

**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG
KHOA CÔNG NGHỆ THÔNG TIN**



Học phần: **Kỹ Thuật theo dõi và giám sát an toàn mạng**

Thực hành:
Bài Thực hành số 2

Giảng viên hướng dẫn: Ninh Thị Thu Trang

Sinh viên thực hiện:

Đỗ Quang Huy B18DCAT106

Hà Nội 2022

I Tìm hiểu lý thuyết

Giám sát chi tiết các mạng sử dụng nhật ký

Một tệp nhật ký rất hữu ích khi phân tích các loại sự cố mạng, bao gồm cả những sự kiện làm tổn hại đến tính toàn vẹn bảo mật của nó. Zeek tận dụng rất tốt điều này, cung cấp một tệp tóm tắt một phần tốt của nhật ký mà nó có thể tạo, dựa trên các giao thức khác nhau. Một số giao thức mà chúng tôi có thể trích dẫn là:

- DHCP
- DNS
- FTP
- HTTP
- SNMP
- SMTP
- SSL và nhiều hơn nữa

Ở trên, chúng tôi thấy ảnh chụp màn hình của tất cả các trường có trong nhật ký của DNS kết nối. Có thể thấy rằng mỗi trường mô tả chi tiết loại dữ liệu có thể được xem và một mô tả thông tin ngắn gọn. Hãy trích dẫn một vài trường làm ví dụ:

- trans_id: một số duy nhất được tạo để xác định nhật ký được tạo.
- mật mã: giá trị của mã phản hồi DNS.
- từ chối: đây là trường giá trị boolean (đúng hoặc sai) cho chúng tôi biết nếu yêu cầu kết nối DNS bị từ chối hay không.

Một khía cạnh thường được nhận xét liên quan đến nhật ký là chúng rất rộng và phức tạp để hiểu. Thông qua này tài liệu hỗ trợ, bạn sẽ có thể hiểu rõ hơn nội dung của nhật ký và đạt được sự kiểm soát các sự kiện bảo mật.

Giám sát tập lệnh

Một cơ sở khác mà chúng ta có thể nêu bật từ Zeek là có thể có một số tập lệnh được cấu hình sẵn và sẵn sàng sử dụng. Chúng được sử dụng để thực hiện các hoạt động giám sát mạng riêng, được sử dụng thường xuyên, vì vậy bạn sẽ tiết kiệm thời gian.

Một trong những đoạn script mà chúng ta có thể làm nổi bật là đoạn script tương ứng với Máy phát hiện đình trệ HTTP . Điều này được sử dụng để phát hiện các cuộc tấn công DDoS loại đình chỉ HTTP, để có ý tưởng, loại DDoS này tận dụng một trong những lỗi có liên quan nhất của máy chủ web.

Nó bao gồm việc không thể xác định xem máy khách từ xa có được kết nối với máy chủ thông qua liên kết kết nối chậm hay không. Hoặc, nếu cùng một khách hàng đang gửi dữ liệu mà không có bất kỳ điều khiển nào ở tốc độ rất chậm. Do đó, máy chủ web không thể tạo thời gian chờ để hủy kết nối đó sau một thời gian nhất định hoặc đơn giản là chấm dứt nó. Nếu một máy chủ web có dung lượng hạn chế, nó có thể dễ dàng bị ảnh hưởng bởi các loại tấn công này.

Nếu bạn muốn tận dụng lợi thế của tập lệnh này hoặc tập lệnh khác, bạn phải nhập công thông tin chính thức của Ánh sáng mặt trời công ty, hỗ trợ Zeek, để truy cập chúng thông qua kho lưu trữ Github chính thức của nó. Các tài nguyên khác cũng có sẵn trên cùng một trang để giúp bạn bắt đầu sử dụng công cụ.

