

**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG**  
**KHOA CÔNG NGHỆ THÔNG TIN 2**  
**NGÀNH AN TOÀN THÔNG TIN**



**BÀI BÁO CÁO**

**SNORT**  
**PHÁT HIỆN VÀ NGĂN CHẶN RCE ATTACK**

**Môn:** An toàn mạng  
**Giảng viên hướng dẫn:** ThS. Trần Thị Dung

**Nhóm sinh viên thực hiện:** Nhóm 9

Quách Trường Giang	N18DCAT018
Võ Ngọc Minh	N18DCAT050
Võ Thế Anh	N18DCAT005
Hồ Tiểu Long	N18DCAT042
Phạm Ngọc Hưng	N18DCAT032

*Thành phố Hồ Chí Minh – Năm 2021*

## MỤC LỤC

I. TỔNG QUAN .....	3
1. Giới thiệu về Snort.....	3
2. Kiến trúc của Snort .....	3
3. Bộ rule của Snort .....	4
a. Giới thiệu.....	4
b. Cấu trúc rule của Snort.....	4
4. RCE.....	7
II. THỰC HIỆN .....	8
1. Mô hình và bảng địa chỉ mức cơ bản .....	8
2. Mô hình và bảng địa chỉ mức nâng cao.....	8
3. Cài đặt.....	8
c. Bước 1. Cài đặt các gói phần mềm hỗ trợ.....	8
d. Bước 2. Cài đặt Snort .....	9
e. Bước 3. Cấu hình Snort chạy ở chế độ phát hiện xâm nhập mạng .....	10
f. Bước 4. Kiểm tra sự hoạt động của Snort .....	14
4. Cấu hình.....	14
a. Cấu hình thiết lập phát hiện tấn công mức cơ bản (Low).....	14
b. Cấu hình ngăn chặn RCE attacker mức Medium.....	18
III. KẾT QUẢ NHẬN XÉT .....	24
1. Kết quả:.....	24
2. Nhận xét:.....	24
IV. THAM KHẢO .....	24

# I. TỔNG QUAN

## 1. Giới thiệu về Snort

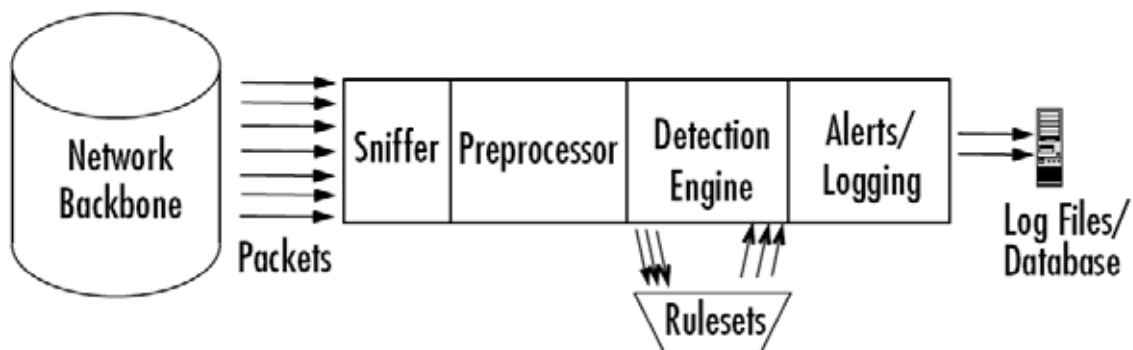
**Snort** là một hệ thống phát hiện và ngăn chặn xâm nhập mạng miễn phí và nguồn mở. Nó sử dụng ngôn ngữ dựa trên quy tắc, thực hiện phân tích giao thức, tìm kiếm kết hợp nội dung và có thể được sử dụng để phát hiện nhiều loại tấn công và thăm dò khác nhau. Snort cố gắng phát hiện các hoạt động độc hại, tấn công từ chối dịch vụ và quét cổng bằng cách giám sát lưu lượng mạng.

## 2. Kiến trúc của Snort

Snort được chia thành năm thành phần chính, với mỗi phần có một chức năng riêng. Các phần đó là:

- Module giải mã gói tin (Packet Decoder)
- Module tiền xử lý (Preprocessor)
- Module phát hiện (Detection Engine)
- Module log và cảnh báo (Logging and Alerting System)
- Module kết xuất thông tin (Output Modules)

Kiến trúc của Snort được mô tả trong hình sau:



*Hình 1: Mô hình kiến trúc hệ thống Snort*

Khi Snort hoạt động nó sẽ thực hiện việc lắng nghe và thu bắt tất cả các gói tin nào di chuyển qua nó. Các gói tin sau khi bị bắt được đưa vào Module Giải mã gói tin. Tiếp theo gói tin sẽ được đưa vào module Tiền xử lý, rồi module Phát hiện. Tại đây tùy theo việc có phát hiện được xâm nhập hay không mà gói tin có thể được bỏ qua để lưu thông tiếp hoặc được đưa vào module Log và cảnh báo để xử lý. Khi các cảnh báo được xác định module Kết xuất thông tin sẽ thực hiện việc đưa cảnh báo ra theo đúng định dạng mong muốn.

Có 3 chế độ: Packet Sniffer, Packet Logger, NIPDS (Network Intrusion and Prevention Detection System).

### 3. Bộ rule của Snort

#### a. Giới thiệu

Một rule có thể được sử dụng để tạo nên một thông điệp cảnh báo, ghi log hay có thể bỏ qua một gói tin.

#### b. Cấu trúc rule của Snort

Rule Header	Rule Option
-------------	-------------

**Hình 2: Cấu trúc rule của Snort**

Tất cả các rule của Snort về logic đều gồm 2 phần: Phần Header và phần Option.

- Phần Header chứa thông tin về hành động mà rule đó sẽ thực hiện khi phát hiện ra có xâm nhập nằm trong gói tin và nó cũng chứa các tiêu chuẩn để áp dụng rule với gói tin đó.

- Phần Option chứa một thông điệp cảnh báo và các thông tin về các phần của gói tin dùng để tạo nên cảnh báo. Phần Option chứa các tiêu chuẩn phụ thêm để đối sánh rule với gói tin. Một rule có thể phát hiện được một hay nhiều hoạt động thăm dò hay tấn công. Các rule thông minh có khả năng áp dụng cho nhiều dấu hiệu xâm nhập.

- **Phần tiêu đề (Header)**

Cấu trúc chung của phần Header của một rule Snort:

Action	Protocol	Address	Port	Direction	Address	Port
--------	----------	---------	------	-----------	---------	------

**Hình 3: Rule Header của Snort**

❖ **Hành động của rule(Rule Action)**

- Pass: Hành động này hướng dẫn Snort bỏ qua gói tin này
- Log: Hành động này dùng để log gói tin. Có thể log vào file hay vào cơ sở dữ liệu tùy thuộc vào nhu cầu của mình.
- Alert: Gửi một thông điệp cảnh báo khi dấu hiệu xâm nhập được phát hiện.
- Activate: sử dụng để tạo ra một cảnh báo và kích hoạt một rule khác kiểm tra thêm các điều kiện của gói tin.
- Dynamic: chỉ ra đây là rule được gọi bởi các rule khác có hành động là Activate.

❖ **Protocols**

Là phần thứ hai của một rule có chức năng chỉ ra loại gói tin mà rule sẽ được áp dụng.

#### ❖ *Address*

Có hai phần địa chỉ trong một rule của Snort. Các địa chỉ này được dùng để kiểm tra nguồn sinh ra và đích đến của gói tin. Địa chỉ có thể là địa chỉ của một IP đơn hoặc là địa chỉ của một mạng. Ta có thể dùng từ any để áp dụng rule cho tất cả các địa chỉ.

Trong hai địa chỉ của một rule Snort thì có một địa chỉ là địa chỉ nguồn và địa chỉ còn lại là địa chỉ đích. Việc xác định đâu là địa chỉ nguồn, đâu là địa chỉ đích thì phụ thuộc vào phần hướng (direction).

#### ❖ *Ngăn chặn địa chỉ hay loại trừ địa chỉ*

Snort cung cấp cho ta kỹ thuật để loại trừ địa chỉ bằng cách sử dụng dấu phủ định (dấu !). Dấu phủ định này đứng trước địa chỉ sẽ chỉ cho Snort không kiểm tra các gói tin đến từ hay đi tới địa chỉ đó.

#### ❖ *Danh sách địa chỉ*

Ta có thể định rõ ra danh sách các địa chỉ trong một rule của Snort.

### ***Cổng (Port Number)***

Số hiệu cổng dùng để áp dụng rule cho các gói tin đến từ hoặc đi đến một cổng hay một phạm vi cổng cụ thể nào đó.

❖ ***Dãy cổng hay phạm vi cổng:***

Ta có thể áp dụng rule cho dãy các cổng thay vì chỉ cho một cổng nào đó. Cổng bắt đầu và cổng kết thúc phân cách nhau bởi dấu hai chấm “:”.

## ***Hướng – Direction***

Chỉ ra đâu là nguồn đâu là đích, có thể là -> hay <- hoặc <>. Trường hợp <> là khi ta muốn kiểm tra cả Client và Server.

- **Các tùy chọn**

Phần Rule Option nằm ngay sau phần Rule Header và được bao bọc trong dấu ngoặc đơn. Nếu có nhiều option thì các option sẽ được phân cách với nhau bằng dấu chấm phẩy ”,”. Nếu nhiều option được sử dụng thì các option này phải đồng thời được thỏa mãn tức là theo logic các option này liên kết với nhau bằng AND.

- ❖ ***Từ khoá ack***

Trong header TCP có chứa trường Acknowledgement Number với độ dài 32 bit. Trường này có ý nghĩa là chỉ ra số thứ tự tiếp theo gói tin TCP của bên gửi đang được chờ để nhận. Trường này chỉ có ý nghĩa khi mà cờ ACK được thiết lập.

- ❖ ***Từ khoá classtype***

Các rule có thể được phân loại và gán cho một số chỉ độ ưu tiên nào đó để nhóm và phân biệt chúng với nhau.

