

BÁO CÁO THỰC HÀNH

Môn học: Hệ thống tìm kiếm, phát hiện và ngăn ngừa xâm nhập

Lab 3: Viết rule trên Snort

Lớp: NT204.P22.ANTT.2

THÀNH VIÊN THỰC HIỆN (Nhóm 10):

STT	Họ và tên	MSSV
1	Nguyễn Xuân Huy	22520568
2	Nguyễn Khang Hưng	22520515

Điểm tự đánh giá

10

Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.

- Máý victim:

```
msfadmin@metasploitable:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 00:0c:29:fa:dd:2a brd ff:ff:ff:ff:ff:ff
    inet 192.168.85.200/24 scope global eth0
    inet6 fe80::20c:29ff:fe8a:dd2a/64 scope link
        valid_lft forever preferred_lft forever
msfadmin@metasploitable:~$ ip route
192.168.85.0/24 dev eth0 proto kernel scope link src 192.168.85.200
default via 192.168.85.1 dev eth0
```

- Máý attacker:

```
(kali㉿kali)-[~]
$ ifconfig
docker0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    inet 172.17.0.1 netmask 255.255.0.0 broadcast 172.17.255.255
    ether 02:42:9a:f5:48:fa txqueuelen 0 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.81.85.100 netmask 255.255.255.0 broadcast 10.81.85.255
    inet6 fe80::20c:29ff:fe3f:1f45 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:3f:1f:45 txqueuelen 1000 (Ethernet)
    RX packets 20 bytes 1732 (1.6 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 52 bytes 5640 (5.5 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 8 bytes 480 (480.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 8 bytes 480 (480.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(kali㉿kali)-[~]
$ ip route
default via 10.81.85.1 dev eth0 onlink
10.81.85.0/24 dev eth0 proto kernel scope link src 10.81.85.100
172.17.0.0/16 dev docker0 proto kernel scope link src 172.17.0.1 linkdown
```

- **Máy snort:**

```
xhuy2@xhuy2-virtual-machine:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:f5:e7:15 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.30.129/24 brd 192.168.30.255 scope global dynamic noprefixroute ens33
        valid_lft 1761sec preferred_lft 1761sec
    inet6 fe80::b8b8:40f1:369d:ded1/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
3: ens37: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:f5:e7:1f brd ff:ff:ff:ff:ff:ff
    altname enp2s5
    inet6 fe80::bde2:a97e:a457:c81f/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
4: ens38: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:f5:e7:29 brd ff:ff:ff:ff:ff:ff
    altname enp2s6
    inet6 fe80::304b:e04b:7d7d:d000/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
xhuy2@xhuy2-virtual-machine:~$
```

- **Router:**

```

xhuy@xhuy-virtual-machine:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:aa:6f:86 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.30.128/24 brd 192.168.30.255 scope global dynamic noprefixroute ens33
        valid_lft 974sec preferred_lft 974sec
    inet6 fe80::c808:7aea:6d4d:91f3/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
3: ens37: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:aa:6f:90 brd ff:ff:ff:ff:ff:ff
    altname enp2s5
    inet 10.81.85.1/24 scope global ens37
        valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:feaa:6f90/64 scope link
        valid_lft forever preferred_lft forever
4: ens38: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:aa:6f:9a brd ff:ff:ff:ff:ff:ff
    altname enp2s6
    inet 192.168.85.1/24 scope global ens38
        valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:feaa:6f9a/64 scope link
        valid_lft forever preferred_lft forever
xhuy@xhuy-virtual-machine:~$

```

- Attacker ping ra google:

```

(kali㉿kali)-[~]
$ ping google.com
PING google.com (74.125.130.101) 56(84) bytes of data:
64 bytes from sb-in-f101.1e100.net (74.125.130.101): icmp_seq=1 ttl=127 time=24.6 ms
64 bytes from sb-in-f101.1e100.net (74.125.130.101): icmp_seq=2 ttl=127 time=23.2 ms
^C
— google.com ping statistics —
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 23.168/23.902/24.637/0.734 ms

```

- Attacker ping victim:

```
(kali㉿kali)-[~]
$ ping 192.168.85.200
PING 192.168.85.200 (192.168.85.200) 56(84) bytes of data.
64 bytes from 192.168.85.200: icmp_seq=1 ttl=63 time=2.96 ms
64 bytes from 192.168.85.200: icmp_seq=2 ttl=63 time=4.99 ms
64 bytes from 192.168.85.200: icmp_seq=3 ttl=63 time=6.41 ms
^C
— 192.168.85.200 ping statistics —
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 2.959/4.785/6.413/1.417 ms
```

- Victim ping google:

```
msfadmin@metasploitable:~$ ping google.com
PING google.com (74.125.130.113) 56(84) bytes of data.
64 bytes from sb-in-f113.1e100.net (74.125.130.113): icmp_seq=1 ttl=127 time=24.6 ms
64 bytes from sb-in-f113.1e100.net (74.125.130.113): icmp_seq=2 ttl=127 time=26.1 ms

--- google.com ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1007ms
rtt min/avg/max/mdev = 24.625/25.374/26.124/0.766 ms
```

Yêu cầu 1.1 Giới hạn gói tin đến dịch vụ DNS

- Trước khi viết rule:

```
(kali㉿kali)-[~]
$ sudo hping3 --udp -p 53 -i u1000 192.168.85.200
[sudo] password for kali:
HPING 192.168.85.200 (eth0 192.168.85.200): udp mode set, 28 headers + 0 data bytes
^C
— 192.168.85.200 hping statistic —
17804 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

Sử dụng hping3 để gửi 1000 gói tin udp trong 1 giây đến cổng DNS của máy victim.

```

02:55:51.778870 IP 10.81.85.100.14663 > 192.168.85.200.domain: [!domain]
02:55:51.780029 IP 10.81.85.100.14664 > 192.168.85.200.domain: [!domain]
02:55:51.781102 IP 10.81.85.100.14665 > 192.168.85.200.domain: [!domain]
02:55:51.782200 IP 10.81.85.100.14666 > 192.168.85.200.domain: [!domain]
02:55:51.783284 IP 10.81.85.100.14667 > 192.168.85.200.domain: [!domain]
02:55:51.784380 IP 10.81.85.100.14668 > 192.168.85.200.domain: [!domain]
02:55:51.785581 IP 10.81.85.100.14669 > 192.168.85.200.domain: [!domain]
02:55:51.786610 IP 10.81.85.100.14670 > 192.168.85.200.domain: [!domain]
02:55:51.787801 IP 10.81.85.100.14671 > 192.168.85.200.domain: [!domain]
02:55:51.788927 IP 10.81.85.100.14672 > 192.168.85.200.domain: [!domain]
02:55:51.791118 IP 10.81.85.100.14673 > 192.168.85.200.domain: [!domain]
02:55:51.791359 IP 10.81.85.100.14674 > 192.168.85.200.domain: [!domain]
02:55:51.792291 IP 10.81.85.100.14675 > 192.168.85.200.domain: [!domain]
02:55:51.793440 IP 10.81.85.100.14676 > 192.168.85.200.domain: [!domain]
02:55:51.794682 IP 10.81.85.100.14677 > 192.168.85.200.domain: [!domain]
02:55:51.795761 IP 10.81.85.100.14678 > 192.168.85.200.domain: [!domain]
02:55:51.796915 IP 10.81.85.100.14679 > 192.168.85.200.domain: [!domain]
02:55:51.797866 IP 10.81.85.100.14680 > 192.168.85.200.domain: [!domain]
02:55:51.798876 IP 10.81.85.100.14681 > 192.168.85.200.domain: [!domain]
02:55:51.799873 IP 10.81.85.100.14682 > 192.168.85.200.domain: [!domain]

