Lab 4-Working with Yara

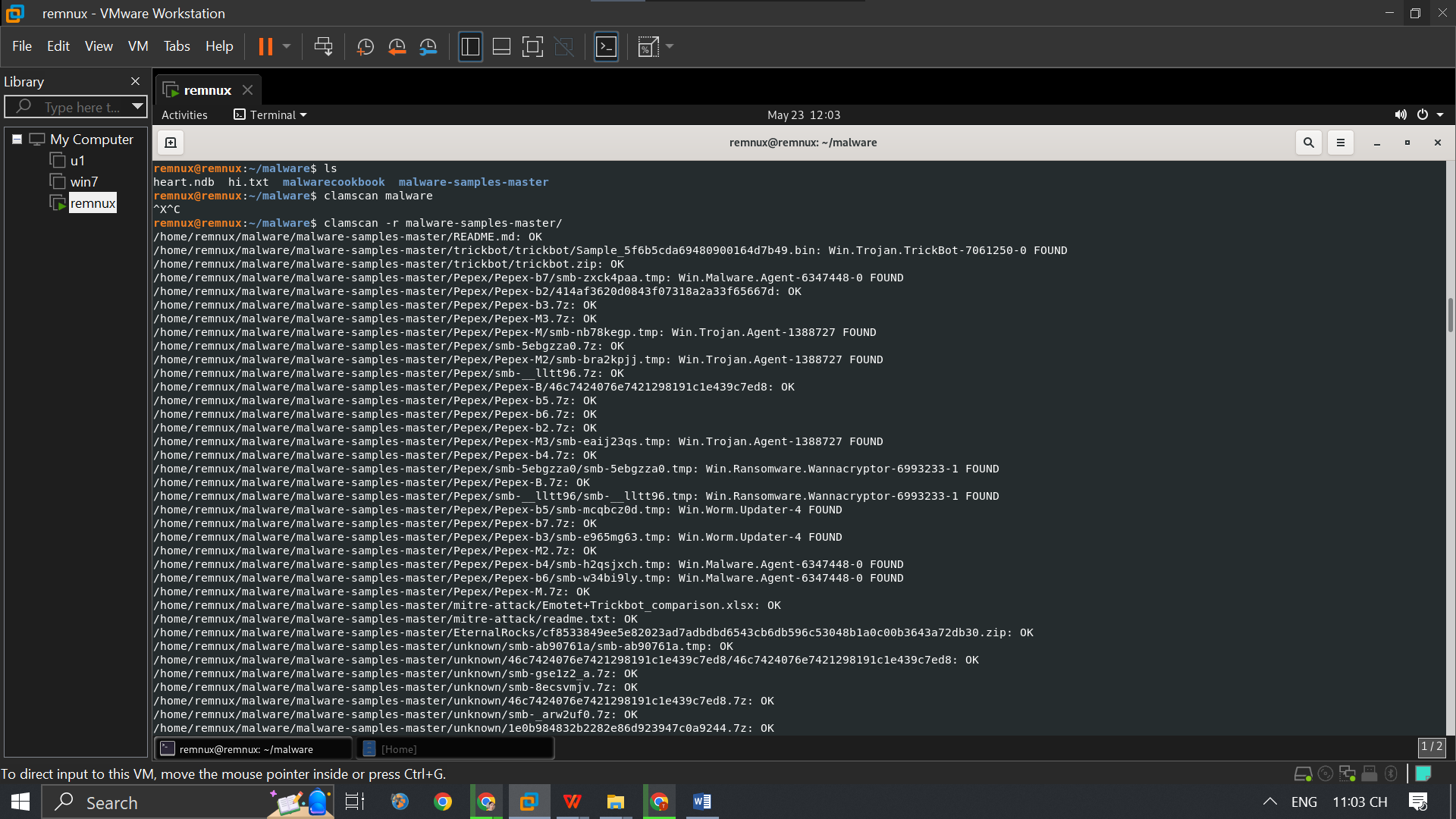
Sinh viên chụp ảnh quá trình thực hiện các yêu cầu sau:

