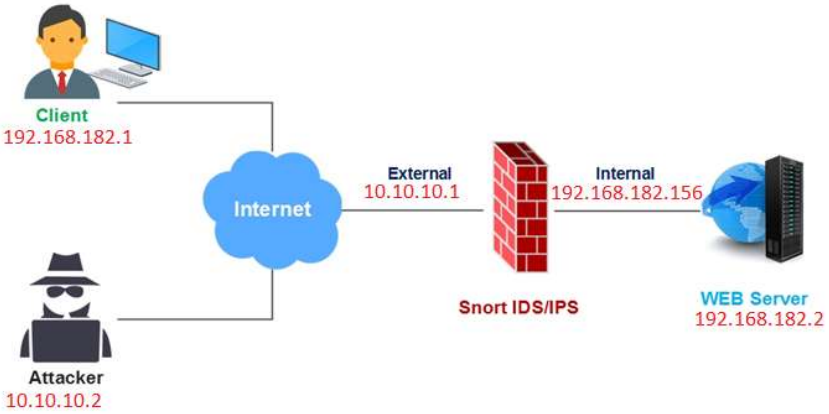
Báo Cáo Bảo Vệ Mạng Bằng Snort



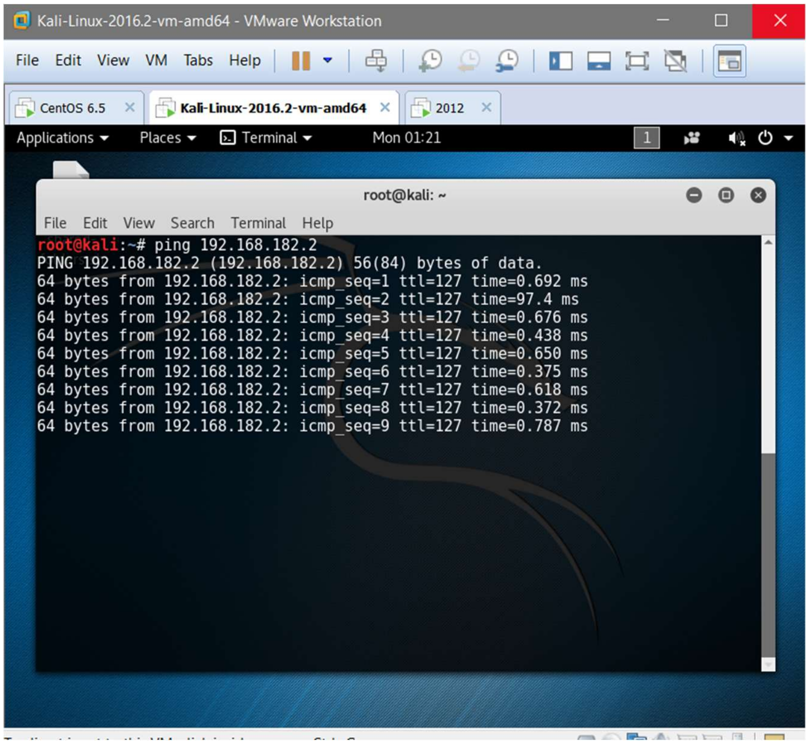
Mô hình lab thực hiện

- **VMware Workstation Pro 12**
- Các máy ảo:
  - ✓ **Client windows 10 : 192.168.182.1**
  - ✓ **Attacker Kali linux 2016.2 : 10.10.10.2**
  - ✓ **Snortd server centos 6.9 : 10.10.10.1**
    192.168.182.156
  - ✓ **Web server windows 2012 : 192.168.182.2**

1.Phát hiện ping

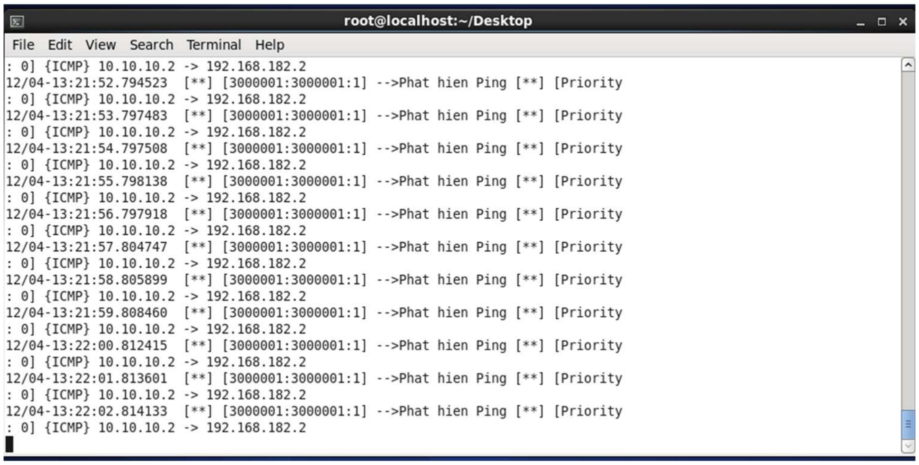
- Rules phát hiện ping vào /etc/rules/local.rules