1687 packets captured
2027 packets received by filter
0 packets dropped by kernel
msfadmin@metasploitable:~$

```

Kiểm tra TCPdump trên máy victim thì thấy rất nhiều gói tin được gửi đến trong thời gian ngắn.

- Sau khi viết rule:

```

xhuy2@xhuy2-virtual-machine:/etc/snort/rules$ sudo cat nhom10.rules
drop udp any any -> 192.168.85.200 53 (msg:"block DNS flood"; threshold: type th
reshold, track by_src, count 200, seconds 5;sid:1000002;)
drop tcp any any -> 192.168.85.200 53 (msg:"block DNS flood"; threshold: type th
reshold, track by_src, count 200, seconds 5;sid:1000003;)

```

```

04/11-14:14:33.570420 10.81.85.100:28759 -> 192.168.85.200:53
UDP TTL:63 TOS:0x0 ID:63823 IpLen:20 DgmLen:28
Len: 0

[**] [1:1000002:1] block DNS flood [**]
[Priority: 0]
04/11-14:14:33.796457 10.81.85.100:28959 -> 192.168.85.200:53
UDP TTL:63 TOS:0x0 ID:29183 IpLen:20 DgmLen:28
Len: 0

[**] [1:1000002:1] block DNS flood [**]
[Priority: 0]
04/11-14:14:34.023603 10.81.85.100:29159 -> 192.168.85.200:53
UDP TTL:63 TOS:0x0 ID:22510 IpLen:20 DgmLen:28
Len: 0

[**] [1:1000002:1] block DNS flood [**]
[Priority: 0]
04/11-14:14:34.241717 10.81.85.100:29359 -> 192.168.85.200:53
UDP TTL:63 TOS:0x0 ID:27110 IpLen:20 DgmLen:28
Len: 0

xhuy2@xhuy2-virtual-machine:/etc/snort/rules$

```

Kiểm tra alert của snort đã phát hiện và chặn cuộc tấn công.

```

03:14:10.655583 IP6 fe80::bde2:a97e:a457:c81f.mdns > ff02::fb.mdns: 0 [2q] PTR (
QM)? _ipps._tcp.local.[!domain]
03:14:10.657888 IP6 fe80::304b:e04b:7d7d:d000.mdns > ff02::fb.mdns: 0 [2q] PTR (
QM)? _ipps._tcp.local.[!domain]
03:14:11.056740 IP 0.0.0.0.bootpc > 255.255.255.255.bootps: BOOTP/DHCP, Request
from 00:0c:29:f5:e7:29 (oui Unknown), length 299
03:14:17.417104 IP6 fe80::bde2:a97e:a457:c81f > ip6-allrouters: ICMP6, router so
licitation, length 8
03:14:17.698643 IP6 fe80::304b:e04b:7d7d:d000 > ip6-allrouters: ICMP6, router so
licitation, length 8
03:14:18.649681 IP 0.0.0.0.bootpc > 255.255.255.255.bootps: BOOTP/DHCP, Request
from 00:0c:29:f5:e7:1f (oui Unknown), length 299
03:14:18.664637 IP6 fe80::304b:e04b:7d7d:d000.mdns > ff02::fb.mdns: 0 [2q] PTR (
QM)? _ipps._tcp.local.[!domain]
03:14:18.664883 IP6 fe80::bde2:a97e:a457:c81f.mdns > ff02::fb.mdns: 0 [2q] PTR (
QM)? _ipps._tcp.local.[!domain]
03:14:19.556239 arp who-has 192.168.85.200 tell 192.168.85.1
03:14:19.556283 arp reply 192.168.85.200 is-at 00:0c:29:fa:dd:2a (oui Unknown)
03:14:19.809209 IP 0.0.0.0.bootpc > 255.255.255.255.bootps: BOOTP/DHCP, Request
from 00:0c:29:f5:e7:29 (oui Unknown), length 299

71 packets captured
71 packets received by filter
0 packets dropped by kernel
msfadmin@metasploitable:~$ _

```

Kiểm tra tcpdump trên máy victim thì thấy nếu vượt ngưỡng 200 gói tin trong 5s thì sẽ chặn hết nên không có gói tin nào qua.

Snort 2.x không hỗ trợ các tính năng nâng cao như rate-limiting hoặc tính năng lọc gói tin theo số lượng gói trong một khoảng thời gian cụ thể (như yêu cầu chặn từ gói thứ 201 trở đi trong 5 giây). Việc thực hiện các yêu cầu này yêu cầu các tính năng như `rate_filter` hoặc `flowbits` mà không có sẵn trong Snort 2.x mà chỉ hỗ trợ trong Snort 3.x. Điều này dẫn đến việc Snort 2.x không thể chỉ chặn một số gói tin sau khi vượt quá ngưỡng mà không làm gián đoạn tất cả các gói tin từ cùng một nguồn.

Yêu cầu 1.2 Chỉ cho phép truy cập đến một số dịch vụ

- Kiểm tra các cổng đang mở trên victim:

```
(kali㉿kali)-[~]
$ nmap -p- 192.168.85.200
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-11 14:28 +07
Nmap scan report for 192.168.85.200
Host is up (0.034s latency).
Not shown: 65505 closed tcp ports (conn-refused)
PORT      STATE      SERVICE
21/tcp    open      ftp
22/tcp    open      ssh
23/tcp    open      telnet
25/tcp    open      smtp
53/tcp    filtered  domain
80/tcp    open      http
111/tcp   open      rpcbind
139/tcp   open      netbios-ssn
445/tcp   open      microsoft-ds
512/tcp   open      exec
513/tcp   open      login
514/tcp   open      shell
1099/tcp  open      rmiregistry
1524/tcp  open      ingreslock
2049/tcp  open      nfs
2121/tcp  open      ccproxy-ftp
3306/tcp  open      mysql
3632/tcp  open      distccd
5432/tcp  open      postgresql
5900/tcp  open      vnc
6000/tcp  open      X11
6667/tcp  open      irc
6697/tcp  open      ircs-u
8009/tcp  open      ajp13
8180/tcp  open      unknown
8787/tcp  open      msgsrvr
34369/tcp open      unknown
46486/tcp open      unknown
49479/tcp open      unknown
52573/tcp open      unknown

Nmap done: 1 IP address (1 host up) scanned in 35.56 seconds
```

- Trước khi viết rule:


```
(kali㉿kali)-[~]
$ telnet 192.168.85.200 111
Trying 192.168.85.200 ...
Connected to 192.168.85.200.
Escape character is '^]'.
^]
telnet> quit
Connection closed.
```

telnet thành công tới cổng 111 của máy victim.

