Stephanie Vergil

ZEEK INSTRUSION DETECTION SERIES

Lab 7: Introduction to Zeek Signatures

Using Zeek's signature framework, we can craft pattern-based filters to analyze log files efficiently. Below are examples of how to use Zeek signatures for network analysis.

2.1 Starting a new instance of Zeek.

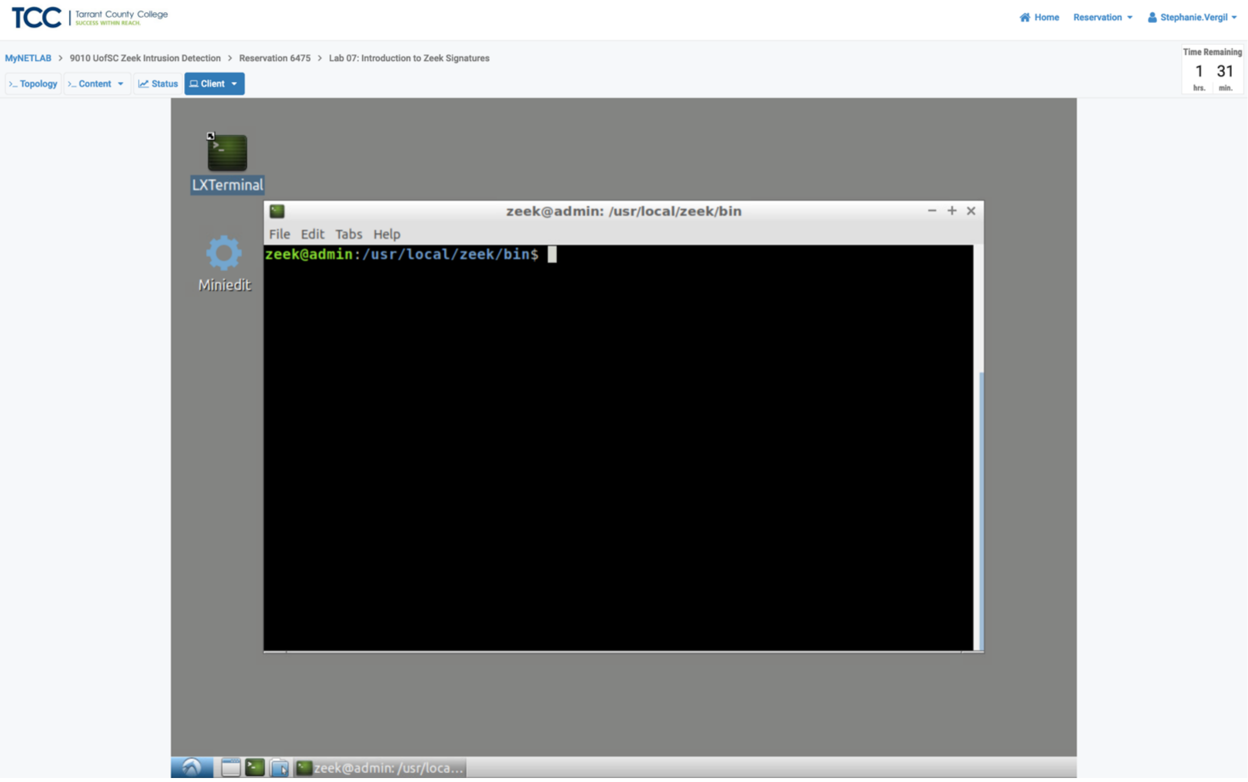
Step 1. Click on the Client button to launch the client machine.

Step2. Once the client machine is open, the desktop will display and on the left side of the screen double click on the LXTerminal to launch.

Step 3. To start Zeek enter the following command:

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

once prompt enter the password to continue. This command enters Zeek's default installation directory and invokes Zeekctl tool to start a new instance.


TCC | Tarrant County College
Home
Reservation
Stephanie.Vergil
MyNETLAB > 9010 UofSC Zeek Intrusion Detection > Reservation 6475 > Lab 07: Introduction to Zeek Signatures
Time Remaining 1 hrs. 31 min.
Topology
Content
Status
Client
LXTerminal
Miniedit
zeek@admin: /usr/local/zeek/bin
File Edit Tabs Help
zeek@admin: /usr/loca...

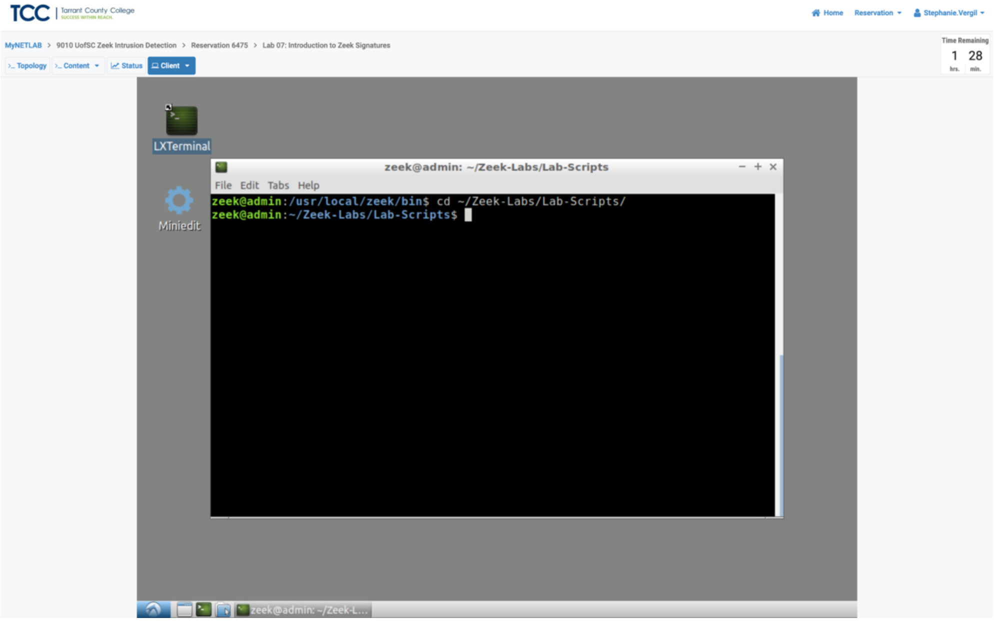
```
zeek@admin:/usr/local/zeek/bin$
```

2.2 Viewing a premade Zeek signature file.

Stephanie Vergil

Step 1. Enter the following command to Navigate to the Lab-Scripts directory:

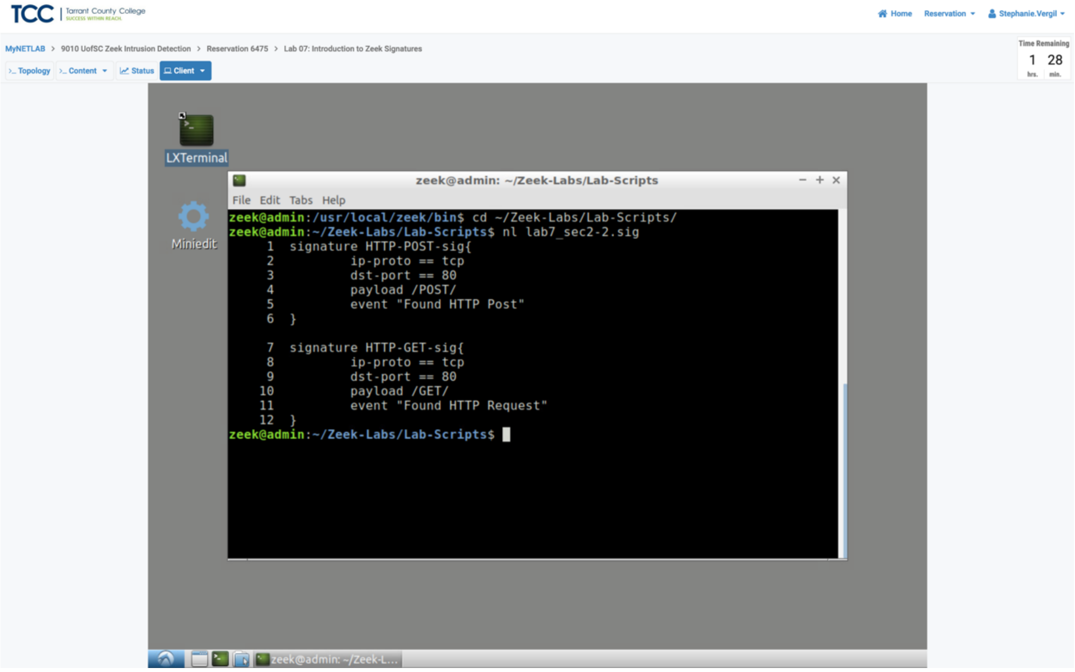
cd ~/Zeek-Labs/Lab-Scripts/


TCC | Tarrant County College SUCCESS WITHIN REACH
Home
Reservation
Stephanie.Vergil
MyNETLAB > 9010 UofSC Zeek Intrusion Detection > Reservation 6475 > Lab 07: Introduction to Zeek Signatures
Topology
Content
Status
Client
Time Remaining
1 28
hrs. min.
LXTerminal
Miniedit
zeek@admin: ~/Zeek-Labs/Lab-Scripts
File Edit Tabs Help
zeek@admin: ~/Zeek-L...

```
zeek@admin:/usr/local/zeek/bin$ cd ~/Zeek-Labs/Lab-Scripts/
zeek@admin:~/Zeek-Labs/Lab-Scripts$ 
```

Step 2. Enter the following command to display the contents of the lab7_sec2-2.sig file using nl:

nl lab7_sec2-2.sig


TCC | Tarrant County College SUCCESS WITHIN REACH
Home
Reservation
Stephanie.Vergil
MyNETLAB > 9010 UofSC Zeek Intrusion Detection > Reservation 6475 > Lab 07: Introduction to Zeek Signatures
Topology
Content
Status
Client
Time Remaining
1 28
hrs. min.
LXTerminal
Miniedit
zeek@admin: ~/Zeek-Labs/Lab-Scripts
File Edit Tabs Help
zeek@admin: ~/Zeek-L...

```
zeek@admin:/usr/local/zeek/bin$ cd ~/Zeek-Labs/Lab-Scripts/
zeek@admin:~/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  }
zeek@admin:~/Zeek-Labs/Lab-Scripts$ 
```

This signature file contains two signatures to be matched during network traffic analysis and is explained as follows.

Each number represents the respective line number:

1. This line defines a new signature object, with the name HTTP-POST-sig.

2. Defines the desired match’s transport protocol to be TCP.

3. Defines the desired match’s destination port to be 80.

4. Defines the desired match’s payload to contain the regular expression equivalent to ‘POST’.

5. Defines an event if the match is found. Currently, the event will post a “Found HTTP Post” message. 7. This line defines a new signature object, with the name HTTP-GET-sig.

8. Defines the desired match’s transport protocol to be TCP.

9. Defines the desired match’s destination port to be 80.

10. Defines the desired match’s payload to contain the regular expression equivalent to ‘GET’.

11. Defines an event if the match is found. Currently, the event will post a “Found HTTP Request” message.

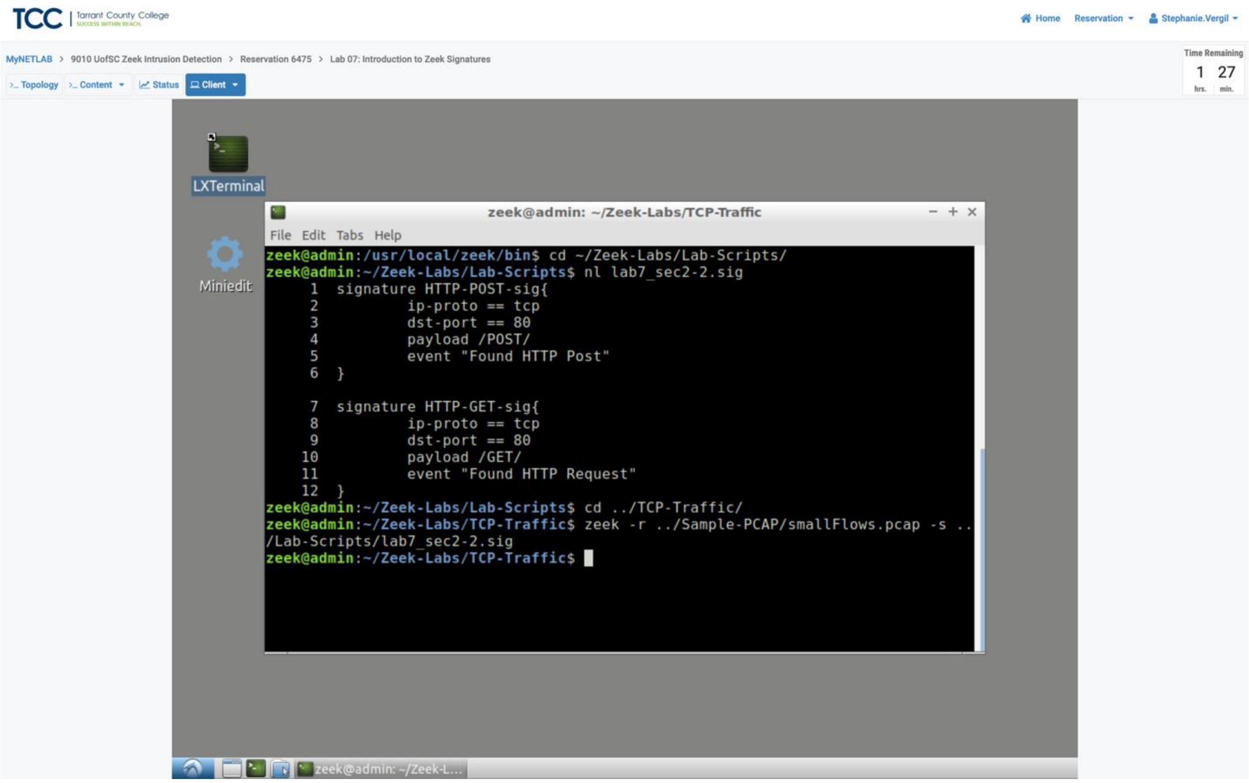
2.3 Executing the premade Zeek signature file.

Step 1. Enter the following command to navigate to the TCP-Traffic directory:

```
cd ../TCP-Traffic/
```

Step 2. Enter the following command to Process the smallFlows.pcap packet capture file using the signature file lab7_sec2- 2.sig.