**ClamAV to Yara signature**

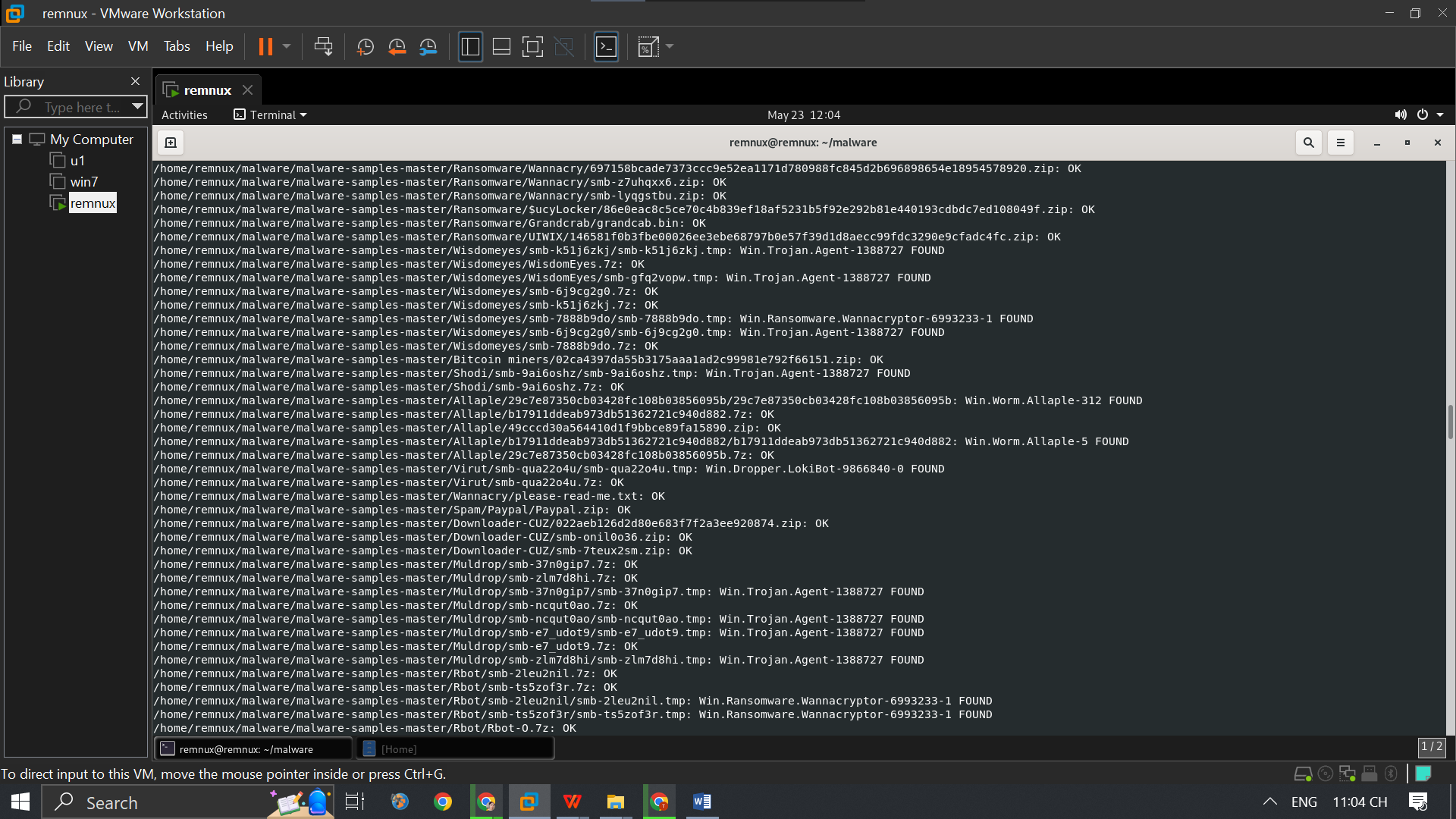
* Chọn 1 trong số các file malware bất kỳ trong folder malware-samples-master, chọn 1 từ khoá trong signature name và dùng clamav\_to\_yara.py để chuyển đổi sang Yara signature tất cả các ClamAV signature có từ khoá này