```
(kali㉿kali)-[~]
$ telnet 192.168.85.200 21
Trying 192.168.85.200 ...
Connected to 192.168.85.200.
Escape character is '^]'.
220 (vsFTPD 2.3.4)
^]
telnet> quit
Connection closed.
```

telnet thành công tới cổng 21 của máy victim.

- Sau khi viết rule:

```
drop tcp any any -> 192.168.85.200 ![21,22,25,80,137,138,139,443,445,3306,514,5432] (msg:"port không được phép truy cập";sid:1000004;)
drop udp any any -> 192.168.85.200 ![137,138,514] (msg:"port không được phép truy cập";sid:1000005;)
```

```
drop tcp any any -> 192.168.85.200 ![21,22,25,80,137,138,139,443,445,3306,514,5432] (
msg:"port không được phép truy cập";sid:1000004;)
```

```
drop udp any any -> 192.168.85.200 ![137,138,514] (msg:" port không được phép truy cập ";
sid:1000005;)
```

```
(kali㉿kali)-[~]
$ telnet 192.168.85.200 111
Trying 192.168.85.200 ...
```

Port 111 của máy victim không phản hồi, chứng tỏ đã bị chặn.

```

[**] [1:1000004:0] port khong duoc phep truy cap [**]
[Priority: 0]
04/11-14:43:57.843625 10.81.85.100:39178 -> 192.168.85.200:111
TCP TTL:63 TOS:0x0 ID:52638 IpLen:20 DgmLen:60 DF
*****S* Seq: 0xCB6BC6D9 Ack: 0x0 Win: 0x7D78 TcpLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 4274849239 0 NOP WS: 7

[**] [1:1000004:0] port khong duoc phep truy cap [**]
[Priority: 0]
04/11-14:44:06.034833 10.81.85.100:39178 -> 192.168.85.200:111
TCP TTL:63 TOS:0x0 ID:52639 IpLen:20 DgmLen:60 DF
*****S* Seq: 0xCB6BC6D9 Ack: 0x0 Win: 0x7D78 TcpLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 4274857431 0 NOP WS: 7

[**] [1:1000004:0] port khong duoc phep truy cap [**]
[Priority: 0]
04/11-14:44:22.162517 10.81.85.100:39178 -> 192.168.85.200:111
TCP TTL:63 TOS:0x0 ID:52640 IpLen:20 DgmLen:60 DF
*****S* Seq: 0xCB6BC6D9 Ack: 0x0 Win: 0x7D78 TcpLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 4274873559 0 NOP WS: 7

xhuy2@xhuy2-virtual-machine:/etc/snort/rules$

```

Kiểm tra alert của snort thì thấy đã có thông báo về port không được phép truy cập.

```

(kali㉿kali)-[~]
$ telnet 192.168.85.200 25
Trying 192.168.85.200 ...
Connected to 192.168.85.200.
Escape character is '^]'.

```

Kiểm tra cổng 25 thì thấy vẫn truy cập được.

```

(kali㉿kali)-[~]
$ telnet 192.168.85.200 21
Trying 192.168.85.200 ...
Connected to 192.168.85.200.
Escape character is '^]'.
220 (vsFTPd 2.3.4)

```

Cổng 21 vẫn truy cập được.

```

(kali㉿kali)-[~]
$ telnet 192.168.85.200 5900
Trying 192.168.85.200 ...

```

Cổng 5900 không truy cập được do không nằm trong danh sách bị chặn.

```
[**] [1:1000004:0] port khong duoc phep truy cap [**]
[Priority: 0]
04/11-14:47:21.424602 10.81.85.100:49290 -> 192.168.85.200:5900
TCP TTL:63 TOS:0x0 ID:45445 IpLen:20 DgmLen:60 DF
*****S* Seq: 0x29EBCA5B Ack: 0x0 Win: 0x7D78 TcpLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 4275052823 0 NOP WS: 7

[**] [1:1000004:0] port khong duoc phep truy cap [**]
[Priority: 0]
04/11-14:47:25.456494 10.81.85.100:49290 -> 192.168.85.200:5900
TCP TTL:63 TOS:0x0 ID:45446 IpLen:20 DgmLen:60 DF
*****S* Seq: 0x29EBCA5B Ack: 0x0 Win: 0x7D78 TcpLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 4275056855 0 NOP WS: 7

[**] [1:1000004:0] port khong duoc phep truy cap [**]
[Priority: 0]
04/11-14:47:33.648825 10.81.85.100:49290 -> 192.168.85.200:5900
TCP TTL:63 TOS:0x0 ID:45447 IpLen:20 DgmLen:60 DF
*****S* Seq: 0x29EBCA5B Ack: 0x0 Win: 0x7D78 TcpLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 4275065047 0 NOP WS: 7

xhuy2@xhuy2-virtual-machine:/etc/snort/rules$
```

Alert cảnh báo về port 5900.

Yêu cầu 1.3 Chỉ cho phép các truy vấn DNS đến các tên miền thuộc quản lý của UIT

- Trước khi cài đặt rule:

Tiến hành nslookup với server là ip của máy victim:

```
(kali㉿kali)-[~]
$ nslookup
> server 192.168.85.200
Default server: 192.168.85.200
Address: 192.168.85.200#53
> daa.uit.edu.vn
;; communications error to 192.168.85.200#53: host unreachable
;; communications error to 192.168.85.200#53: host unreachable
;; communications error to 192.168.85.200#53: host unreachable
;; no servers could be reached
> daa.uit.edu.vn
Server:      192.168.85.200
Address:     192.168.85.200#53

** server can't find daa.uit.edu.vn: REFUSED
>
```

Kiểm tra tcpdump trên máy victim:

```
06:19:27.926104 IP 10.81.85.100.50758 > 192.168.85.200.domain: 46492+ A? daa.uit.edu.vn. (32)
06:19:27.926733 IP 192.168.85.200.domain > 10.81.85.100.50758: 46492 Refused- 0/0/0 (32)
```

- Sau khi viết rule:

drop udp any any -> 192.168.85.200 53 (msg:"chỉ cho phép domain UIT";content:!"|03|uit|03|edu|02|vn|00|"; nocase; offset: 12; sid:10000015;)

drop tcp any any -> 192.168.85.200 53 (msg:"chỉ cho phép domain UIT";content:!"|03|uit|03|edu|02|vn|00|"; nocase; offset: 12; sid:10000016;)

```
xhuy2@xhuy2-virtual-machine:/etc/snort/rules$ sudo cat nhom10.rules
drop udp any any -> 192.168.85.200 53 (msg:"chỉ cho phép domain UIT";content:!"|03|uit|03|edu|02|vn|00|"; nocase; offset: 12; sid:10000015;)
drop tcp any any -> 192.168.85.200 53 (msg:"chỉ cho phép domain UIT";content:!"|03|uit|03|edu|02|vn|00|"; nocase; offset: 12; sid:10000016;)
```

Thực hiện truy vấn đến domain UIT:

```

(kali@kali)-[~]
$ nslookup
> server 192.168.85.200
Default server: 192.168.85.200
Address: 192.168.85.200#53
> daa.uit.edu.vn
Server:      192.168.85.200
Address:     192.168.85.200#53

** server can't find daa.uit.edu.vn: REFUSED
> google.com
;; communications error to 192.168.85.200#53: timed out
;; communications error to 192.168.85.200#53: timed out
;; communications error to 192.168.85.200#53: timed out
;; no servers could be reached
> facebook.com
;; communications error to 192.168.85.200#53: timed out
;; communications error to 192.168.85.200#53: timed out
;; communications error to 192.168.85.200#53: timed out
;; no servers could be reached
>

```

Tên miền có UIT thì vẫn quy vẫn được nhưng tên miền khác thì không (timed out).

```

06:29:30.959184 arp who-has 192.168.85.200 tell 192.168.85.1
06:29:30.959220 arp reply 192.168.85.200 is-at 00:0c:29:fa:dd:2a (oui Unknown)

```

Kiểm tra tcpdump trên máy victim.

```

[**] [1:10000015:0] chi cho phep domain UIT [**]
[Priority: 0]
04/12-23:48:58.182587 10.81.85.100:38602 -> 192.168.85.200:53
UDP TTL:63 TOS:0x0 ID:23326 IpLen:20 DgmLen:56
Len: 28

[**] [1:10000015:0] chi cho phep domain UIT [**]
[Priority: 0]
04/12-23:49:03.188162 10.81.85.100:53299 -> 192.168.85.200:53
UDP TTL:63 TOS:0x0 ID:50258 IpLen:20 DgmLen:56
Len: 28

[**] [1:10000015:0] chi cho phep domain UIT [**]
[Priority: 0]
04/12-23:49:08.189628 10.81.85.100:37617 -> 192.168.85.200:53
UDP TTL:63 TOS:0x0 ID:59406 IpLen:20 DgmLen:56
Len: 28

