

Họ và tên: Trần Trí Dũng

Mã số sinh viên: HE190680

Lớp: IA1901

Lab 7:

Install Docker.io -> Launch a transient instance of an Ubuntu container -> Launch the Thug honeyclient container:

```
thug@b300ebac065:~$ sudo apt-get install docker.io
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
docker.io is already the newest version (27.5.1-0ubuntu3-22.04.2).
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
dungthel190680@dungthel190680:~$ sudo docker run --rm -it ubuntu bash
root@cf7ff4ba7622e:/# exit
exit
dungthel190680@dungthel190680:~$ sudo docker run --rm -it --entrypoint bash remnux/thug
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

thug@b7a38536c0c6:~$ exit
exit
dungthel190680@dungthel190680:~$ sudo docker run --rm -it --entrypoint bash remnux/thug
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

thug@b300ebac065:~$ thug -F http://Lnx.ima3a.it/c2L6ZT0xM0B4O2Zvbnc2VpZ2h0YVh3MTQ0M0NFjMTG4Zm0ODg4ZjUxMjFiZTU=/Redirection/
[2025-06-04 05:21:07] [window open redirection] about:blank -> http://Lnx.ima3a.it/c2L6ZT0xM0B4O2Zvbnc2VpZ2h0YVh3MTQ0M0NFjMTG4Zm0ODg4ZjUxMjFiZTU=/Redirection/
[2025-06-04 05:21:07] [HTTPSession] HTTPConnectionPool(host='Lnx.ima3a.it', port=80): Max retries exceeded with url: /c2L6ZT0xM0B4O2Zvbnc2VpZ2h0YVh3MTQ0M0NFjMTG4Zm0ODg4ZjUxMjFiZTU=/Redirection/ (Caused by NewConnectionError(<urllib3.connection.HTTPConnection object at 0x7f35d8951b10>: Failed to establish a new connection: [Errno -2] Name or service not known'))
[2025-06-04 05:21:07] Thug analysis logs saved at /tmp/thug/logs/dfee0aa173f3d5051c906a9fed5bfa8/20250604052107
thug@b300ebac065:~$
```

Create the directory on the underlying host and make it world-accessible -> Use “-v” to map the host’s directory into the container:

```

dungththe190680@dungththe190680:~$ mkdir logs && chmod a+wx logs
dungththe190680@dungththe190680:~$ sudo docker run --rm -it -v ~/logs:/home/thug/logs --entrypoint bash remnux/thug
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

thug@921796c1b990c:~$ thug -F http://lnx.ima3a.it/c216ZToxWtB402ZvbnQtd2VpZ2h0OjYwM3MTQ0NWFiMTg4ZmVxODg4ZjUxMjFiZTUu=/Redirection/
[2025-06-04 05:26:13] [window open redirection] about:blank -> http://lnx.ima3a.it/c216ZToxWtB402ZvbnQtd2VpZ2h0OjYwM3MTQ0NWFiMTg4ZmVxODg4ZjUxMjFiZTUu=/Redirection/
[2025-06-04 05:26:13] [HTTPSession] HTTPConnectionPool(host='lnx.ima3a.it', port=80): Max retries exceeded with url: /c216ZToxWtB402ZvbnQtd2VpZ2h0OjYwM3MTQ0NWFiMTg4ZmVxODg4ZjUxMjFiZTUu=/Redirection/ (Caused by
NewConnectionError(<curlib3.connection.HTTPConnection object at 0x7f7d85331ed0>: Failed to establish a new connection: [Errno -2] Name or service not known'))
[2025-06-04 05:26:13] Thug analysis logs saved at /tmp/thug/Logs/dfee0aa173f3d5851c906a9fed5bfaf8/20250604052613
thug@921796c1b990c:~$ exit
exit
dungththe190680@dungththe190680:~$ ls logs/
dfee0aa173f3d5851c906a9fed5bfaf8  thug.csv
dungththe190680@dungththe190680:~$