+ Đầu tiên ta dùng *clamscan* để scan toàn bộ các con malware có trong *malware-samples-master*

Command : *clamscan -r malware-samples-master*



+Trong các con malware có sẵn trong file *malware-samples-master* thì chúng ta chọn đi 1 con để làm việc. Thì ở đây chọn con Win.Worm.Allaple-5

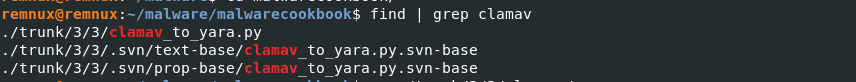


lun

+Tool mà ta cần sử dụng ở đây có tên là *clamav\_to\_yara.py*, tool này có sẵn trong folder *malwarecookbook* nên ta đến thư mục malwarecookbook .

Command : *find | grep clamav*

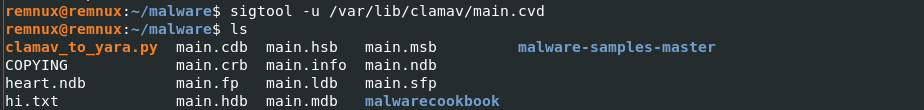
Thì ta thấy được đường dẫn của tool clamav\_to\_yara.py : ./trunk/3/3/clamav\_to\_yara.py



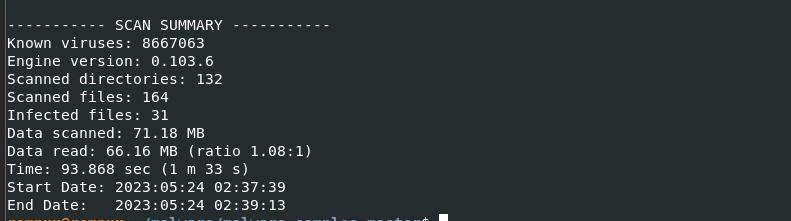
+Dùng cp để copy file đến thư mũ mà ta thuận tiện để sử dụng : */home/remnux/malware*.

Command: *cp ./trunk/3/3/clamav\_to\_yara.py /home/remnux/malware/*



+Dùng lệnh *sigtool –u /var/lib/clamav/main.cvd* để tạo ra file *main.ndb*

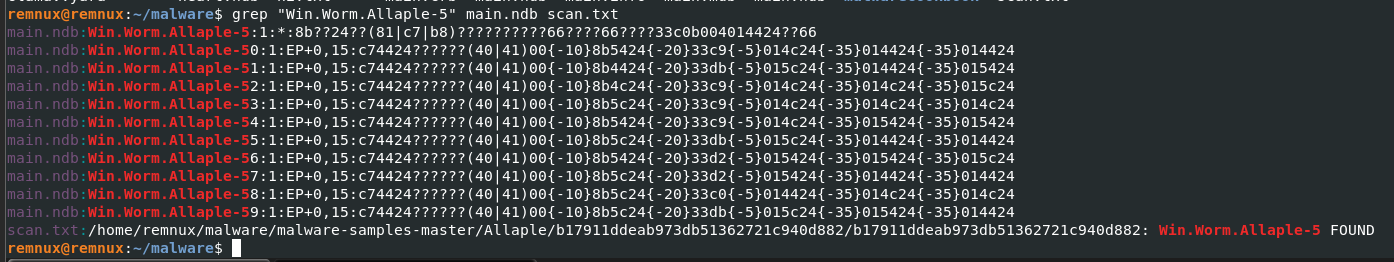
+Ở đây file main.ndb có nhiều malware nhưng trong folder *malware-samples-master* chỉ có 31 còn malware như hình dưới. Vì vậy sẽ rất có để lọc ra 1 con malware xuất hiện ở cả *main.ndb* và folder *malware-samples-master*



+Nên ta scan folder *malware-samples-master* và tạo ra 1 file để tiện hơn: *scan.txt*



