

Lab #4: Bảng đánh giá

Sử dụng Yara để scan file

Khóa học: ____Malware Analysis and Reverse Engineering (IAM302) ____

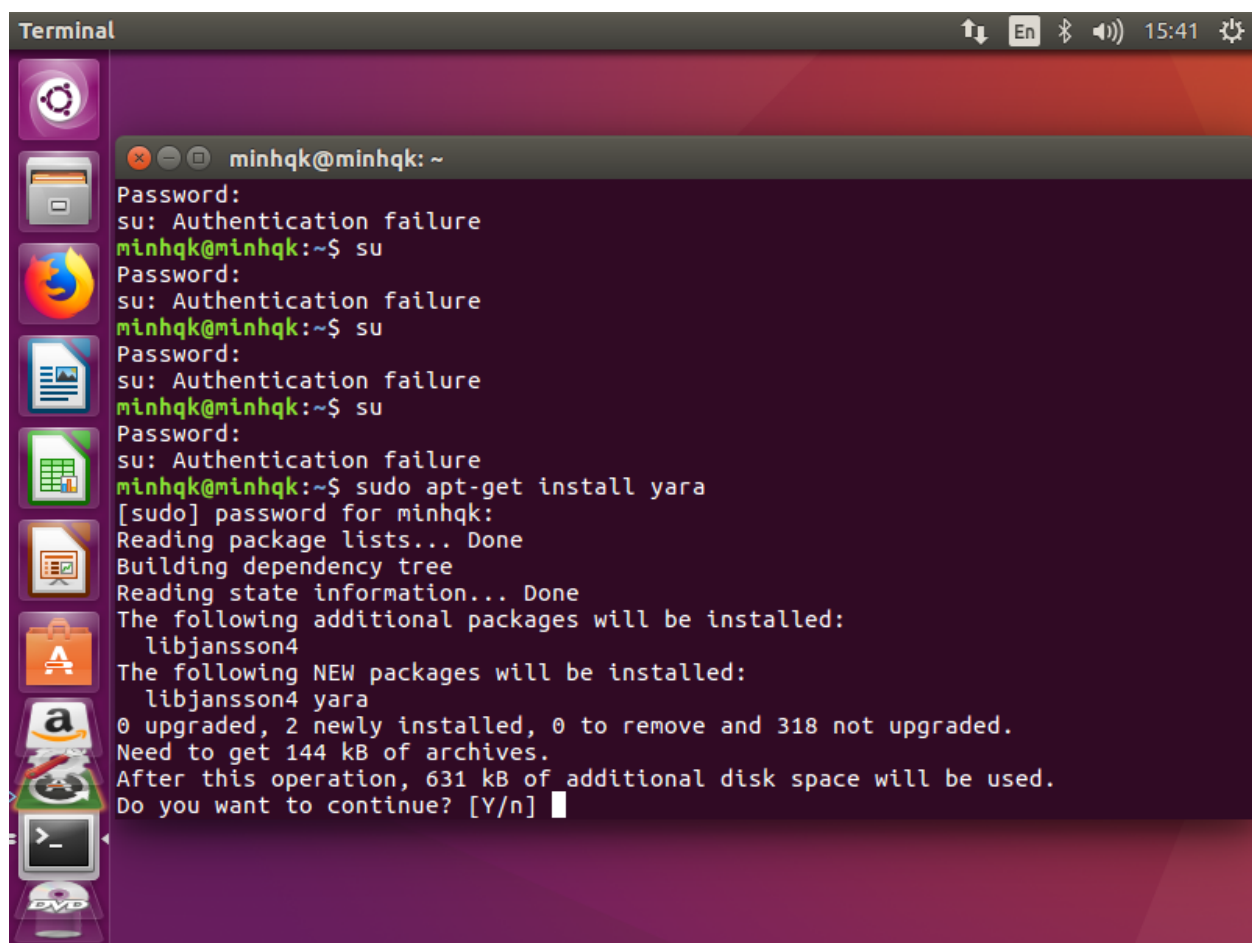
Họ và tên: ____

Giảng viên hướng dẫn: ____

Deadline: ____

Cài đặt Yara:

Cmd: sudo apt-get install yara

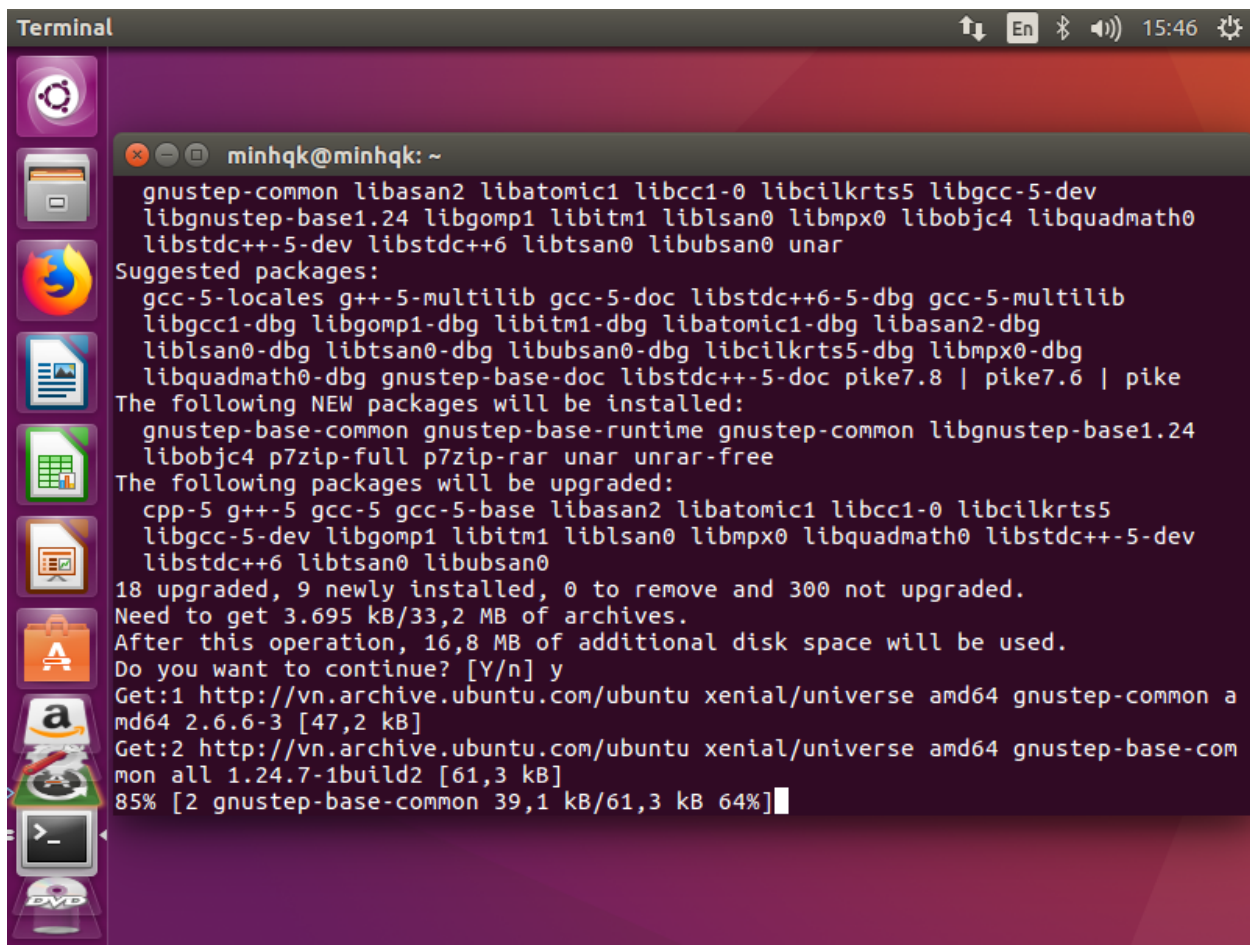


```
Terminal
minhmqk@minhmqk: ~
Password:
su: Authentication failure
minhmqk@minhmqk:~$ su
Password:
su: Authentication failure
minhmqk@minhmqk:~$ su
Password:
su: Authentication failure
minhmqk@minhmqk:~$ su
Password:
su: Authentication failure
minhmqk@minhmqk:~$ sudo apt-get install yara
[sudo] password for minhmqk:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  libjansson4
The following NEW packages will be installed:
  libjansson4 yara
0 upgraded, 2 newly installed, 0 to remove and 318 not upgraded.
Need to get 144 kB of archives.
After this operation, 631 kB of additional disk space will be used.
Do you want to continue? [Y/n]
```

```
Terminal
minhqk@minhqk: ~
The following NEW packages will be installed:
  libjansson4 yara
0 upgraded, 2 newly installed, 0 to remove and 318 not upgraded.
Need to get 144 kB of archives.
After this operation, 631 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://vn.archive.ubuntu.com/ubuntu xenial-updates/main amd64 libjansson4
amd64 2.7-3ubuntu0.1 [27,1 kB]
Get:2 http://vn.archive.ubuntu.com/ubuntu xenial/universe amd64 yara amd64 3.4.0
+dfsg-2build1 [117 kB]
Fetched 144 kB in 3s (37,9 kB/s)
Selecting previously unselected package libjansson4:amd64.
(Reading database ... 178796 files and directories currently installed.)
Preparing to unpack .../libjansson4_2.7-3ubuntu0.1_amd64.deb ...
Unpacking libjansson4:amd64 (2.7-3ubuntu0.1) ...
Selecting previously unselected package yara.
Preparing to unpack .../yara_3.4.0+dfsg-2build1_amd64.deb ...
Unpacking yara (3.4.0+dfsg-2build1) ...
Processing triggers for libc-bin (2.23-0ubuntu10) ...
Processing triggers for man-db (2.7.5-1) ...
Setting up libjansson4:amd64 (2.7-3ubuntu0.1) ...
Setting up yara (3.4.0+dfsg-2build1) ...
Processing triggers for libc-bin (2.23-0ubuntu10) ...
minhqk@minhqk:~$
```

