HỌC VIỆN KỸ THUẬT MẬT MÃ

KHOA AN TOÀN THÔNG TIN

BÀI THỰC HÀNH SỐ 03

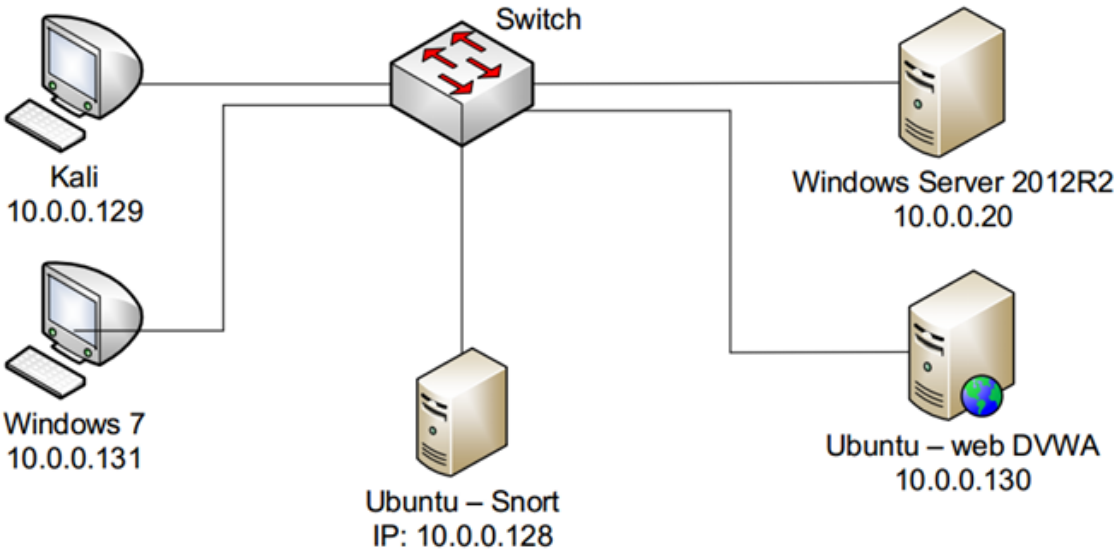
TRIỂN KHAI HỆ THỐNG PHÁT HIỆN XÂM NHẬP SNORT

Sinh viên thực hiện: **Nguyễn Hữu Văn – AT190157**

Hà Nội, 2025

Mục Lục

I. Mô hình cài đặt



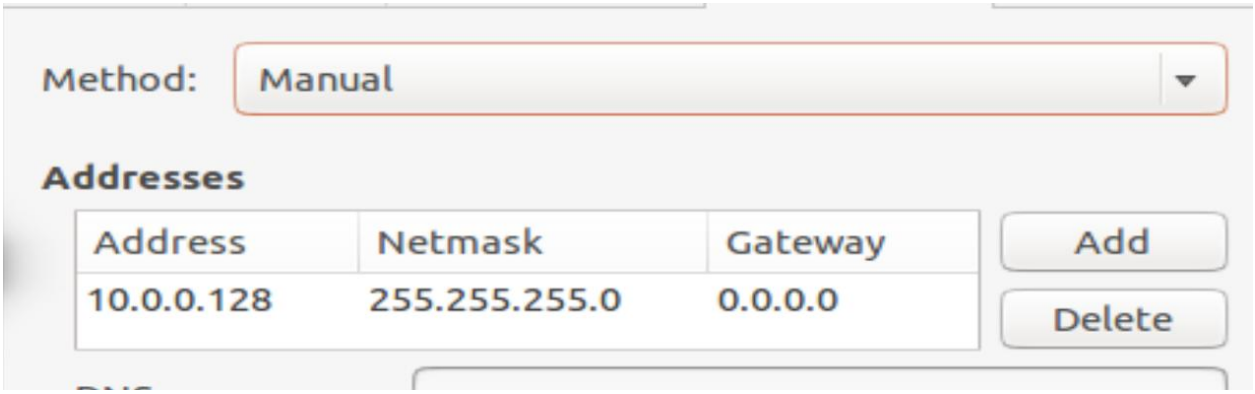
Đặt máy snort là card NAT để có thể kết nối internet, tiến hành cài snort

Cài đặt Snort trên máy Ubuntu Snort thành công:

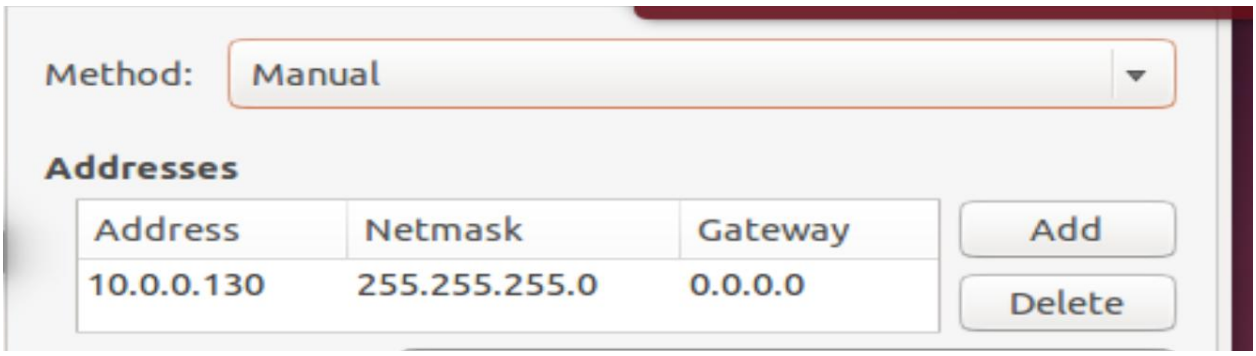
```
at190157@at190157:~$ snort -V

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.20 GRE (Build 82)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014-2022 Cisco and/or its affiliates. All rights reserved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using libpcap version 1.10.4 (with TPACKET_V3)
           Using PCRE version: 8.39 2016-06-14
           Using ZLIB version: 1.3
```

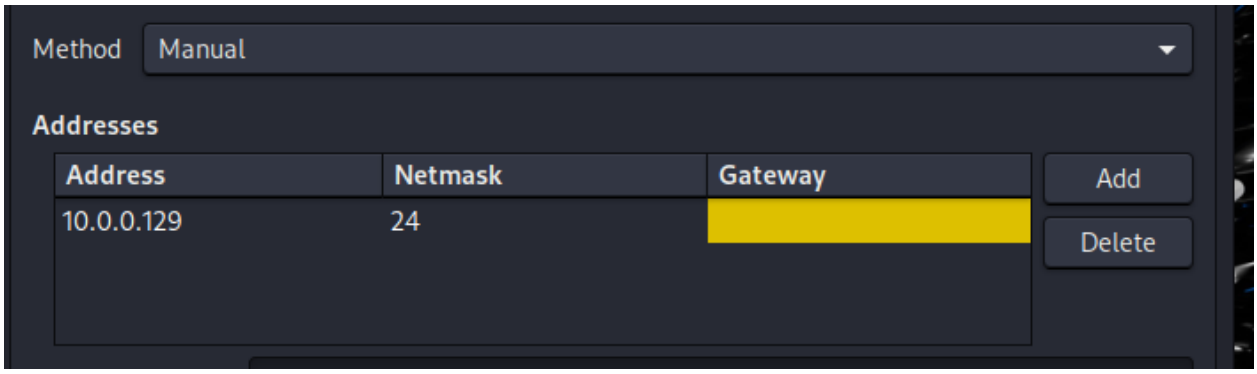
Đặt IP cho máy Ubuntu Snort:



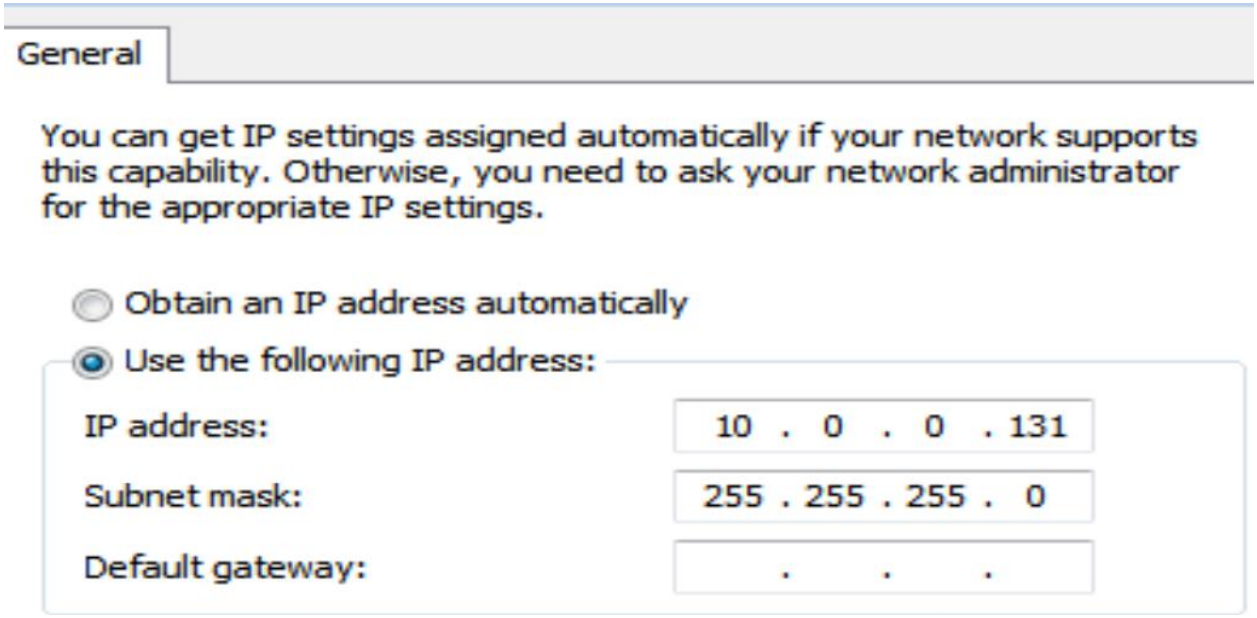
Đặt IP cho máy Ubuntu DVWA:



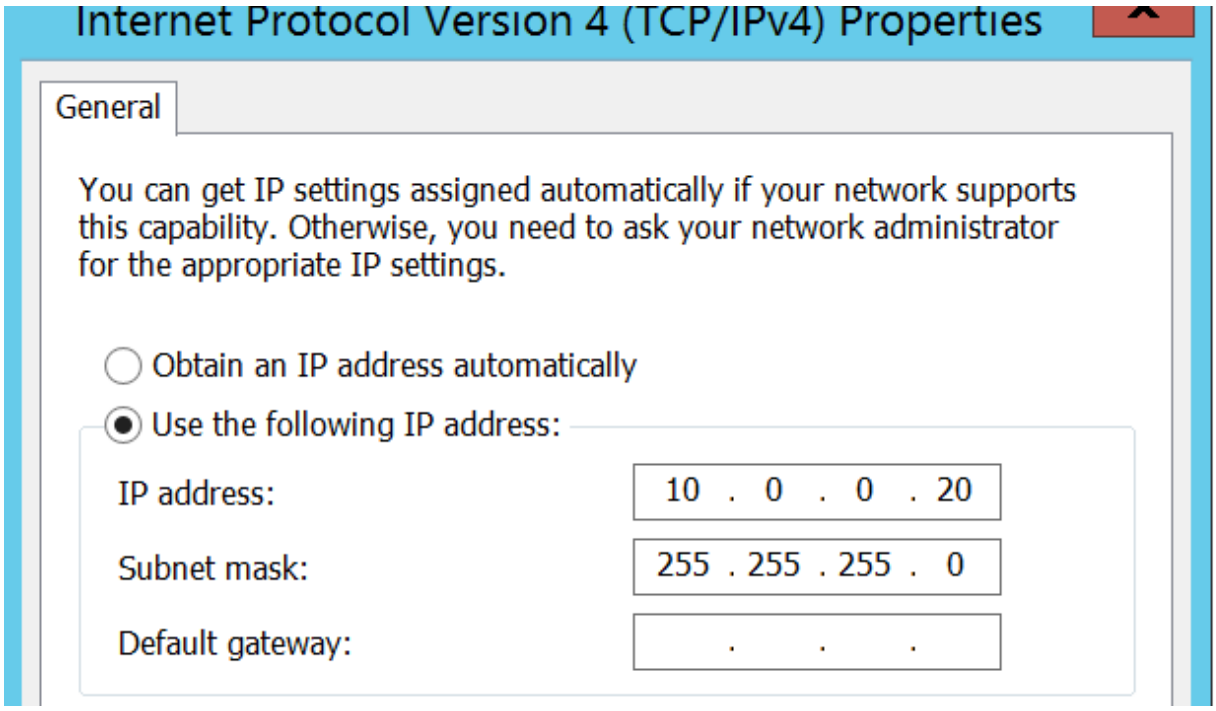
Đặt IP cho máy Kali:



Đặt IP cho máy Win 7:



Đặt IP cho máy Win server 2012:



Cấu hình Snort chạy ở chế độ phát hiện xâm nhập mạng:

Tạo các thư mục cho Snort:

```
at190157@at190157:~$ sudo mkdir /etc/snort
at190157@at190157:~$ sudo mkdir /etc/snort/rules
at190157@at190157:~$ sudo mkdir /etc/snort/rules/iplists
at190157@at190157:~$ sudo mkdir /etc/snort/preproc_rules
at190157@at190157:~$ sudo mkdir /usr/local/lib/snort_dynamicrules
at190157@at190157:~$ sudo mkdir /etc/snort/so_rules
```

Tạo các tệp tin chứa tập luật cơ bản cho Snort:

```
at190157@at190157:~$ sudo touch /etc/snort/rules/iplists/black_list.rules
at190157@at190157:~$ sudo touch /etc/snort/rules/iplists/white_list.rules
at190157@at190157:~$ ]sudo touch /etc/snort/rules/local.rules
Floppy Disk
sudo' not found, did you mean:
 'sudo' from deb sudo (1.9.14p2-1ubuntu1)
  command 'sudo' from deb sudo-ldap (1.9.14p2-1ubuntu1)
Try: sudo apt install <deb name>
at190157@at190157:~$ sudo touch /etc/snort/rules/local.rules
at190157@at190157:~$ sudo touch /etc/snort/sid-msg.map
```

Tạo thư mục chứa log:

```
at190157@at190157:~$ sudo mkdir /var/log/snort
at190157@at190157:~$ sudo mkdir /var/log/snort/archived_logs
```

Tạo các bản sao tệp tin cấu hình của Snort:

```
at190157@at190157:~/snort_src/snort-2.9.20/etc$ sudo cp *.conf* /etc/snort
Trash 57@at190157:~/snort_src/snort-2.9.20/etc$ sudo cp *.map /etc/snort
at190157@at190157:~/snort_src/snort-2.9.20/etc$ sudo cp *.dtd /etc/snort
at190157@at190157:~/snort_src/snort-2.9.20/etc$ cd ~/snort_src/snort-2.9.20/src/dynamic-preprocessors/build/usr/local/
lib/snort_dynamicpreprocessor/
at190157@at190157:~/snort_src/snort-2.9.20/src/dynamic-preprocessors/build/usr/local/lib/snort_dynamicpreprocessor$ su
do cp * /usr/local/lib/snort_dynamicpreprocessor/
at190157@at190157:~/snort_src/snort-2.9.20/src/dynamic-preprocessors/build/usr/local/lib/snort_dynamicpreprocessor$
```

Chỉnh sửa các tham số trong tệp tin: /etc/snort/snort.conf

```
# Setup the network addresses you are protecting
ipvar HOME_NET 10.0.0.0/24

# Set up the external network addresses. Leave as "ar
ipvar EXTERNAL_NET !$HOME_NET
```

```
var RULE_PATH /etc/snort/rules
var SO_RULE_PATH /etc/snort/so_rules
var PREPROC_RULE_PATH /etc/snort/preproc_rules

# If you are using reputation preprocessor set these
# Currently there is a bug with relative paths, they are
# not relative to snort.conf like the above variables
# This is completely inconsistent with how other vars wo
# Set the absolute path appropriately
var WHITE_LIST_PATH /etc/snort/rules/iplists
var BLACK_LIST_PATH /etc/snort/rules/iplists
```

```
# site specific rules
include $RULE_PATH/local.rules
```

Kiểm tra sự hoạt động của Snort:

```
   o"  )~   Version 2.9.20 GRE (Build 82)
    ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact
            Copyright (C) 2014-2022 Cisco and/or its affiliates. All rights
            Copyright (C) 1998-2013 Sourcefire, Inc., et al.
            Using libpcap version 1.10.4 (with TPACKET_V3)
            Using PCRE version: 8.39 2016-06-14
            Using ZLIB version: 1.3

            Rules Engine: SF_SNORT_DETECTION_ENGINE  Version 3.2  <Build 1>
            Preprocessor Object: SF_DCERPC2  Version 1.0  <Build 3>
            Preprocessor Object: SF_SSH  Version 1.1  <Build 3>
            Preprocessor Object: SF_SIP  Version 1.1  <Build 1>
            Preprocessor Object: SF_DNS  Version 1.1  <Build 4>
            Preprocessor Object: SF_REPUTATION  Version 1.1  <Build 1>
            Preprocessor Object: SF_POP  Version 1.0  <Build 1>
            Preprocessor Object: SF_DNP3  Version 1.1  <Build 1>
CDROM       Preprocessor Object: SF_FTPTELNET  Version 1.2  <Build 13>
            Preprocessor Object: SF_SMTP  Version 1.1  <Build 9>
            Preprocessor Object: SF_SSLPP  Version 1.1  <Build 4>
            Preprocessor Object: SF_S7COMMPLUS  Version 1.0  <Build 1>
            Preprocessor Object: SF_MODBUS  Version 1.1  <Build 1>
            Preprocessor Object: SF_IMAP  Version 1.0  <Build 1>
            Preprocessor Object: SF_SDF  Version 1.1  <Build 1>
            Preprocessor Object: SF_GTP  Version 1.1  <Build 1>

Total snort Fixed Memory Cost - MaxRss:46712
Snort successfully validated the configuration!
Snort exiting
at190157@at190157:~$
```