II Thực hành

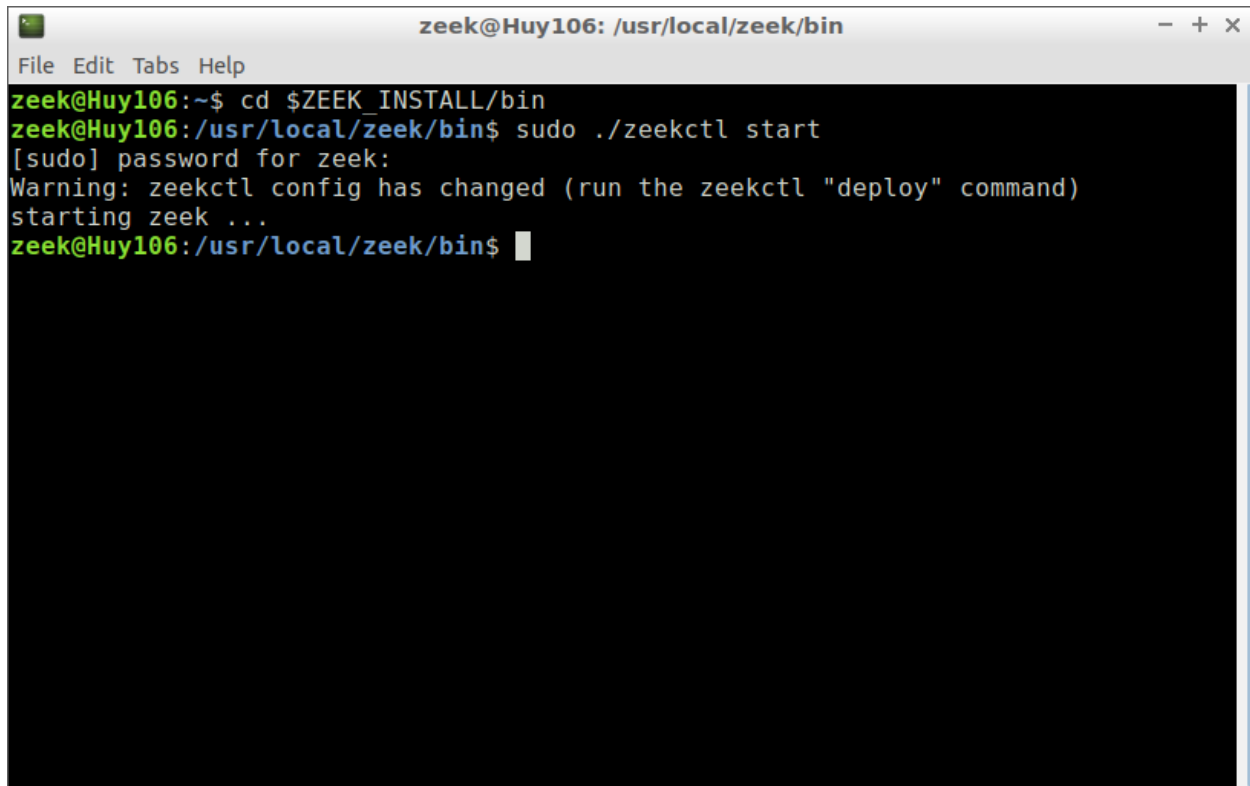
1 Phân tích log file sử dụng Zeek Scripting

Tcpdump và lưu file Pcap

```
zeek@Huy106:~/Zeek-Labs/Sample-PCAP$ sudo tcpdump -i ens33 -w Huy106.pcap
[sudo] password for zeek:
tcpdump: listening on ens33, link-type EN10MB (Ethernet), capture size 262144 bytes
^C8541 packets captured
8542 packets received by filter
0 packets dropped by kernel
zeek@Huy106:~/Zeek-Labs/Sample-PCAP$ ls
bigFlows.pcap      Huy106.pcap      sshguess.pcap
bruteforce.pcap   proxy.pcap       testset.arff
DecisionTable.model smallFlows.pcap  trainset.arff
```