Cài đặt p7zip-full:

Cmd: `sudo apt-get install p7zip-full p7zip-rar unrar-free`



The image shows a terminal window titled "Terminal" with a dark purple background. The user is logged in as "minhqk" at the prompt "minhqk@minhqk: ~". The terminal displays the output of a package manager command, likely 'dpkg-query -f='\${Package} \${Version} \${Architecture}\n'. It lists several installed packages including gnustep-common, libasan2, libatomic1, libgcc-5-dev, libgnustep-base1.24, libgomp1, libitm1, liblsan0, libmpx0, libobjc4, libquadmath0, libstdc++-5-dev, libstdc++6, libtsan0, libubsan0, and unrar. Below the list, it shows suggested packages, packages to be installed, and packages to be upgraded. It also displays disk space requirements and a progress bar for downloading gnustep-base-common.

```
Terminal
minhqk@minhqk: ~
gnustep-common libasan2 libatomic1 libgcc-5-dev libgnustep-base1.24 libgomp1 libitm1 liblsan0 libmpx0 libobjc4 libquadmath0 libstdc++-5-dev libstdc++6 libtsan0 libubsan0 unrar
Suggested packages:
gcc-5-locales g++-5-multilib gcc-5-doc libstdc++6-5-dbg gcc-5-multilib libgcc1-dbg libgomp1-dbg libitm1-dbg libatomic1-dbg libasan2-dbg liblsan0-dbg libtsan0-dbg libubsan0-dbg libquadmath0-dbg gnustep-base-doc libstdc++-5-doc pike7.8 | pike7.6 | pike
The following NEW packages will be installed:
gnustep-base-common gnustep-base-runtime gnustep-common libgnustep-base1.24 libobjc4 p7zip-full p7zip-rar unrar unrar-free
The following packages will be upgraded:
cpp-5 g++-5 gcc-5 gcc-5-base libasan2 libatomic1 libgcc-5-dev libgomp1 libitm1 liblsan0 libmpx0 libquadmath0 libstdc++-5-dev libstdc++6 libtsan0 libubsan0
18 upgraded, 9 newly installed, 0 to remove and 300 not upgraded.
Need to get 3.695 kB/33,2 MB of archives.
After this operation, 16,8 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://vn.archive.ubuntu.com/ubuntu xenial/universe amd64 gnustep-common a
md64 2.6.6-3 [47,2 kB]
Get:2 http://vn.archive.ubuntu.com/ubuntu xenial/universe amd64 gnustep-base-com
mon all 1.24.7-1build2 [61,3 kB]
85% [2 gnustep-base-common 39,1 kB/61,3 kB 64%]
```

Download package.01.ful.7z:

Link tải: <https://code.google.com/archive/p/clamsrch/downloads>

Download file clam to yara.py:

Link tải: https://github.com/mattulm/volgui/blob/master/tools/clamav_to_yara.py

Convert file clamav sang yara:

Cmd: `cd /home/minhqk/Desktop/` (Vào location chứa package vừa extract và là nơi chứa file clam_to_yara.py)

Cmd: `sudo python clamav_to_yara.py -f package/clamsrch.ndb -o clamsrch.yara`

```
Terminal
minhqk@minhqk: ~/Desktop

#####

Usage: clamav_to_yara.py [options]

clamav_to_yara.py: error: no such option: -r
minhqk@minhqk:~/Desktop$ sudo python clamav_to_yara.py -f package/clamsrch.
ndb -o clamsrch.yara

#####
      Malware Analyst's Cookbook - ClamAV to YARA Converter 0.0.1
#####

[+] Read 2291 lines from package/clamsrch.ndb
      found 0 - 20
      found 0 - 20
      found 0 - 20
      found 0 - 20
      found 0 - 20
      found 0 - 20
      found 0 - 20
      found 0 - 20

clamsrch.yara
```