+Giờ thì chúng ta tìm đc con malware có ở cả hai file "Win.Worm.Allaple-5"



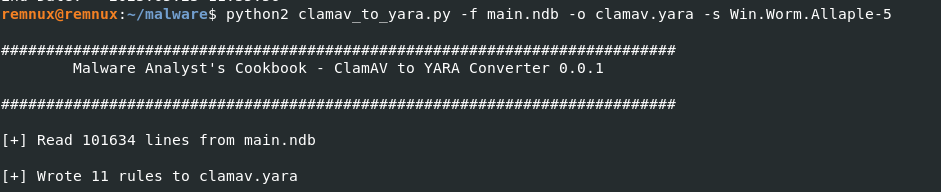
* Dùng file Yara signature mới quét lại file đã chọn ở trên:

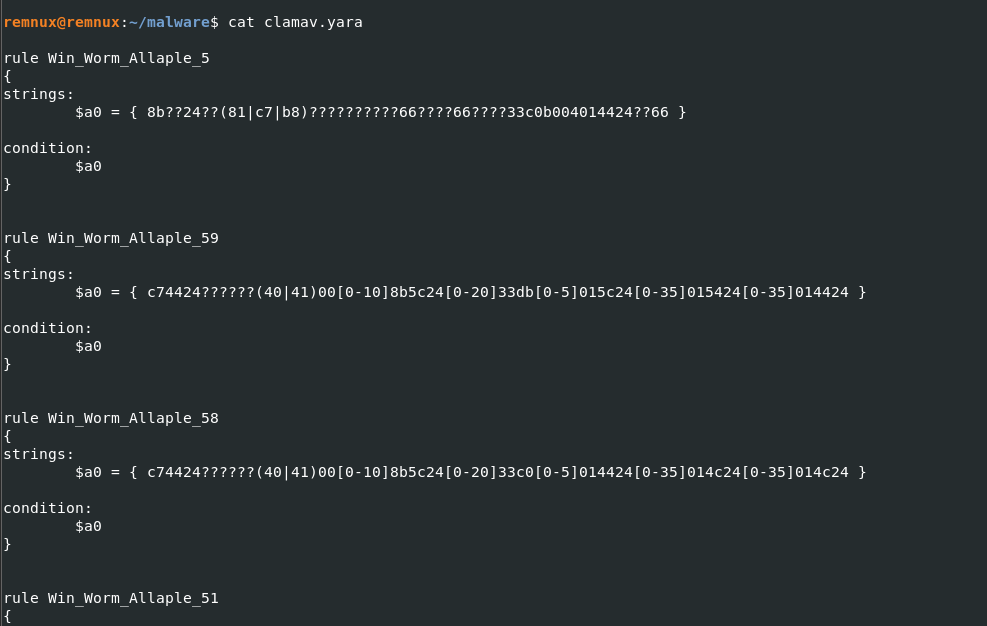
+ -f : lấy database của 1 file , như ở đây đó là file main.ndb

+ -o : từ database trên xuất ra output có đuôi là .yara

+ -s : là signure để tìm ra con malware mình cần

+ Sau khi quét tất cả 101634 malware thì ta nhận được 11 rules





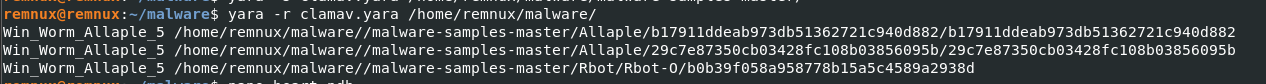
+Tiếp đến mình quét lại folder *malware*

+Thì ở file *scan.txt* có 1 con malware Win.Worm.Allaple-5



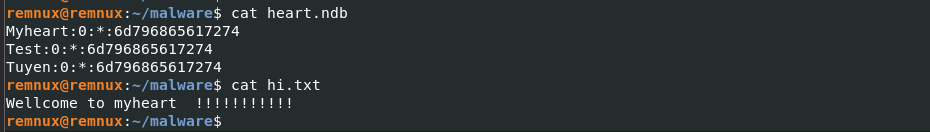
+Dùng yara để quét lại để xem chúng ta có thành công chưa nha.