Khởi chạy zeekctl

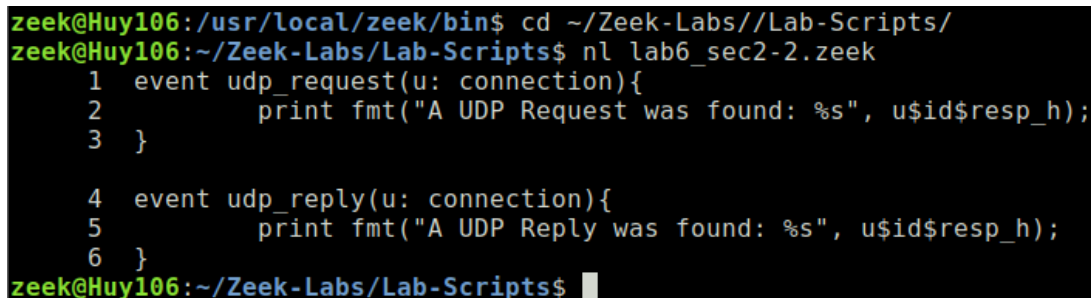
cd \$ZEEK_INSTALL/bin && sudo ./zeekctl start



```
zeek@Huy106: /usr/local/zeek/bin
File Edit Tabs Help
zeek@Huy106:~$ cd $ZEEK_INSTALL/bin
zeek@Huy106:/usr/local/zeek/bin$ sudo ./zeekctl start
[sudo] password for zeek:
Warning: zeekctl config has changed (run the zeekctl "deploy" command)
starting zeek ...
zeek@Huy106:/usr/local/zeek/bin$
```

Phân tích lưu lượng UDP với Zeek Script:

✓ Di chuyển đến thư mục Zeek-Labs//Labs-scripts. Tại đây mở file lab6_sec2-2.zeek để xem nội dung:



```
zeek@Huy106:/usr/local/zeek/bin$ cd ~/Zeek-Labs//Lab-Scripts/
zeek@Huy106:~/Zeek-Labs/Lab-Scripts$ nl lab6_sec2-2.zeek
 1 event udp_request(u: connection){
 2     print fmt("A UDP Request was found: %s", u$id$resp_h);
 3 }
 4 event udp_reply(u: connection){
 5     print fmt("A UDP Reply was found: %s", u$id$resp_h);
 6 }
zeek@Huy106:~/Zeek-Labs/Lab-Scripts$
```

➔ Nếu bắt được 1 udp request thì in nó ra

✓ Di chuyển đến thư mục Zeek-Labs/UDP-Traffics và thực hiện câu lệnh sau rồi chụp màn hình kết quả sau khi thực hiện lệnh

zeek -C -r ../Sample-PCAP/Ten_MaSV.pcap ../Lab-Scripts/ lab6_sec2-2.zeek

```

zeek@Huy106:~/Zeek-Labs/UDP-Traffic$ sudo zeek -C -r ../Sample-PCAP/Huy106.pcap
../Lab-Scripts/lab6_sec2-2.zeek
A UDP Request was found: 192.168.1.1
A UDP Request was found: 192.168.1.1
A UDP Reply was found: 192.168.1.1
A UDP Reply was found: 192.168.1.1
A UDP Request was found: 192.168.1.1
A UDP Request was found: 192.168.1.1
A UDP Reply was found: 192.168.1.1
A UDP Reply was found: 192.168.1.1

```

```

A UDP Request was found: ff02::c
A UDP Request was found: 192.168.1.1
A UDP Request was found: 192.168.1.1
A UDP Reply was found: 192.168.1.1
A UDP Reply was found: 192.168.1.1
A UDP Request was found: 91.189.89.199
A UDP Reply was found: 91.189.89.199
A UDP Request was found: 239.255.255.250

```

Phân tích lưu lượng TCP với Zeek Script:

✓ Mở file lab6_sec2-3.zeek để xem nội dung:

```

zeek@Huy106:~/Zeek-Labs/UDP-Traffic$ nl ../Lab-Scripts/lab6_sec2-3.zeek
1  event tcp_packet(c: connection, is_orig: bool, flags: string, seq: count
, ack: count, len: count, payload: string) {
2      print fmt("Destination Port #: %s", c$id$resp_p);
3  }
zeek@Huy106:~/Zeek-Labs/UDP-Traffic$

```

➔ Show ra port bắt được ở gói tin Pcap

✓ Thực hiện câu lệnh sau rồi chụp màn hình kết quả sau khi thực hiện lệnh:

zeek -C -r ../Sample-PCAP/Ten_MaSV.pcap ../Lab-Scripts/ lab6_sec2-3.zeek

```
zeek@Huy106: ~/Zeek-Labs/UDP-Irampc
File Edit Tabs File Edit Tabs Help
zeek@Huy106:~ Destination Port #: 443/tcp
EnableProfil Destination Port #: 443/tcp
lab10_sec2-1 Destination Port #: 443/tcp
lab11_benign Destination Port #: 443/tcp
lab11_create Destination Port #: 443/tcp
lab11_malicio Destination Port #: 443/tcp
lab3_sec3-2.a Destination Port #: 443/tcp
zeek@Huy106:~ Destination Port #: 443/tcp
Destination Port #: 443/tcp
Destination Port #: 443/tcp
Destination Port #: 443/tcp
Destination Port #: 443/tcp
Destination Port #: 80/tcp
Destination Port #: 80/tcp
Destination Port #: 80/tcp
Destination Port #: 80/tcp
Destination Port #: 443/tcp
Destination Port #: 443/tcp
Destination Port #: 443/tcp
Destination Port #: 80/tcp
Destination Port #: 80/tcp
Destination Port #: 443/tcp
```

Đổi tên file conn.log thành UpdatedConn.log

✓ Mở file lab6_sec3-1.zeek để xem script nl ../Lab-Scripts/lab6_sec3-1.zeek

```
zeek@Huy106:~/Zeek-Labs/UDP-Traffic$ nl ../Lab-Scripts/lab6_sec3-1.zeek
1  event zeek_init(){
2
3      local update = Log::get_filter(Conn::LOG, "default");
4      update$path = "UpdatedConn";
5      Log::add_filter(Conn::LOG, update);
6  }
```

➔ Đơn giản chỉ là update file conn.log và sửa tên

✓ Thực hiện phân tích file Ten_MaSV.pcap sử dụng script trong file lab6_sec3-1.zeek

zeek -C -r ../Sample-PCAP/Ten_MaSV.pcap ../Lab-Scripts/lab6_sec3-1.zeek

```
zeek@Huy106:~/Zeek-Labs/UDP-Traffic$ sudo zeek -C -r ../Sample-PCAP/Huy106.pcap
../Lab-Scripts/lab6_sec3-1.zeek
zeek@Huy106:~/Zeek-Labs/UDP-Traffic$ ls
```

✓ Kiểm tra file UpdatedConn.log đã tạo được.

```
zeek@Huy106:~/Zeek-Labs/UDP-Traffic$ ls
conn.log  dpd.log  ntp.log  ssl.log  weird.log
dhcp.log  files.log packet_filter.log  udptraffic.pcap  x509.log
dns.log   http.log snmp.log  UpdatedConn.log
```

Cập nhật file conn.log

✓ Mở file lab6_sec3-2.zeeb để xem script

nl ../Lab-Scripts/lab6_sec3-2.zeeb

```
zeek@Huy106:~/Zeek-Labs/UDP-Traffic$ nl ../Lab-Scripts/lab6_sec3-2.zeeb
1 function http_only(rec: Conn::Info) : bool {
2
3     return rec?$service && rec$service == "http";
4 }
5
6 event zeek_init(){
7     local filter: Log::Filter = [$name="http-only", $path="conn-http", $pred=http_only];
8     Log::add_filter(Conn::LOG, filter);
9 }
zeek@Huy106:~/Zeek-Labs/UDP-Traffic$
```