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


Kali-Linux-2016.2-vm-amd64 - VMware Workstation
File Edit View VM Tabs Help
CentOS 6.5
Kali-Linux-2016.2-vm-amd64
2012
Applications
Places
Terminal
Mon 01:21
root@kali: ~
File Edit View Search Terminal Help

```
root@kali:~# ping 192.168.182.2
PING 192.168.182.2 (192.168.182.2) 56(84) bytes of data.
64 bytes from 192.168.182.2: icmp_seq=1 ttl=127 time=0.692 ms
64 bytes from 192.168.182.2: icmp_seq=2 ttl=127 time=97.4 ms
64 bytes from 192.168.182.2: icmp_seq=3 ttl=127 time=0.676 ms
64 bytes from 192.168.182.2: icmp_seq=4 ttl=127 time=0.438 ms
64 bytes from 192.168.182.2: icmp_seq=5 ttl=127 time=0.650 ms
64 bytes from 192.168.182.2: icmp_seq=6 ttl=127 time=0.375 ms
64 bytes from 192.168.182.2: icmp_seq=7 ttl=127 time=0.618 ms
64 bytes from 192.168.182.2: icmp_seq=8 ttl=127 time=0.372 ms
64 bytes from 192.168.182.2: icmp_seq=9 ttl=127 time=0.787 ms
```

Ping từ máy kali đến web 192.168.182.2



```
: 0] {ICMP} 10.10.10.2 -> 192.168.182.2
12/04-13:21:52.794523  [**] [3000001:3000001:1] -->Phat hien Ping [**] [Priority
: 0] {ICMP} 10.10.10.2 -> 192.168.182.2
12/04-13:21:53.797483  [**] [3000001:3000001:1] -->Phat hien Ping [**] [Priority
: 0] {ICMP} 10.10.10.2 -> 192.168.182.2
12/04-13:21:54.797508  [**] [3000001:3000001:1] -->Phat hien Ping [**] [Priority
: 0] {ICMP} 10.10.10.2 -> 192.168.182.2
12/04-13:21:55.798138  [**] [3000001:3000001:1] -->Phat hien Ping [**] [Priority
: 0] {ICMP} 10.10.10.2 -> 192.168.182.2
12/04-13:21:56.797918  [**] [3000001:3000001:1] -->Phat hien Ping [**] [Priority
: 0] {ICMP} 10.10.10.2 -> 192.168.182.2
12/04-13:21:57.804747  [**] [3000001:3000001:1] -->Phat hien Ping [**] [Priority
: 0] {ICMP} 10.10.10.2 -> 192.168.182.2
12/04-13:21:58.805899  [**] [3000001:3000001:1] -->Phat hien Ping [**] [Priority
: 0] {ICMP} 10.10.10.2 -> 192.168.182.2
12/04-13:21:59.808460  [**] [3000001:3000001:1] -->Phat hien Ping [**] [Priority
: 0] {ICMP} 10.10.10.2 -> 192.168.182.2
12/04-13:22:00.812415  [**] [3000001:3000001:1] -->Phat hien Ping [**] [Priority
: 0] {ICMP} 10.10.10.2 -> 192.168.182.2
12/04-13:22:01.813601  [**] [3000001:3000001:1] -->Phat hien Ping [**] [Priority
: 0] {ICMP} 10.10.10.2 -> 192.168.182.2
12/04-13:22:02.814133  [**] [3000001:3000001:1] -->Phat hien Ping [**] [Priority
: 0] {ICMP} 10.10.10.2 -> 192.168.182.2
```