Command: *yara –r clamav.yara /home/remnux/malware/*



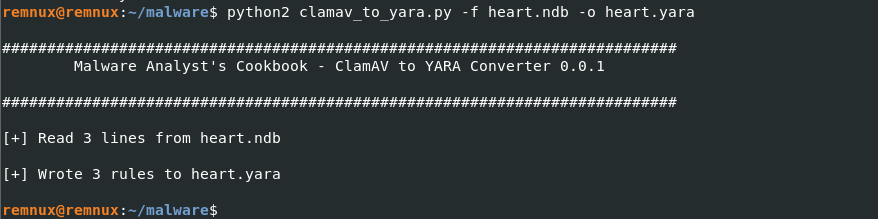
* Dùng *clamav\_to\_yara.py* để chuyển đổi signature tự tạo trong Lab 3 sang Yara signature và tiến hành quét lại các file *malware* tự tạo bằng các yara signature mới này

+Lab 3 đã tạo sẵn 2 file heart.ndb vad hi.txt

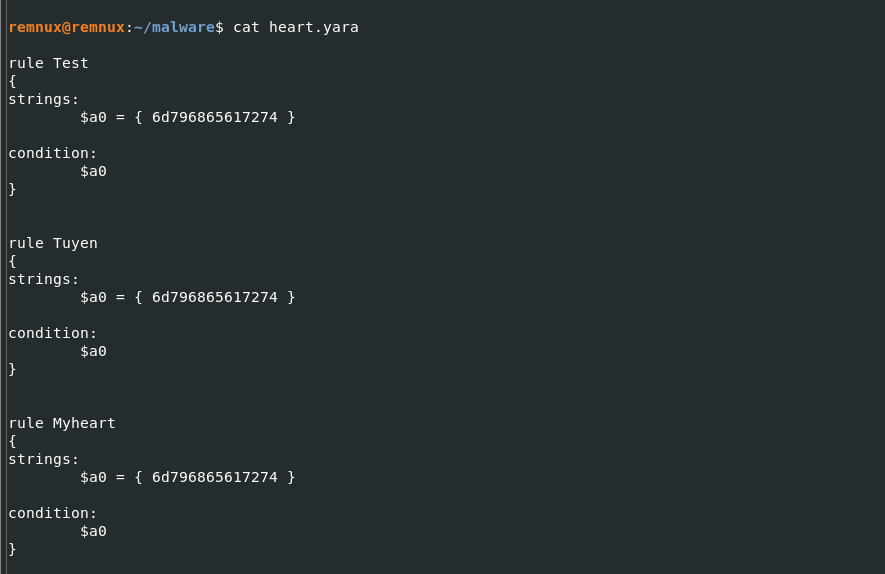


+Tiếp theo ta tạo ra file yara

Command: *python2 clamav\_to\_yara.py –f heart.ndb –o hi.txt*

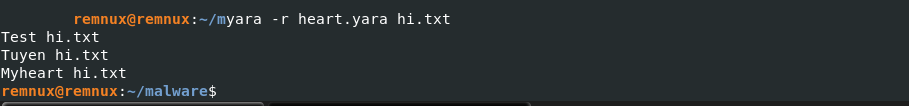


+Kiểm tra file yara vừa tạo xem có gì.



+Dùng yara để quét:

Command: *yara –r heart.yara hi.txt*



Detect Packer

* Tải file peid\_to\_yara.py và userdb.txt đính kèm trong lab. File .py là công cụ để chuyển các PEiD signature sang Yara Signature. Dùng lệnh chuyển file trên và lưu thành packer.yara