```

Store data on underlying host while running apps in transient environments:

```

nonroot@2b9563a41516: ~/jw - sshroot@C:\Users\46613\ - jw - ssh
dunsthe19068@dungthe190680: ~$ mkdir samples && chmod +xwr samples && cd samples
dunsthe19068@dungthe190680: ~/samples$ wget -q https://zeltser.com/media/archive/gootkit.zip && unzip gootkit.zip
Archive: gootkit.zip
[gootkit.zip] about.txt password:
  inflating: about.txt
  inflating: aggressive.exe
  inflating: grabber.exe
  inflating: gtk1.exe
  inflating: jhg26ff.sys
  inflating: ritaglo_unpack.dll
dunsthe19068@dungthe190680: ~/samples$ sudo docker run --rm -it -v ~/samples:/home/nonroot/workdir --entrypoint bash remnux/viper
[sudo] password for dungthe190680:
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

nonroot@2b9563a41516: ~/workdir$ viper

  O
  W
  I
  P
  E
  R
  v2.0-rc11

You have 0 files in your default repository.
You have 41 modules installed.
viper > store -folder ../workdir --file-type PE32
[+] Stored file "ritaglo_unpack.dll" to /home/nonroot/.viper/binaries/9/4/d/a/0/9da8a02de59b991aa305f9a0dd977d16b7b6156db36b6fela94de8bb6667d8
[+] Session opened on /home/nonroot/.viper/binaries/9/4/d/a/0/9da8a02de59b991aa305f9a0dd977d16b7b6156db36b6fela94de8bb6667d8
[+] Running command "yara scan -t"
[+] Scanning ritaglo_unpack.dll (9da8a02de59b991aa305f9a0dd977d16b7b6156db36b6fela94de8bb6667d8)
[+] Running command "triage"
[+] ritaglo_unpack.dll is a DLL
[+] Stored file "gtk1.exe" to /home/nonroot/.viper/binaries/e/8/f/c/e8fcd095758a8ela4bf945f4913e10557b80120f25e329f06d8642017dd353787
[+] Session opened on /home/nonroot/.viper/binaries/e/8/f/c/e8fcd095758a8ela4bf945f4913e10557b80120f25e329f06d8642017dd353787
[+] Running command "yara scan -t"
[+] Scanning gtk1.exe (e8fcd095758a8ela4bf945f4913e10557b80120f25e329f06d8642017dd353787)
[+] Running command "triage"
[+] Stored file "aggressive.exe" to /home/nonroot/.viper/binaries/1/2/6/8/1268d1f0bf4fcddeb8953bd3e7e9b4350660e402ca24f56ee5d2bcla2e9e3741a
[+] Session opened on /home/nonroot/.viper/binaries/1/2/6/8/1268d1f0bf4fcddeb8953bd3e7e9b4350660e402ca24f56ee5d2bcla2e9e3741a
[+] Running command "yara scan -t"
[+] Scanning aggressive.exe (1268d1f0bf4fcddeb8953bd3e7e9b4350660e402ca24f56ee5d2bcla2e9e3741a)
[+] Running command "triage"
[+] Stored file "jhg26ff.sys" to /home/nonroot/.viper/binaries/2/8/7/8/28789eadfd97e38238579419e85a2f4db55ec71c3966303a3e4858048a30f05
[+] Session opened on /home/nonroot/.viper/binaries/2/8/7/8/28789eadfd97e38238579419e85a2f4db55ec71c3966303a3e4858048a30f05
[+] Running command "yara scan -t"
[+] Scanning jhg26ff.sys (28789eadfd97e38238579419e85a2f4db55ec71c3966303a3e4858048a30f05)
[+] Running command "triage"
[+] jhg26ff.sys is a Windows driver
[+] Stored file "grabber.exe" to /home/nonroot/.viper/binaries/8/8/e/8/08e858ca6e1a8db965400f9738368d5fbb491fc3658267e8a3f64d7661c0f
[+] Session opened on /home/nonroot/.viper/binaries/8/8/e/8/08e858ca6e1a8db965400f9738368d5fbb491fc3658267e8a3f64d7661c0f
[+] Running command "yara scan -t"
[+] Scanning grabber.exe (08e858ca6e1a8db965400f9738368d5fbb491fc3658267e8a3f64d7661c0f)
[+] Running command "triage"
viper >