- ❖ ***Từ khoá content***

Một đặc tính quan trọng của Snort là nó có khả năng tìm một mẫu dữ liệu bên trong một gói tin.

- ❖ ***Từ khoá dsize***

Dùng để đối sánh theo chiều dài của phần dữ liệu.

- ❖ ***Từ khoá flags***

Từ khoá này được dùng để phát hiện xem những bit cờ flag nào được bật (thiết lập) trong phần TCP header của gói tin.

- ❖ ***Từ khoá fragbits***

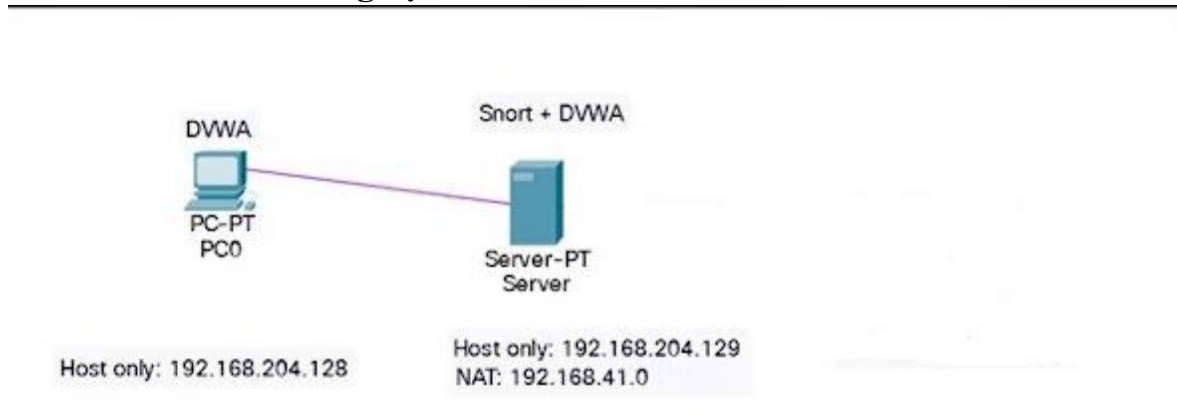
Phần IP header của gói tin chứa 3 bit dùng để chống phân mảnh và tổng hợp các gói tin IP.

## **4. RCE**

RCE là một kiểu tấn công trong đó kẻ tấn công có khả năng chạy các lệnh hoặc mã tùy ý trên máy mục tiêu. Lỗ hổng này cho phép những kẻ tấn công điều hành mã độc để chiếm quyền kiểm soát các thiết bị bị ảnh hưởng. Kiểu tấn công này hầu như luôn được thực hiện bởi một tập lệnh tự động và thường nhằm cung cấp quyền truy cập quản trị cho những kẻ tấn công. Khi hệ thống bị xâm nhập, những kẻ tấn công có thể truy cập bất kỳ thông tin nào trên mạng bị xâm phạm.

## II. THỰC HIỆN

### 1. Mô hình và bảng địa chỉ mức cơ bản

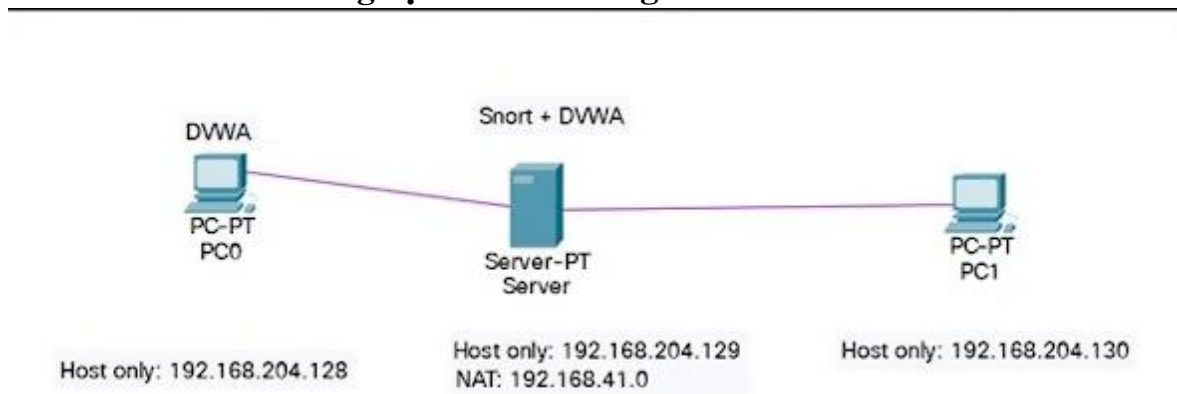


*Hình 4: Mô hình cài đặt mức cơ bản*

Kali + Snort + DVWA (victim)	192.168.204.129
Windows server 2012 (attacker)	192.168.204.128

*Bảng 1: Bảng địa chỉ mức cơ bản*

### 2. Mô hình và bảng địa chỉ mức nâng cao



*Hình 5: Mô hình cài đặt mức nâng cao*

Kali + Snort	192.168.204.129
Windows server 2012 + DVWA (victim)	192.168.204.128
Windows 7 (Attacker)	192.168.204.130

*Bảng 2: Bảng địa chỉ mức nâng cao*

### 3. Cài đặt

Cấu hình giao diện mạng của máy ảo Kali Linux sao cho máy có thể kết nối được Internet (chuyển card mạng sang chế độ NAT hoặc Bridged).

#### c. Bước 1. Cài đặt các gói phần mềm hỗ trợ

Snort có bốn phần mềm hỗ trợ yêu cầu phải cài đặt trước:



- pcap (libpcap-dev)
- PCRE (libpcre3-dev)
- Libdnet (libdumbnet-dev)
- DAQ Khởi động máy ảo Kali Linux, mở cửa sổ dòng lệnh bắt đầu cài đặt.

```
[root@kali:~$]sudo apt-get install -y build-essential
[root@kali:~$]sudo apt-get install -y libpcap-dev libpcre3-dev
libdumbnet-dev
[root@kali:~$]sudo apt-get install -y bison flex
```

Tạo thư mục chứa mã nguồn Snort và các phần mềm liên quan:

```
[root@kali:~$]mkdir ~/snort_src
[root@kali:~$]cd ~/snort_src
[root@kali:~$]sudo wget https://www.snort.org/downloads/snort/daq-2.0.6.tar.gz
[root@kali:~$]sudo tar -xvzf daq-2.0.6.tar.gz
[root@kali:~$]cd daq-2.0.6
[root@kali:~$]sudo ./configure
[root@kali:~$]sudo make
[root@kali:~$]sudo make install
[root@kali:~$]sudo apt-get install -y zlib1g-dev liblzma-dev openssl
libssl-dev
```

#### **d. Bước 2. Cài đặt Snort**

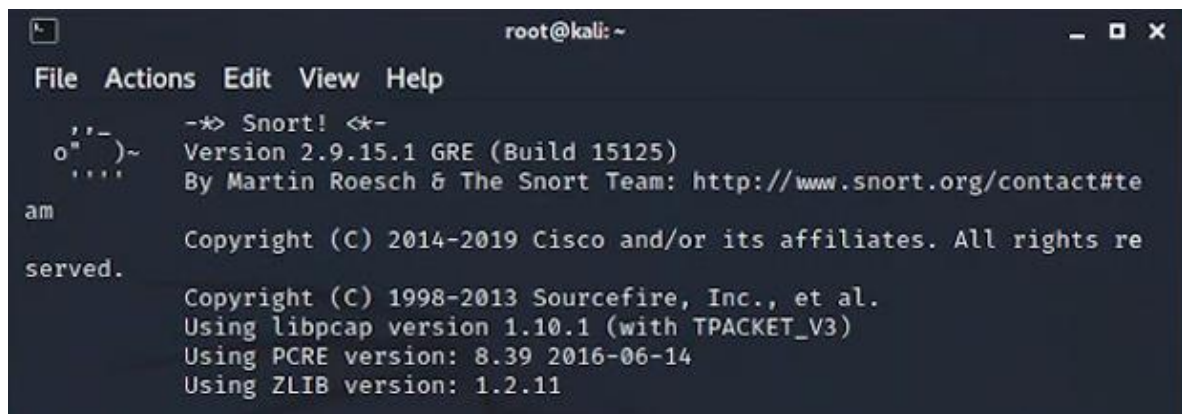
```
[root@kali:~$]cd ~/snort_src
[root@kali:~$]wget https://snort.org/downloads/snort/snort-2.9.12.tar.gz
```

\*Chú ý: \*Tại thời điểm 06/01/2019 là phiên bản 2.9.12, cần kiểm tra phiên bản trước khi chạy lệnh.

```
[root@kali:~/snort_src$]sudo tar -zxf snort-2.9.12.tar.gz
[root@kali:~/snort_src$]cd snort-2.9.12/
[root@kali:~/snort_src/snort-2.9.12$]sudo ./configure --enable-
sourcefire --disable-open-appid
[root@kali:~/snort_src/snort-2.9.12$]sudo make
[root@kali:~/snort_src/snort-2.9.12$]sudo make install
[root@kali:~/snort_src/snort-2.9.12$]sudo ldconfig
```

```
[root@kali:~/snort_src/snort-2.9.12$]sudo ln -s  
/usr/local/bin/snort /usr/sbin/snort
```

Chạy thử để kiểm tra Snort:



```
root@kali: ~  
File Actions Edit View Help  
-*> Snort! <*-  
o" )~ Version 2.9.15.1 GRE (Build 15125)  
'''' By Martin Roesch & The Snort Team: http://www.snort.org/contact#te  
am Copyright (C) 2014-2019 Cisco and/or its affiliates. All rights re  
served. Copyright (C) 1998-2013 Sourcefire, Inc., et al.  
Using libpcap version 1.10.1 (with TPACKET_V3)  
Using PCRE version: 8.39 2016-06-14  
Using ZLIB version: 1.2.11
```

Snort đã được cài thành công.