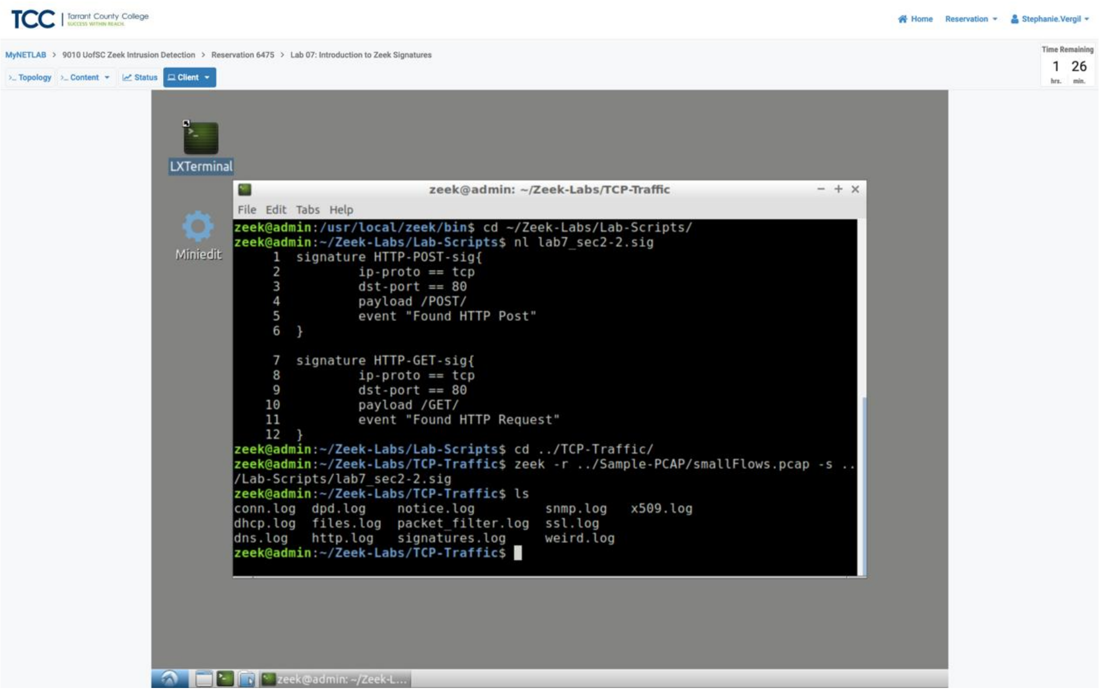
```
zeek –r ../Sample-PCAP/smallFlows.pcap –s ../Lab-Scripts/lab7_sec2-2.sig
```


TCC | Tarrant County College
SUCCESS WITHIN REACH.
Home
Reservation
Stephanie.Vergil
MyNETLAB > 9010 UofSC Zeek Intrusion Detection > Reservation 6475 > Lab 07: Introduction to Zeek Signatures
Topology
Content
Status
Client
Time Remaining
1 27
hrs. min.
LXTerminal
Miniedit
zeek@admin: ~/Zeek-Labs/TCP-Traffic
File Edit Tabs Help
zeek@admin: ~/Zeek-L...

```
zeek@admin:/usr/local/zeek/bin$ cd ~/Zeek-Labs/Lab-Scripts/
zeek@admin:~/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  }
zeek@admin:~/Zeek-Labs/Lab-Scripts$ cd ../TCP-Traffic/
zeek@admin:~/Zeek-Labs/TCP-Traffic$ zeek -r ../Sample-PCAP/smallFlows.pcap -s ..
/Lab-Scripts/lab7_sec2-2.sig
zeek@admin:~/Zeek-Labs/TCP-Traffic$ 
```

Step 3. Enter the following command to list the generated log files in the current directory:

ls

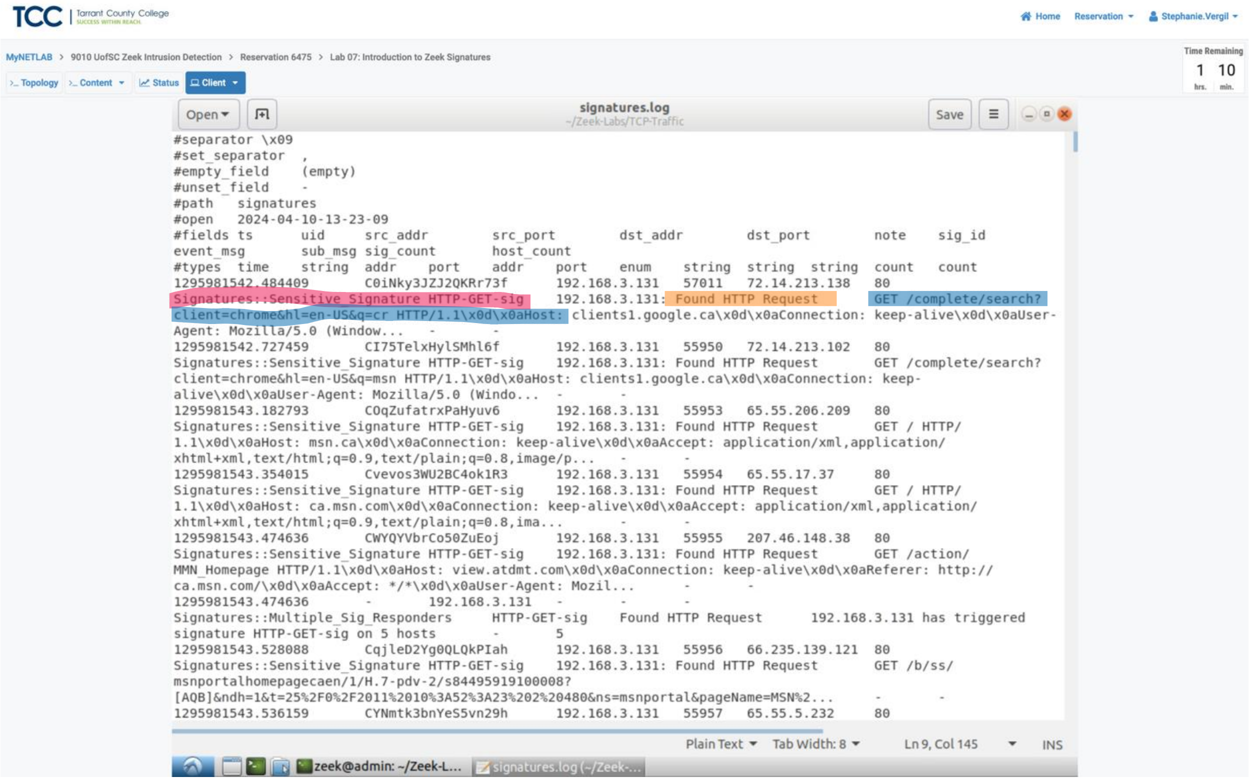

TCC | Tarrant County College
SUCCESS WITHIN REACH.
Home
Reservation
Stephanie.Vergil
MyNETLAB > 9010 UofSC Zeek Intrusion Detection > Reservation 6475 > Lab 07: Introduction to Zeek Signatures
Topology
Content
Status
Client
Time Remaining
1 26
hrs. min.
LXTerminal
Miniedit
zeek@admin: ~/Zeek-Labs/TCP-Traffic
File Edit Tabs Help
zeek@admin: ~/Zeek-L...

```
zeek@admin:/usr/local/zeek/bin$ cd ~/Zeek-Labs/Lab-Scripts/
zeek@admin:~/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  }
zeek@admin:~/Zeek-Labs/Lab-Scripts$ cd ../TCP-Traffic/
zeek@admin:~/Zeek-Labs/TCP-Traffic$ zeek -r ../Sample-PCAP/smallFlows.pcap -s ..
/Lab-Scripts/lab7_sec2-2.sig
zeek@admin:~/Zeek-Labs/TCP-Traffic$ ls
conn.log  dpd.log    notice.log         snmp.log   x509.log
dhcp.log  files.log  packet_filter.log  ssl.log
dns.log   http.log   signatures.log     weird.log
zeek@admin:~/Zeek-Labs/TCP-Traffic$ 
```