```

```
nonroot@2b9563a41516: ~/workdir$ viper > find all
+-----+-----+-----+-----+
# | Name | Mime | MD5 | Tags |
+-----+-----+-----+-----+
1 | ritaglio_unpack.dll | application/x-dosexec; charset=binary | ca438d4b536ef02ad0abe2860ff789c5 | dll |
2 | gtk1.exe | application/x-dosexec; charset=binary | 639819ee45daaa30e53d866938cb72ad | |
3 | aggressive.exe | application/x-dosexec; charset=binary | 3315287968320a0dc4d845d3dae935b4 | |
4 | jhg26ff.sys | application/x-dosexec; charset=binary | cd58e1e49a88854b8d463db6a957b | driver |
5 | grabber.exe | application/x-dosexec; charset=binary | ca39d7cd301e61f0a01bda488af8f5fb | |
+-----+-----+-----+-----+

viper > open ca39d7cd301e61f0a01bda488af8f5fb
[*] Session opened on /home/nonroot/.viper/binaries/0/8/e/8/08e858ca8e6a1e8bdb965406f9738368d5fbb91fc3658267e843f64d7661c0f
viper grabber.exe > virustotal
[*] 63 out of 72 antivirus detected ca39d7cd301e61f0a01bda488af8f5fb as malicious.
[*] https://www.virustotal.com/gui/file/08e858ca8e6a1e8bdb965406f9738368d5fbb91fc3658267e843f64d7661c0f/detection/f-08e858ca8e6a1e8bdb965406f9738368d5fbb91fc3658267e843f64d7661c0f-1742589871

viper grabber.exe > exit
nonroot@2b9563a41516: ~/workdir$ ls -l
total 1388
-rw-rw-r-- 1 1000 1000 99 Jan 5 2015 about.txt
-rw-rw-r-- 1 1000 1000 159264 Jun 20 2010 aggressive.exe
-rw-rw-r-- 1 1000 1000 518842 Jun 12 2015 gootkit.zip
-rw-rw-r-- 1 1000 1000 258948 Jun 2 2010 grabber.exe
-rw-rw-r-- 1 1000 1000 117760 Jun 9 2010 gtk1.exe
-rw-rw-r-- 1 1000 1000 138272 Jun 20 2010 jhg26ff.sys
-rw-rw-r-- 1 1000 1000 167936 Jun 28 2010 ritaglio_unpack.dll
-rw-rw-r-- 1 nonroot nonroot 40960 Jun 4 07:40 viper.db
nonroot@2b9563a41516: ~/workdir$
```

Expose container's TCP port 9090 to interact with the application from localhost -> Use “-p” to access network ports within a container -> Use “ps” to show running containers and “stop” to stop them:

```
dungtthe190680@dungtthe190680: ~/samples$ sudo docker run --rm -p 9090:9090 -v ~/samples:/home/nonroot/workdir remnux/viper
dungtthe190680@dungtthe190680: ~/samples$ sudo docker ps
CONTAINER ID   IMAGE          COMMAND                  CREATED        STATUS        PORTS                    NAMES
e70608432bal   remnux/viper   "/bin/bash"             9 seconds ago Up 8 seconds    0.0.0.0:9090->9090/tcp, :::9090->9090/tcp   sleepy_thompson
dungtthe190680@dungtthe190680: ~/samples$ sudo docker stop sleepy_thompson
sleepy_thompson
dungtthe190680@dungtthe190680: ~/samples$ ls -l
total 1388
-rw-rw-r-- 1 dungtthe190680 dungtthe190680 99 Jan 5 2015 about.txt
-rw-rw-r-- 1 dungtthe190680 dungtthe190680 159264 Jun 20 2010 aggressive.exe
drwxr-xr-x 2 lxd 999 4096 Jun 4 08:51 binaries
-rw-rw-r-- 1 dungtthe190680 dungtthe190680 518842 Jun 12 2015 gootkit.zip
-rw-rw-r-- 1 dungtthe190680 dungtthe190680 258948 Jun 2 2010 grabber.exe
-rw-rw-r-- 1 dungtthe190680 dungtthe190680 117760 Jun 9 2010 gtk1.exe
-rw-rw-r-- 1 dungtthe190680 dungtthe190680 138272 Jun 20 2010 jhg26ff.sys
-rw-rw-r-- 1 dungtthe190680 dungtthe190680 167936 Jun 28 2010 ritaglio_unpack.dll
-rw-rw-r-- 1 lxd 999 40960 Jun 4 07:40 viper.db
dungtthe190680@dungtthe190680: ~/samples$
```