### ***e. Bước 3. Cấu hình Snort chạy ở chế độ phát hiện xâm nhập mạng***

Tạo các thư mục cho Snort:

```
[root@kali:~$]sudo mkdir /etc/snort  
[root@kali:~$]sudo mkdir /etc/snort/rules  
[root@kali:~$]sudo mkdir /etc/snort/rules/iplists  
[root@kali:~$]sudo mkdir /etc/snort/preproc_rules  
[root@kali:~$]sudo mkdir /usr/local/lib/snort_dynamicrules  
[root@kali:~$]sudo mkdir /etc/snort/so_rules
```

Tạo các tệp tin chứa tập rule cơ bản cho Snort

```
[root@kali:~$]sudo touch /etc/snort/rules/iplists/black_list.rules  
[root@kali:~$]sudo touch /etc/snort/rules/iplists/white_list.rules  
[root@kali:~$]sudo touch /etc/snort/rules/local.rules  
[root@kali:~$]sudo touch /etc/snort/sid-msg.map
```

Tạo thư mục chứa log:

```
[root@kali:~$]sudo mkdir /var/log/snort  
[root@kali:~$]sudo mkdir /var/log/snort/archived_logs
```

Tạo các bản sao tệp tin cấu hình của Snort

The configuration files are:

- classification.config
- file magic.conf
- reference.config
- snort.conf
- threshold.conf
- attribute table.dtd
- gen-msg.map
- unicode.map

```
[root@kali:~$]cd snort_src/snort-2.9.12/etc  
[root@kali:~/snort_src/snort-2.9.12/etc$]sudo cp *.conf* /etc/snort  
[root@kali:~/snort_src/snort-2.9.12/etc$]sudo cp *.map /etc/snort  
[root@kali:~/snort_src/snort-2.9.12/etc$]sudo cp *.dtd /etc/snort  
[root@kali:~$]cd ~/snort_src/snort-2.9.12/src/dynamic-
```

```
preprocessors/build/usr/local/lib/snort_dynamicpreprocessor/sudo cp *  
/usr/local/lib/snort_dynamicpreprocessor/
```

Bây giờ chúng ta có các thư mục và tệp tin của Snort theo các đường dẫn sau:

Tệp thực thi của Snort: `/usr/local/bin/snort`

Tệp tin cấu hình: `/etc/snort/snort.conf`

Thư mục chứa log: `/var/log/snort`

Thư mục chứa tập rule: `/etc/snort/rules`

```
/etc/snort/so_rules  
/etc/snort/preproc_rules  
/usr/local/lib/snort_dynamicrules
```

Thư mục chứa IP: `/etc/snort/rules/iplists`

Thư mục tiền xử lý động: `/usr/local/lib/snort_dynamicpreprocessor/`

Tiếp theo cần sử dụng trình soạn thảo văn bản: nano hoặc vi để chỉnh sửa các tham số trong tệp tin: `/etc/snort/snort.conf`

```
[root@kali:~]sudo nano /etc/snort/snort.conf
```

Tìm đến dòng 45, chỉnh sửa địa chỉ IP cho mạng của máy cần bảo vệ.

```
ipvar HOME_NET 192.168.204.128/24|  
ipvar EXTERNAL_NET !$HOME_NET (dòng 48)
```

Tìm đến các dòng sau chỉnh sửa đường dẫn chứa tập rule.

```
var RULE_PATH /etc/snort/rules (dòng 104)  
var SO_RULE_PATH /etc/snort/so_rules (dòng 105)  
var PREPROC_RULE_PATH /etc/snort/preproc_rules (dòng 106)  
var WHITE_LIST_PATH /etc/snort/iplists (dòng 113)  
var BLACK_LIST_PATH /etc/snort/iplists (dòng 114)
```

Đường dẫn tập rule: `include $RULE_PATH/local.rules (dòng 546)` Tệp tin này chứa tập rule sử dụng để kiểm tra sự hoạt động của Snort, cần bỏ dấu # trước dòng này.

Các dòng từ 548 đến 651 chứa tập rule cho mỗi loại hình tấn công, trong quá trình kiểm tra cần đóng lại bằng cách đặt dấu # trước mỗi dòng.

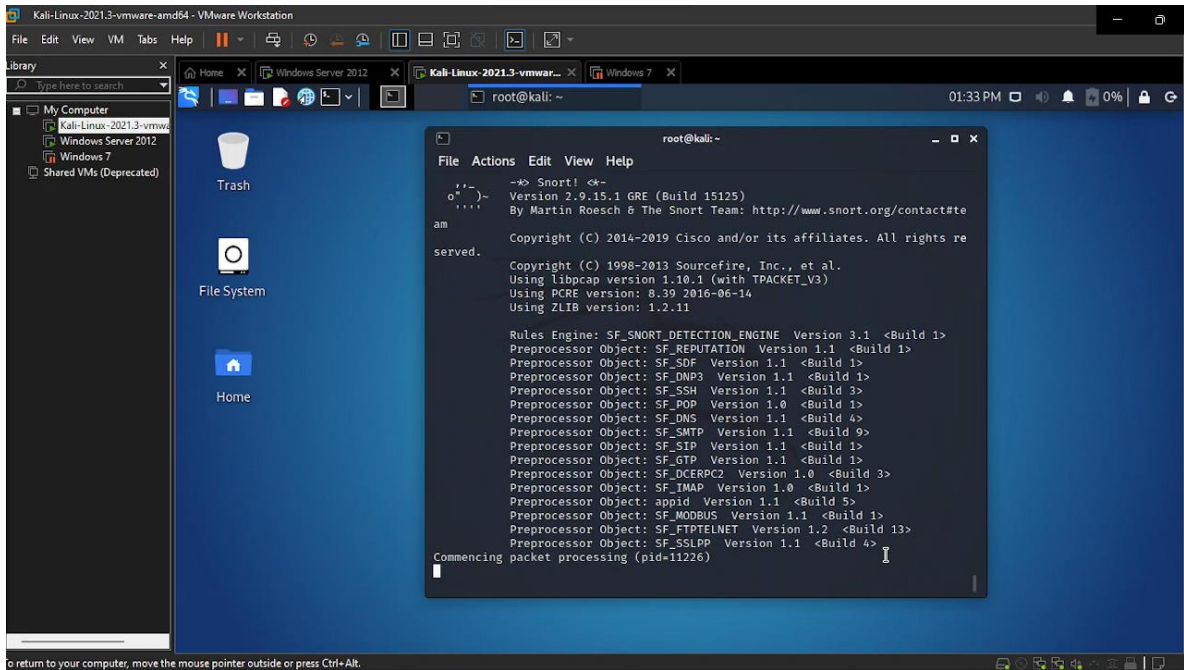
Kết thúc quá trình cấu hình, lưu và thoát khỏi trình chỉnh sửa.

## f. Bước 4. Kiểm tra sự hoạt động của Snort

Tại cửa sổ dòng lệnh chạy lệnh sau:

```
[root@kali:~$] sudo snort -i eth0 -c /etc/snort/snort.conf -T
```

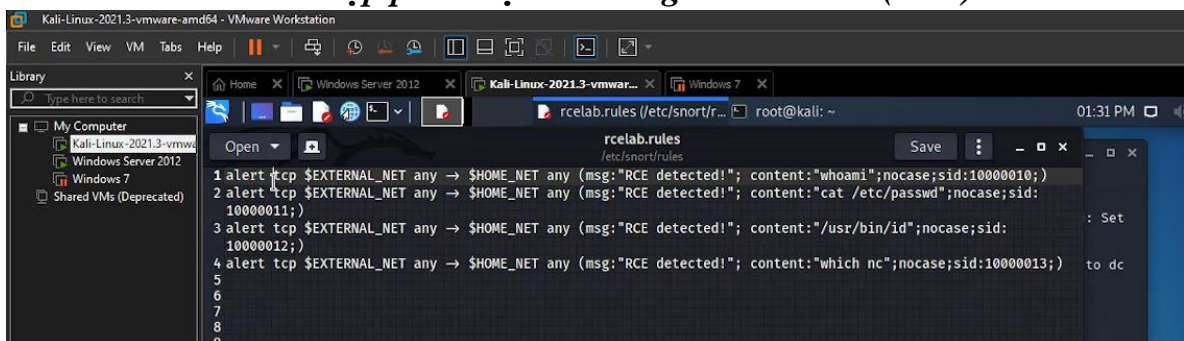
Kết quả như sau:



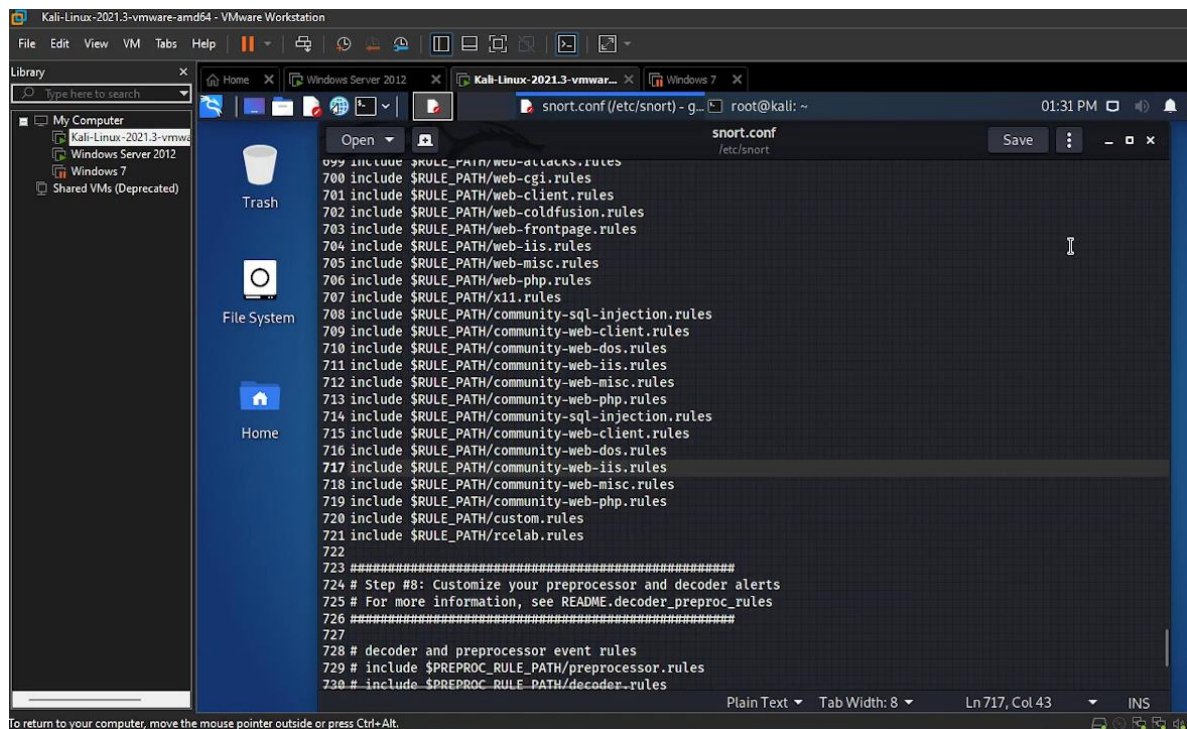
Kết quả cài đặt và cấu hình Snort thành công.