➔ Cập nhật file update log vào file conn

Thực hiện phân tích file Ten_MaSV.pcap sử dụng script trong file lab6_sec3-2.zeeb

zeek -C -r ../Sample-PCAP/Ten_MaSV.pcap ../Lab-Scripts/ lab6_sec3-2.zeeb

```
zeek@Huy106:~/Zeek-Labs/UDP-Traffic$ sudo zeek -C -r ../Sample-PCAP/Huy106.pcap ../Lab-Scripts/lab6_sec3-2.zeeb
zeek@Huy106:~/Zeek-Labs/UDP-Traffic$ ls
conn-http.log  dns.log      http.log      snmp.log      UpdatedConn.log
conn.log       dpd.log      ntp.log       ssl.log       weird.log
dhcp.log       files.log    packet_filter.log  udptraffic.pcap  x509.log
zeek@Huy106:~/Zeek-Labs/UDP-Traffic$ cat conn-http.log
cat: conn-http.log: No such file or directory
zeek@Huy106:~/Zeek-Labs/UDP-Traffic$ cat conn-http.log
#separator \x09
#set_separator ,
#empty_field (empty)
#unset_field -
#path conn-http
#open 2022-04-24-22-52-42
#fields ts uid id.orig_h id.orig_p id.resp_h id.resp_h id.resp_
p proto service duration orig_bytes resp_bytes conn_sta
te local_orig local_resp missed_bytes history orig_pkts o
rig_ip_bytes resp_pkts resp_ip_bytes tunnel_parents
#types time string addr port addr port enum string interval
count count string bool bool count string count count count c
ount set[string]
1650853335.987097 C0zYry4iHJrmWJT9ql 192.168.1.188 49132 27.71.11
2.177 80 tcp http 42.239368 756 1777 SF - -
0 ShAdadEf 11 1336 8 2201 -
```

2 Phân tích log file sử dụng Zeek Signatures

- o Khởi chạy zeekctl
- o Di chuyển đến thư mục /Zeek-Labs/Lab-Scripts/
- o Mở file lab7_sec2-2.sig để xem nội dung

```

zeek@Huy106: ~/Zeek-Labs/Lab-Scripts
File Edit Tabs Help
zeek@Huy106:~/Zeek-Labs/Lab-Scripts$ cd ..
zeek@Huy106:~/Zeek-Labs$ cd ,,
bash: cd: ,,: No such file or directory
zeek@Huy106:~/Zeek-Labs$ cd ..
zeek@Huy106:~$ cd $ZEEK_INSTALL/bin/ && sudo ./zeekctl start
[sudo] password for zeek:
Warning: zeekctl config has changed (run the zeekctl "deploy" command)
starting zeek ...
zeek@Huy106:~/usr/local/zeek/bin$ cd ~/Zeek-Labs/Lab-Scripts/
zeek@Huy106:~/Zeek-Labs/Lab-Scripts$ nl lab7_sec2-2.sig
  1 signature HTTP-POST-sig{
  2     ip-proto == tcp
  3     dst-port == 80
  4     payload /POST/
  5     event "Found HTTP Post"
  6 }

  7 signature HTTP-GET-sig{
  8     ip-proto == tcp
  9     dst-port == 80
 10     payload /GET/
 11     event "Found HTTP Request"
 12 }