Bắt đầu scan với yara:

Cmd: yara -r clamsrch.yara /home/minhqk/Desktop/Test


Terminal

minhqk@minhqk: ~/Desktop

```
minhqk@minhqk:~/Desktop$ yara -r clamsrch.yara /home/
clamsrch.yara(45): warning: $a0 is slowing down scanning
clamsrch.yara(185): warning: $a0 is slowing down scanning
clamsrch.yara(335): warning: $a0 is slowing down scanning
clamsrch.yara(455): warning: $a0 is slowing down scanning
clamsrch.yara(716): warning: $a0 is slowing down scanning
clamsrch.yara(766): warning: $a0 is slowing down scanning
clamsrch.yara(996): warning: $a0 is slowing down scanning
clamsrch.yara(1046): warning: $a0 is slowing down scanning
clamsrch.yara(1086): warning: $a0 is slowing down scanning
clamsrch.yara(1386): warning: $a0 is slowing down scanning
clamsrch.yara(1426): warning: $a0 is slowing down scanning
clamsrch.yara(1496): warning: $a0 is slowing down scanning
clamsrch.yara(1566): warning: $a0 is slowing down scanning
clamsrch.yara(1676): warning: $a0 is slowing down scanning
clamsrch.yara(1776): warning: $a0 is slowing down scanning
clamsrch.yara(1876): warning: $a0 is slowing down scanning
clamsrch.yara(1956): warning: $a0 is slowing down scanning (critical!)
clamsrch.yara(1986): warning: $a0 is slowing down scanning
clamsrch.yara(2327): warning: $a0 is slowing down scanning
clamsrch.yara(2377): warning: $a0 is slowing down scanning
clamsrch.yara(2457): warning: $a0 is slowing down scanning
clamsrch.yara(2567): warning: $a0 is slowing down scanning
clamsrch.yara(2647): warning: $a0 is slowing down scanning
```

clamsrch.yara

Tao yara rules:



*custome.yara (~/.Desktop) - gedit

Open ▾ Save

```
rule ConditionsExample {
  strings:
    $string1 = "hello"
    $string2 = "hello"
    $string3 = "hello"

  condition:
    any of them
}

global rule GlobalRuleExample {
  condition:
    filesize < 2MB
}

rule NumberStringsExample {
  strings:
    $hello = "hello"

  condition:
    #hello >= 5
}


rule CheckImage {
  strings:
    $a = {89 50 4e 47 0d 0a 1a 0a}

  condition:
    any of them
}
```

Plain Text ▾ Tab Width: 8 ▾ Ln 5, Col 27 ▾ INS

Test yara rules:

```
minhqb@minhqb: ~/Desktop
43 cd /home/desktop/
44 cd /home/minhqb/desktop/
45 cd /home/minhqb/Desktop/
46 sudo python clamav_to_yara.py -f package/clamsrch.ndb -o clamsrch.ya
ra -r clamsrch.yara /home/
47 sudo python clamav_to_yara.py -f package/clamsrch.ndb -o clamsrch.ya
ra
48 yara -r clamsrch.yara /home/
49 yara -r clamsrch.yara /home/minhqb/Desktop/Test/
50 history
minhqb@minhqb:~/Desktop$ rule over_500kb {condition:filesize > 500Kb}
rule: command not found
minhqb@minhqb:~/Desktop$ yara -r custome.yara /home/minhqb/Desktop/Test/
GlobalRuleExample /home/minhqb/Desktop/Test//file-3.png
CheckImage /home/minhqb/Desktop/Test//file-3.png
GlobalRuleExample /home/minhqb/Desktop/Test//Clam_HelloWorld.ndb
ConditionsExample /home/minhqb/Desktop/Test//test2.txt
GlobalRuleExample /home/minhqb/Desktop/Test//test2.txt
NumberStringsExample /home/minhqb/Desktop/Test//test2.txt
GlobalRuleExample /home/minhqb/Desktop/Test//eicar_com.zip
GlobalRuleExample /home/minhqb/Desktop/Test//eicar.com.txt
ConditionsExample /home/minhqb/Desktop/Test//test.txt
GlobalRuleExample /home/minhqb/Desktop/Test//test.txt
minhqb@minhqb:~/Desktop$
```



clamsrch.yara