## 4. Cấu hình

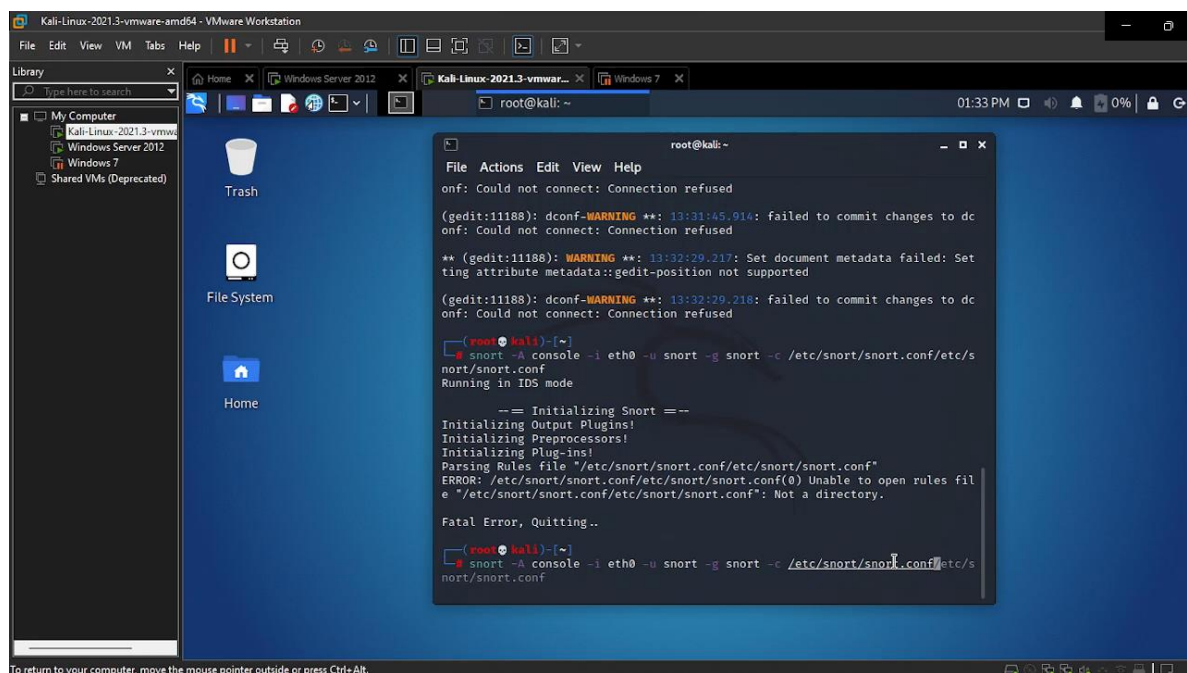
### a. Cấu hình thiết lập phát hiện tấn công mức cơ bản (Low)



Thiết lập rule phát hiện tấn công RCE bằng các content. Sau đó lưu lại vào file rcelab.rules



Thêm rule rcelab.rules vào file snort.conf

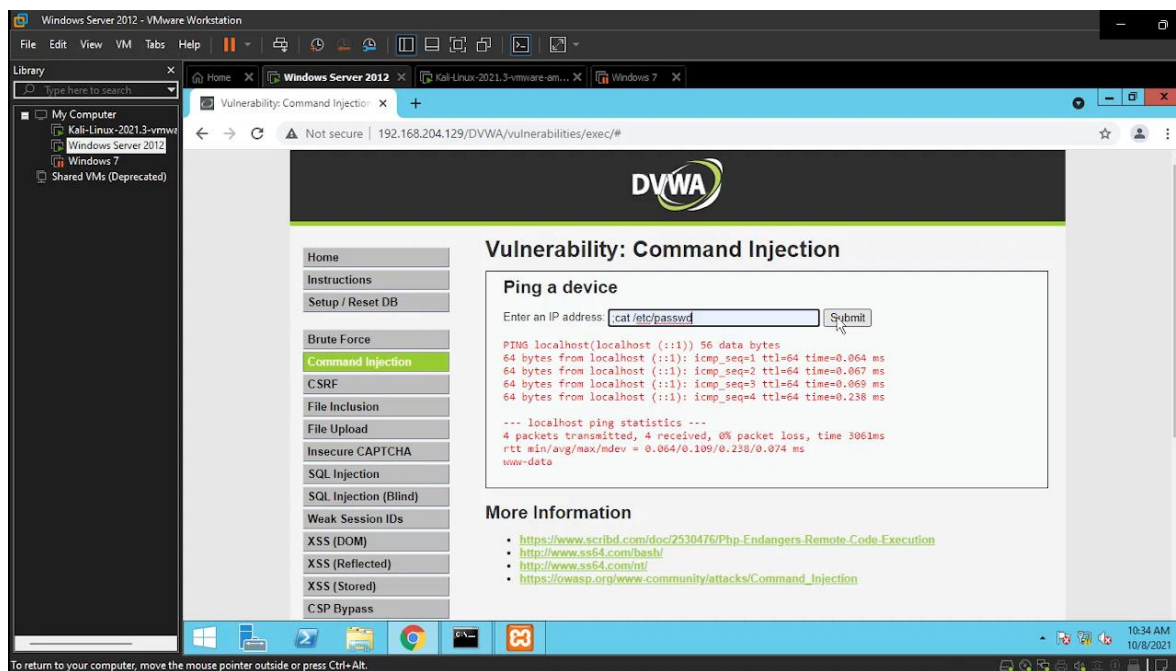


Khởi động snort bằng lệnh **snort -A console -i eth0 -u snort -g snort -c /etc/snort/snort.conf**



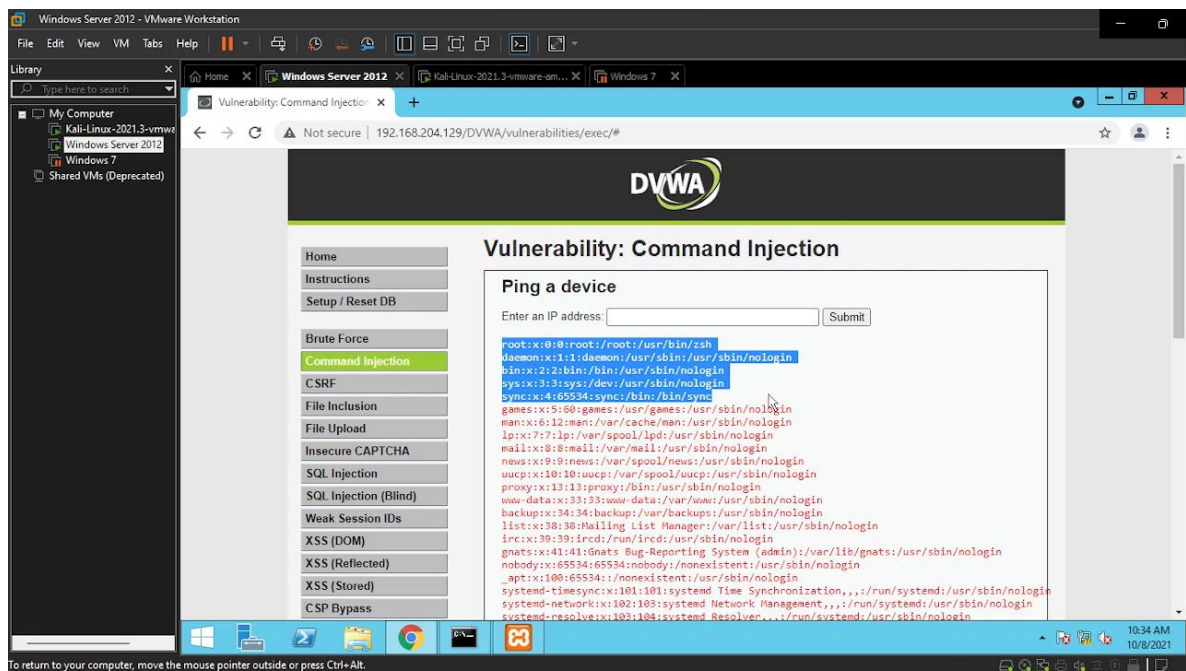
```
root@kali: ~  
File Actions Edit View Help  
-*> Snort! <*-  
o" )~  
  ~  
  ~  
am  
served.  
Copyright (C) 2014-2019 Cisco and/or its affiliates. All rights re  
Copyright (C) 1998-2013 Sourcefire, Inc., et al.  
Using libpcap version 1.10.1 (with TPACKET_V3)  
Using PCRE version: 8.39 2016-06-14  
Using ZLIB version: 1.2.11  
Rules Engine: SF_SNORT_DETECTION_ENGINE Version 3.1 <Build 1>  
Preprocessor Object: SF_REPUTATION Version 1.1 <Build 1>  
Preprocessor Object: SF_SDF Version 1.1 <Build 1>  
Preprocessor Object: SF_DNP3 Version 1.1 <Build 1>  
Preprocessor Object: SF_SSH Version 1.1 <Build 3>  
Preprocessor Object: SF_POP Version 1.0 <Build 1>  
Preprocessor Object: SF_DNS Version 1.1 <Build 4>  
Preprocessor Object: SF_SMTP Version 1.1 <Build 9>  
Preprocessor Object: SF_SIP Version 1.1 <Build 1>  
Preprocessor Object: SF_GTP Version 1.1 <Build 1>  
Preprocessor Object: SF_DCEPC2 Version 1.0 <Build 3>  
Preprocessor Object: SF_IMAP Version 1.0 <Build 1>  
Preprocessor Object: appid Version 1.1 <Build 5>  
Preprocessor Object: SF_MODBUS Version 1.1 <Build 1>  
Preprocessor Object: SF_FTPTELNET Version 1.2 <Build 13>  
Preprocessor Object: SF_SSLPP Version 1.1 <Build 4>  
Commencing packet processing (pid=11226)
```