```

⇒ Bắt giao thức Post và Get khi duyệt mạng lướt web

Phân tích lưu lượng từ một file pcap và chữ ký Zeek

✓ Di chuyển đến thư mục TCP-Traffic

✓ Thực hiện câu lệnh sau:

zeek -r ../Sample-PCAP/Ten_MaSV.pcap -s ../Lab-Scripts/lab7_sec2-2.sig

✓ Mở file signature.log để xem:

gedit signatures.log

```

zeek@Huy106:~/Zeek-Labs/TCP-Traffic$ zeek -C -r ../Sample-PCAP/Huy106.pcap -s ../Lab-Scripts/lab7_sec2-2.sig
1650853335.661753 error: notice/Log::WRITER_ASCII: cannot open notice.log: Permission denied
1650853335.661753 error: notice/Log::WRITER_ASCII: terminating thread
1650853335.730194 error: reporter/Log::WRITER_ASCII: cannot open reporter.log: Permission denied
1650853335.730194 error: reporter/Log::WRITER_ASCII: terminating thread

```



```

zeek@Huy106:~/Zeek-Labs/TCP-Traffic$ ls
benign.csv      dpd.log         output.csv      prof.log        tcptraffic-pcap weird.log
browser.txt     files.log       output.txt      randomized.csv  tcptraffic.pcap x509.log
christelle.csv  http.log        packet2.csv     reporter.log    tctraffic.pcap  test.csv
conn.log        malicious.csv   packet3.csv     scantraffic.pcap testset.arff
dataset.csv     notice.log      packet4.csv     signatures.log  testset.arff
dhcp.log        ntp.log         packet.csv      snmp.log        trainset.arff
dns.log         ntraffic.pcap  packet_filter.log ssl.log         udptraffic.pcap
zeek@Huy106:~/Zeek-Labs/TCP-Traffic$ gedit signatures.log

(gedit:1764): dbind-WARNING **: 23:31:22.542: Error retrieving accessibility bus address: org.freedesktop.DBus.Error.ServiceUnknown: The name org.ally.Bus was not provided by any .service files

```

```

#separator \x09
#set separator ,
#empty_field (empty)
#unset field -
#path signatures
#open 2022-04-24-23-29-57
#fields ts uid src_addr src_port dst_addr dst_port note sig_id
event_msg sub_msg sig_count host_count
#types time string addr port addr port enum string string string count count
1650853335.623154 ChZP9j5UXn3YRb1Pj 192.168.1.188 51470 34.107.221.82 80
Signatures::Sensitive_Signature HTTP-GET-sig 192.168.1.188: Found HTTP Request GET /success.txt HTTP/
1.1\x0d\x0aHost: detectportal.firefox.com\x0d\x0aUser-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:71.0)
Gecko/20100101 Firef... -
1650853335.784601 C49YB0AX3Y7ul4Qqf 192.168.1.188 51472 34.107.221.82 80
Signatures::Sensitive_Signature HTTP-GET-sig 192.168.1.188: Found HTTP Request GET /success.txt?ipv4
HTTP/1.1\x0d\x0aHost: detectportal.firefox.com\x0d\x0aUser-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:
71.0) Gecko/20100101 ...
1650853336.038281 CELPhrcEPFV0hpSwe 192.168.1.188 49132 27.71.112.177 80
Signatures::Sensitive_Signature HTTP-POST-sig 192.168.1.188: Found HTTP Post POST / HTTP/1.1\x0d\x0aHost:
r3.o.lencr.org\x0d\x0aUser-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:71.0) Gecko/20100101 Firefox/
71.0\x0d\x0aAccept: */*...
1650853336.122941 C2Trjxlyy6GJ12Xaue 192.168.1.188 35154 172.217.27.3 80
Signatures::Sensitive_Signature HTTP-POST-sig 192.168.1.188: Found HTTP Post POST /gts1c3 HTTP/
1.1\x0d\x0aHost: ocsf.pki.goog\x0d\x0aUser-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:71.0) Gecko/
20100101 Firefox/71.0\x0d\x0aAccept...
1650853336.400276 Cz8t593ur8v6HdCMYd 192.168.1.188 41856 204.246.169.219 80
Signatures::Sensitive_Signature HTTP-POST-sig 192.168.1.188: Found HTTP Post POST / HTTP/1.1\x0d\x0aHost:
ocsp.scalb.amazontrust.com\x0d\x0aUser-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:71.0) Gecko/20100101
Firefox/71.0\x0d...
1650853337.023157 C0QJil33JyAhtqCPV6 192.168.1.188 40982 117.18.237.29 80
Signatures::Sensitive_Signature HTTP-POST-sig 192.168.1.188: Found HTTP Post POST / HTTP/1.1\x0d\x0aHost:
ocsp.digicert.com\x0d\x0aUser-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:71.0) Gecko/20100101 Firefox/
71.0\x0d\x0aAccept: ...
1650853342.015530 Cxu0AM2bl2sbwL0Yfi 192.168.1.188 41004 117.18.237.29 80
Signatures::Sensitive_Signature HTTP-POST-sig 192.168.1.188: Found HTTP Post POST / HTTP/1.1\x0d\x0aHost:
ocsp.digicert.com\x0d\x0aUser-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:71.0) Gecko/20100101 Firefox/
71.0\x0d\x0aAccept: ...
1650853345.274227 CivX3i2azSwa9B04F7 192.168.1.188 35954 142.250.204.78 80
Plain Text Tab Width: 8 Ln 5, Col 1 INS