Snortd đã phát hiện đc gói tin ping từ 10.10.10.2 chuyển đến 192.168.182.2

2.Test phát hiện và chặn ping of death

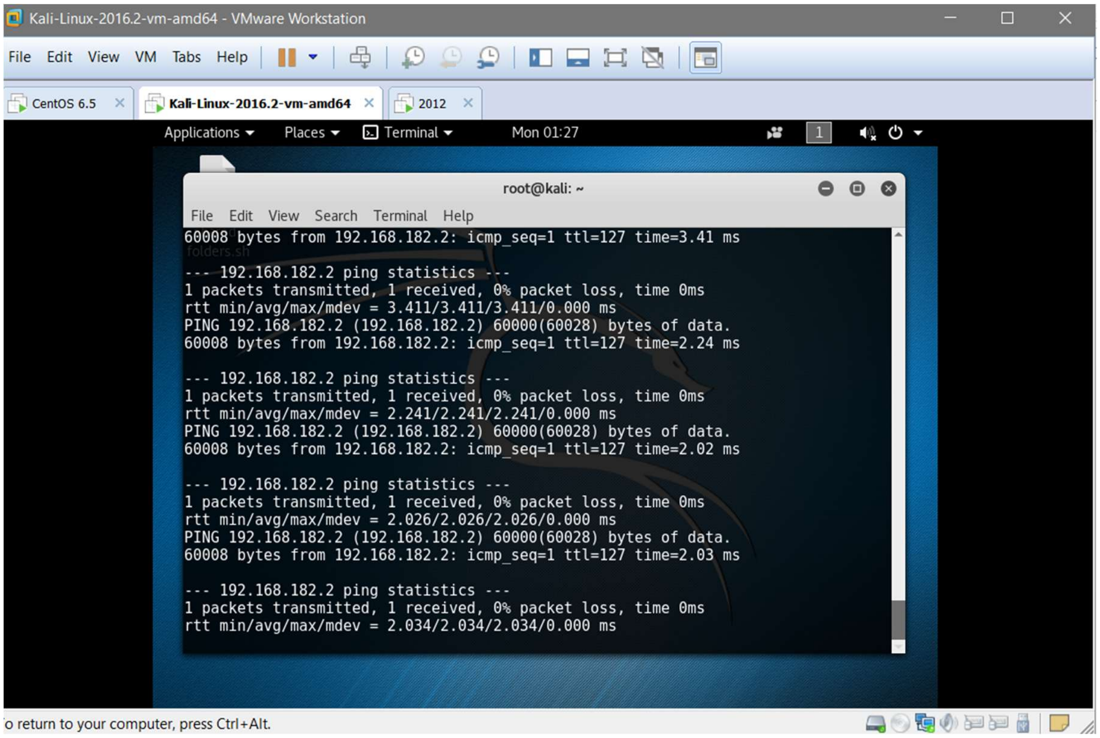
-Thêm rules phát hiện ping với 1 gói tin số lượng lớn ở đây để >20000

alert icmp any any -> $HOME_NET any (msg:"-->Phat hien Ping Of Dead !"; dsize:>20000; gid:1000001; sid:1000001;rev:1;)

-Thêm rules chặn gói tin ping

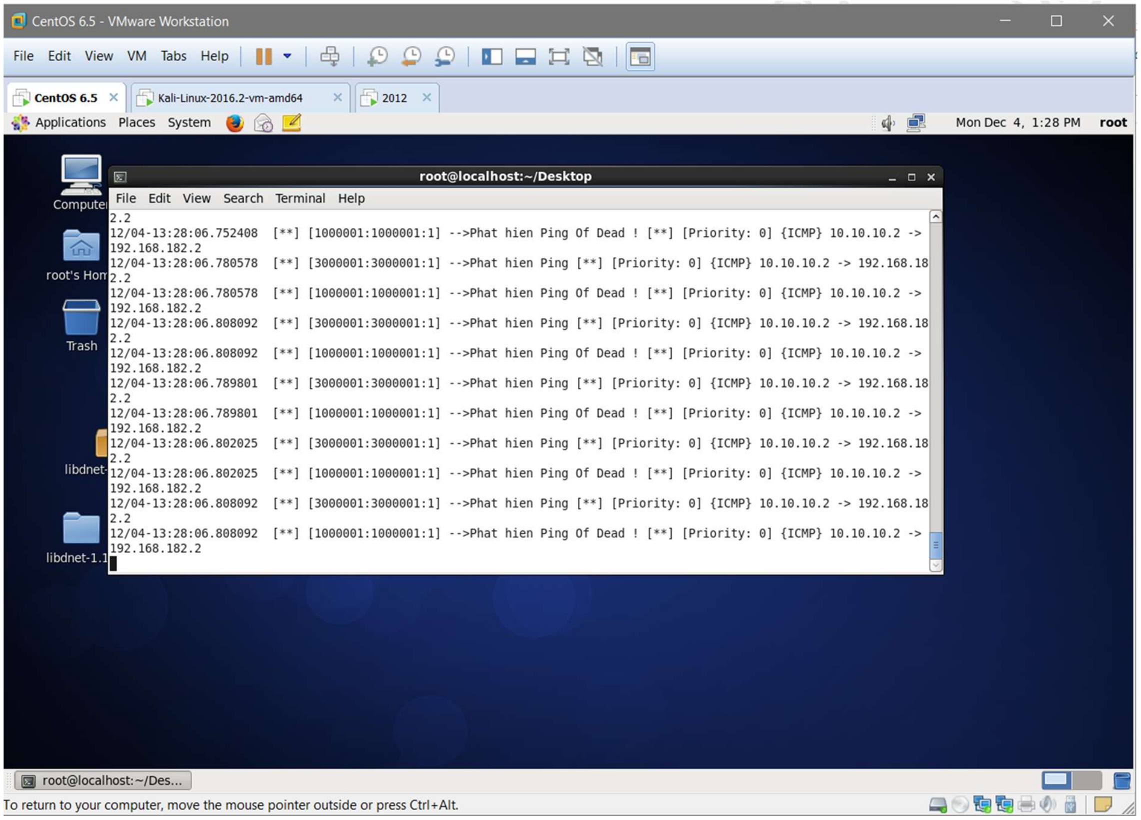
drop icmp any any -> $HOME_NET any (msg:"-->Da chan Ping Of Dead !"; dsize:>20000; gid:1000002; sid:1000002;rev:1;)

-Thực hiện ping of death từ kali đến web server (10.10.10.2 -> 192.168.182.2)


Kali-Linux-2016.2-vm-amd64 - VMware Workstation
File Edit View VM Tabs Help
CentOS 6.5
Kali-Linux-2016.2-vm-amd64
2012
Applications Places Terminal
Mon 01:27
root@kali: ~
File Edit View Search Terminal Help
o return to your computer, press Ctrl+Alt.