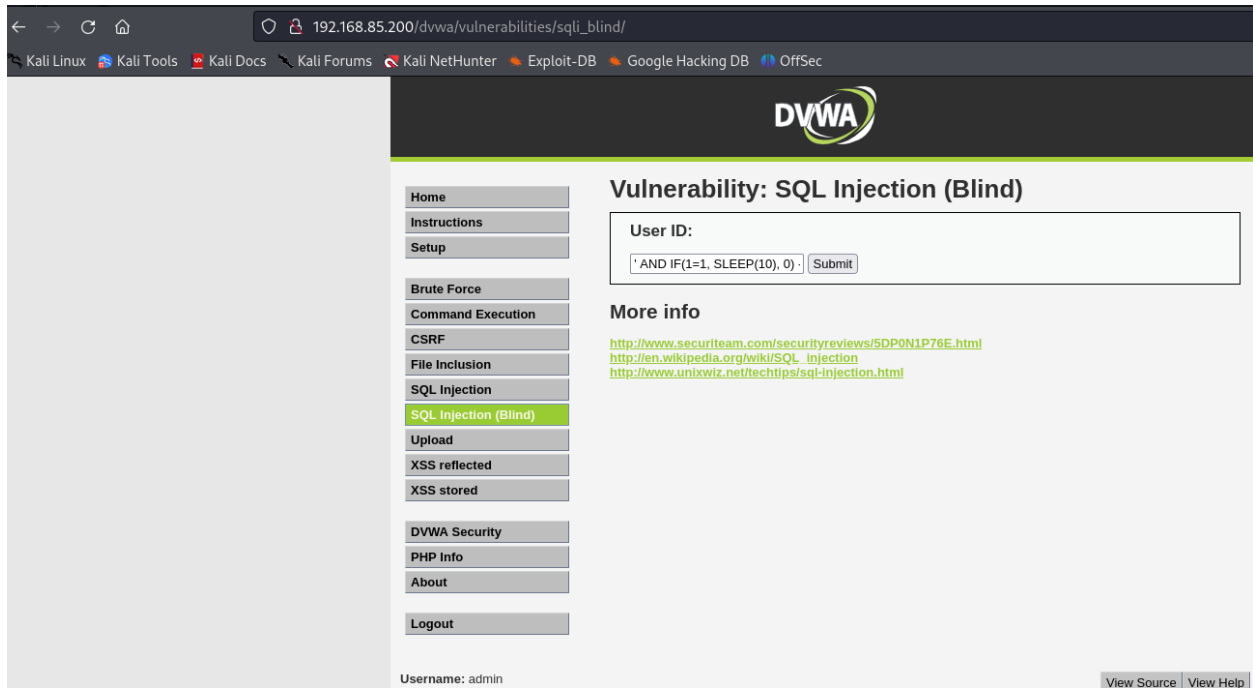
xhuy2@xhuy2-virtual-machine:/etc/snort/rules$

```

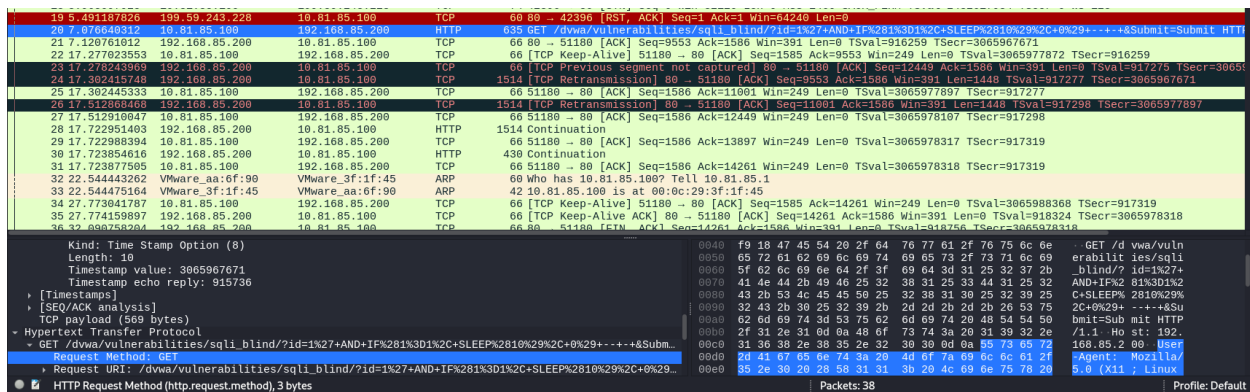
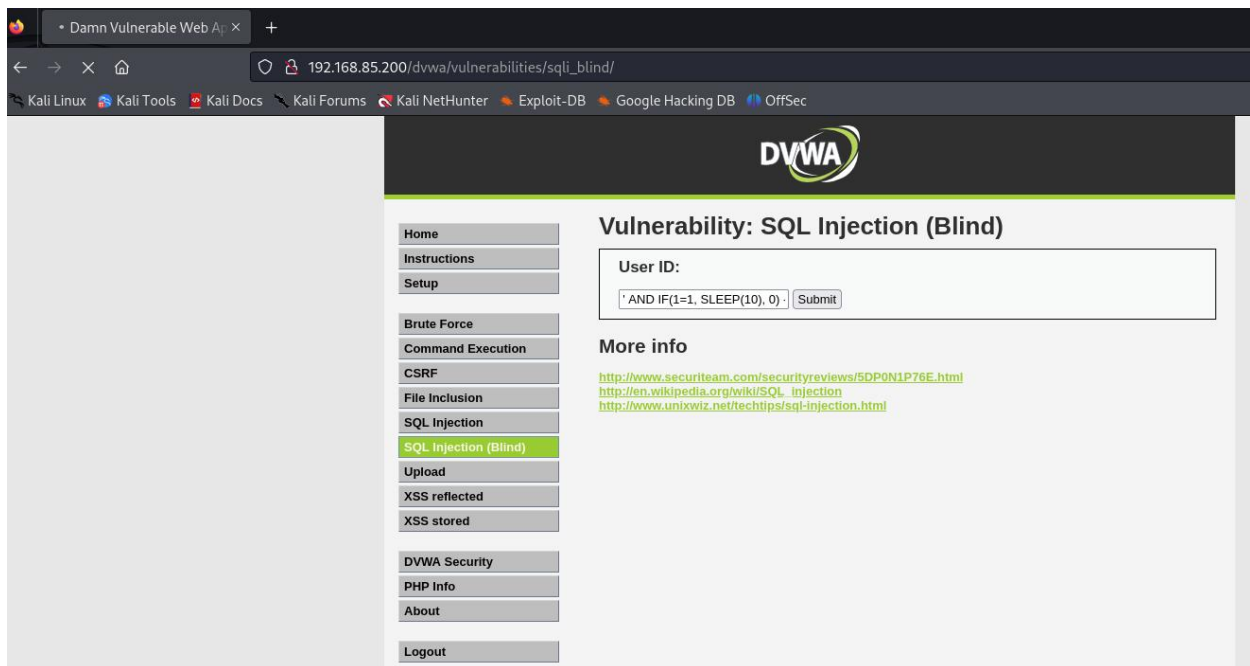
Cảnh báo từ snort đã xuất hiện.

Yêu cầu 1.4 Ngăn chặn tấn công Time-based SQL injection

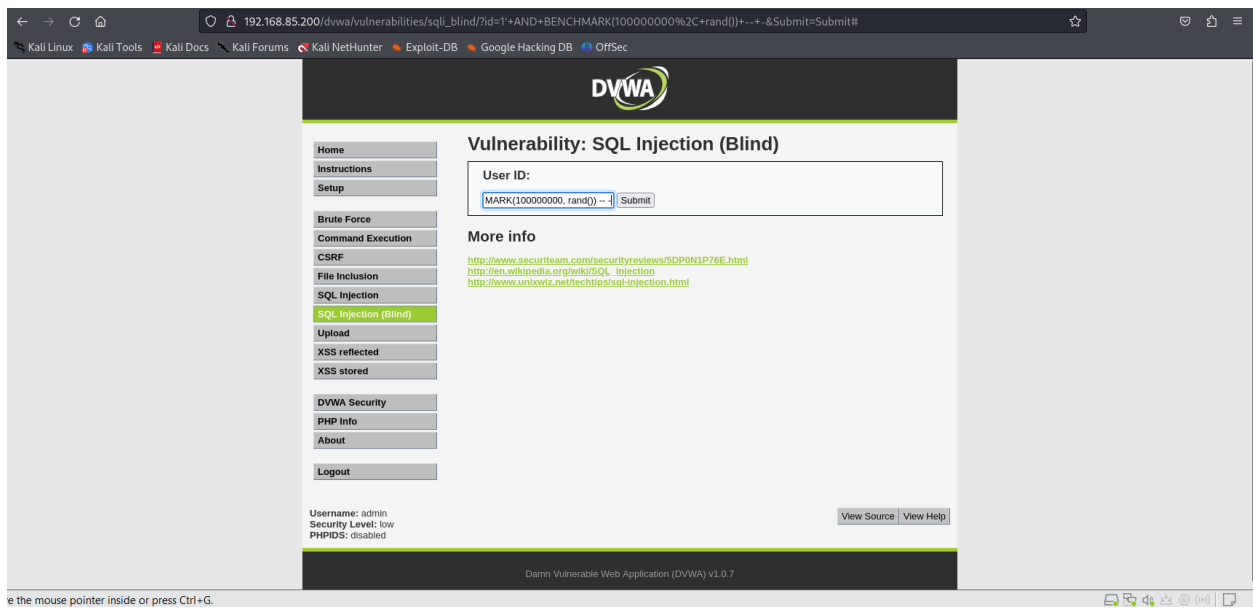
- Trước khi viết rule:



Thực hiện time-based SQL injection với câu truy vấn `1' AND IF(1=1, SLEEP(10), 0) -- -` thì thấy trang web đợi khoảng 10 giây trước khi trả về kết quả



Thực hiện time-based SQL injection với câu truy vấn `1' AND BENCHMARK(100000000, rand()) -- -`. Câu truy vấn này sẽ thực hiện tạo 1 số random 100000000 lần, thấy rằng trang web sẽ load 1 khoảng thời gian trước khi trả về 200 OK



Move the mouse pointer inside or press Ctrl+G.