A new log file that has not been previously introduced is now displayed: signatures.log. Log will contain all signature matches and their corresponding events and notices.

Step 4. To view the contents of the signatures.log file using the gedit text editor enter the following command:

gedit signatures.log



```
#separator \x09
#set_separator  ,
#empty_field    (empty)
#unset_field    -
#path   signatures
#open   2024-04-10-13-23-09
#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
1295981542.484409       C0iNky3JZJ2QKRr73f      192.168.3.131   57011   72.14.213.138   80
Signatures::Sensitive_Signature HTTP-GET-sig    192.168.3.131: Found HTTP Request       GET /complete/search?
client=chrome&hl=en-US&q=cr HTTP/1.1\x0d\x0aHost: clients1.google.ca\x0d\x0aConnection: keep-alive\x0d\x0aUser-
Agent: Mozilla/5.0 (Window...    -       -
1295981542.727459       CI75TelxHylSMhl6f       192.168.3.131   55950   72.14.213.102   80
Signatures::Sensitive_Signature HTTP-GET-sig    192.168.3.131: Found HTTP Request       GET /complete/search?
client=chrome&hl=en-US&q=msn HTTP/1.1\x0d\x0aHost: clients1.google.ca\x0d\x0aConnection: keep-
alive\x0d\x0aUser-Agent: Mozilla/5.0 (Windo...  -       -
1295981543.182793       COqZufatrxPaHyuv6       192.168.3.131   55953   65.55.206.209   80
Signatures::Sensitive_Signature HTTP-GET-sig    192.168.3.131: Found HTTP Request       GET / HTTP/
1.1\x0d\x0aHost: msn.ca\x0d\x0aConnection: keep-alive\x0d\x0aAccept: application/xml,application/
xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/p...   -       -
1295981543.354015       Cvevos3WU2BC4ok1R3      192.168.3.131   55954   65.55.17.37     80
Signatures::Sensitive_Signature HTTP-GET-sig    192.168.3.131: Found HTTP Request       GET / HTTP/
1.1\x0d\x0aHost: ca.msn.com\x0d\x0aConnection: keep-alive\x0d\x0aAccept: application/xml,application/
xhtml+xml,text/html;q=0.9,text/plain;q=0.8,ima...       -       -
1295981543.474636       CWYQYVbrCo50ZuEoj       192.168.3.131   55955   207.46.148.38   80
Signatures::Sensitive_Signature HTTP-GET-sig    192.168.3.131: Found HTTP Request       GET /action/
MMN_Homepage HTTP/1.1\x0d\x0aHost: view.atdmt.com\x0d\x0aConnection: keep-alive\x0d\x0aReferer: http://
ca.msn.com/\x0d\x0aAccept: */*\x0d\x0aUser-Agent: Mozil...      -       -
1295981543.474636       -       192.168.3.131   -       -       -
Signatures::Multiple_Sig_Responders     HTTP-GET-sig    Found HTTP Request      192.168.3.131 has triggered
signature HTTP-GET-sig on 5 hosts       -       5
1295981543.528088       CqjleD2Yg0QLQkPIah      192.168.3.131   55956   66.235.139.121  80
Signatures::Sensitive_Signature HTTP-GET-sig    192.168.3.131: Found HTTP Request       GET /b/ss/
msnportalhomepagecaen/1/H.7-pdv-2/s84495919100008?
[AQB]&ndh=1&t=25%2F0%2F2011%2010%3A52%3A23%202%20480&ns=msnportal&pageName=MSN%2...      -       -
1295981543.536159       CYNmtk3bnYeS5vn29h      192.168.3.131   55957   65.55.5.232     80
```

The file is explained as follows:

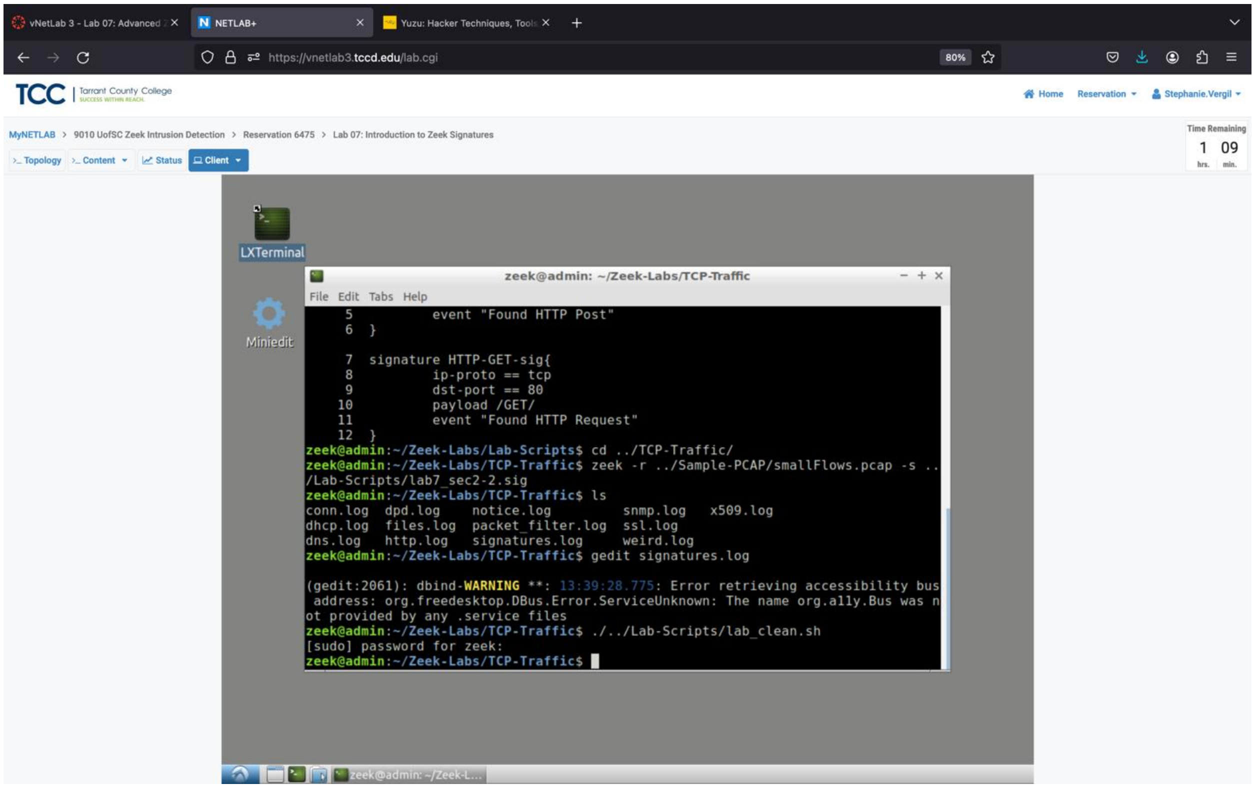
The red box indicates the name of the signature that was matched.