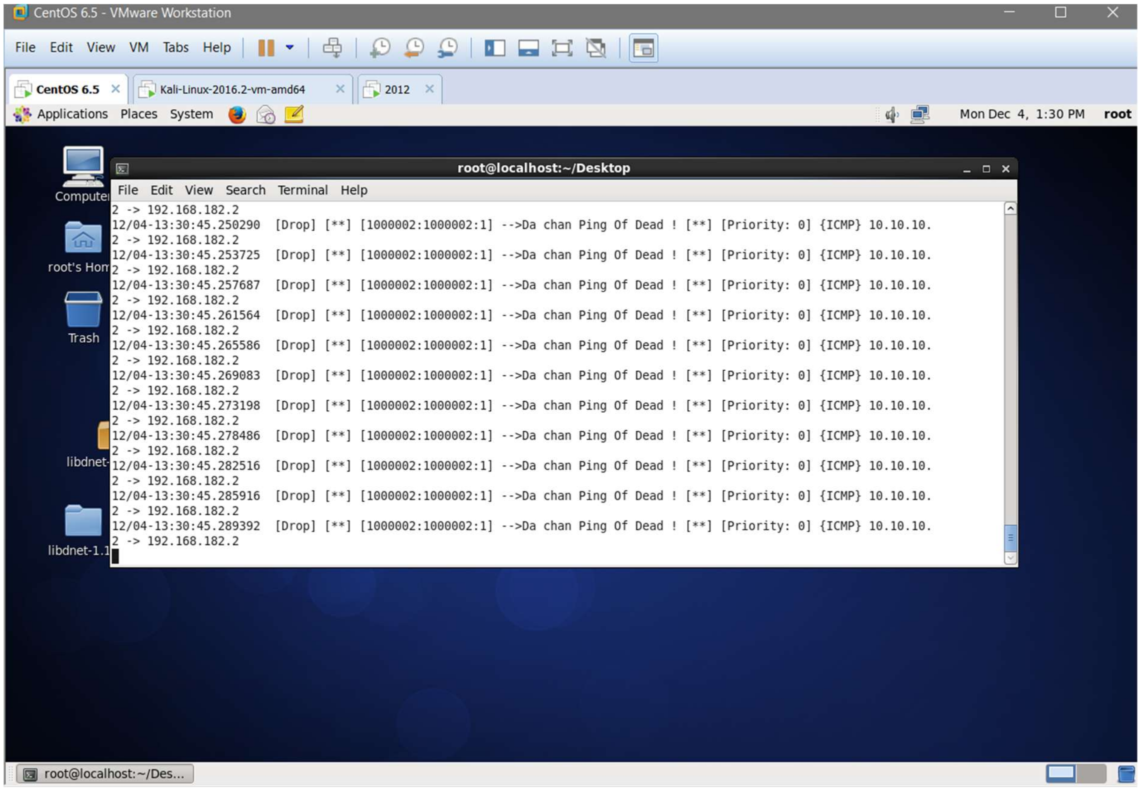
```
60008 bytes from 192.168.182.2: icmp_seq=1 ttl=127 time=3.41 ms

--- 192.168.182.2 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 3.411/3.411/3.411/0.000 ms
PING 192.168.182.2 (192.168.182.2) 60000(60028) bytes of data.
60008 bytes from 192.168.182.2: icmp_seq=1 ttl=127 time=2.24 ms

--- 192.168.182.2 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 2.241/2.241/2.241/0.000 ms
PING 192.168.182.2 (192.168.182.2) 60000(60028) bytes of data.
60008 bytes from 192.168.182.2: icmp_seq=1 ttl=127 time=2.02 ms

--- 192.168.182.2 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 2.026/2.026/2.026/0.000 ms
PING 192.168.182.2 (192.168.182.2) 60000(60028) bytes of data.
60008 bytes from 192.168.182.2: icmp_seq=1 ttl=127 time=2.03 ms

--- 192.168.182.2 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 2.034/2.034/2.034/0.000 ms
```

