BAN CƠ YẾU CHÍNH PHỦ

HỌC VIỆN KỸ THUẬT MẬT MÃ

MODULE THỰC HÀNH

AN TOÀN MẠNG MÁY TÍNH

BÀI THỰC HÀNH SỐ 03

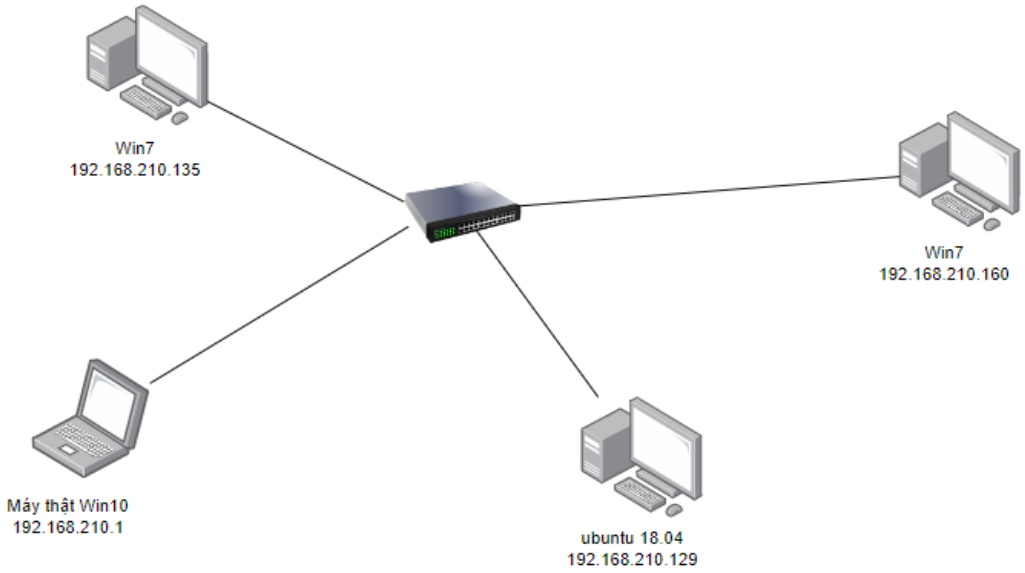
Triển khai hệ thống phát hiện xâm nhập Snort

Sinh viên thực hiện:

Nguyễn Đức Mạnh - AT170432

1. CHUẨN BỊ

Vẽ lại mô hình mạng chuẩn bị thực hành *(bao gồm các kết nối, địa chỉ IP, hệ điều hành, tên máy, ứng dụng được cài đặt)* và dán vào bên dưới.



2. THỰC HÀNH

Kịch bản 1. Phát hiện tấn công dò quét

Chụp ảnh cấu hình luật trên Snort để cho phép phát hiện tấn công dò quét và dán vào bên dưới.

```
 GNU nano 2.9.3                    icmp.rules                         Modified

alert icmp any any -> any any (msg:"Phat hien Ping"; sid:1000001; rev:1;)
```

```
C:\Users\admin>ping 192.168.210.129

Pinging 192.168.210.129 with 32 bytes of data:
Reply from 192.168.210.129: bytes=32 time<1ms TTL=64
Reply from 192.168.210.129: bytes=32 time<1ms TTL=64
Reply from 192.168.210.129: bytes=32 time=1ms TTL=64
Reply from 192.168.210.129: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.210.129:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\admin>_
```

```
attt@web:~$ tail -f /var/log/snort/alert
[**] [1:1000001:1] Phat hien Ping [**]
[Priority: 0]
05/26-07:52:34.596511 192.168.210.135 -> 192.168.210.129
ICMP TTL:128 TOS:0x0 ID:92 IpLen:20 DgmLen:60
Type:8  Code:0  ID:1   Seq:1  ECHO

[**] [1:1000001:1] Phat hien Ping [**]
[Priority: 0]
05/26-07:52:34.596537 192.168.210.129 -> 192.168.210.135
ICMP TTL:64 TOS:0x0 ID:53117 IpLen:20 DgmLen:60
Type:0  Code:0  ID:1  Seq:1  ECHO REPLY

[**] [1:1000001:1] Phat hien Ping [**]
[Priority: 0]
05/26-07:52:35.605448 192.168.210.135 -> 192.168.210.129
ICMP TTL:128 TOS:0x0 ID:93 IpLen:20 DgmLen:60
Type:8  Code:0  ID:1   Seq:2  ECHO

[**] [1:1000001:1] Phat hien Ping [**]
[Priority: 0]
05/26-07:52:35.605483 192.168.210.129 -> 192.168.210.135
ICMP TTL:64 TOS:0x0 ID:53135 IpLen:20 DgmLen:60
Type:0  Code:0  ID:1  Seq:2  ECHO REPLY
```