Snort đã khởi động thành công

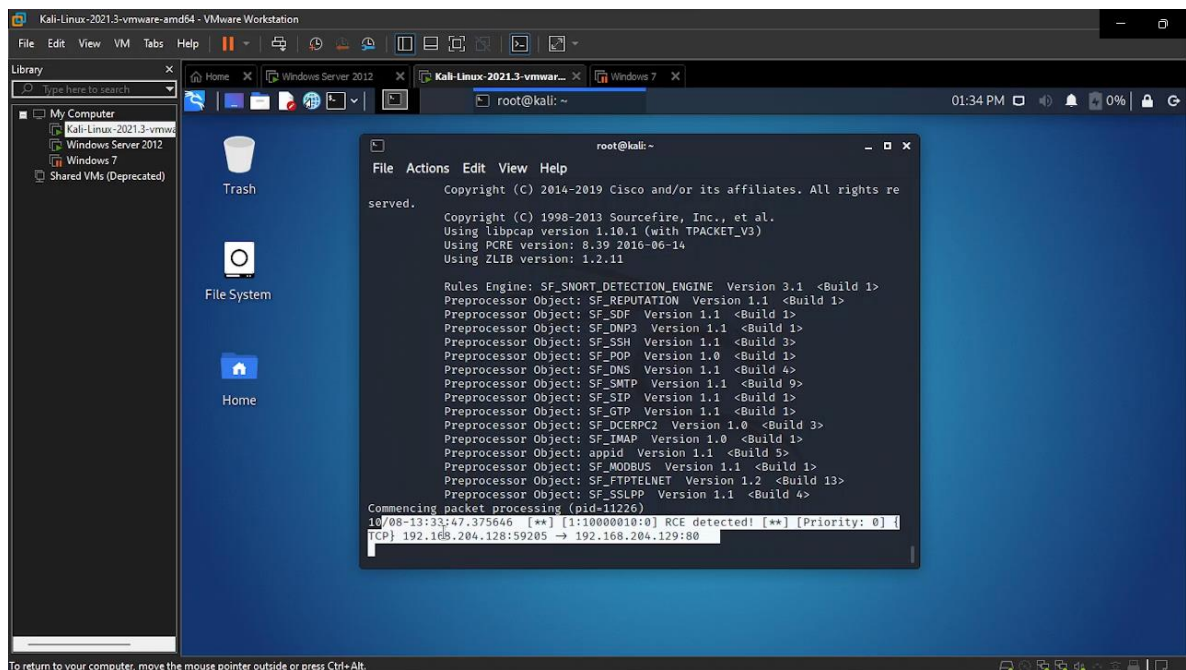


Tiếp theo sang máy attacker thử tấn công vào DVWA đã cài đặt ở Kali bằng lệnh  
**;cat /etc/passwd**



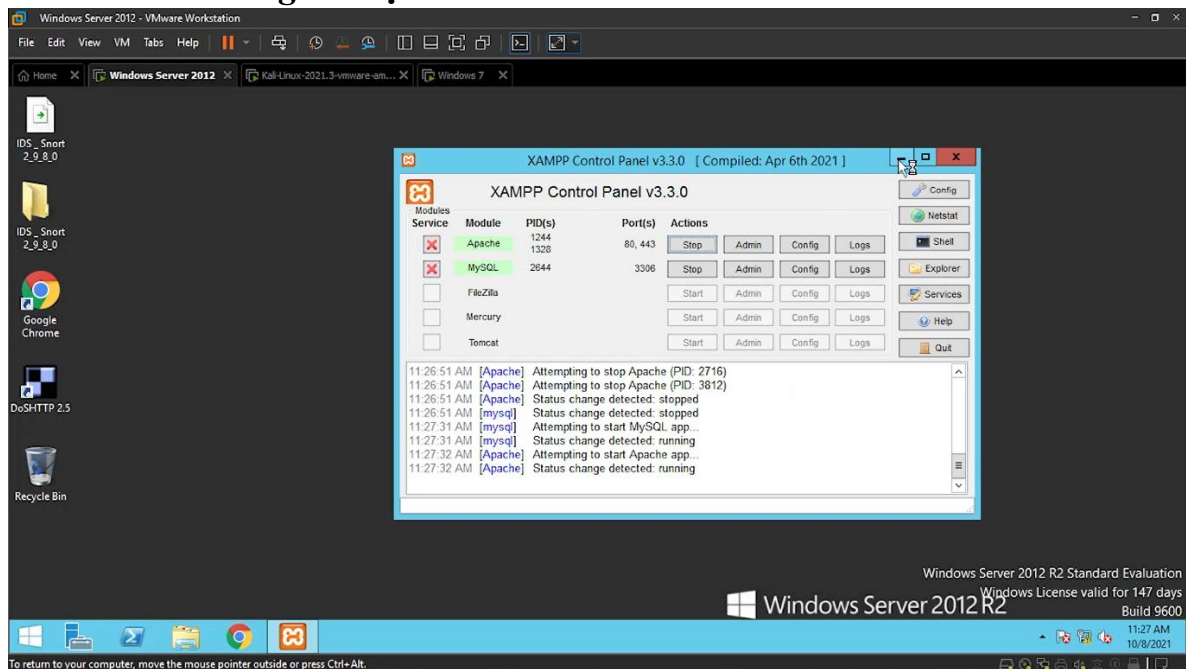


Tấn công RCE thành công, tiếp theo sẽ sang máy cài đặt Webserver xem có cảnh báo gì không?

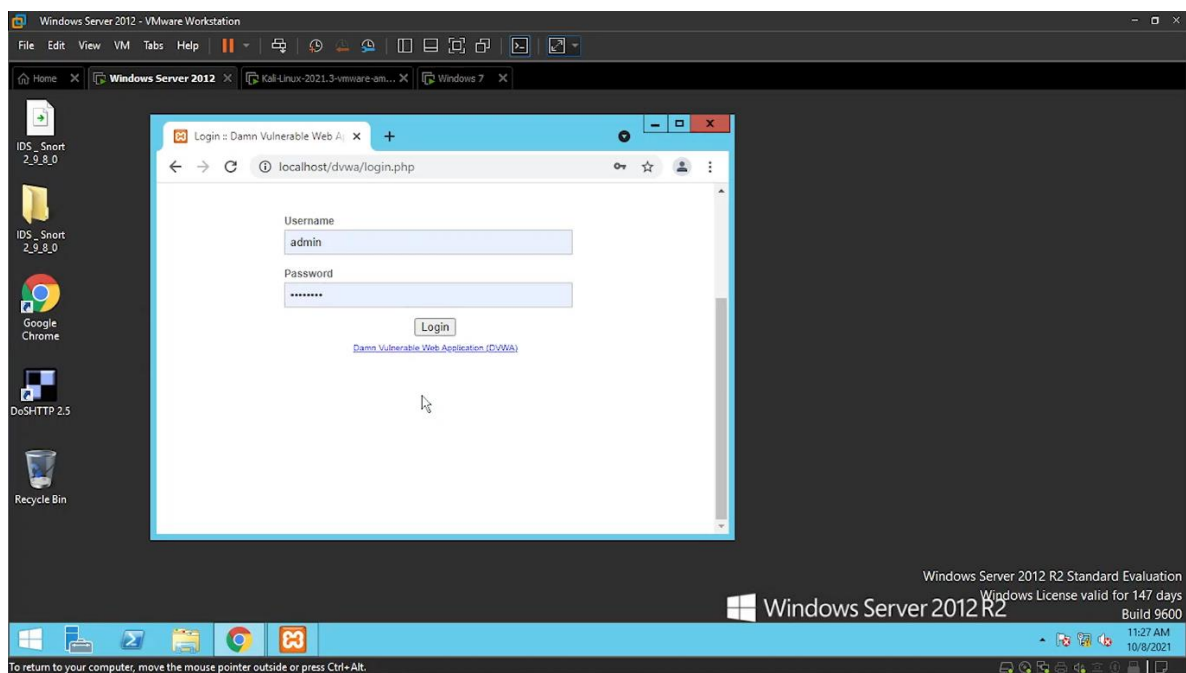


Đã phát hiện thành công “**RCE detected**”. Alert cho ta thấy IP của attacker là **192.168.204.128** (windows server 2012) với port 59205.