*Từ kali gửi thực hiện ping of death đến web **192.168.182.2***


CentOS 6.5 - VMware Workstation
File Edit View VM Tabs Help
CentOS 6.5
Kali-Linux-2016.2-vm-amd64
2012
Applications Places System
Mon Dec 4, 1:28 PM
root
Computer
root's Hom
Trash
libdnet
libdnet-1.1
root@localhost:~/Desktop
File Edit View Search Terminal Help
root@localhost:~/Des...
To return to your computer, move the mouse pointer outside or press Ctrl+Alt.

```
2.2
12/04-13:28:06.752408  [**] [1000001:1000001:1] -->Phat hien Ping Of Dead ! [**] [Priority: 0] {ICMP} 10.10.10.2 ->
192.168.182.2
12/04-13:28:06.780578  [**] [3000001:3000001:1] -->Phat hien Ping [**] [Priority: 0] {ICMP} 10.10.10.2 -> 192.168.18
2.2
12/04-13:28:06.780578  [**] [1000001:1000001:1] -->Phat hien Ping Of Dead ! [**] [Priority: 0] {ICMP} 10.10.10.2 ->
192.168.182.2
12/04-13:28:06.808092  [**] [3000001:3000001:1] -->Phat hien Ping [**] [Priority: 0] {ICMP} 10.10.10.2 -> 192.168.18
2.2
12/04-13:28:06.808092  [**] [1000001:1000001:1] -->Phat hien Ping Of Dead ! [**] [Priority: 0] {ICMP} 10.10.10.2 ->
192.168.182.2
12/04-13:28:06.789801  [**] [3000001:3000001:1] -->Phat hien Ping [**] [Priority: 0] {ICMP} 10.10.10.2 -> 192.168.18
2.2
12/04-13:28:06.789801  [**] [1000001:1000001:1] -->Phat hien Ping Of Dead ! [**] [Priority: 0] {ICMP} 10.10.10.2 ->
192.168.182.2
12/04-13:28:06.802025  [**] [3000001:3000001:1] -->Phat hien Ping [**] [Priority: 0] {ICMP} 10.10.10.2 -> 192.168.18
2.2
12/04-13:28:06.802025  [**] [1000001:1000001:1] -->Phat hien Ping Of Dead ! [**] [Priority: 0] {ICMP} 10.10.10.2 ->
192.168.182.2
12/04-13:28:06.808092  [**] [3000001:3000001:1] -->Phat hien Ping [**] [Priority: 0] {ICMP} 10.10.10.2 -> 192.168.18
2.2
12/04-13:28:06.808092  [**] [1000001:1000001:1] -->Phat hien Ping Of Dead ! [**] [Priority: 0] {ICMP} 10.10.10.2 ->
192.168.182.2
```

*Phát hiện gói Tin **Ping of Death***


CentOS 6.5 - VMware Workstation
File Edit View VM Tabs Help
CentOS 6.5
Kali-Linux-2016.2-vm-amd64
2012
Applications Places System
Mon Dec 4, 1:30 PM
root
Computer
root's Hom
Trash
libdnet-
libdnet-1.1
root@localhost:~/Desktop
File Edit View Search Terminal Help
root@localhost:~/Des...

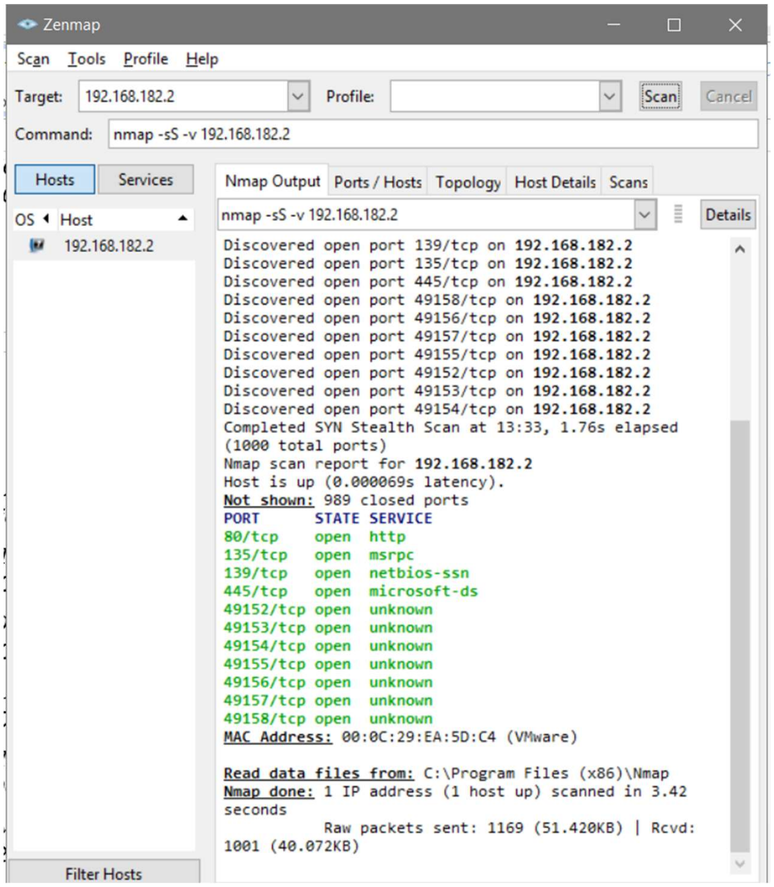
```
2 -> 192.168.182.2
12/04-13:30:45.250290  [Drop] [**] [1000002:1000002:1] -->Da chan Ping Of Dead ! [**] [Priority: 0] {ICMP} 10.10.10.
2 -> 192.168.182.2
12/04-13:30:45.253725  [Drop] [**] [1000002:1000002:1] -->Da chan Ping Of Dead ! [**] [Priority: 0] {ICMP} 10.10.10.
2 -> 192.168.182.2
12/04-13:30:45.257687  [Drop] [**] [1000002:1000002:1] -->Da chan Ping Of Dead ! [**] [Priority: 0] {ICMP} 10.10.10.
2 -> 192.168.182.2
12/04-13:30:45.261564  [Drop] [**] [1000002:1000002:1] -->Da chan Ping Of Dead ! [**] [Priority: 0] {ICMP} 10.10.10.
2 -> 192.168.182.2
12/04-13:30:45.265586  [Drop] [**] [1000002:1000002:1] -->Da chan Ping Of Dead ! [**] [Priority: 0] {ICMP} 10.10.10.
2 -> 192.168.182.2
12/04-13:30:45.269083  [Drop] [**] [1000002:1000002:1] -->Da chan Ping Of Dead ! [**] [Priority: 0] {ICMP} 10.10.10.
2 -> 192.168.182.2
12/04-13:30:45.273198  [Drop] [**] [1000002:1000002:1] -->Da chan Ping Of Dead ! [**] [Priority: 0] {ICMP} 10.10.10.
2 -> 192.168.182.2
12/04-13:30:45.278486  [Drop] [**] [1000002:1000002:1] -->Da chan Ping Of Dead ! [**] [Priority: 0] {ICMP} 10.10.10.
2 -> 192.168.182.2
12/04-13:30:45.282516  [Drop] [**] [1000002:1000002:1] -->Da chan Ping Of Dead ! [**] [Priority: 0] {ICMP} 10.10.10.
2 -> 192.168.182.2
12/04-13:30:45.285916  [Drop] [**] [1000002:1000002:1] -->Da chan Ping Of Dead ! [**] [Priority: 0] {ICMP} 10.10.10.
2 -> 192.168.182.2
12/04-13:30:45.289392  [Drop] [**] [1000002:1000002:1] -->Da chan Ping Of Dead ! [**] [Priority: 0] {ICMP} 10.10.10.
2 -> 192.168.182.2
```