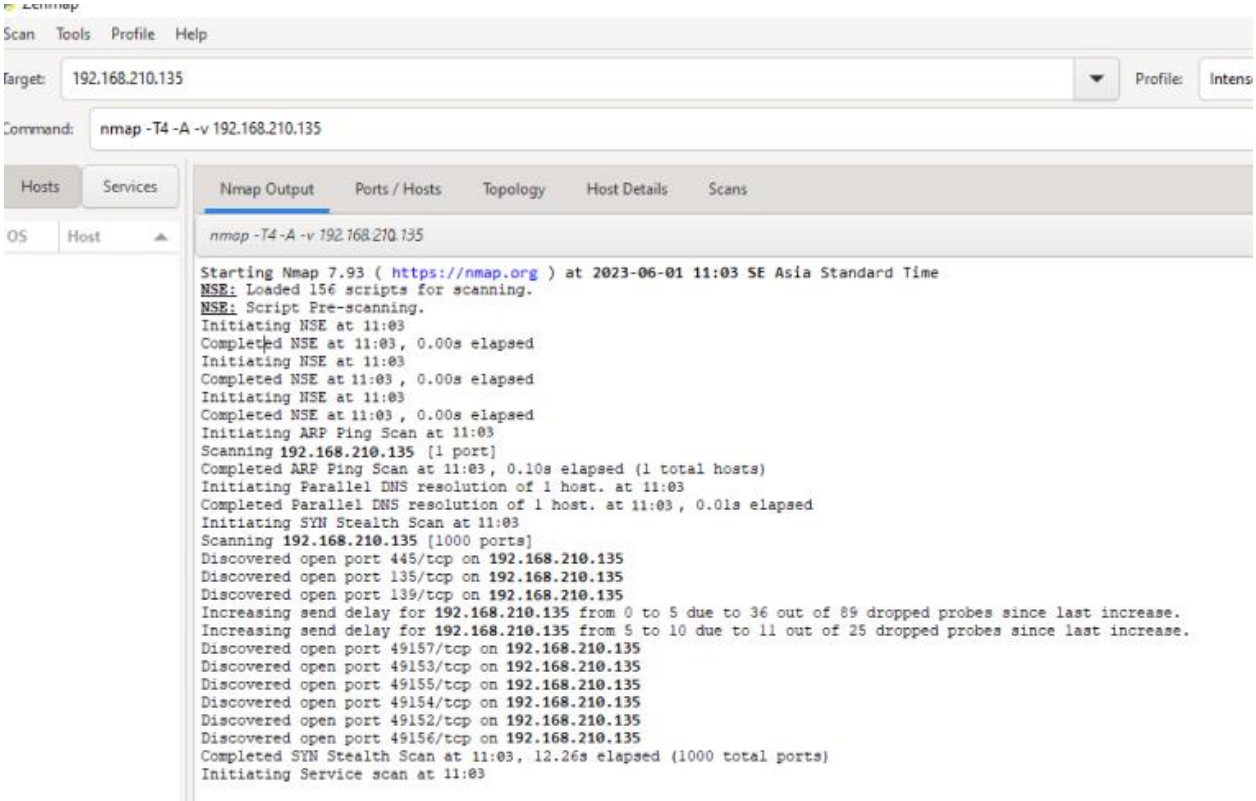
Kịch bản 2. Phát hiện tấn công dò quét dịch vụ và cổng