```

Thực thi chữ ký Zeek cho phân tích lưu lượng mạng ✓ Mở file lab7_sec3-1.sig trong thư mục Lab-Scripts để xem nội dung.

```
zeek@Huy106: ~/Zeek-Labs/Lab-Scripts
File Edit Tabs Help
zeek@Huy106:~/Zeek-Labs/TCP-Traffic$ cd ../Lab-Scripts/
zeek@Huy106:~/Zeek-Labs/Lab-Scripts$ nl lab7_sec3-1.sig
 1 signature SNMP-REQUEST-sig{
 2     ip-proto == udp
 3     dst-port == 161
 4     event "Found SNMP Request"
 5 }
 6 signature SNMP-RESPONSE-sig{
 7     ip-proto == udp
 8     dst-port == 52400
 9     event "Found SNMP Response"
10 }
11 signature DNS-REQUEST-sig{
12     ip-proto == udp
13     dst-port == 53
14     event "Found DNS Request"
15 }
zeek@Huy106:~/Zeek-Labs/Lab-Scripts$
```

⇒ Bắt các dịch vụ
SNMP request -respond ở cổng 161 – 52400.
DNS request ở cổng 53

✓ Thực hiện 2 câu lệnh sau và chụp lại màn hình kết quả:

```
zeek@Huy106:~/Zeek-Labs/TCP-Traffic$ zeek -r ../Sample-PCAP/smallFlows.pcap -s ../Lab-Scripts/lab7_sec3-1.sig
1295981655.926096 error: notice/Log::WRITER_ASCII: cannot open notice.log: Permission denied
1295981655.926096 error: notice/Log::WRITER_ASCII: terminating thread
1295981655.932294 error: reporter/Log::WRITER_ASCII: cannot open reporter.log: Permission denied
1295981655.932294 error: reporter/Log::WRITER_ASCII: terminating thread
1295981840.989753 fatal error: cannot lock mutex: Invalid argument
Aborted (core dumped)
zeek@Huy106:~/Zeek-Labs/TCP-Traffic$ grep SNMP ~/Zeek-Labs/TCP-Traffic/signatures.log
1295981744.511002 CfEX0N2Up51qu1p4R2 192.168.3.131 52400 192.168.3.99 161 Signa
tures::Sensitive_Signature SNMP-REQUEST-sig 192.168.3.131: Found SNMP Request (empty) -
1295981744.570907 CfEX0N2Up51qu1p4R2 192.168.3.99 161 192.168.3.131 52400 Signa
tures::Sensitive_Signature SNMP-RESPONSE-sig 192.168.3.99: Found SNMP Response (empty) -
zeek@Huy106:~/Zeek-Labs/TCP-Traffic$
```