The orange box indicates the event or message that was included when defining the signature.

The blue box indicates the packet payload that was matched against the input signatures.

Step 5. Close the gedit window and enter the following command to clear the contents of the TCP-Traffic directory:

./ ../Lab-Scripts/lab_clean.sh


vNetLab 3 - Lab 07: Advanced
NETLAB+
Yuzu: Hacker Techniques, Tools
https://vnetlab3.tccd.edu/lab.cgi
80%
TCC | Tarrant County College
Home
Reservation
Stephanie.Vergil
MyNETLAB > 9010 UofSC Zeek Intrusion Detection > Reservation 6475 > Lab 07: Introduction to Zeek Signatures
Topology
Content
Status
Client
Time Remaining
1 hrs.
09 min.
LXTerminal
Miniedit
zeek@admin: ~/Zeek-Labs/TCP-Traffic
File
Edit
Tabs
Help
zeek@admin: ~/Zeek-L...

```
     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  }
zeek@admin:~/Zeek-Labs/Lab-Scripts$ cd ../TCP-Traffic/
zeek@admin:~/Zeek-Labs/TCP-Traffic$ zeek -r ../Sample-PCAP/smallFlows.pcap -s ..
/Lab-Scripts/lab7_sec2-2.sig
zeek@admin:~/Zeek-Labs/TCP-Traffic$ ls
conn.log  dpd.log    notice.log         snmp.log   x509.log
dhcp.log  files.log  packet_filter.log  ssl.log
dns.log   http.log   signatures.log     weird.log
zeek@admin:~/Zeek-Labs/TCP-Traffic$ gedit signatures.log

(gedit:2061): dbind-WARNING **: 13:39:28.775: Error retrieving accessibility bus
 address: org.freedesktop.DBus.Error.ServiceUnknown: The name org.a11y.Bus was n
ot provided by any .service files
zeek@admin:~/Zeek-Labs/TCP-Traffic$ ./../Lab-Scripts/lab_clean.sh
[sudo] password for zeek:
zeek@admin:~/Zeek-Labs/TCP-Traffic$ 
```

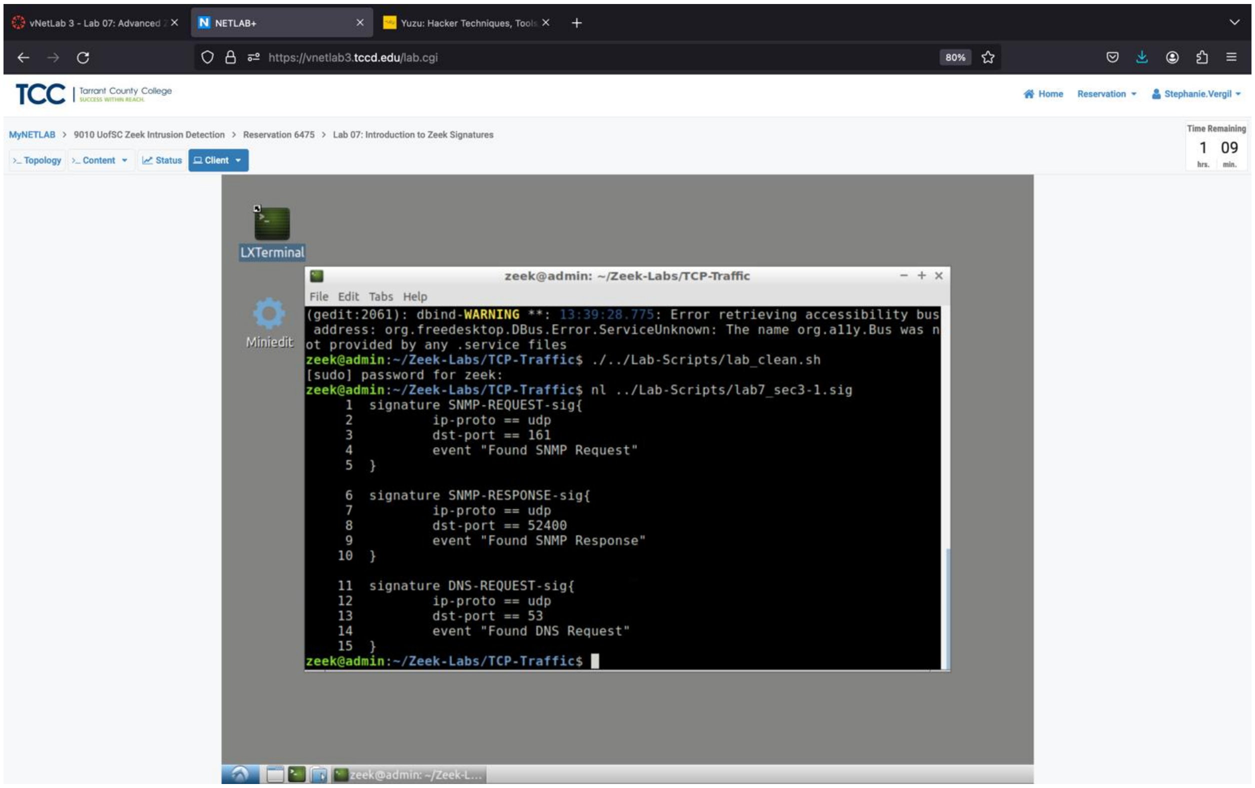
3 Executing Zeek signature matching for network traffic analysis

This section modifies the existing signature file to generate additional signature events and notices. We will be modifying the previous signatures from TCP-based HTTP messages to UDP-based SNMP and DNS messages.

3.1 Modifying the premade Zeek signature file.

Step 1. Enter the following command to view the contents of the lab7_sec3-1.sig file using nl:

nl ../Lab-Scripts/lab7_sec3-1.sig

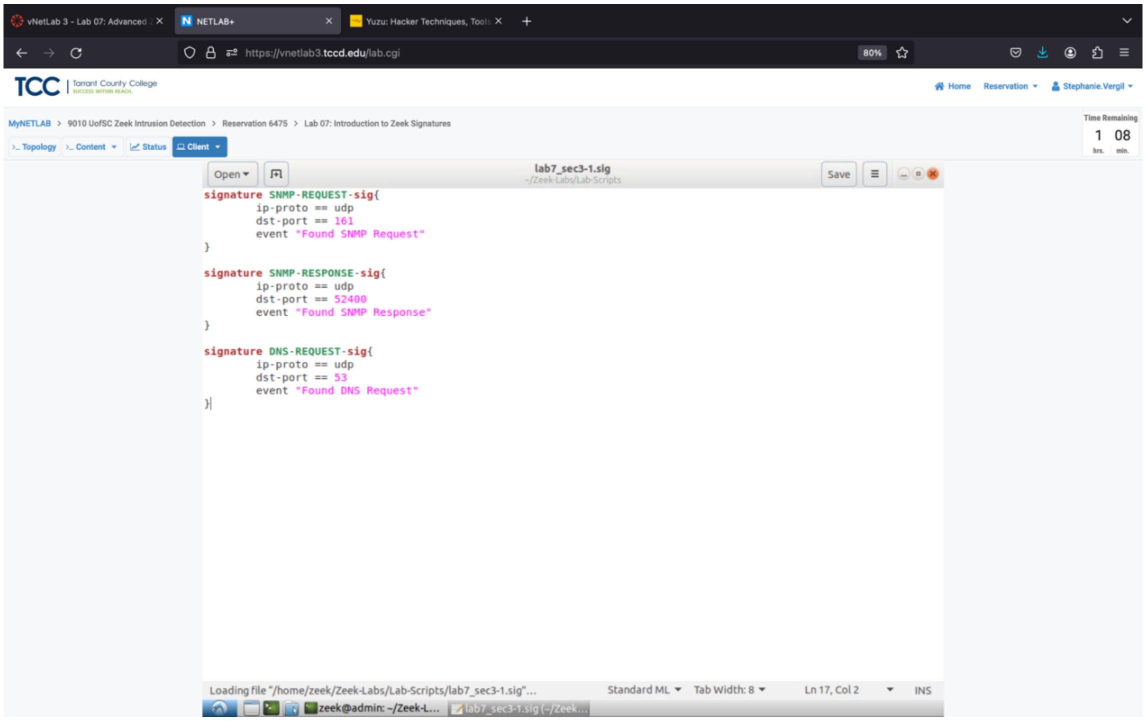

vNetLab 3 - Lab 07: Advanced
NETLAB+
Yuzu: Hacker Techniques, Tools
https://vnetlab3.tccd.edu/lab.cgi
80%
TCC | Tarrant County College
Home
Reservation
Stephanie.Vergil
MyNETLAB > 9010 UofSC Zeek Intrusion Detection > Reservation 6475 > Lab 07: Introduction to Zeek Signatures
Topology
Content
Status
Client
Time Remaining
1 hrs. 09 min.
LXTerminal
Miniedit
zeek@admin: ~/Zeek-Labs/TCP-Traffic
File Edit Tabs Help
zeek@admin: ~/Zeek-L...

```
(gedit:2061): dbind-WARNING **: 13:39:28.775: Error retrieving accessibility bus
 address: org.freedesktop.DBus.Error.ServiceUnknown: The name org.ally.Bus was n
ot provided by any .service files
zeek@admin:~/Zeek-Labs/TCP-Traffic$ ./../Lab-Scripts/lab_clean.sh
[sudo] password for zeek:
zeek@admin:~/Zeek-Labs/TCP-Traffic$ nl ../Lab-Scripts/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@admin:~/Zeek-Labs/TCP-Traffic$ 
```

Step 2. Enter the following command to open the lab7_sec3-1.sig file with the gedit text editor:

gedit ../Lab-Scripts/lab7_sec3-1.sig

Step 3. Update the lab7_sec3-1.sig file to include the following signatures. Then, close out the gedit once finish editing.



vNetLab 3 - Lab 07: Advanced
NETLAB+
Yuzu: Hacker Techniques, Tools
https://vnetlab3.tccd.edu/lab.cgi
80%
TCC | Tarrant County College
Home
Reservation
Stephanie.Vergil
MyNETLAB > 9010 UofSC Zeek Intrusion Detection > Reservation 6475 > Lab 07: Introduction to Zeek Signatures
Time Remaining
1 08
hrs. min.
Topology
Content
Status
Client
Open
lab7_sec3-1.sig
~/Zeek-Labs/Lab-Scripts
Save
Standard ML
Tab Width: 8
Ln 17, Col 2
INS
zeek@admin: ~/Zeek-L...
lab7_sec3-1.sig (~/Zeek...

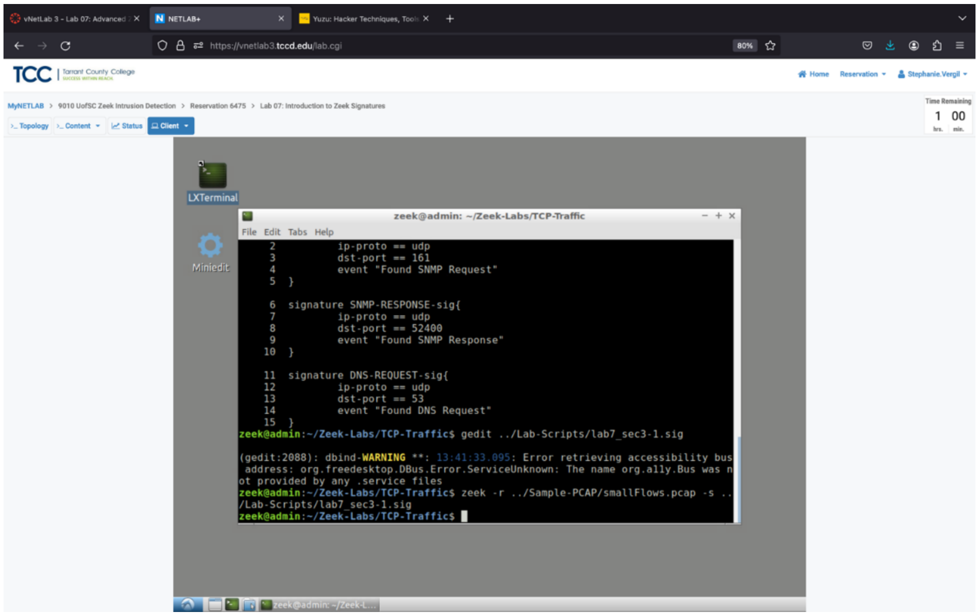
```
signature SNMP-REQUEST-sig{
        ip-proto == udp
        dst-port == 161
        event "Found SNMP Request"
}

signature SNMP-RESPONSE-sig{
        ip-proto == udp
        dst-port == 52400
        event "Found SNMP Response"
}

signature DNS-REQUEST-sig{
        ip-proto == udp
        dst-port == 53
        event "Found DNS Request"
}
```

```
Loading file "/home/zeek/Zeek-Labs/Lab-Scripts/lab7_sec3-1.sig"...
```

3.2 Executing the updated Zeek signature file.

Step 1. Enter the following command to process the smallFlows.pcap packet capture file using the signature file lab7_sec3-1.sig:

Zeek –r ../Sample-PCAP/smallFlows.pcap –s ../Lab-Scripts/lab7_sec3-1.sig

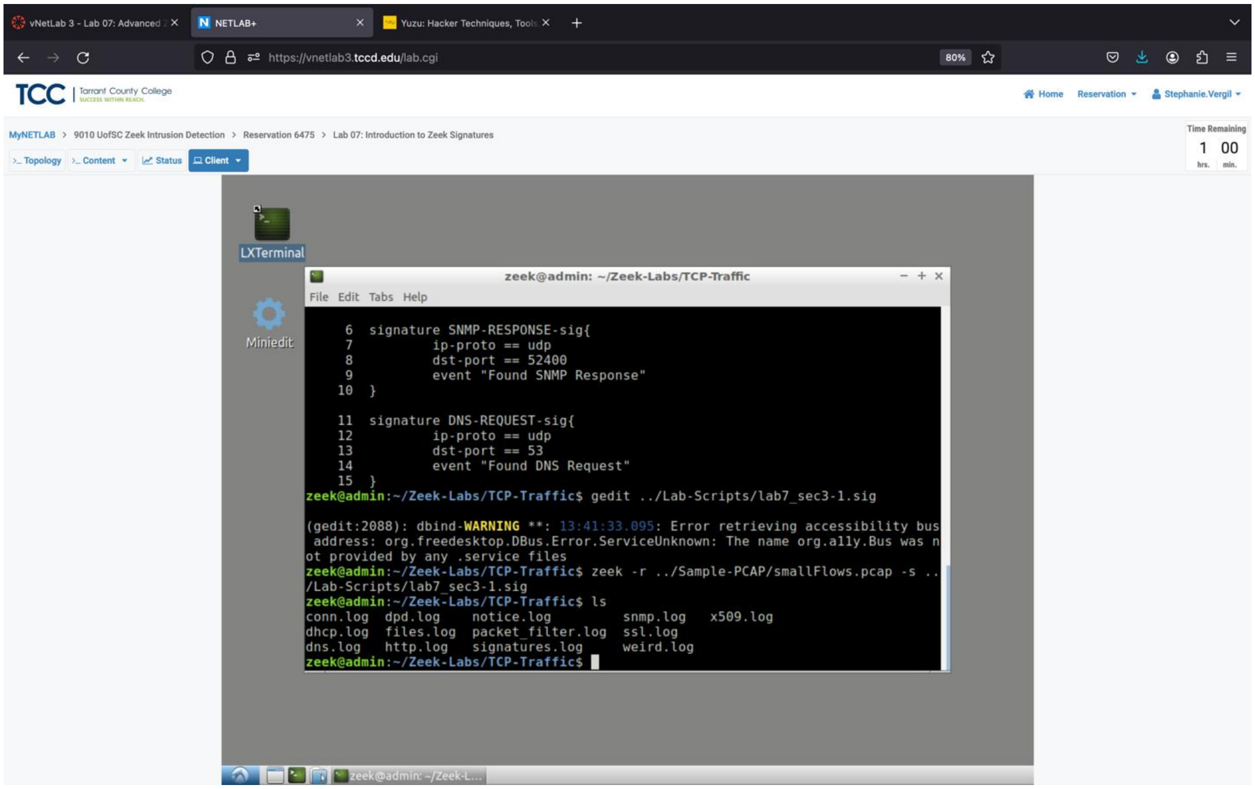


vNetLab 3 - Lab 07: Advanced
NETLAB+
Yuzu: Hacker Techniques, Tools
https://vnetlab3.tccd.edu/lab.cgi
80%
TCC | Tarrant County College
Home
Reservation
Stephanie.Vergil
MyNETLAB > 9010 UofSC Zeek Intrusion Detection > Reservation 6475 > Lab 07: Introduction to Zeek Signatures
Time Remaining
1 00
hrs. min.
Topology
Content
Status
Client
LXTerminal
Miniedit
zeek@admin: ~/Zeek-Labs/TCP-Traffic
File Edit Tabs Help
zeek@admin: ~/Zeek-L...

```
     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@admin:~/Zeek-Labs/TCP-Traffic$ gedit ../Lab-Scripts/lab7_sec3-1.sig

(gedit:2088): dbind-WARNING **: 13:41:33.095: Error retrieving accessibility bus
 address: org.freedesktop.DBus.Error.ServiceUnknown: The name org.ally.Bus was n
ot provided by any .service files
zeek@admin:~/Zeek-Labs/TCP-Traffic$ zeek -r ../Sample-PCAP/smallFlows.pcap -s ..
/Lab-Scripts/lab7_sec3-1.sig
zeek@admin:~/Zeek-Labs/TCP-Traffic$ 
```

Step 2. Enter the following command to list the generated log files in the current directory:

ls


vNetLab 3 - Lab 07: Advanced
NETLAB+
Yuzu: Hacker Techniques, Tools
https://vnetlab3.tccd.edu/lab.cgi
80%
TCC | Tarrant County College
Home
Reservation
Stephanie.Vergil
MyNETLAB > 9010 UofSC Zeek Intrusion Detection > Reservation 6475 > Lab 07: Introduction to Zeek Signatures
Topology
Content
Status
Client
Time Remaining
1 hrs. 00 min.
LXTerminal
Miniedit
zeek@admin: ~/Zeek-Labs/TCP-Traffic
File
Edit
Tabs
Help
zeek@admin: ~/Zeek-L...

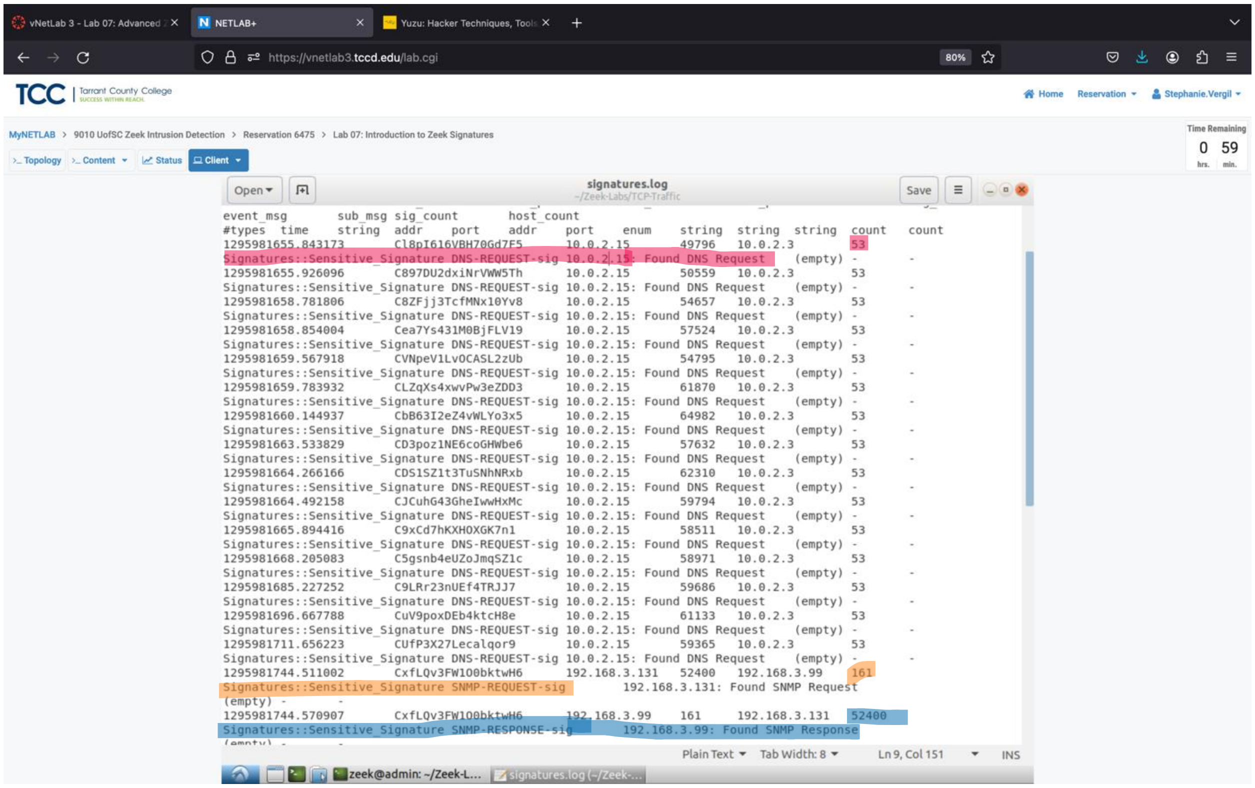
```
     6  signature SNMP-RESPONSE-sig{
     7          ip-proto == udp
     8          dst-port == 52400
     9          event "Found SNMP Response"
    10  }

    11  signature DNS-REQUEST-sig{
    12          ip-proto == udp
    13          dst-port == 53
    14          event "Found DNS Request"
    15  }
zeek@admin:~/Zeek-Labs/TCP-Traffic$ gedit ../Lab-Scripts/lab7_sec3-1.sig

(gedit:2088): dbind-WARNING **: 13:41:33.095: Error retrieving accessibility bus
 address: org.freedesktop.DBus.Error.ServiceUnknown: The name org.ally.Bus was n
ot provided by any .service files
zeek@admin:~/Zeek-Labs/TCP-Traffic$ zeek -r ../Sample-PCAP/smallFlows.pcap -s ..
/Lab-Scripts/lab7_sec3-1.sig
zeek@admin:~/Zeek-Labs/TCP-Traffic$ ls
conn.log  dpd.log    notice.log         snmp.log   x509.log
dhcp.log  files.log  packet_filter.log  ssl.log
dns.log   http.log   signatures.log     weird.log
zeek@admin:~/Zeek-Labs/TCP-Traffic$
```