Create Dockerfile:

```

dungthethe190680@dungthethe190680:~/thug$ cat Dockerfile
FROM ubuntu:14.04
LABEL maintainer="Lenny Zeltser <lenny@zeltser.com>"

USER root
RUN apt-get update
RUN apt-get install -y --no-install-recommends \
    python2.7 \
    python2.7-dev \
    python-html5lib \
    python3-pip \
    curl \
    build-essential

RUN rm -rf /var/lib/apt/lists/*

RUN pip3 install -q \
    jsbeautifier \
    rarfile \
    BeautifulSoup4 \
    pefile \
    six

RUN groupadd -r thug
RUN useradd -r -g thug -d /home/thug -s /sbin/nologin -c "Thug User" thug

RUN curl -SL https://sourceforge.net/projects/ssdeep/files/ssdeep-2.12/ssdeep-2.12.tar.gz/download | tar -xzc .
RUN cd ssdeep-2.12 && ./configure && make install && cd ..
RUN rm -rf ssdeep-2.12
RUN BUILD_LIB=1 apt-get update && apt-get install ssdeep
RUN mkdir -p /home/thug && chown -R thug:thug /home/thug

USER thug
ENV HOME=/home/thug
ENV USER=thug
WORKDIR /home/thug/src
CMD ["/usr.py"]
dungthethe190680@dungthethe190680:~/thug$
```

Use “docker build” to build the image out of the Dockerfile:

```

dungthethe190680@dungthethe190680:~/thug$ mkdir thug && cd thug
dungthethe190680@dungthethe190680:~/thug$ vim Dockerfile
dungthethe190680@dungthethe190680:~/thug$ sudo docker build -t thug .
[sudo] password for dungthethe190680:
DEPRECATED: The legacy builder is deprecated and will be removed in a future release.
Install the buildx component to build images with BuildKit:
https://docs.docker.com/go/buildx/

Sending build context to Docker daemon  2.56kB
Step 1/19 : FROM ubuntu:14.04
--> 13b66b487594
Step 2/19 : LABEL maintainer="Lenny Zeltser <lenny@zeltser.com>"
--> Using cache
--> e3404fc973c72
Step 3/19 : USER root
--> Using cache
--> 257a638a0972
Step 4/19 : RUN apt-get update
--> Using cache
--> 0d4f5a1a25b6
Step 5/19 : RUN apt-get install -y --no-install-recommends python2.7 python2.7-dev python-html5lib python3-pip curl build-essential
--> Using cache
--> 58b34970e9d7
Step 6/19 : RUN rm -rf /var/lib/apt/lists/*
--> Using cache
--> 2f20b6f2dc02
Step 7/19 : RUN pip3 install -q jsbeautifier rarfile BeautifulSoup4 pefile six
--> Using cache
--> 0d76c4219a2b
Step 8/19 : RUN groupadd -r thug
--> Using cache
--> 53f622aaea81
Step 9/19 : RUN useradd -r -g thug -d /home/thug -s /sbin/nologin -c "Thug User" thug
--> Using cache
--> a26fa5f73ae5
Step 10/19 : RUN curl -SL https://sourceforge.net/projects/ssdeep/files/ssdeep-2.12/ssdeep-2.12.tar.gz/download | tar -xzc .
--> Using cache
--> f477c4d420b9
Step 11/19 : RUN cd ssdeep-2.12 && ./configure && make install && cd ..
--> Using cache
--> e2f091ff8fba
Step 12/19 : RUN rm -rf ssdeep-2.12
--> Using cache
--> b77b87c1f4dd
Step 13/19 : RUN BUILD_LIB=1 apt-get update && apt-get install ssdeep
--> Using cache
--> a848cbb33c17
Step 14/19 : RUN mkdir -p /home/thug && chown -R thug:thug /home/thug
--> Using cache
--> 32f9a77380ba
Step 15/19 : USER thug
--> Using cache
--> d050ae98b323
Step 16/19 : ENV HOME=/home/thug
--> Using cache
--> 519d87f7d676
Step 17/19 : ENV USER=thug
--> Using cache
```