```

42 29.097991872 10.81.85.100 192.168.85.200 TCP 66 56526 → 80 [ACK] Seq=1 Ack=1 Win=32128 Len=0 TSval=3066152860 TSecr=934774
43 29.098091050 10.81.85.100 192.168.85.200 HTTP 705 GET /dvwa/vulnerabilities/sqli_blind/?id=1'+AND+BENCHMARK(100000000%2C+rand())+--+&Submit=Submit#
44 29.098082122 192.168.85.200 10.81.85.100 TCP 66 80 → 56526 [ACK] Seq=1 Ack=640 Win=7072 Len=0 TSval=934774 TSecr=3066152861
45 30.478776671 192.168.85.200 10.81.85.100 TCP 1514 80 → 56526 [ACK] Seq=1 Ack=640 Win=7072 Len=1448 TSval=934912 TSecr=3066152861
46 30.478815891 10.81.85.100 192.168.85.200 TCP 66 56526 → 80 [ACK] Seq=640 Ack=1449 Win=31872 Len=0 TSval=3066154241 TSecr=934912
47 30.481878958 192.168.85.200 10.81.85.100 TCP 431 [TCP Previous segment not captured] 80 → 56526 [PSH, ACK] Seq=4345 Ack=640 Win=7072 Len=365 TSval=934912 TSecr=3066154244
48 30.481896844 10.81.85.100 192.168.85.200 TCP 78 [TCP Dup ACK 46v1] 56526 → 80 [ACK] Seq=640 Ack=1449 Win=31872 Len=0 TSval=3066154244 TSecr=934912
49 30.687676091 192.168.85.200 10.81.85.100 TCP 1514 [TCP Retransmission] 80 → 56526 [ACK] Seq=1449 Ack=640 Win=7072 Len=1448 TSval=934933 TSecr=3066154244
50 30.687799940 10.81.85.100 192.168.85.200 TCP 78 56526 → 80 [ACK] Seq=640 Ack=2897 Win=31872 Len=0 TSval=3066154450 TSecr=934933
51 30.688610452 192.168.85.200 10.81.85.100 TCP 1514 [TCP Retransmission] 80 → 56526 [ACK] Seq=2897 Ack=640 Win=7072 Len=1448 TSval=934933 TSecr=3066154450
52 30.688624721 10.81.85.100 192.168.85.200 TCP 66 56526 → 80 [ACK] Seq=640 Ack=4710 Win=31872 Len=0 TSval=3066154451 TSecr=934933
53 31.064943792 10.81.85.100 192.168.85.200 TCP 54 32902 → 80 [FIN, ACK] Seq=1 Ack=1 Win=32120 Len=0
54 31.065672121 199.59.243.228 10.81.85.100 TCP 60 80 → 32902 [ACK] Seq=1 Ack=2 Win=64239 Len=0
55 31.068557746 199.59.243.228 10.81.85.100 TCP 60 80 → 32902 [FIN, PSH, ACK] Seq=1 Ack=2 Win=64239 Len=0
56 31.068576677 10.81.85.100 199.59.243.228 TCP 54 32902 → 80 [ACK] Seq=2 Ack=2 Win=32120 Len=0
57 32.065465453 10.81.85.100 199.59.243.228 TCP 54 32886 → 80 [FIN, ACK] Seq=1 Ack=1 Win=32120 Len=0
58 32.065895935 10.81.85.100 199.59.243.228 TCP 54 32918 → 80 [FIN, ACK] Seq=1 Ack=1 Win=32120 Len=0
59 32.066253833 199.59.243.228 10.81.85.100 TCP 60 80 → 32886 [ACK] Seq=1 Ack=2 Win=64239 Len=0
60 32.066388108 199.59.243.228 10.81.85.100 TCP 60 80 → 32918 [ACK] Seq=1 Ack=2 Win=64239 Len=0
61 32.067396126 199.59.243.228 10.81.85.100 TCP 60 80 → 32886 [FIN, PSH, ACK] Seq=1 Ack=2 Win=64239 Len=0
62 32.067413747 10.81.85.100 199.59.243.228 TCP 54 32886 → 80 [ACK] Seq=2 Ack=2 Win=32120 Len=0
63 32.068715984 199.59.243.228 10.81.85.100 TCP 60 80 → 32918 [FIN, PSH, ACK] Seq=1 Ack=2 Win=64239 Len=0
64 32.068726197 10.81.85.100 199.59.243.228 TCP 54 32918 → 80 [ACK] Seq=2 Ack=2 Win=32120 Len=0
65 40.702226190 10.81.85.100 192.168.85.200 TCP 66 [TCP Keep-Alive] 56526 → 80 [ACK] Seq=639 Ack=4710 Win=31872 Len=0 TSval=3066164465 TSecr=934933

Kind: Time Stamp Option (8)
Length: 10
Timestamp value: 3066152861
Timestamp echo reply: 934774
+ [Timestamps]
+ [SEQ/ACK analysis]
+ TCP payload (639 bytes)
+ Hypertext Transfer Protocol
+ GET /dvwa/vulnerabilities/sqli_blind/?id=1'+AND+BENCHMARK(100000000%2C+rand())+--+&Submit=Submit# HTTP/1.1
Request Method: GET
Content-Type: application/javascript
Host: 192.168.85.200
User-Agent: Mozilla/5.0 (X11; Linux i686_32; rv:1.9.0.1) Gecko/20100801 Firefox/3.0.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.85.200/dvwa/vulnerabilities/sqli_blind/?id=1'+AND+BENCHMARK(100000000%2C+rand())+--+&Submit=Submit#
Packets: 65
Profile: Default

```

- Sau khi viết rule:

drop tcp any any -> 192.168.85.200 80 (msg:"block time-based SQL Injection Attack";flow:to_server, established; content:"SLEEP%28", nocase; sid:100002;)

drop tcp any any -> 192.168.85.200 80 (msg:"block time-based SQL Injection Attack";flow:to_server, established; content:"BENCHMARK%28", nocase; sid:100003;)