Cấu hình luật trên Snort để cho phép phát hiện tấn công dò quét dịch vụ và cổng

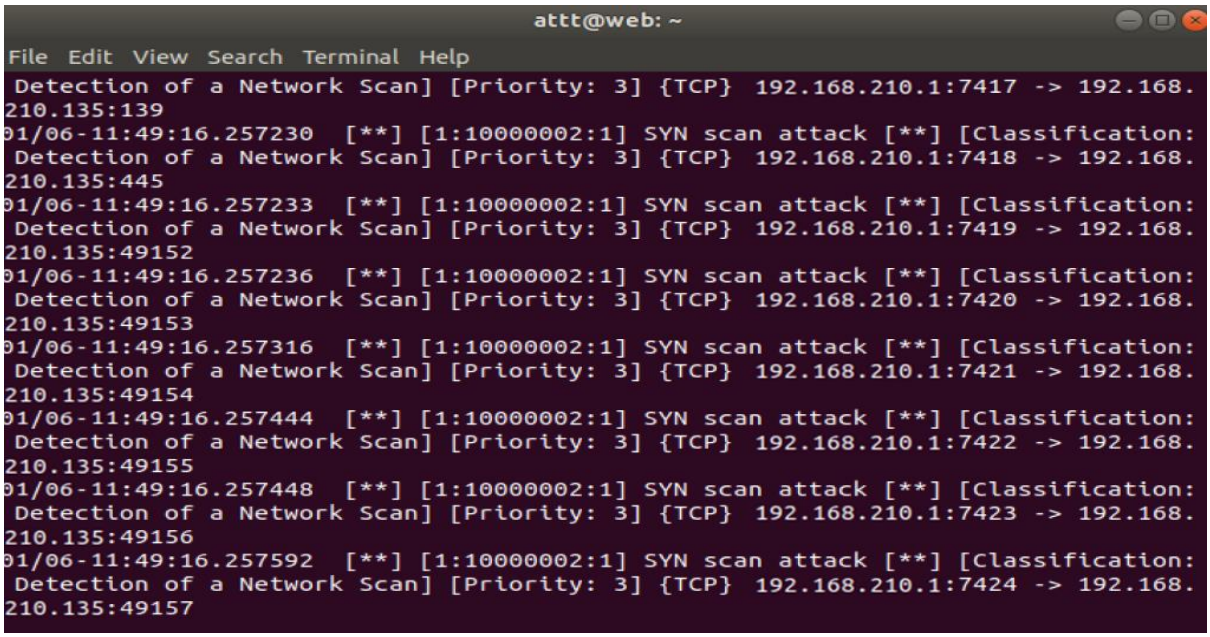
```
  GNU nano 2.9.3                        scan.rules                          Modified

alert tcp any any -> $HOME_NET any (msg:"SYN scan attack"; detection_filter:tra$
```