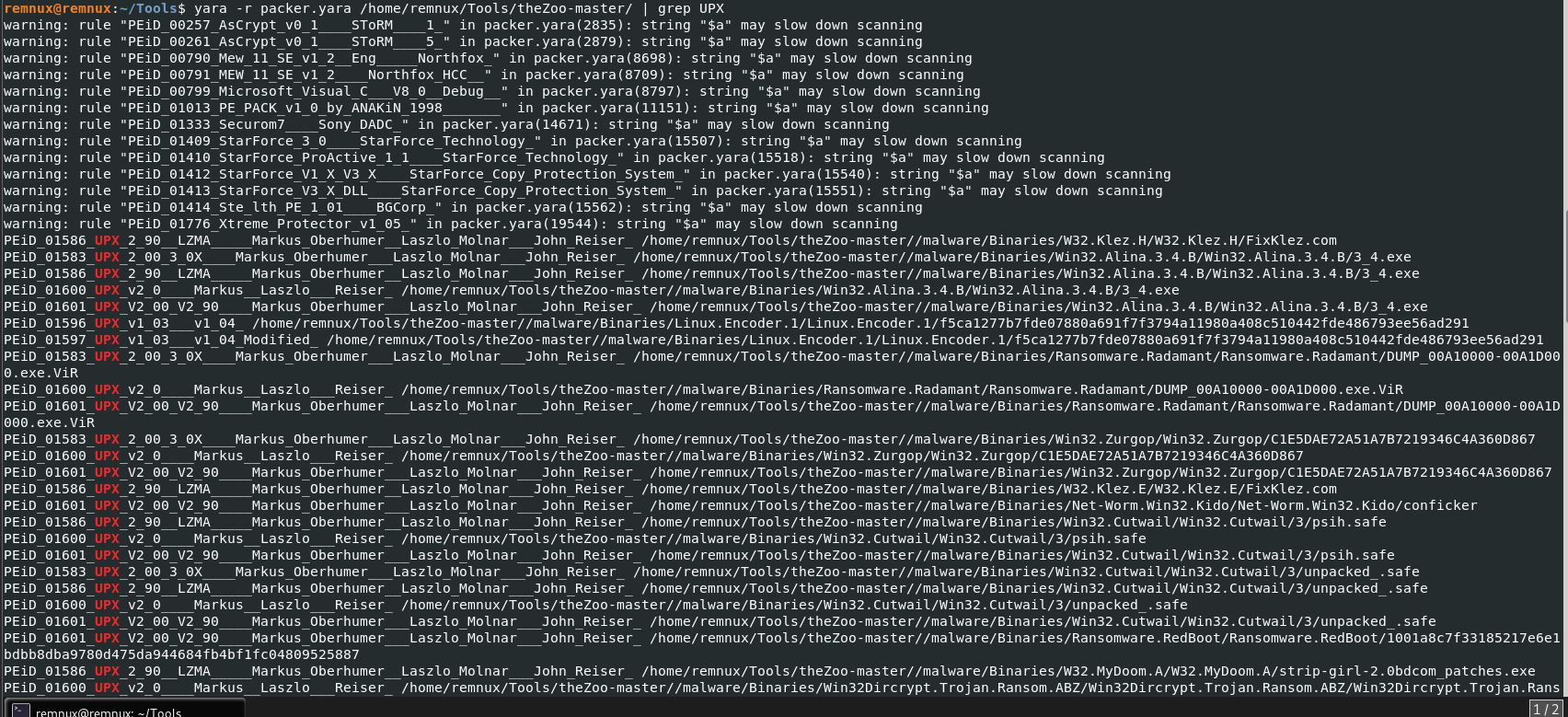
+Tải hêtd mọi thứ vào lưu vào folder Tools