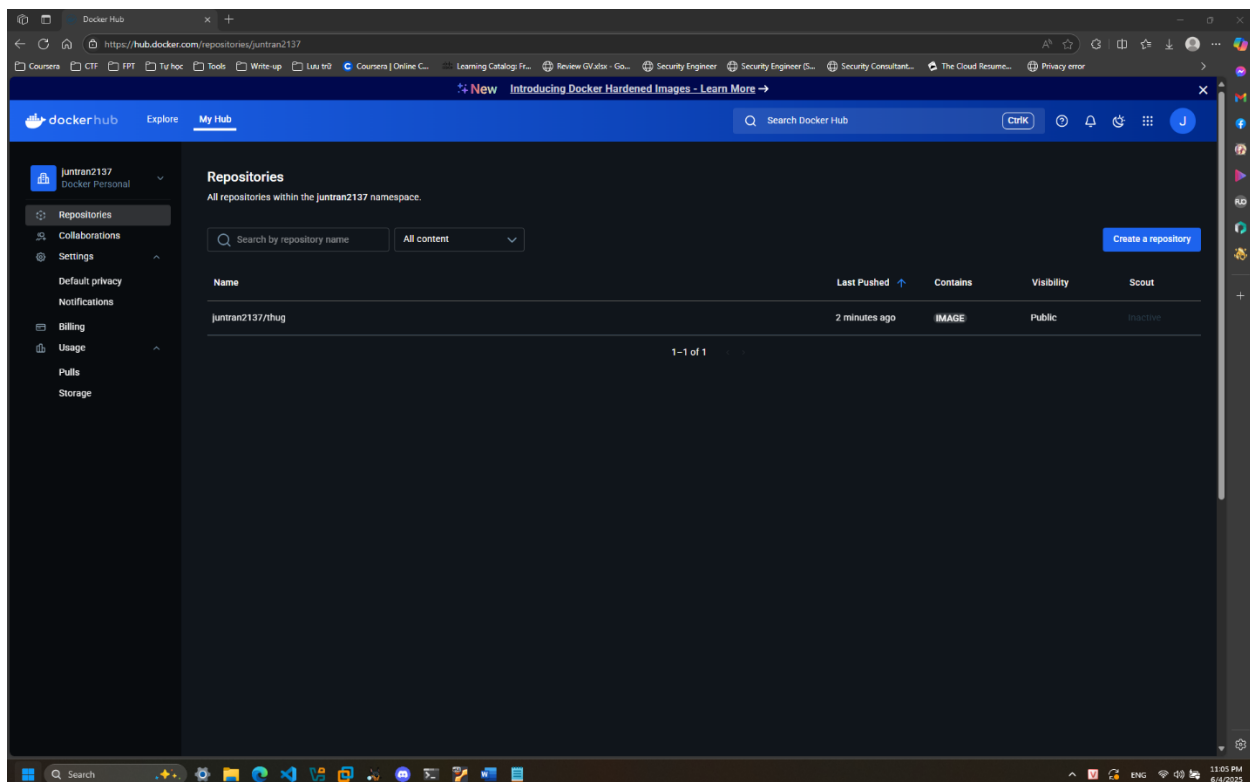
Use “docker images” and “docker rmi” to list and remove images:

```

dungtthe190680@dungtthe190680:~/thug$ sudo docker images
REPOSITORY    TAG       IMAGE ID       CREATED        SIZE
thug           latest    7f2d025b2dd3   5 hours ago    881MB
ubuntu         latest    bf16bdcff9c9   6 days ago     78.1MB