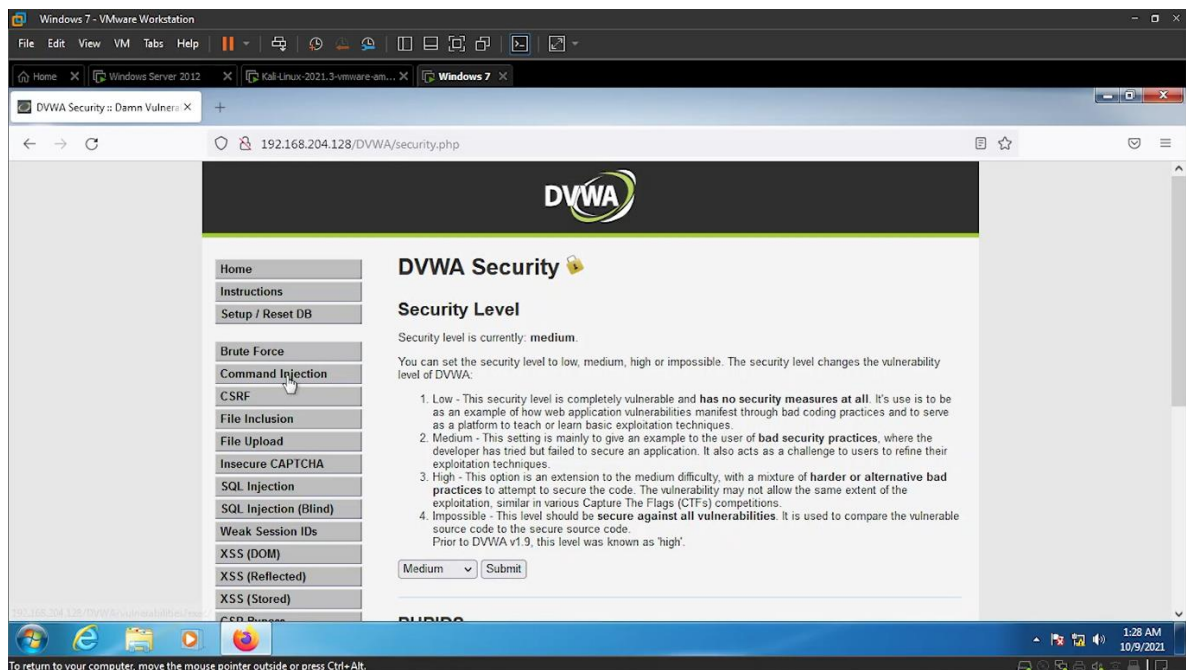
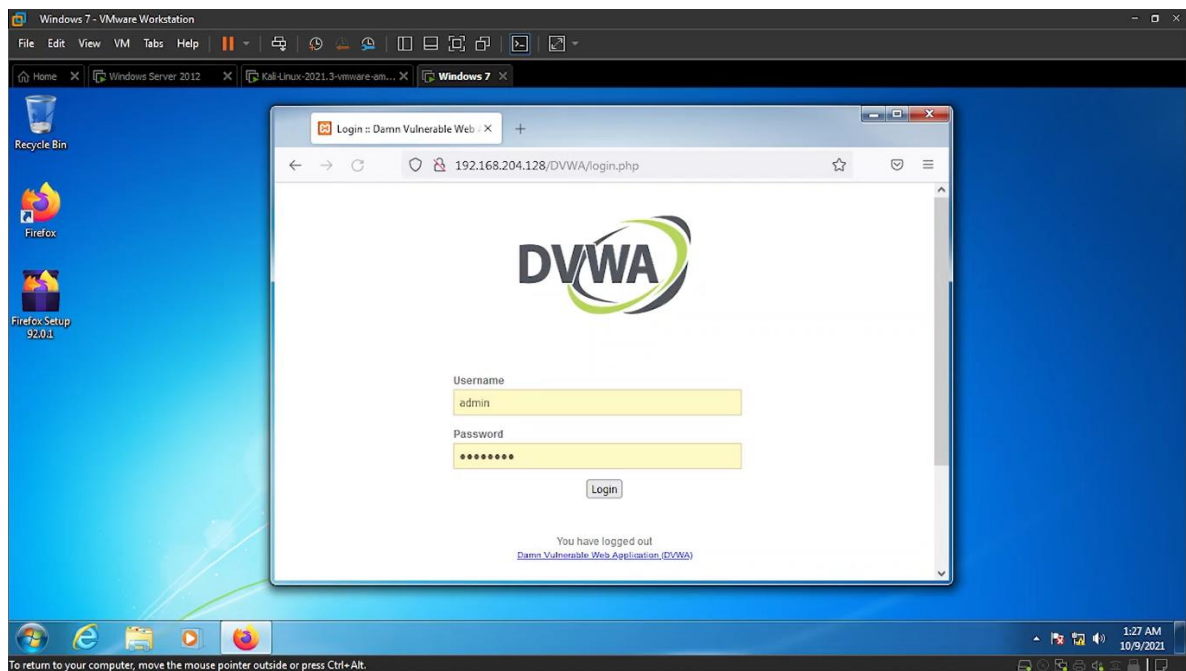
## b. Cấu hình ngăn chặn RCE attacker mức Medium



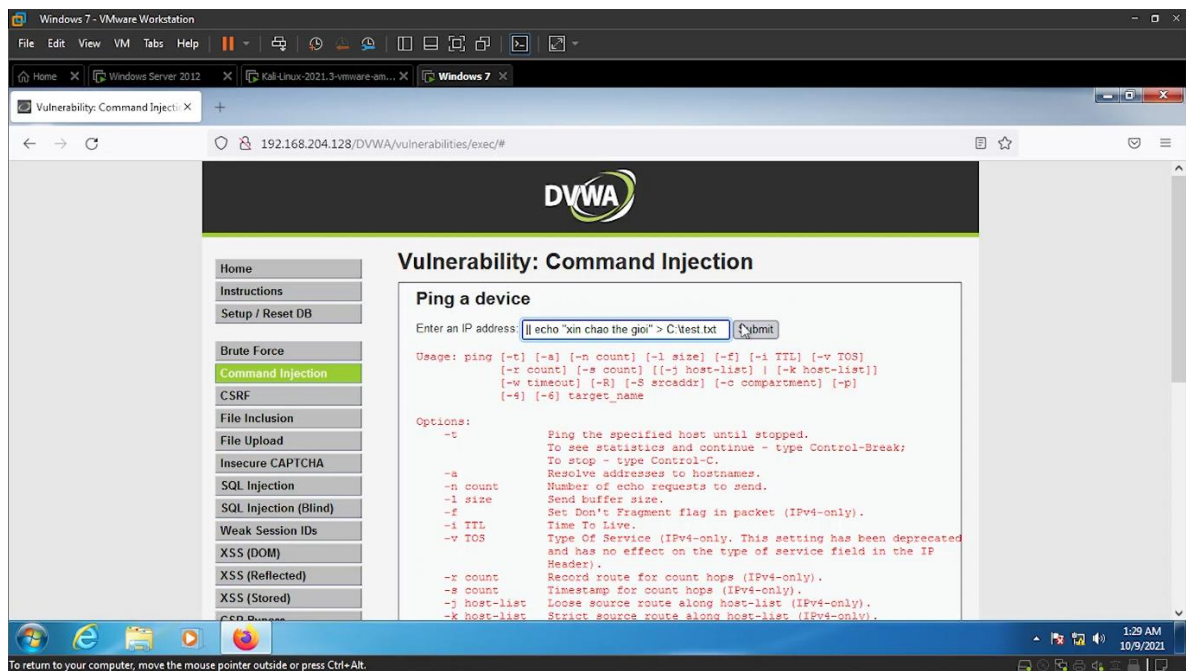
Khởi động Webserver DVWA được cài đặt trên Windows server 2012 (victim) bằng phần mềm XAMPP



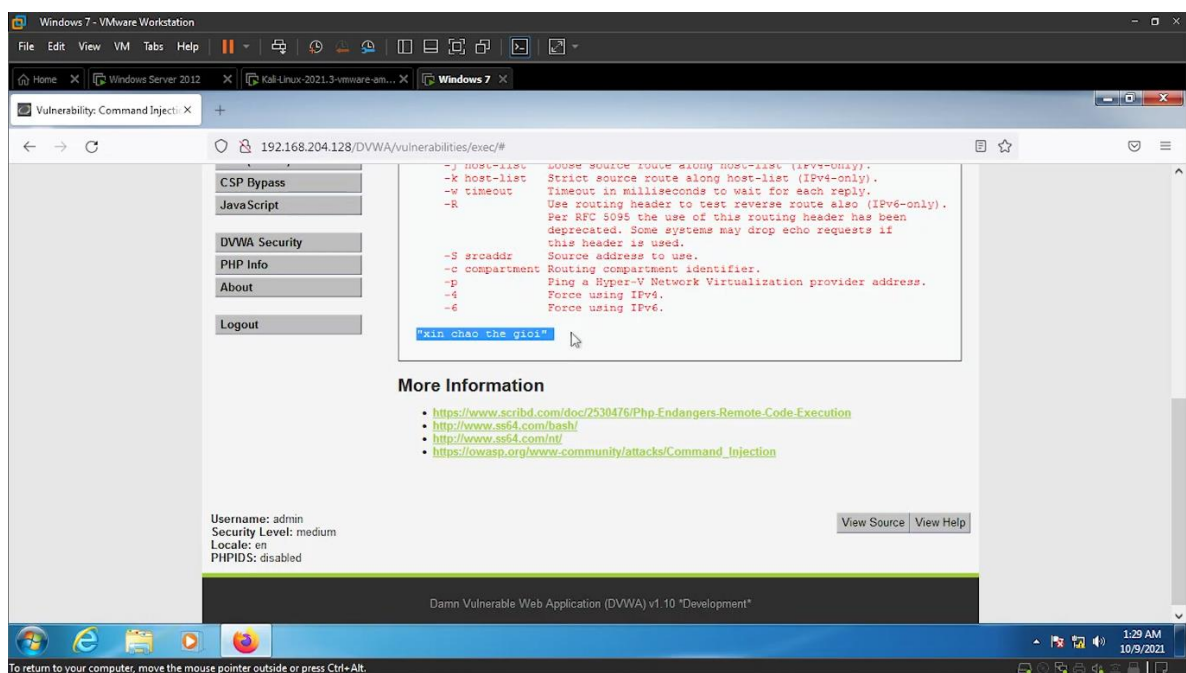
Truy cập vào localhost/dvwa ta thấy đã khởi động Webserver thành công.



Tiếp tục sang windows 7 (attacker) truy cập tới địa chỉ Webserver 192.168.204.128/DVWA. Và như hình ta đã truy cập thành công.