*Drop các gói tin ping of death từ **10.10.10.2** đến **192.168.182.2***

3.Phát hiện và Ngăn Chặn Nmap

-Rules phát hiện Nmap

```
alert tcp any any -> $HOME_NET any (msg:"-->Phat hien SYN FIN Scan ! "; flags: S;gid: 2000001;sid:2000001;)

alert tcp any any -> $HOME_NET any (msg:"-->Phat hien FIN Scan !"; flags: F;gid:2000002; sid:2000002;)

alert tcp any any -> $HOME_NET any (msg:" -->Phat hien NULL Scan !"; flags: 0;gid:2000003; sid:2000003;)

alert tcp any any -> $HOME_NET any (msg:" -->Phat hien XMAS Scan !"; flags: FPU;gid:2000004; sid:2000004;)

alert tcp any any -> $HOME_NET any (msg:" -->Phat hien Full XMAS Scan !"; flags: SRAFPU;gid:2000005; sid:2000005;)

alert tcp any any -> $HOME_NET any (msg:" -->Phat hien URG Scan !"; flags: U;gid:2000006; sid:2000006;)

alert tcp any any -> $HOME_NET any (msg:" -->Phat hien URG FIN Scan !"; flags: U;gid:2000007; sid:2000007;)

alert tcp any any -> $HOME_NET any (msg:" -->Phat hien PUSH FIN Scan !"; flags: P;gid:2000008; sid:2000008;)

alert tcp any any -> $HOME_NET any (msg:" -->Phat hien URG PUSH Scan !"; flags: U;gid:2000009;sid:2000009;)

alert tcp any any -> $HOME_NET any (flags: A; ack: 0; msg:" -->Phat hien NMAP TCP ping !";gid:2000010; sid:2000010;)
```



Target: 192.168.182.2

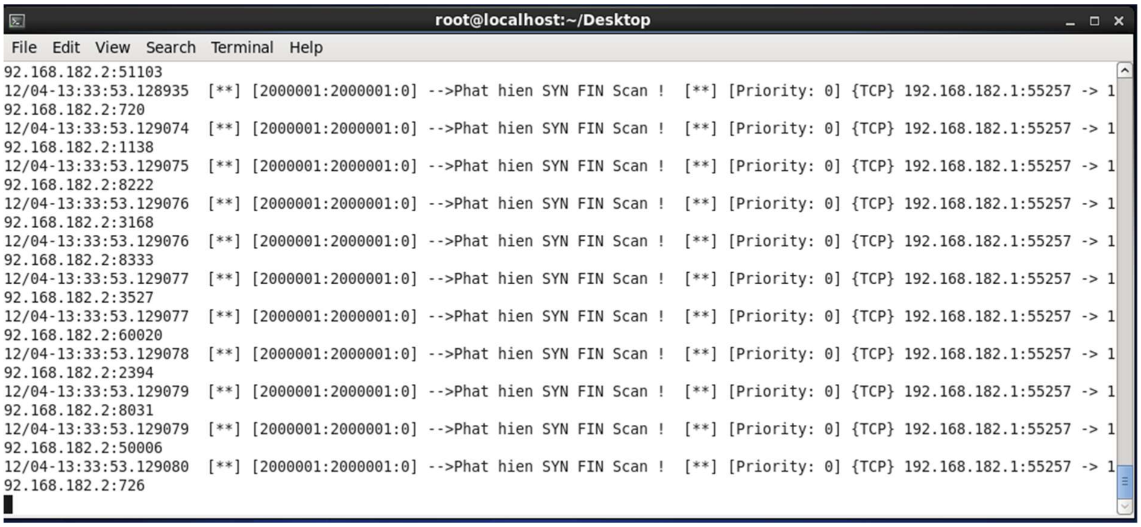
Profile:

Command: nmap -sS -v 192.168.182.2

192.168.182.2

```
nmap -sS -v 192.168.182.2
Discovered open port 139/tcp on 192.168.182.2
Discovered open port 135/tcp on 192.168.182.2
Discovered open port 445/tcp on 192.168.182.2
Discovered open port 49158/tcp on 192.168.182.2
Discovered open port 49156/tcp on 192.168.182.2
Discovered open port 49157/tcp on 192.168.182.2
Discovered open port 49155/tcp on 192.168.182.2
Discovered open port 49152/tcp on 192.168.182.2
Discovered open port 49153/tcp on 192.168.182.2
Discovered open port 49154/tcp on 192.168.182.2
Completed SYN Stealth Scan at 13:33, 1.76s elapsed
(1000 total ports)
Nmap scan report for 192.168.182.2
Host is up (0.000069s latency).
Not shown: 989 closed ports
PORT      STATE SERVICE
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown
49158/tcp open  unknown
MAC Address: 00:0C:29:EA:5D:C4 (VMware)

Read data files from: C:\Program Files (x86)\Nmap
Nmap done: 1 IP address (1 host up) scanned in 3.42
seconds
           Raw packets sent: 1169 (51.420KB) | Rcvd:
1001 (40.072KB)
```

Thực hiện lệnh ***nmap -v -sS 192.168.182.**2 từ client*



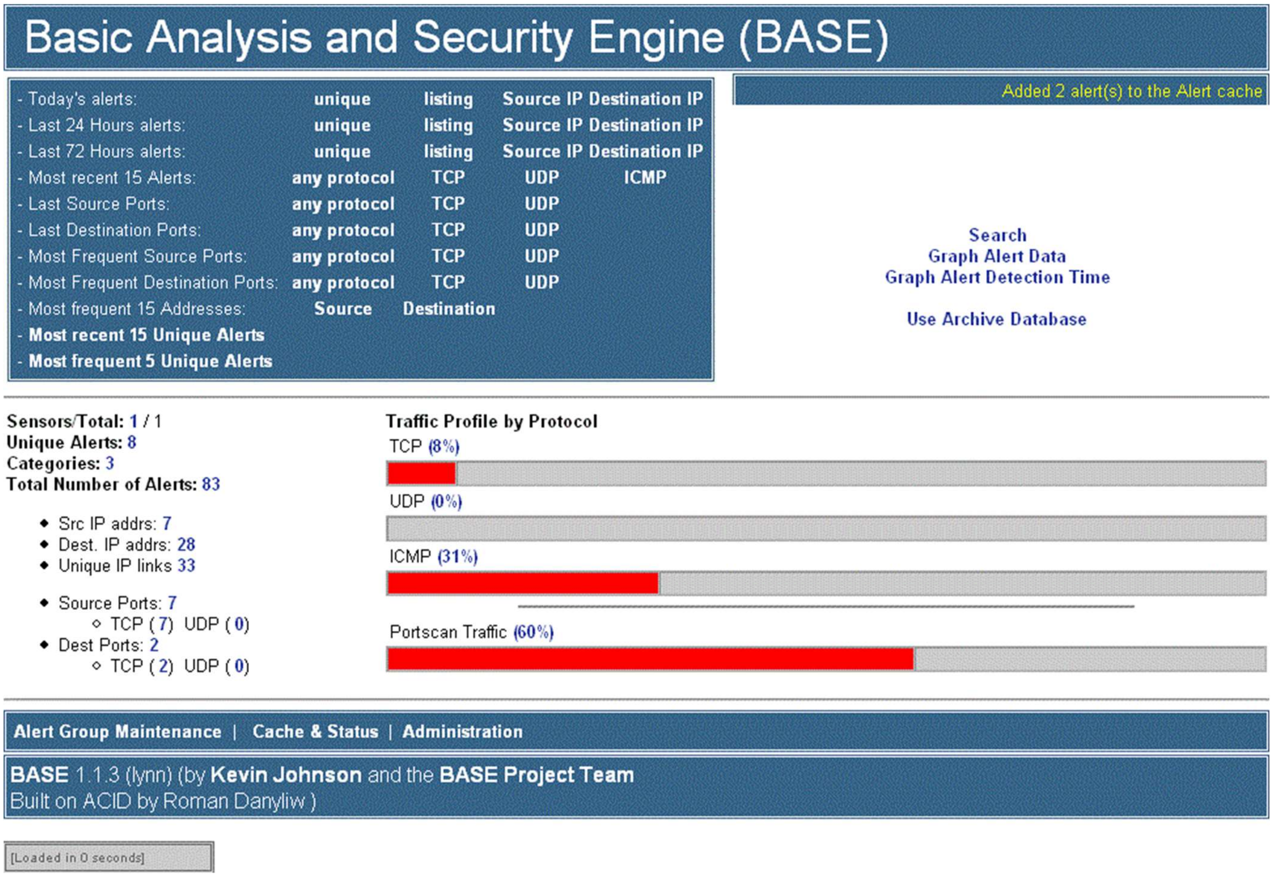
```
92.168.182.2:51103
12/04-13:33:53.128935  [**] [2000001:2000001:0] -->Phat hien SYN FIN Scan !  [**] [Priority: 0] {TCP} 192.168.182.1:55257 -> 1
92.168.182.2:720
12/04-13:33:53.129074  [**] [2000001:2000001:0] -->Phat hien SYN FIN Scan !  [**] [Priority: 0] {TCP} 192.168.182.1:55257 -> 1
92.168.182.2:1138
12/04-13:33:53.129075  [**] [2000001:2000001:0] -->Phat hien SYN FIN Scan !  [**] [Priority: 0] {TCP} 192.168.182.1:55257 -> 1
92.168.182.2:8222
12/04-13:33:53.129076  [**] [2000001:2000001:0] -->Phat hien SYN FIN Scan !  [**] [Priority: 0] {TCP} 192.168.182.1:55257 -> 1
92.168.182.2:3168
12/04-13:33:53.129076  [**] [2000001:2000001:0] -->Phat hien SYN FIN Scan !  [**] [Priority: 0] {TCP} 192.168.182.1:55257 -> 1
92.168.182.2:8333
12/04-13:33:53.129077  [**] [2000001:2000001:0] -->Phat hien SYN FIN Scan !  [**] [Priority: 0] {TCP} 192.168.182.1:55257 -> 1
92.168.182.2:3527
12/04-13:33:53.129077  [**] [2000001:2000001:0] -->Phat hien SYN FIN Scan !  [**] [Priority: 0] {TCP} 192.168.182.1:55257 -> 1