remnux/viper   latest    e463da33155f   3 years ago    1.28GB
ubuntu         18.04     13b66da87594   4 years ago    197MB
dungtthe190680@dungtthe190680:~/thug$ sudo docker rmi thug
Untagged: thug:latest
Deleted: sha256:7f2d025b2dd38b7dbed84891ce92a1d354af4a8dccc661e69357952fdda8db928
dungtthe190680@dungtthe190680:~/thug$

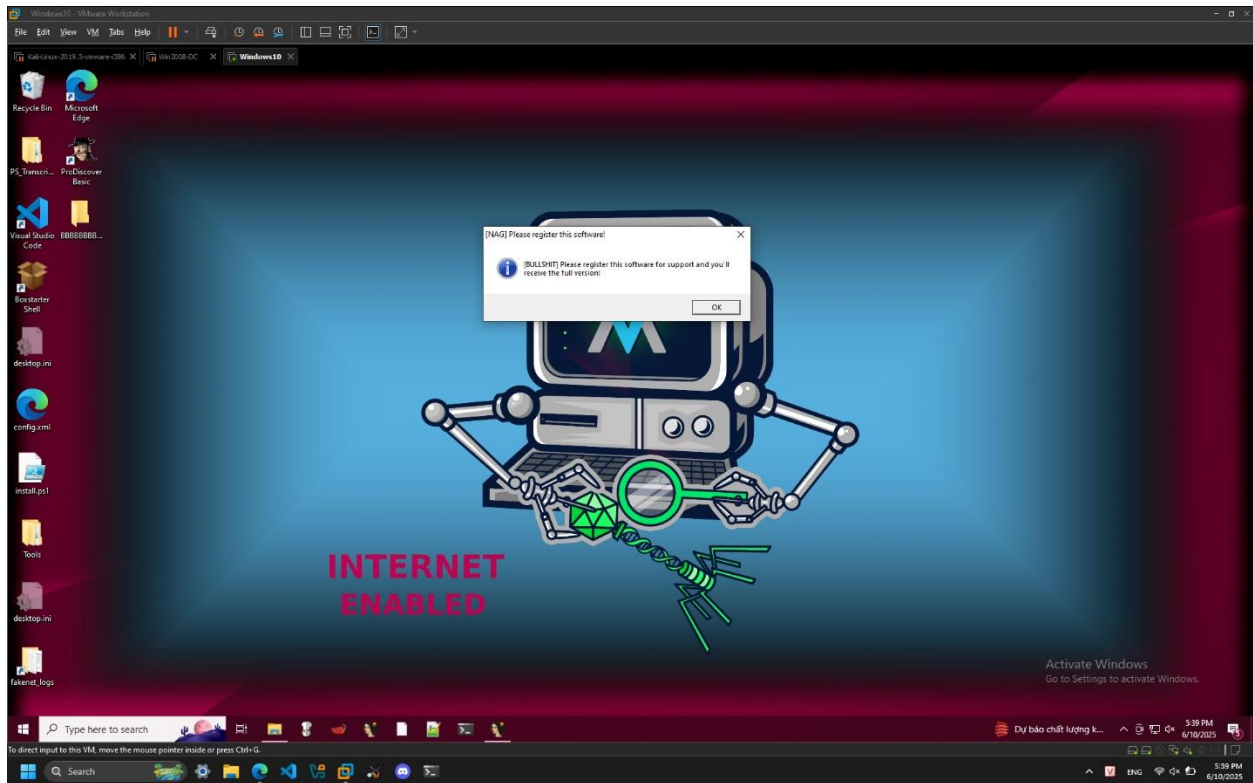
```

