

BAN CƠ YẾU CHÍNH PHỦ
HỌC VIỆN KỸ THUẬT MẬT MÃ



MODULE THỰC HÀNH
AN TOÀN MẠNG MÁY TÍNH

BÀI THỰC HÀNH SỐ 03

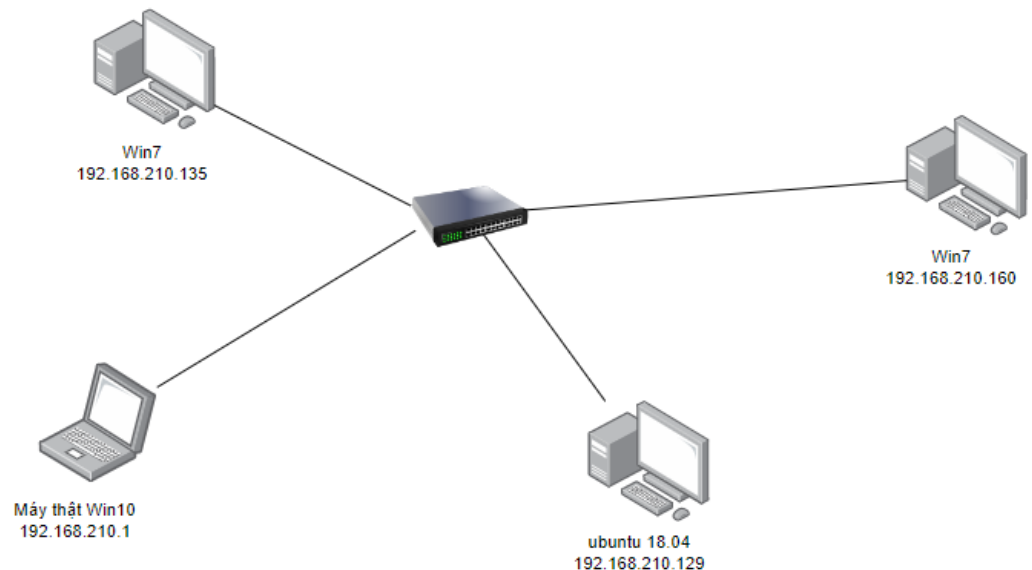
Triển khai hệ thống phát hiện xâm nhập Snort

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

```

Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-01 11:03 SE Asia Standard Time
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 11:03
Completed NSE at 11:03, 0.00s elapsed
Initiating NSE at 11:03
Completed NSE at 11:03, 0.00s elapsed
Initiating NSE at 11:03
Completed NSE at 11:03, 0.00s elapsed
Initiating ARP Ping Scan at 11:03
Scanning 192.168.210.135 [1 port]
Completed ARP Ping Scan at 11:03, 0.10s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 11:03
Completed Parallel DNS resolution of 1 host. at 11:03, 0.01s elapsed
Initiating SYN Stealth Scan at 11:03
Scanning 192.168.210.135 [1000 ports]
Discovered open port 445/tcp on 192.168.210.135
Discovered open port 135/tcp on 192.168.210.135
Discovered open port 139/tcp on 192.168.210.135
Increasing send delay for 192.168.210.135 from 0 to 5 due to 36 out of 89 dropped probes since last increase.
Increasing send delay for 192.168.210.135 from 5 to 10 due to 11 out of 25 dropped probes since last increase.
Discovered open port 49157/tcp on 192.168.210.135
Discovered open port 49153/tcp on 192.168.210.135
Discovered open port 49155/tcp on 192.168.210.135
Discovered open port 49154/tcp on 192.168.210.135
Discovered open port 49152/tcp on 192.168.210.135
Discovered open port 49156/tcp on 192.168.210.135
Completed SYN Stealth Scan at 11:03, 12.26s elapsed (1000 total ports)
Initiating Service scan at 11:03