Scan port

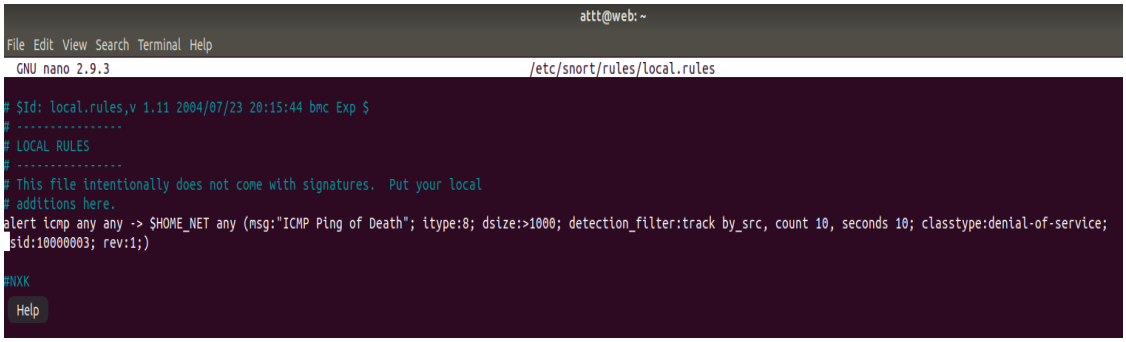


Kết quả

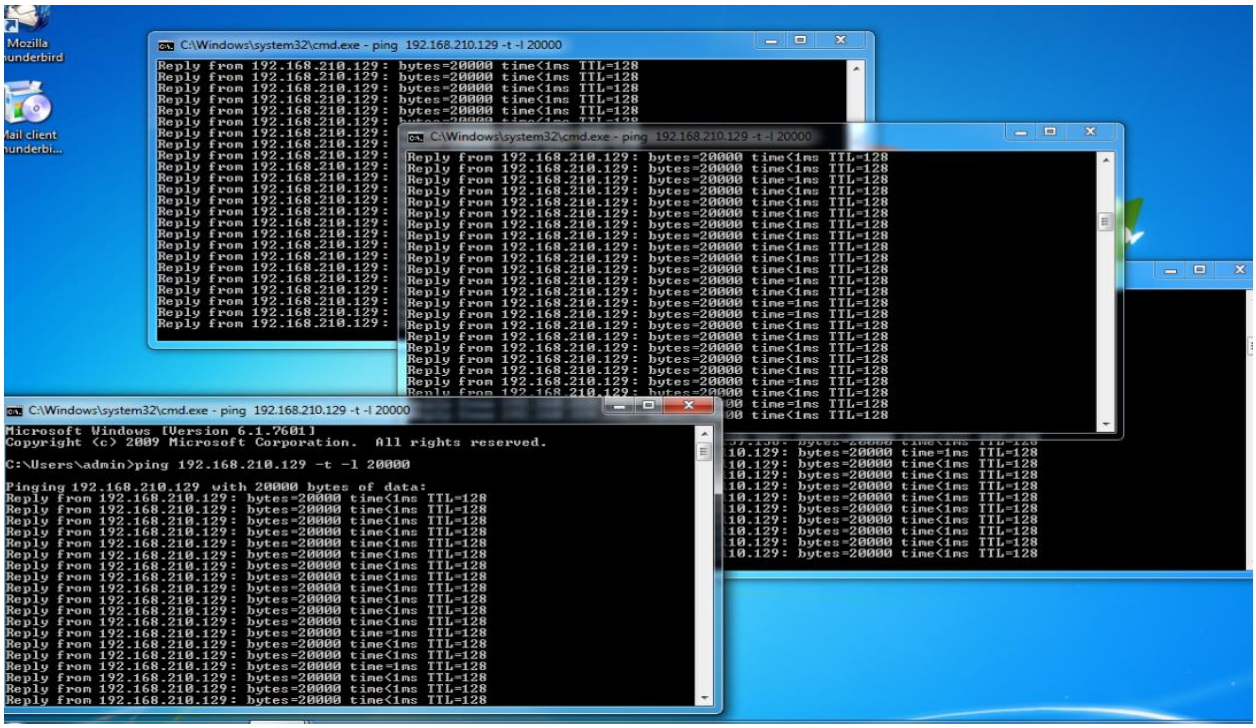


Kịch bản 3. Phát hiện tấn công từ chối dịch vụ

Cấu hình luật trên Snort để cho phép phát hiện tấn công từ chối dịch vụ



Tấn công



Kết quả

```
attt@web:~$ sudo snort -A console -q -l ens33 -c /etc/snort/snort.conf
06/01-11:54:44.976043  [**] [1:10000003:1] ICMP Ping of Death [**] [Classification: Detection of a Denial of Service Attack] [Priority: 2] {ICMP} 192.168.210.160 -> 192.168.210.129
06/01-11:54:45.241165  [**] [1:10000003:1] ICMP Ping of Death [**] [Classification: Detection of a Denial of Service Attack] [Priority: 2] {ICMP} 192.168.210.160 -> 192.168.210.129
06/01-11:54:45.881282  [**] [1:10000003:1] ICMP Ping of Death [**] [Classification: Detection of a Denial of Service Attack] [Priority: 2] {ICMP} 192.168.210.160 -> 192.168.210.129
06/01-11:54:46.001993  [**] [1:10000003:1] ICMP Ping of Death [**] [Classification: Detection of a Denial of Service Attack] [Priority: 2] {ICMP} 192.168.210.160 -> 192.168.210.129
06/01-11:54:46.255297  [**] [1:10000003:1] ICMP Ping of Death [**] [Classification: Detection of a Denial of Service Attack] [Priority: 2] {ICMP} 192.168.210.160 -> 192.168.210.129
06/01-11:54:46.895025  [**] [1:10000003:1] ICMP Ping of Death [**] [Classification: Detection of a Denial of Service Attack] [Priority: 2] {ICMP} 192.168.210.160 -> 192.168.210.129
06/01-11:54:47.003787  [**] [1:10000003:1] ICMP Ping of Death [**] [Classification: Detection of a Denial of Service Attack] [Priority: 2] {ICMP} 192.168.210.160 -> 192.168.210.129
06/01-11:54:47.269101  [**] [1:10000003:1] ICMP Ping of Death [**] [Classification: Detection of a Denial of Service Attack] [Priority: 2] {ICMP} 192.168.210.160 -> 192.168.210.129
06/01-11:54:47.893051  [**] [1:10000003:1] ICMP Ping of Death [**] [Classification: Detection of a Denial of Service Attack] [Priority: 2] {ICMP} 192.168.210.160 -> 192.168.210.129
06/01-11:54:48.018456  [**] [1:10000003:1] ICMP Ping of Death [**] [Classification: Detection of a Denial of Service Attack] [Priority: 2] {ICMP} 192.168.210.160 -> 192.168.210.129
06/01-11:54:48.283308  [**] [1:10000003:1] ICMP Ping of Death [**] [Classification: Detection of a Denial of Service Attack] [Priority: 2] {ICMP} 192.168.210.160 -> 192.168.210.129
06/01-11:54:48.906742  [**] [1:10000003:1] ICMP Ping of Death [**] [Classification: Detection of a Denial of Service Attack] [Priority: 2] {ICMP} 192.168.210.160 -> 192.168.210.129
06/01-11:54:49.032386  [**] [1:10000003:1] ICMP Ping of Death [**] [Classification: Detection of a Denial of Service Attack] [Priority: 2] {ICMP} 192.168.210.160 -> 192.168.210.129
06/01-11:54:49.297700  [**] [1:10000003:1] ICMP Ping of Death [**] [Classification: Detection of a Denial of Service Attack] [Priority: 2] {ICMP} 192.168.210.160 -> 192.168.210.129
06/01-11:54:49.920799  [**] [1:10000003:1] ICMP Ping of Death [**] [Classification: Detection of a Denial of Service Attack] [Priority: 2] {ICMP} 192.168.210.160 -> 192.168.210.129