Thử tấn công tới file test.txt bằng lệnh `|| echo "xin chao the gioi" > C:\test.txt`

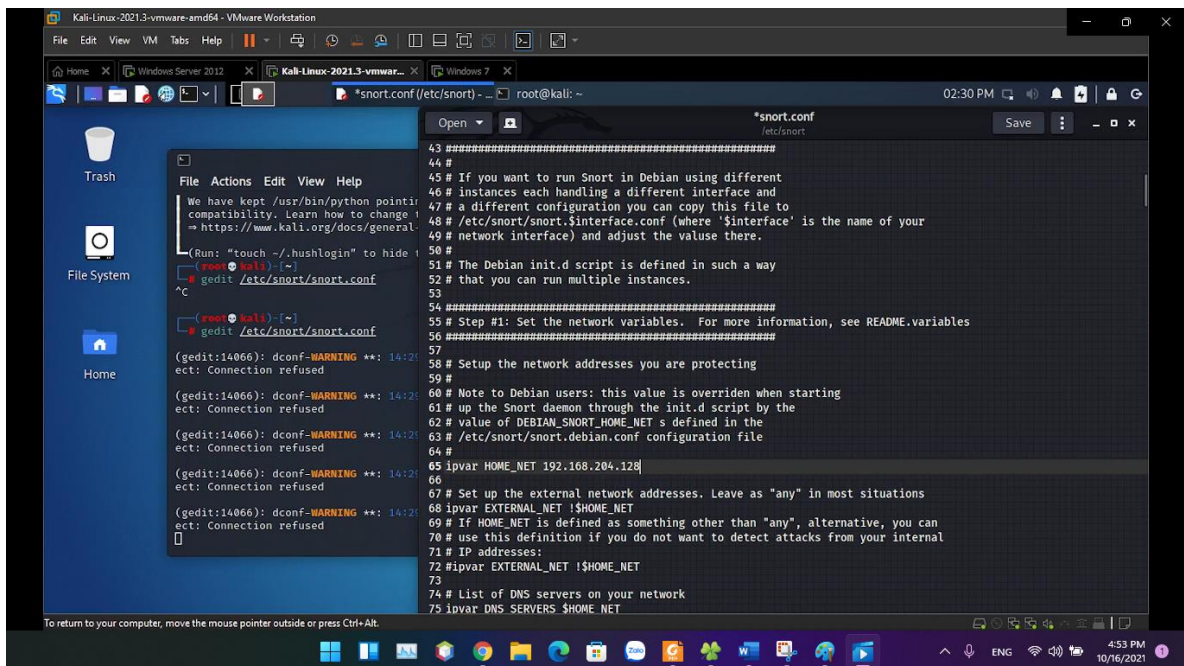


Rồi dùng lệnh `|| more C:\test.txt` để xem bên trong file test có gì

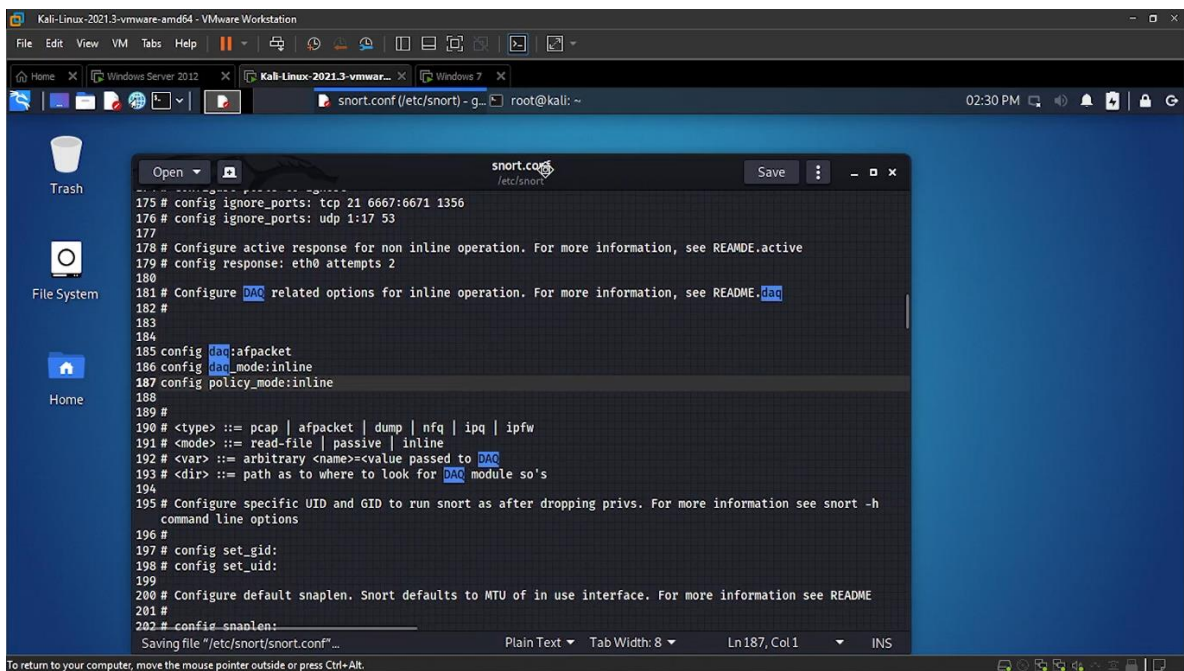
Và như trên hình chúng ta đã tấn công và thêm dòng chữ “xin chao the gioi” vào file test.txt thành công.



Tiếp theo ta sẽ config ở máy cài Snort.

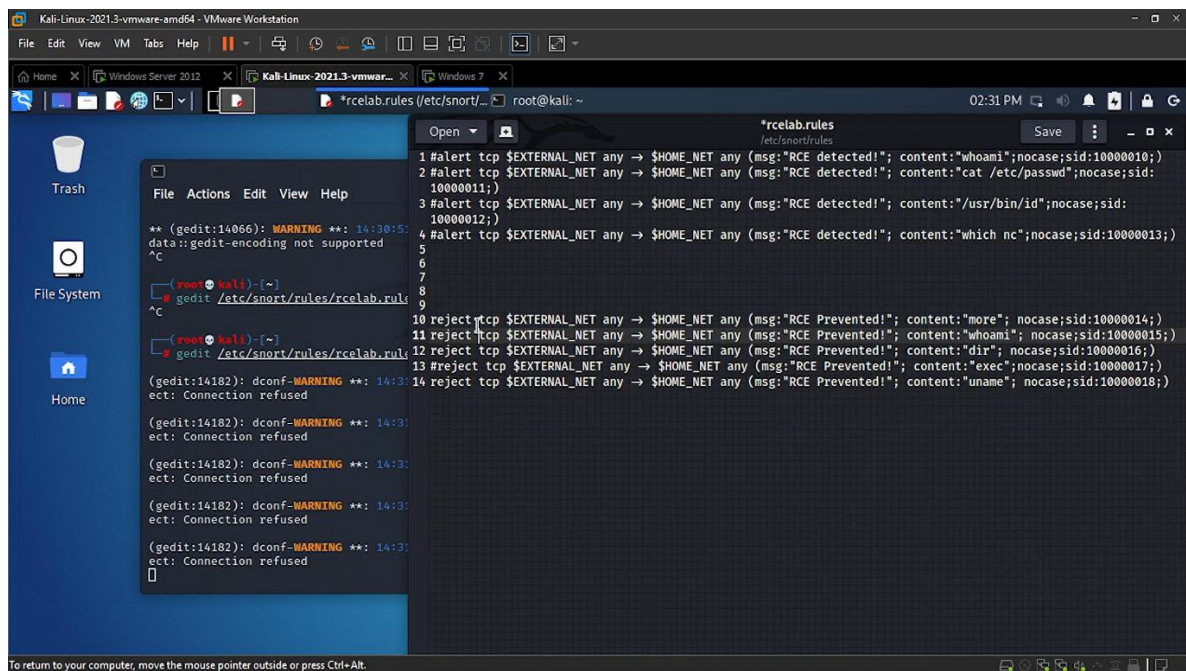


Thay đổi địa chỉ `ipvar HOME_NET` trở tới địa chỉ Webserver được bảo vệ là `192.168.204.128` ở file `snort.conf`