II. Các kịch bản thực hiện tấn công và phát hiện

Kịch bản 1: Phát hiện tấn công dò quét

Cấu hình alert cho icmp:

```
                                                        Jun 18  15:00
                                        at190157@at190157: /etc/snort/rules
  GNU nano 7.2                                                  icmp.rules *
alert icmp any any -> any any (msg:"Nmap ICMP scaning"; sid:10000001; rev:1;)
```

Chạy snort ở chế độ lắng nghe và phát hiện:

```
at190157@at190157:~$ sudo snort -i ens37 -c /etc/snort/snort.conf
Running in IDS mode

        --== Initializing Snort ==--
```

Sử dụng Nmap trên Kali dò quét các máy tính đang chạy:

```
┌──(at190157㉿kali)-[~/Desktop]
└─$ nmap -sP 10.0.0.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-06-18 04:17 EDT
Nmap scan report for 10.0.0.20
Host is up (0.00082s latency).
MAC Address: 00:0C:29:9D:5B:F2 (VMware)
Nmap scan report for 10.0.0.128
Host is up (0.0032s latency).
MAC Address: 00:0C:29:2D:D6:D6 (VMware)
Nmap scan report for 10.0.0.131
Host is up (0.00055s latency).
MAC Address: 00:0C:29:54:F8:64 (VMware)
Nmap scan report for 10.0.0.129
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 28.02 seconds
```

Đã phát hiện các máy ảo
Kết qủa giao diện hiển thị của lệnh tail:

```
at190157@at190157:~$  tail -f /var/log/snort/alert
[**] [1:10000001:1] Nmap ICMP scaning [**]
[Priority: 0]
06/18-15:16:19.433352 fe80::6cd9:d73f:f4c5:c9c8 -> ff02::16
IPV6-ICMP TTL:1 TOS:0x0 ID:256 IpLen:40 DgmLen:76

[**] [1:10000001:1] Nmap ICMP scaning [**]
[Priority: 0]
06/18-15:16:30.631038 fe80::6cd9:d73f:f4c5:c9c8 -> ff02::2
IPV6-ICMP TTL:255 TOS:0x0 ID:0 IpLen:40 DgmLen:48

[**] [1:10000001:1] Nmap ICMP scaning [**]
[Priority: 0]
06/18-15:17:04.019595 fe80::6cd9:d73f:f4c5:c9c8 -> ff02::2
IPV6-ICMP TTL:255 TOS:0x0 ID:0 IpLen:40 DgmLen:48

[**] [1:10000001:1] Nmap ICMP scaning [**]
[Priority: 0]
06/18-15:18:07.805097 fe80::6cd9:d73f:f4c5:c9c8 -> ff02::2
IPV6-ICMP TTL:255 TOS:0x0 ID:0 IpLen:40 DgmLen:48

[**] [1:10000001:1] Nmap ICMP scaning [**]
[Priority: 0]
06/18-15:18:22.748960 fe80::677f:c5a9:cec1:e4aa -> ff02::2
IPV6-ICMP TTL:255 TOS:0x0 ID:0 IpLen:40 DgmLen:48
```

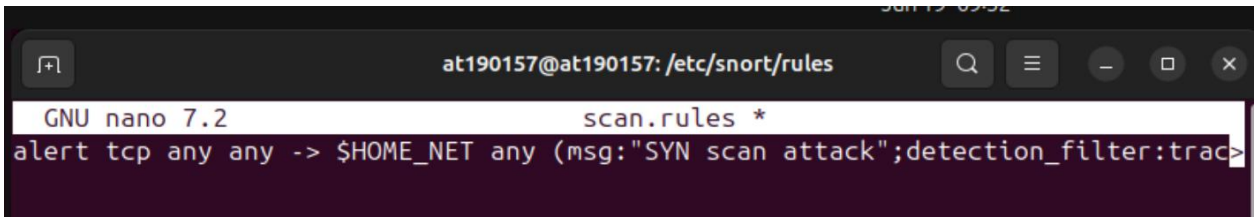
Giao diện thống kê của snort:

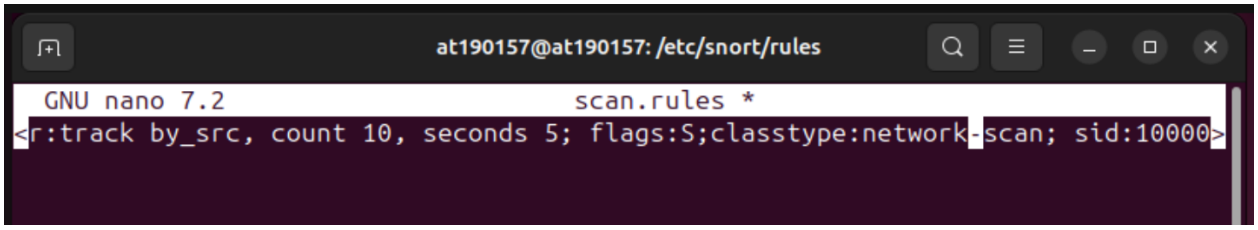
```
===============================================================================
Memory usage summary:
  Total non-mmapped bytes (arena):       7139328
  Bytes in mapped regions (hblkhd):      30130176
  Total allocated space (uordblks):      4931072
  Total free space (fordblks):           2208256
  Topmost releasable block (keepcost):   118016
===============================================================================
Packet I/O Totals:
   Received:         1974
   Analyzed:         1974 (100.000%)
    Dropped:            0 (  0.000%)
   Filtered:            0 (  0.000%)
Outstanding:            0 (  0.000%)
   Injected:            0
===============================================================================
Breakdown by protocol (includes rebuilt packets):
        Eth:         1974 (100.000%)
       VLAN:            0 (  0.000%)
        IP4:         1059 ( 53.647%)
       Frag:            0 (  0.000%)
       ICMP:            3 (  0.152%)
        UDP:          926 ( 46.910%)
        TCP:           85 (  4.306%)
        IP6:          202 ( 10.233%)
    IP6 Ext:          241 ( 12.209%)
   IP6 Opts:           39 (  1.976%)
      Frag6:            0 (  0.000%)
      ICMP6:           65 (  3.293%)
```

```
      Total:          1974
===============================================================
Action Stats:
     Alerts:            68 (  3.445%)
     Logged:            68 (  3.445%)
     Passed:             0 (  0.000%)
Limits:
      Match:             0
      Queue:             0
        Log:             0
      Event:             0
      Alert:             0
```

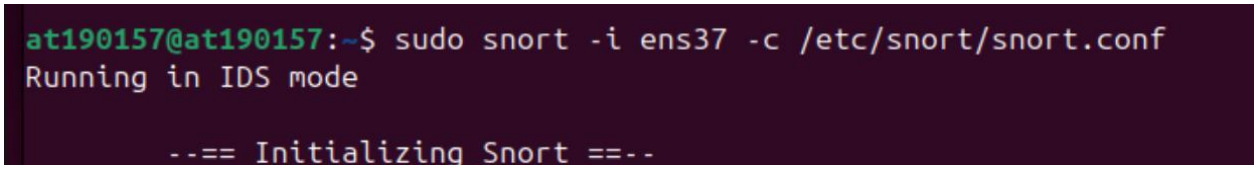
Kịch bản 2: Phát hiện tấn công dò quét dịch vụ và cổng:

Cấu hình alert cho scan:

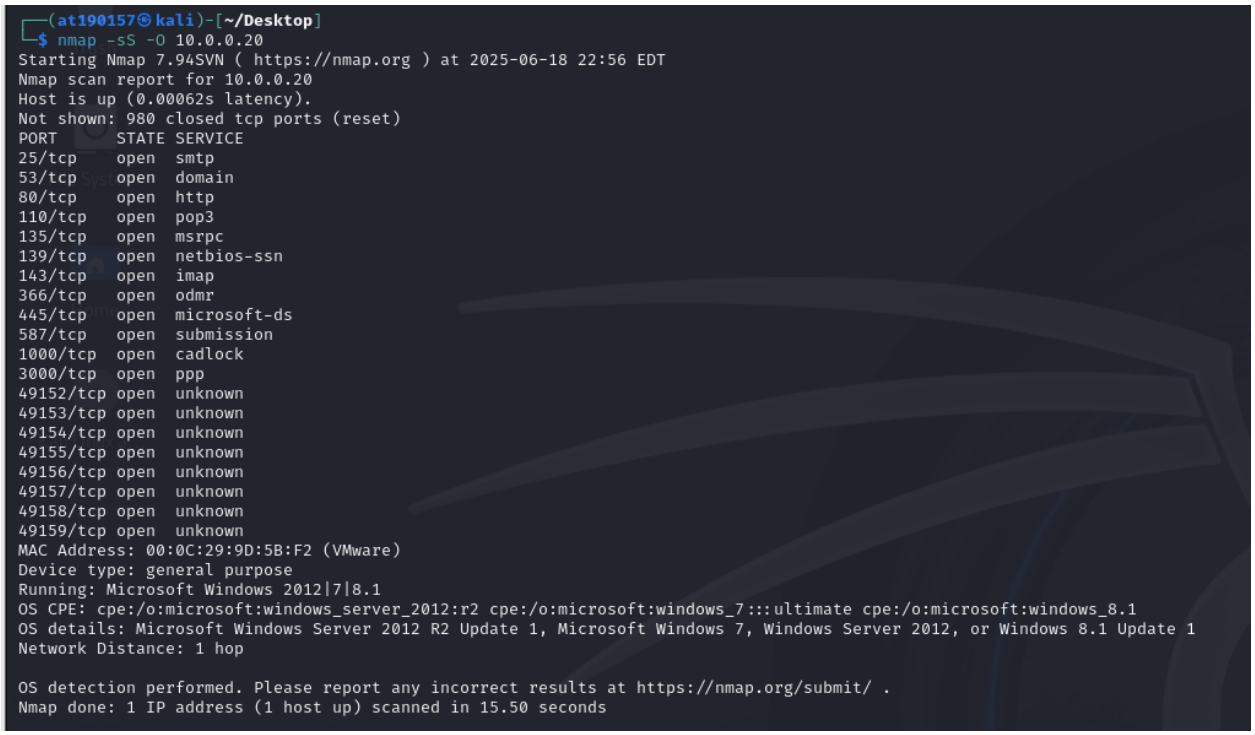




Chạy snort ở chế độ lắng nghe và phát hiện:



Sử dụng Nmap trên Kali tấn công dò quét tới Win server 2012:



Sử dụng lệnh tail như kịch bản 1 xem trực tiếp sự kiện phát hiện tại máy Snort:

```
[**] [1:10000002:1] SYN scan attack [**]
[Classification: Detection of a Network Scan] [Priority: 3]
06/19-09:56:43.598192 10.0.0.129:49342 -> 10.0.0.20:6025
TCP TTL:54 TOS:0x0 ID:51264 IpLen:20 DgmLen:44
******S* Seq: 0x58651078  Ack: 0x0  Win: 0x400  TcpLen: 24
TCP Options (1) => MSS: 1460

[**] [1:10000002:1] SYN scan attack [**]
[Classification: Detection of a Network Scan] [Priority: 3]
06/19-09:56:43.598623 10.0.0.129:49342 -> 10.0.0.20:6100
TCP TTL:54 TOS:0x0 ID:29909 IpLen:20 DgmLen:44
******S* Seq: 0x58651078  Ack: 0x0  Win: 0x400  TcpLen: 24
TCP Options (1) => MSS: 1460

[**] [1:10000002:1] SYN scan attack [**]
[Classification: Detection of a Network Scan] [Priority: 3]
06/19-09:56:43.598798 10.0.0.129:49342 -> 10.0.0.20:1070
TCP TTL:38 TOS:0x0 ID:49326 IpLen:20 DgmLen:44
******S* Seq: 0x58651078  Ack: 0x0  Win: 0x400  TcpLen: 24
TCP Options (1) => MSS: 1460
```

Kịch bản 3. Phát hiện tấn công từ chối dịch vụ ICMP Ping of Death

Thiết lập tập luật phát hiện cho Snort:

```
at190157@at190157: /etc/snort/rules
 GNU nano 7.2                    icmppingofdeath.rules *
alert icmp any any -> $HOME_NET any (msg:"ICMP Ping of Death";itype:8; dsize:>1>
```

```
at190157@at190157: /etc/snort/rules
 GNU nano 7.2                    icmppingofdeath.rules *
<ze:>1000; detection_filter:track by_src, count 1000,seconds 10; classtype:denia>
```