```

Kết quả

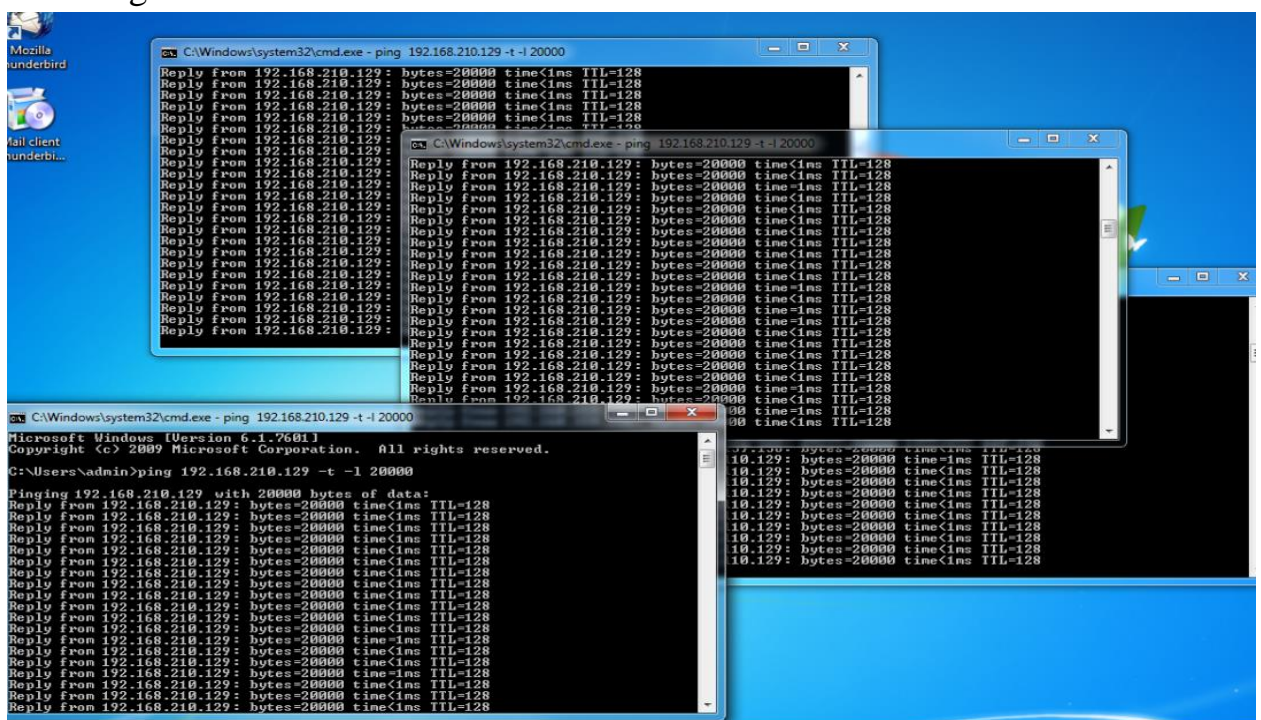
```
att@web: ~  
File Edit View Search Terminal Help  
Detection of a Network Scan] [Priority: 3] {TCP} 192.168.210.1:7417 -> 192.168.210.135:139  
01/06-11:49:16.257230  [**] [1:10000002:1] SYN scan attack [**] [Classification: Detection of a Network Scan] [Priority: 3] {TCP} 192.168.210.1:7418 -> 192.168.210.135:445  
01/06-11:49:16.257233  [**] [1:10000002:1] SYN scan attack [**] [Classification: Detection of a Network Scan] [Priority: 3] {TCP} 192.168.210.1:7419 -> 192.168.210.135:49152  
01/06-11:49:16.257236  [**] [1:10000002:1] SYN scan attack [**] [Classification: Detection of a Network Scan] [Priority: 3] {TCP} 192.168.210.1:7420 -> 192.168.210.135:49153  
01/06-11:49:16.257316  [**] [1:10000002:1] SYN scan attack [**] [Classification: Detection of a Network Scan] [Priority: 3] {TCP} 192.168.210.1:7421 -> 192.168.210.135:49154  
01/06-11:49:16.257444  [**] [1:10000002:1] SYN scan attack [**] [Classification: Detection of a Network Scan] [Priority: 3] {TCP} 192.168.210.1:7422 -> 192.168.210.135:49155  
01/06-11:49:16.257448  [**] [1:10000002:1] SYN scan attack [**] [Classification: Detection of a Network Scan] [Priority: 3] {TCP} 192.168.210.1:7423 -> 192.168.210.135:49156  
01/06-11:49:16.257592  [**] [1:10000002:1] SYN scan attack [**] [Classification: Detection of a Network Scan] [Priority: 3] {TCP} 192.168.210.1:7424 -> 192.168.210.135:49157
```

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

```
att@web: ~  
File Edit View Search Terminal Help  
GNU nano 2.9.3 /etc/snort/rules/local.rules  
# $Id: local.rules,v 1.11 2004/07/23 20:15:44 bmc Exp $  
# -----  
# LOCAL RULES  
# -----  
# This file intentionally does not come with signatures. Put your local  
# additions here.  
alert icmp any any -> $HOME_NET (msg:"ICMP Ping of Death"; itype:8; dsize:>1000; detection_filter:track by_src, count 10, seconds 10; classtype:denial-of-service;  
sid:10000003; rev:1;)  
#-----  
#NXK  
Help
```

Tấn công



Kết quả

[illegible]