```

xhuy2@xhuy2-virtual-machine:/etc/snort/rules$ sudo cat nhom10.rules
drop tcp any any -> 192.168.85.200 80 (msg:"block time-based SQL Injection Attack";flow:to_server, established; content:"SLEEP", nocase; sid:100002;)
drop tcp any any -> 192.168.85.200 80 (msg:"Time-based SQL Injection Attack";flow:to_server, established; content:"BENCHMARK", nocase; sid:100003;)

```

Thực hiện time-based SQL injection với câu truy vấn 1' AND IF(1=1, SLEEP(10), 0) -- - thì thấy trang web load liên tục và không trả về kết quả gì.

Damn Vulnerable Web App

192.168.85.200/dvwa/vulnerabilities/sql_i_blind/?id=1'+AND+IF(1%3D1%2C+SLEEP(10)%2C+0)+--+&

Kali Linux

Kali Tools

Kali Docs

Kali Forums

Kali NetHunter

Exploit-DB

Google Hacking DB

OffSec

DVWA

Home

Instructions

Setup

Brute Force

Command Execution

CSRF

File Inclusion

SQL Injection

SQL Injection (Blind)

Upload

XSS reflected

XSS stored

DVWA Security

PHP Info

About

Logout

Vulnerability: SQL Injection (Blind)

User ID:

ND IF(1=1, SLEEP(10), 0) -- -

Submit

More info

<http://www.securiteam.com/securityreviews/5DP0N1P76E.html>
http://en.wikipedia.org/wiki/SQL_injection
<http://www.unixwiz.net/techtips/sql-injection.html>

192.168.85.200

View Source

View Help

272	361.962154229	10.81.85.100	192.168.85.200	TCP	66	56638	→ 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1546110960 TSecr=1933356
273	361.962113932	10.81.85.100	192.168.85.200	HTTP	636	GET /dvwa/vulnerabilities/sql_i_blind/?id=1%27+AND+IF%281%3D1%2C+SLEEP%2810%29%2C+0%29+--+&Submit=Submit	HTTP
274	362.166023601	10.81.85.100	192.168.85.200	TCP	636	[TCP Retransmission] 56638	→ 80 [PSH, ACK] Seq=1 Ack=1 Win=64256 Len=564 TSval=1546111104 TSecr=1933356
275	362.378027123	10.81.85.100	192.168.85.200	TCP	636	[TCP Retransmission] 56638	→ 80 [PSH, ACK] Seq=1 Ack=1 Win=64256 Len=564 TSval=1546111368 TSecr=1933356
276	362.782039920	10.81.85.100	192.168.85.200	TCP	636	[TCP Retransmission] 56638	→ 80 [PSH, ACK] Seq=1 Ack=1 Win=64256 Len=564 TSval=1546111789 TSecr=1933356
277	363.614011502	10.81.85.100	192.168.85.200	TCP	636	[TCP Retransmission] 56638	→ 80 [PSH, ACK] Seq=1 Ack=1 Win=64256 Len=564 TSval=1546112612 TSecr=1933356
278	364.538408727	fe80::65e4:4737:dd4::ff02::1:ff00:1	ff02::1:ff00:1	ICMPv6	86	Neighbor Solicitation for fe80::1 from 00:59:56:c0:00:02	
279	365.240835310	10.81.85.100	192.168.85.200	TCP	636	[TCP Retransmission] 56638	→ 80 [PSH, ACK] Seq=1 Ack=1 Win=64256 Len=564 TSval=1546114244 TSecr=1933356
280	365.757374429	192.168.85.200	10.81.85.100	TCP	74	[TCP Retransmission] 89	→ 56638 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=1933736 TSecr=1933356
281	365.757397637	10.81.85.100	192.168.85.200	TCP	66	[TCP Dup ACK 272#1] 56638	→ 80 [ACK] Seq=565 Ack=1 Win=64256 Len=0 TSval=1546114755 TSecr=1933356
282	366.814699062	fe80::20c:29ff:feaa::ff02::2		ICMPv6	70	Router Solicitation from 00:0c:29:aa:6f:90	
283	367.326645871	Vmware_aa:6f:90	Vmware_58:e0:d9	ARP	60	Who has 10.81.85.100? Tell 10.81.85.1	
284	367.326660486	Vmware_58:e0:d9	Vmware_aa:6f:90	ARP	42	10.81.85.100 is at 00:0c:29:58:e0:d9	

362	614.392734714	169.254.23.11	224.0.0.251	MDNS	299	Standard query response 0x0000 PTR, cache flush LAPTOP-UE85HH5H._dosvc._tcp.local SRV, cache flush 0 0 7680 ...	
363	614.394676852	fe80::65e4:4737:dd4::ff02::fb		MDNS	319	Standard query response 0x0000 PTR, cache flush LAPTOP-UE85HH5H._dosvc._tcp.local SRV, cache flush 0 0 7680 ...	
364	614.397321699	169.254.23.11	224.0.0.251	MDNS	235	Standard query response 0x0000 SRV, cache flush 0 0 7680 LAPTOP-UE85HH5H.local TXT, cache flush A, cache flu...	
365	614.398278495	fe80::65e4:4737:dd4::ff02::fb		MDNS	255	Standard query response 0x0000 SRV, cache flush 0 0 7680 LAPTOP-UE85HH5H.local TXT, cache flush A, cache flu...	
366	616.638816171	10.81.85.100	192.168.85.200	TCP	74	[TCP Retransmission] 41151	→ 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1546368536 TSecr=0 WS=1..
367	619.710829976	10.81.85.100	192.168.85.200	TCP	74	[TCP Retransmission] 41930	→ 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1546368708 TSecr=0 WS=1..
368	619.744397438	10.81.85.1	10.81.85.100	ICMP	102	Destination unreachable (Host unreachable)	
369	619.744397644	10.81.85.1	10.81.85.100	ICMP	102	Destination unreachable (Host unreachable)	
370	619.745037369	10.81.85.100	192.168.85.200	TCP	74	30090	→ 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1546368743 TSecr=0 WS=128
371	620.766147121	10.81.85.100	192.168.85.200	TCP	74	[TCP Retransmission] 38099	→ 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1546369764 TSecr=0 WS=1..
372	621.790068596	10.81.85.100	192.168.85.200	TCP	74	[TCP Retransmission] 38099	→ 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1546370788 TSecr=0 WS=1..
373	622.814039984	10.81.85.100	192.168.85.200	TCP	74	[TCP Retransmission] 38099	→ 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1546371812 TSecr=0 WS=1..
374	622.816338902	10.81.85.1	10.81.85.100	ICMP	102	Destination unreachable (Host unreachable)	
375	622.816339191	10.81.85.1	10.81.85.100	ICMP	102	Destination unreachable (Host unreachable)	
376	622.816339232	10.81.85.1	10.81.85.100	ICMP	102	Destination unreachable (Host unreachable)	
377	622.816339260	10.81.85.1	10.81.85.100	ICMP	102	Destination unreachable (Host unreachable)	
378	624.864238589	Vmware_aa:6f:90	Vmware_58:e0:d9	ARP	60	Who has 10.81.85.100? Tell 10.81.85.1	
379	624.864254839	Vmware_58:e0:d9	Vmware_aa:6f:90	ARP	42	10.81.85.100 is at 00:0c:29:58:e0:d9	

Kiểm tra wireshark sau 1 thời gian thì thấy trả về Destination unreachable.

```
xhuy2@xhuy2-virtual-machine: /etc/snort/rules

***AP*** Seq: 0x2AD67737 Ack: 0xC87C88D8 Win: 0x1F6 TcpLen: 32
TCP Options (3) => NOP NOP TS: 1545749408 1897160

[**] [1:100002:0] block time-based SQL Injection Attack [**]
[Priority: 0]
04/12-22:38:53.365390 10.81.85.100:59754 -> 192.168.85.200:80
TCP TTL:63 TOS:0x0 ID:50072 IpLen:20 DgmLen:616 DF
***AP*** Seq: 0x2AD67737 Ack: 0xC87C88D8 Win: 0x1F6 TcpLen: 32
TCP Options (3) => NOP NOP TS: 1545749832 1897160

[**] [1:100002:0] block time-based SQL Injection Attack [**]
[Priority: 0]
04/12-22:38:54.191828 10.81.85.100:59754 -> 192.168.85.200:80
TCP TTL:63 TOS:0x0 ID:50073 IpLen:20 DgmLen:616 DF
***AP*** Seq: 0x2AD67737 Ack: 0xC87C88D8 Win: 0x1F6 TcpLen: 32
TCP Options (3) => NOP NOP TS: 1545750660 1897160

[**] [1:100002:0] block time-based SQL Injection Attack [**]
[Priority: 0]
04/12-22:38:55.823903 10.81.85.100:59754 -> 192.168.85.200:80
TCP TTL:63 TOS:0x0 ID:50075 IpLen:20 DgmLen:616 DF
***AP*** Seq: 0x2AD67737 Ack: 0xC87C88D8 Win: 0x1F6 TcpLen: 32
TCP Options (3) => NOP NOP TS: 1545752292 1897160
```

Kiểm tra alert của snort thì thấy phát hiện tấn công.

Thực hiện time-based SQL injection với câu truy vấn 1' AND BENCHMARK(100000000, rand()) -- -. Kết quả thì trang web vẫn cứ load và không trả về gì cả.

Damn Vulnerable Web App x

192.168.85.200/dvwa/vulnerabilities/sql_i_blind/

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

DVWA

Vulnerability: SQL Injection (Blind)

Home
Instructions
Setup
Brute Force
Command Execution
CSRF
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored
DVWA Security
PHP Info
About
Logout

User ID:
MARK(100000000, rand()) -- - Submit

More info
<http://www.securiteam.com/securityreviews/5DP0N1P76E.html>
http://en.wikipedia.org/wiki/SQL_injection
<http://www.unlwxiv.net/techtips/sql-injection.html>

192.168.85.200 View Source View Help

Kiểm tra wireshark thì thấy