92.168.182.2:60020
12/04-13:33:53.129078  [**] [2000001:2000001:0] -->Phat hien SYN FIN Scan !  [**] [Priority: 0] {TCP} 192.168.182.1:55257 -> 1
92.168.182.2:2394
12/04-13:33:53.129079  [**] [2000001:2000001:0] -->Phat hien SYN FIN Scan !  [**] [Priority: 0] {TCP} 192.168.182.1:55257 -> 1
92.168.182.2:8031
12/04-13:33:53.129079  [**] [2000001:2000001:0] -->Phat hien SYN FIN Scan !  [**] [Priority: 0] {TCP} 192.168.182.1:55257 -> 1
92.168.182.2:50006
12/04-13:33:53.129080  [**] [2000001:2000001:0] -->Phat hien SYN FIN Scan !  [**] [Priority: 0] {TCP} 192.168.182.1:55257 -> 1
92.168.182.2:726
```

Phát hiện ra việc scan

Rules drop : drop tcp any any -> $HOME_NET any (msg:"-->Da chan SYN FIN Attack ! "; flags: S;gid: 2000001;sid:2000001;)

4.Base và Barnyard2

Cài đặt **Base** và **Barnyard2** để quản lí phân tích log của snort trên web



Basic Analysis and Security Engine (BASE)

- Today's alerts:	unique	listing	Source IP	Destination IP
- Last 24 Hours alerts:	unique	listing	Source IP	Destination IP
- Last 72 Hours alerts:	unique	listing	Source IP	Destination IP
- Most recent 15 Alerts:	any protocol	TCP	UDP	ICMP
- Last Source Ports:	any protocol	TCP	UDP	
- Last Destination Ports:	any protocol	TCP	UDP	
- Most Frequent Source Ports:	any protocol	TCP	UDP	
- Most Frequent Destination Ports:	any protocol	TCP	UDP	
- Most frequent 15 Addresses:	Source	Destination		
- **Most recent 15 Unique Alerts**				
- **Most frequent 5 Unique Alerts**				

Added 2 alert(s) to the Alert cache

Search
Graph Alert Data
Graph Alert Detection Time

Use Archive Database

Sensors/Total: 1 / 1
Unique Alerts: 8
Categories: 3
Total Number of Alerts: 83

- Src IP addrs: 7
- Dest. IP addrs: 28
- Unique IP links 33

- Source Ports: 7
  - TCP (7) UDP (0)
- Dest Ports: 2
  - TCP (2) UDP (0)

Traffic Profile by Protocol

TCP (8%)

UDP (0%)

ICMP (31%)

Portscan Traffic (60%)

Alert Group Maintenance | **Cache & Status** | **Administration**

BASE 1.1.3 (lynn) (by **Kevin Johnson** and the **BASE Project Team**
Built on ACID by Roman Danyliw)

[Loaded in 0 seconds]