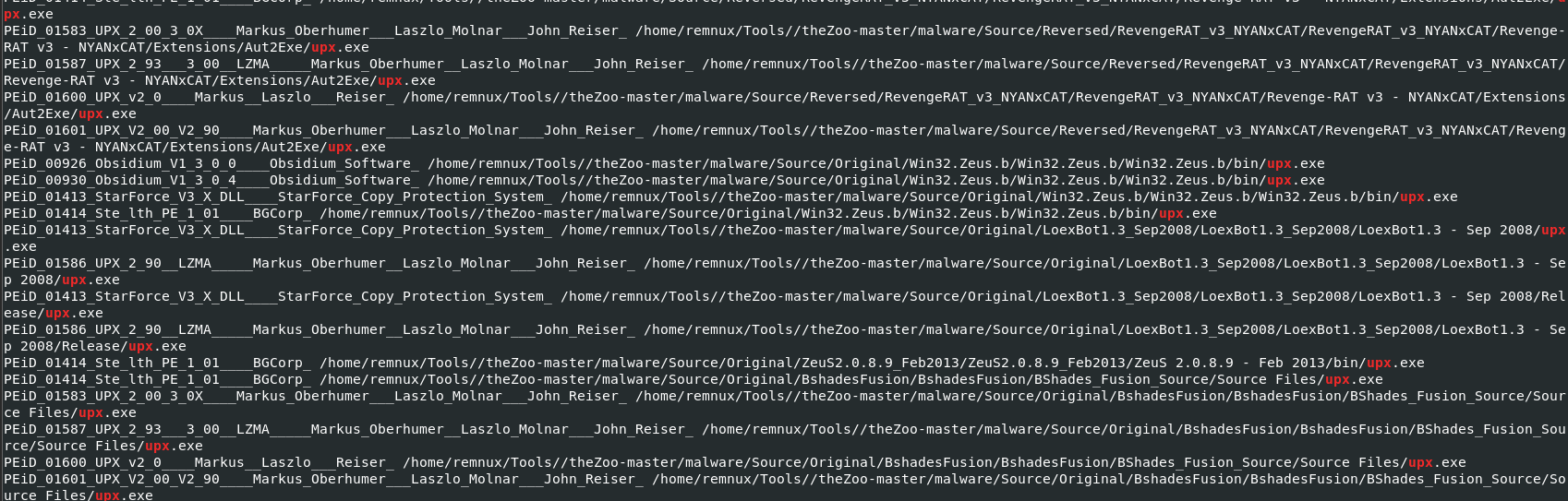
+Dùng tool *peid\_to\_yara.py* để chuyển file *userdb.txt* thành *packer.yara*