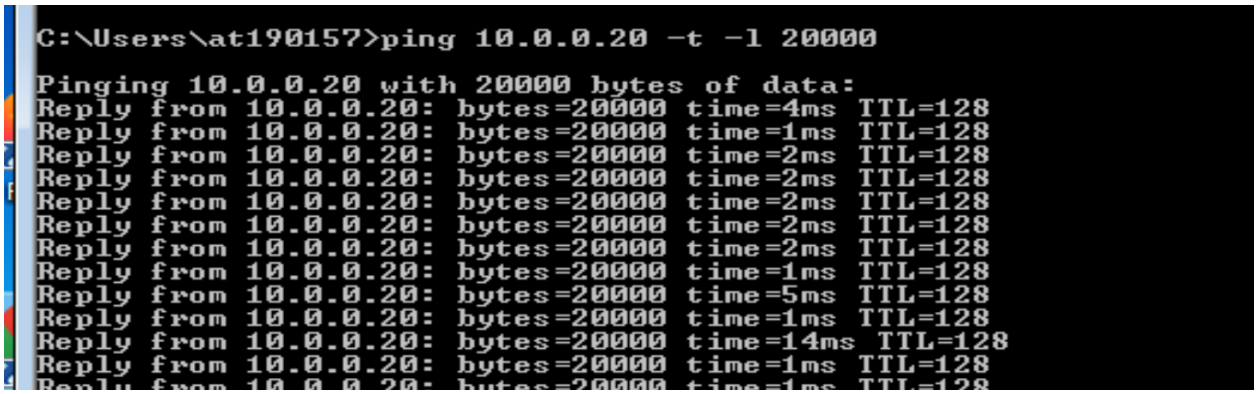
```
at190157@at190157: /etc/snort/rules
 GNU nano 7.2                    icmppingofdeath.rules *
<:denial-of-service; sid:10000003; rev:1;)
```

Chạy snort ở chế độ lắng nghe và phát hiện:

```
at190157@at190157:~$ sudo snort -i ens37 -c /etc/snort/snort.conf
Running in IDS mode

        --== Initializing Snort ==--
```

Tấn công Tại máy tính Windows 7, sử dụng chương trình dòng lệnh CMD để ping với số lượng lớn các gói tin ICMP có kích thước lớn tới máy chủ Windows Server



Sử dụng lệnh tail như kịch bản 1 xem trực tiếp sự kiện phát hiện tại máy Snort:

```
[**] [1:10000003:1] ICMP Ping of Death [**]
[Classification: Detection of a Denial of Service Attack] [Priority: 2]
06/19-10:16:32.911200 10.0.0.131 -> 10.0.0.20
ICMP TTL:128 TOS:0x0 ID:358 IpLen:20 DgmLen:20028
Type:8  Code:0  ID:1   Seq:158  ECHO

[**] [1:10000003:1] ICMP Ping of Death [**]
[Classification: Detection of a Denial of Service Attack] [Priority: 2]
06/19-10:16:33.441503 10.0.0.131 -> 10.0.0.20
ICMP TTL:128 TOS:0x0 ID:359 IpLen:20 DgmLen:20028
Type:8  Code:0  ID:1   Seq:159  ECHO

[**] [1:10000003:1] ICMP Ping of Death [**]
[Classification: Detection of a Denial of Service Attack] [Priority: 2]
06/19-10:16:33.908649 10.0.0.131 -> 10.0.0.20
ICMP TTL:128 TOS:0x0 ID:360 IpLen:20 DgmLen:20028
Type:8  Code:0  ID:1   Seq:160  ECHO

[**] [1:10000003:1] ICMP Ping of Death [**]
[Classification: Detection of a Denial of Service Attack] [Priority: 2]
06/19-10:16:34.908170 10.0.0.131 -> 10.0.0.20
ICMP TTL:128 TOS:0x0 ID:361 IpLen:20 DgmLen:20028
Type:8  Code:0  ID:1   Seq:161  ECHO
```

Với cảnh báo này người quản trị biết được rằng đang có cuộc tấn công dạng từ chối dịch vụ sử dụng giao thức ICMP có nguồn xuất phát từ máy có địa chỉ IP 10.0.0.131 tới máy đích 10.0.0.20

III. Kết luận

Với bài thực hành này đã hướng dẫn cài đặt phần mềm phát hiện xâm nhập Snort, cấu hình và chạy các tập luật để phát hiện một số dạng tấn công cơ bản lên tài nguyên mạng.