Share images via the public Docker Hub registry:

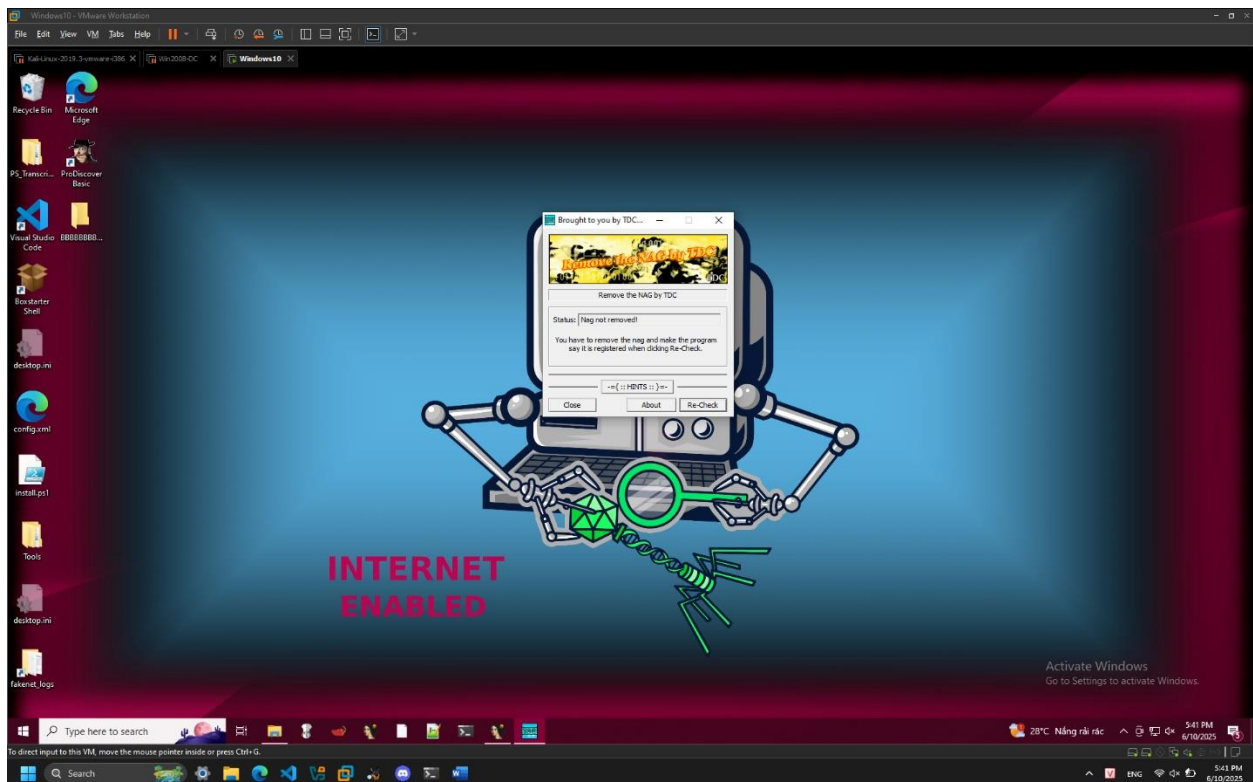


CrackMe #6

Đầu tiên em thử chạy chương trình và nhận được thông báo có từ khóa “BULLSHIT”:

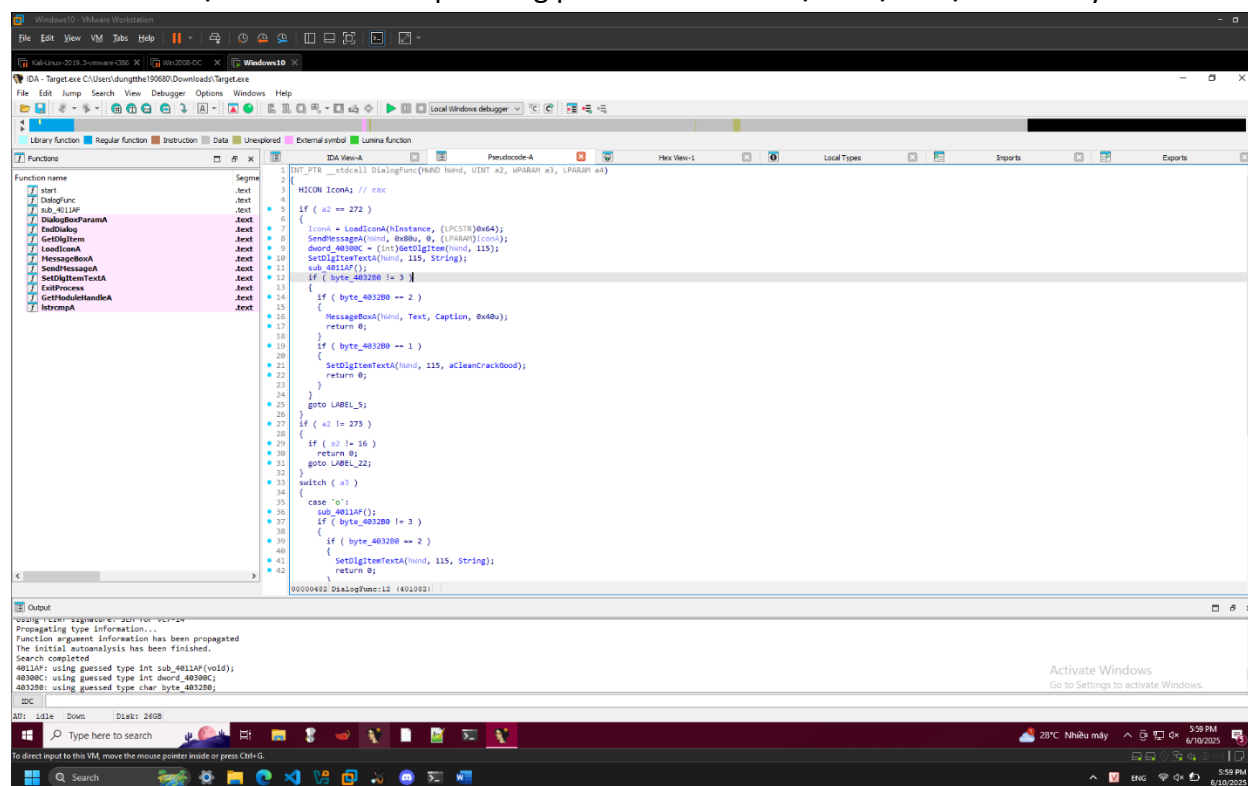


Sau khi tắt thông báo đầu tiên thì em nhận được thông báo khác là Nag chưa được loại bỏ:

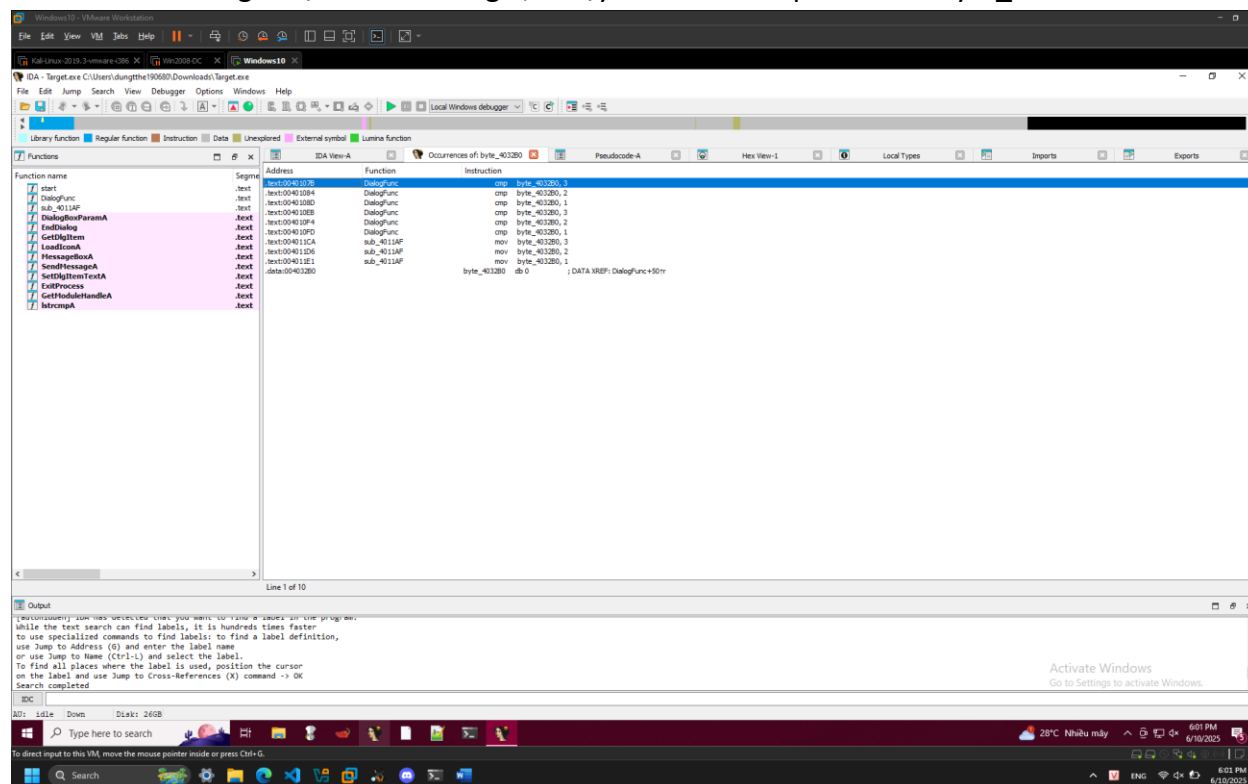


[illegible]

Em bôi đen đoạn code và decompile sang pseudocode thì nhận được đoạn code này:



Có thể thấy thông báo được hiển thị phụ thuộc vào giá trị của biến byte_4032B0, Nag được loại bỏ hoàn toàn khi giá trị của biến bằng 1, vì vậy em search tiếp từ khóa “byte_4032B0”:



The screenshot shows the Immunity Debugger interface with the assembly view of the DialogBoxParam function. The assembly code is disassembled from x86_64. The function starts with a push of the offset string 'Value1', followed by a call to lstrcpA. The assembly view shows the function's body, including a loop that calls EndDialog, LoadIconA, MessageBoxA, SendDlgItemTextA, and GetDlgItemTextA. The function ends with a ret instruction. The 'Previous line' window is open, showing the instruction 'jmp short loc_40110F' at address 0x1:0x0110F.