* Dùng file *packer.yara* ở trên để quét toàn bộ folder Tools

+Dùng yara để quét và dùng *grep upx* để kiểm tra xem có bao nhiê upx

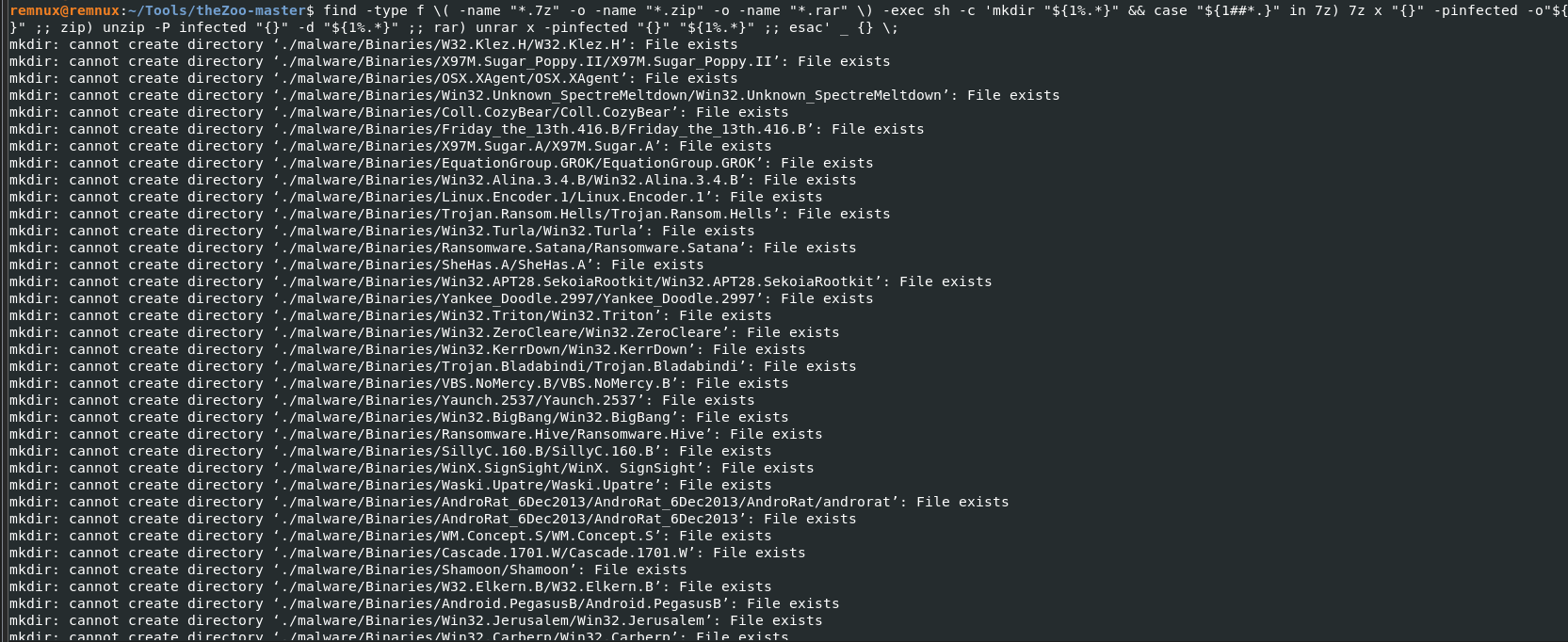




* Kiểm tra xem có những file malware nào được đóng gói bằng UPX hay không, nếu không thì sinh viên tự tìm 1 file được đóng gói bằng UPX rồi quét lại (có thể cập nhật và dùng thêm các yara signature khác trên mạng)

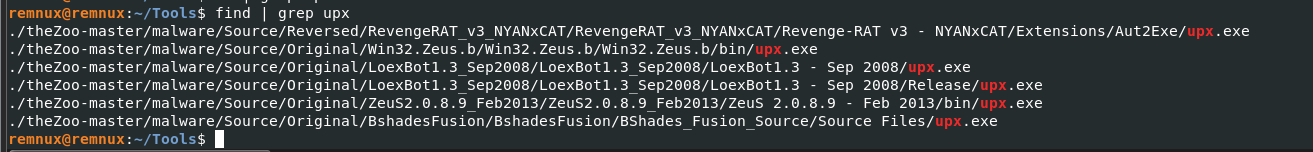
+Ta dùng command để giải nén file *theZoo-master*:

find -type f \( -name "\*.7z" -o -name "\*.zip" -o -name "\*.rar" \) -exec sh -c 'mkdir "${1%.\*}" && case "${1##\*.}" in 7z) 7z x "{}" -pinfected -o"${1%.\*}" ;; zip) unzip -P infected "{}" -d "${1%.\*}" ;; rar) unrar x -pinfected "{}" "${1%.\*}" ;; esac' \_ {} \;



+Dùng grep để tìm upx

Command: *find | grep upx*

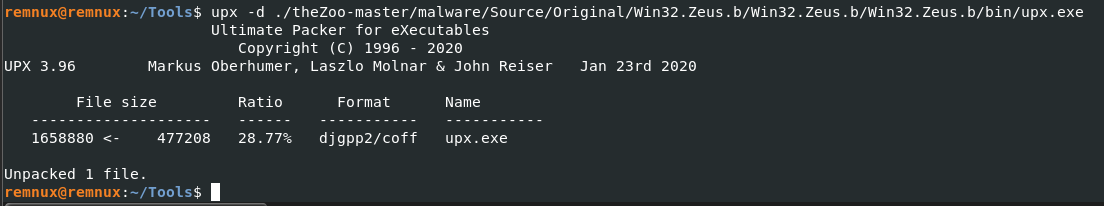


+Chọn file thứ 2 đển unpack

* Dùng UPX để unpack file malware trên, yêu cầu output phải thể hiện dung lượng ban đầu, tỉ lệ nén và file đã unpack.

+Ta dùng upx –d để unpack

Command: upx –d ./theZoomaster/malware/Source/Original/Win32.Zeus.b/Win32.Zeus.b/Win32.Zeus.b/bin/upx.exe



*THE END*