06/01-11:54:50.046446  [**] [1:10000003:1] ICMP Ping of Death [**] [Classification: Detection of a Denial of Service Attack] [Priority: 2] {ICMP} 192.168.210.160 -> 192.168.210.129
06/01-11:54:50.311081  [**] [1:10000003:1] ICMP Ping of Death [**] [Classification: Detection of a Denial of Service Attack] [Priority: 2] {ICMP} 192.168.210.160 -> 192.168.210.129
06/01-11:54:50.935050  [**] [1:10000003:1] ICMP Ping of Death [**] [Classification: Detection of a Denial of Service Attack] [Priority: 2] {ICMP} 192.168.210.160 -> 192.168.210.129
06/01-11:54:51.059715  [**] [1:10000003:1] ICMP Ping of Death [**] [Classification: Detection of a Denial of Service Attack] [Priority: 2] {ICMP} 192.168.210.160 -> 192.168.210.129
06/01-11:54:51.325544  [**] [1:10000003:1] ICMP Ping of Death [**] [Classification: Detection of a Denial of Service Attack] [Priority: 2] {ICMP} 192.168.210.160 -> 192.168.210.129
06/01-11:54:51.949729  [**] [1:10000003:1] ICMP Ping of Death [**] [Classification: Detection of a Denial of Service Attack] [Priority: 2] {ICMP} 192.168.210.160 -> 192.168.210.129
06/01-11:54:52.073782  [**] [1:10000003:1] ICMP Ping of Death [**] [Classification: Detection of a Denial of Service Attack] [Priority: 2] {ICMP} 192.168.210.160 -> 192.168.210.129
06/01-11:54:52.339223  [**] [1:10000003:1] ICMP Ping of Death [**] [Classification: Detection of a Denial of Service Attack] [Priority: 2] {ICMP} 192.168.210.160 -> 192.168.210.129
06/01-11:54:52.963072  [**] [1:10000003:1] ICMP Ping of Death [**] [Classification: Detection of a Denial of Service Attack] [Priority: 2] {ICMP} 192.168.210.160 -> 192.168.210.129
06/01-11:54:53.087812  [**] [1:10000003:1] ICMP Ping of Death [**] [Classification: Detection of a Denial of Service Attack] [Priority: 2] {ICMP} 192.168.210.160 -> 192.168.210.129
06/01-11:54:53.353618  [**] [1:10000003:1] ICMP Ping of Death [**] [Classification: Detection of a Denial of Service Attack] [Priority: 2] {ICMP} 192.168.210.160 -> 192.168.210.129
06/01-11:54:53.977237  [**] [1:10000003:1] ICMP Ping of Death [**] [Classification: Detection of a Denial of Service Attack] [Priority: 2] {ICMP} 192.168.210.160 -> 192.168.210.129
06/01-11:54:54.102547  [**] [1:10000003:1] ICMP Ping of Death [**] [Classification: Detection of a Denial of Service Attack] [Priority: 2] {ICMP} 192.168.210.160 -> 192.168.210.129
06/01-11:54:54.367066  [**] [1:10000003:1] ICMP Ping of Death [**] [Classification: Detection of a Denial of Service Attack] [Priority: 2] {ICMP} 192.168.210.160 -> 192.168.210.129
06/01-11:54:54.991903  [**] [1:10000003:1] ICMP Ping of Death [**] [Classification: Detection of a Denial of Service Attack] [Priority: 2] {ICMP} 192.168.210.160 -> 192.168.210.129
06/01-11:54:55.117021  [**] [1:10000003:1] ICMP Ping of Death [**] [Classification: Detection of a Denial of Service Attack] [Priority: 2] {ICMP} 192.168.210.160 -> 192.168.210.129
06/01-11:54:55.381545  [**] [1:10000003:1] ICMP Ping of Death [**] [Classification: Detection of a Denial of Service Attack] [Priority: 2] {ICMP} 192.168.210.160 -> 192.168.210.129
```