

Yes, that's a palindrome!

Please enter a possible palindrome: [ubuntu@ghidra ~]$

```

Nhiệm vụ 5: Làm gián đoạn dịch vụ.

nhập đầu vào để khiến dịch vụ bị lỗi. Hoàn thành nhiệm vụ nếu netcat hiển thị thông báo “Connection reset by peer”.

```

Please enter a possible palindrome: [ubuntu@ghidra ~]$
[ubuntu@ghidra ~]$ echo "ddqweuoisdhjjxbnsdhuqehshqoosdhqwedsdkljzxhvcjvcnxidugro8et
uoifjhgkcxcvmnkjdjgkhdjghojhoiuqnvckxlq" | nc 172.25.0.2 4955

Welcome to Palindrome Finder

Please enter a possible palindrome: [ubuntu@ghidra ~]$
[ubuntu@ghidra ~]$ echo "ddqweuoisdhjjxbnsdhuqehshqoosdhqwedsdkljzxhvcjvcnxidugro8et
uoifjhgkcxcvmnkjdjgkhdjghojhoiuqnvckxlsdqweczkjxchvcjsdfhgsdj" | nc 172.25.0.2 4955

Welcome to Palindrome Finder

Please enter a possible palindrome: [ubuntu@ghidra ~]$
[ubuntu@ghidra ~]$
[ubuntu@ghidra ~]$
[ubuntu@ghidra ~]$ echo "ddqweuoisdhjjxbnsdhuqehshqoosdhqwedsdkljzxhvcjvcnxidugro8et
uoifjhgkcxcvmnkjdjgkhdjghojhoiuqnvckxlsdqweczkjxchvcjsdf12321ewq214354634hgsdj" | nc 1
72.25.0.2 4955

Welcome to Palindrome Finder

Please enter a possible palindrome: Ncat: Connection reset by peer.
[ubuntu@ghidra ~]$

```

3. Checkwork.

```
student@ubuntu:~/labtainer/labtainer-student$ checkwork
Results stored in directory: /home/student/labtainer_xfer/ghidra
Labname ghidra

Student          |          egg |          crash |
===== | ===== | ===== |
B20DCAT098      |          Y   |          Y   |
What is automatically assessed for this lab:
    egg: Student provided input necessary to display easter egg
    crash: Student provided input necessary to crash the server
```