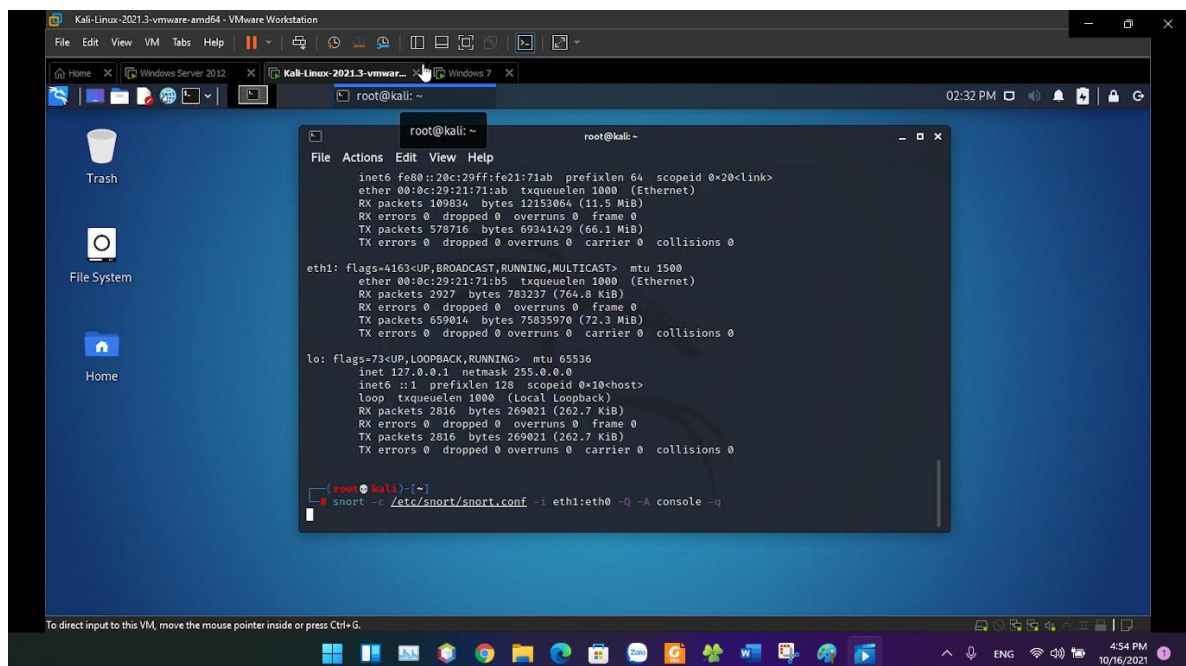


Để bật chế độ IPS (ngăn chặn) thì ta khởi động 3 dòng config ở file `snort.conf`

`config daq:afpacket`  
`config daq_mode:inline`  
`config policy_mode:inline`

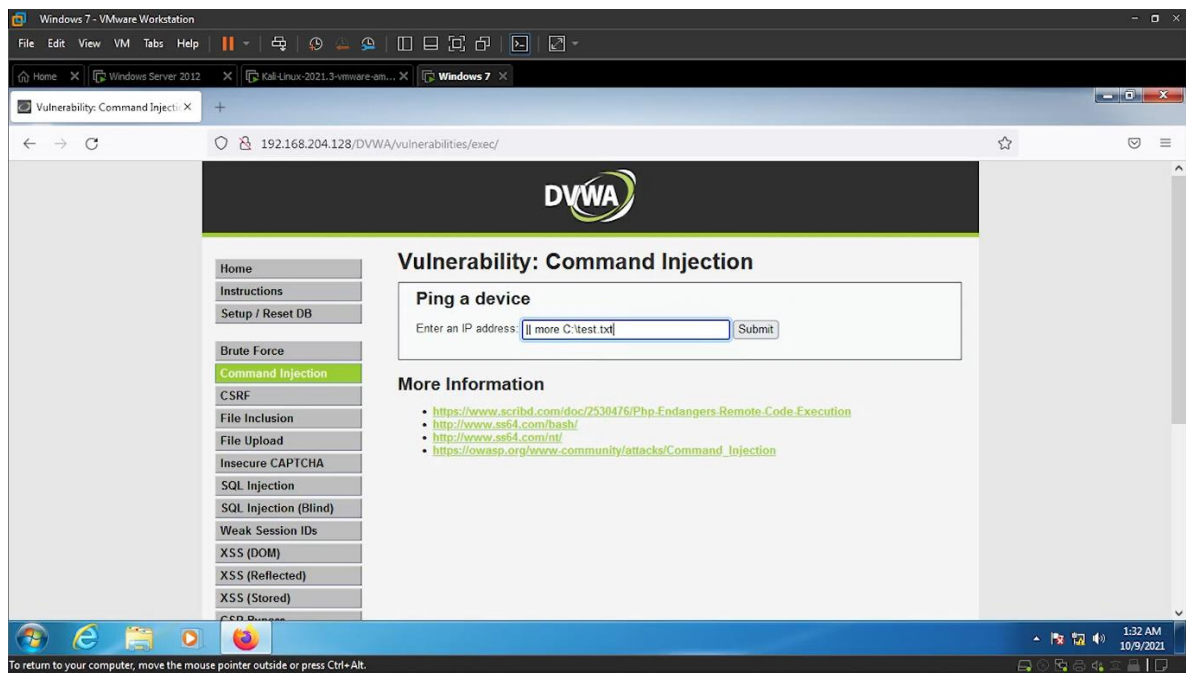


Tiếp theo config lại file rules. Bật các rules reject ở rclab.rules để ngăn chặn tấn công và lưu lại.

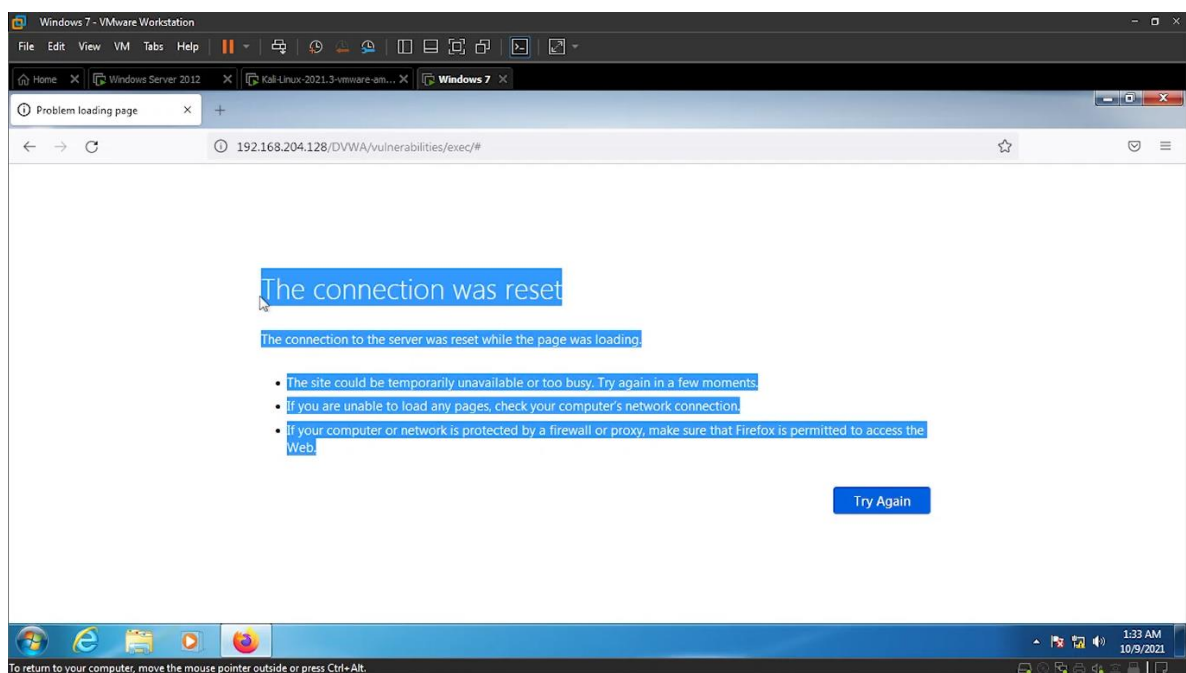


Khởi động Snort (Chế độ ngăn chặn) bằng lệnh:

**snort -c /etc/snort/snort.conf -i eth1:eth0 -Q -A console -q**

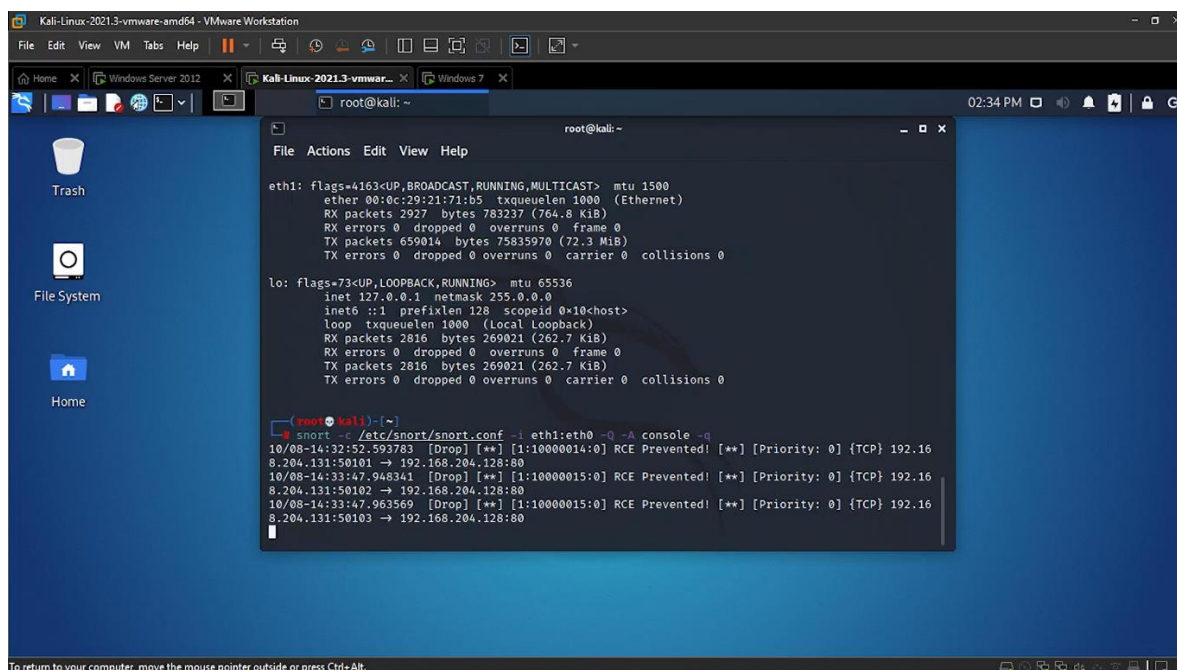


Thử tấn công lại bằng máy attacker bằng lệnh `|| more C:\test.txt`



Ngay lập tức hành động tấn công đã bị SNORT ngăn chặn.





Sang lại máy Kali cài Snort sẽ thấy các rules đã hoạt động trơn tru. DROP được các tấn công RCE.

### III. KẾT QUẢ NHẬN XÉT

#### 1. Kết quả:

Bài Lab đã đạt được một số mục tiêu như hiểu về cách thức hoạt động và cách thức phát hiện, ngăn chặn tấn công của hệ thống IPS/IDS. Cách bố trí một hệ thống phát hiện xâm nhập trong hệ thống mạng.

Nghiên cứu và hiểu cấu trúc và cách thức xử lý gói tin của Snort. Hiểu rõ cấu trúc của một Rule trong Snort. Cách thức viết một rule cho yêu cầu tấn công RCE.

Cài đặt và cấu hình thành công hệ thống, demo các hình thức xâm nhập đơn giản.

#### 2. Nhận xét:

Nhóm em còn khó khăn trong việc tìm hiểu các loại tấn công RCE mới hiện nay.

Việc khó khăn nhất của xây dựng một hệ thống Snort không phải ở quá trình cài đặt, cấu hình hay demo mà quá trình khó khăn nhất nằm ở phía người quản trị. Dù một hệ thống Snort có tốt đến đâu nhưng nếu người quản trị không có kỹ năng phân tích log, phân tích trạng thái của hệ thống, không nắm rõ cấu trúc Rule thì không thể hình thành nên được các tập Rules đối với môi trường doanh nghiệp được.

### IV. THAM KHẢO

[1] Hướng dẫn cấu hình và cài đặt một số rule: <https://www.snort.org/>

[2] Snort documentation: <https://www.snort.org/documents>

**HẾT**