```
616 2121.1056196... 192.168.85.200 10.81.85.100 TCP 74 80 - 51232 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=2109273 TSecr=1547870100 WS=32
617 2121.1056419... 10.81.85.100 192.168.85.200 TCP 66 51232 - 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1547870103 TSecr=2109273
618 2121.1057667... 10.81.85.100 192.168.85.200 HTTP 634 GET /dvwa/vulnerabilities/sql_i_blind/?id=1%27+AND+BENCHMARK(28100000000%2C+rand%28%29%29+...&Submit=Submit
619 2121.3100428... 10.81.85.100 192.168.85.200 TCP 634 [TCP Retransmission] 51232 - 80 [PSH, ACK] Seq=1 Ack=1 Win=64256 Len=568 TSval=1547870908 TSecr=2109273
620 2121.5100161... 10.81.85.100 192.168.85.200 TCP 634 [TCP Retransmission] 51232 - 80 [PSH, ACK] Seq=1 Ack=1 Win=64256 Len=568 TSval=1547870910 TSecr=2109273
621 2121.9500220... 10.81.85.100 192.168.85.200 TCP 634 [TCP Retransmission] 51232 - 80 [PSH, ACK] Seq=1 Ack=1 Win=64256 Len=568 TSval=1547870948 TSecr=2109273
622 2122.7820174... 10.81.85.100 192.168.85.200 TCP 634 [TCP Retransmission] 51232 - 80 [PSH, ACK] Seq=1 Ack=1 Win=64256 Len=568 TSval=1547871780 TSecr=2109273
623 2124.0973848... 192.168.85.200 10.81.85.100 TCP 74 [TCP Retransmission] 80 - 51232 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=2109573 TSecr=
624 2124.0974048... 10.81.85.100 192.168.85.200 TCP 66 [TCP Dup ACK 617#1] 51232 - 80 [ACK] Seq=569 Ack=1 Win=64256 Len=0 TSval=1547873005 TSecr=2109273
625 2124.4400560... 10.81.85.100 192.168.85.200 TCP 634 [TCP Retransmission] 51232 - 80 [PSH, ACK] Seq=1 Ack=1 Win=64256 Len=568 TSval=1547873444 TSecr=2109273
> Frame 618: 634 bytes on wire (5072 bits), 634 bytes captured (5072 bits) on interface eth0, 0000 00 0c 29 aa 6f 90 00 0c 29 58 e0 d9 08 00 45 00 ) o...X...E
> Ethernet II, Src: VMware_58:e0:d9 (00:0c:29:58:e0:d9), Dst: VMware_aa:6f:90 (00:0c:29:aa:6f:90) l @...v Qud...
> Internet Protocol Version 4, Src: 10.81.85.100, Dst: 192.168.85.200 U...P...i...
> Transmission Control Protocol, Src Port: 51232, Dst Port: 80, Seq: 1, Ack: 1, Len: 568 x...AB...
> Hypertext Transfer Protocol 0000 00 0c 29 aa 6f 90 00 0c 29 58 e0 d9 08 00 45 00 /YGET /d vwa/vuln
0000 01 f6 78 84 00 00 01 01 08 0a 5c 42 9f 97 00 20 erabilit ies/sql
0000 00 00 5f 62 6c 69 6e 64 2f 3f 69 64 3d 31 25 32 37 2b _blind/? id=1%27+
0000 41 4e 44 2b 20 42 45 4e 43 48 4d 41 52 4b 25 32 AND+BEN CHMARK%2
0000 39 31 30 30 30 30 30 30 30 30 25 32 43 2b 72 61 81000000 00%2C+ra
0000 6e 64 25 32 38 25 32 39 25 32 39 2b 2d 2d 2d 2d nd%28%29 %29+...
0000 26 53 75 62 6d 69 74 3d 53 75 62 6d 69 74 20 48 &Submit= Submit H
0000 54 54 50 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 31 TTP/1.1 Host: 1
0000 39 32 2e 31 36 38 2e 38 35 2e 32 30 30 0d 0a 55 92.100.8 5.200 U
0000 73 65 72 2d 41 67 05 6e 74 3a 20 4d 6f 7a 69 6c ser-Agen t: Mozil
0000 6c 61 2f 35 2e 30 20 28 58 31 31 3b 20 4c 69 6e la/5.0 ( X11; Lin
0000 75 78 20 78 38 36 5f 30 34 3b 20 72 76 3a 31 32 ux x86_0 4; rv:12
0100 38 2e 30 29 20 47 05 63 6b 6f 2f 32 30 31 30 30 8.0) Geck ko/20100
0110 31 38 31 20 46 69 72 65 66 6f 78 2f 31 32 38 2e 101 Fire fox/128.
0120 30 0d 0a 41 63 63 65 70 74 3a 20 74 65 76 74 2f o Accet t: text/
0130 68 74 6d 6c 2c 61 70 70 6c 69 63 61 74 69 6f 6e html,app lication
```


eth0: <live capture in progress> Packets: 687 Profile: Default

1052	3102.4971792...	10.81.85.1	10.81.85.100	ICMP	102 Destination unreachable (Host unreachable)
1053	3102.4971795...	10.81.85.1	10.81.85.100	ICMP	102 Destination unreachable (Host unreachable)
1054	3102.4971796...	10.81.85.1	10.81.85.100	ICMP	102 Destination unreachable (Host unreachable)
1055	3102.4972737...	10.81.85.1	10.81.85.100	ICMP	102 Destination unreachable (Host unreachable)
1056	3104.9291505...	VMware_aa:6f:90	VMware_58:e0:d9	ARP	60 Who has 10.81.85.100? Tell 10.81.85.1
1057	3104.9291637...	VMware_58:e0:d9	VMware_aa:6f:90	ARP	42 10.81.85.100 is at 00:0c:29:58:e0:d9

Kiểm tra alert của snort thì thấy có cảnh báo

← → ↻ 🏠 192.168.85.200/dvwa/vulnerabilities/sqli_blind/?id=benchmark&Submit=Submit# ☆ 📌

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec



Home

Instructions

Setup

Brute Force

Command Execution

CSRF

File Inclusion

Vulnerability: SQL Injection (Blind)

User ID:

Submit

More info

<http://www.securiteam.com/securityreviews/5DP0N1P76E.html>
http://en.wikipedia.org/wiki/SQL_injection
<http://www.unixwiz.net/techtips/sql-injection.html>

--HẾT--