The signatures.log file has been recreated and will contain the newly updated signature matches.

Step 3. Enter the following command to view the contents of the signatures.log file using the gedit text editor:

gedit signatures.log

Then, exit out the gedit.


vNetLab 3 - Lab 07: Advanced
NETLAB+
Yuzu: Hacker Techniques, Tools
https://vnetlab3.tccd.edu/lab.cgi
80%
TCC | Tarrant County College
SUCCESS WITHIN REACH.
Home
Reservation
Stephanie.Vergil
MyNETLAB > 9010 UofSC Zeek Intrusion Detection > Reservation 6475 > Lab 07: Introduction to Zeek Signatures
Topology
Content
Status
Client
Time Remaining
0 59
hrs. min.
Open
signatures.log
~/Zeek-Labs/TCP-Traffic
Save
Plain Text
Tab Width: 8
Ln 9, Col 151
INS
zeek@admin: ~/Zeek-L...
signatures.log (~/Zeek-...

```
event_msg       sub_msg sig_count       host_count
#types  time    string  addr    port    addr    port    enum    string  string  string  count   count
1295981655.843173       Cl8pI616VBH70Gd7F5      10.0.2.15       49796   10.0.2.3        53
Signatures::Sensitive_Signature DNS-REQUEST-sig 10.0.2.15: Found DNS Request    (empty) -       -
1295981655.926096       C897DU2dxiNrVWW5Th      10.0.2.15       50559   10.0.2.3        53
Signatures::Sensitive_Signature DNS-REQUEST-sig 10.0.2.15: Found DNS Request    (empty) -       -
1295981658.781806       C8ZFjj3TcfMNx10Yv8      10.0.2.15       54657   10.0.2.3        53
Signatures::Sensitive_Signature DNS-REQUEST-sig 10.0.2.15: Found DNS Request    (empty) -       -
1295981658.854004       Cea7Ys431M0BjFLV19      10.0.2.15       57524   10.0.2.3        53
Signatures::Sensitive_Signature DNS-REQUEST-sig 10.0.2.15: Found DNS Request    (empty) -       -
1295981659.567918       CVNpeV1LvOCASL2zUb      10.0.2.15       54795   10.0.2.3        53
Signatures::Sensitive_Signature DNS-REQUEST-sig 10.0.2.15: Found DNS Request    (empty) -       -
1295981659.783932       CLZqXs4xwvPw3eZDD3      10.0.2.15       61870   10.0.2.3        53
Signatures::Sensitive_Signature DNS-REQUEST-sig 10.0.2.15: Found DNS Request    (empty) -       -
1295981660.144937       CbB63I2eZ4vWLYo3x5      10.0.2.15       64982   10.0.2.3        53
Signatures::Sensitive_Signature DNS-REQUEST-sig 10.0.2.15: Found DNS Request    (empty) -       -
1295981663.533829       CD3poz1NE6coGHWbe6      10.0.2.15       57632   10.0.2.3        53
Signatures::Sensitive_Signature DNS-REQUEST-sig 10.0.2.15: Found DNS Request    (empty) -       -
1295981664.266166       CDS1SZ1t3TuSNhNRxb      10.0.2.15       62310   10.0.2.3        53
Signatures::Sensitive_Signature DNS-REQUEST-sig 10.0.2.15: Found DNS Request    (empty) -       -
1295981664.492158       CJCuhG43GheIwwHxMc      10.0.2.15       59794   10.0.2.3        53
Signatures::Sensitive_Signature DNS-REQUEST-sig 10.0.2.15: Found DNS Request    (empty) -       -
1295981665.894416       C9xCd7hKXHOXGK7n1       10.0.2.15       58511   10.0.2.3        53
Signatures::Sensitive_Signature DNS-REQUEST-sig 10.0.2.15: Found DNS Request    (empty) -       -
1295981668.205083       C5gsnb4eUZoJmqSZ1c      10.0.2.15       58971   10.0.2.3        53
Signatures::Sensitive_Signature DNS-REQUEST-sig 10.0.2.15: Found DNS Request    (empty) -       -
1295981685.227252       C9LRr23nUEf4TRJJ7       10.0.2.15       59686   10.0.2.3        53
Signatures::Sensitive_Signature DNS-REQUEST-sig 10.0.2.15: Found DNS Request    (empty) -       -
1295981696.667788       CuV9poxDEb4ktcH8e       10.0.2.15       61133   10.0.2.3        53
Signatures::Sensitive_Signature DNS-REQUEST-sig 10.0.2.15: Found DNS Request    (empty) -       -
1295981711.656223       CUfP3X27Lecalqor9       10.0.2.15       59365   10.0.2.3        53
Signatures::Sensitive_Signature DNS-REQUEST-sig 10.0.2.15: Found DNS Request    (empty) -       -
1295981744.511002       CxfLQv3FW1O0bktwH6      192.168.3.131   52400   192.168.3.99    161
Signatures::Sensitive_Signature SNMP-REQUEST-sig        192.168.3.131: Found SNMP Request
(empty) -       -
1295981744.570907       CxfLQv3FW1O0bktwH6      192.168.3.99    161     192.168.3.131   52400
Signatures::Sensitive_Signature SNMP-RESPONSE-sig       192.168.3.99: Found SNMP Response
(empty) -       -
```

The file is explained as follows:

The red box indicates the DNS-REQUEST-sig signature match as well as the triggered IP address and event message.

The orange box indicates the SNMP-REQUEST-sig signature match as well as the triggered IP address and event message.

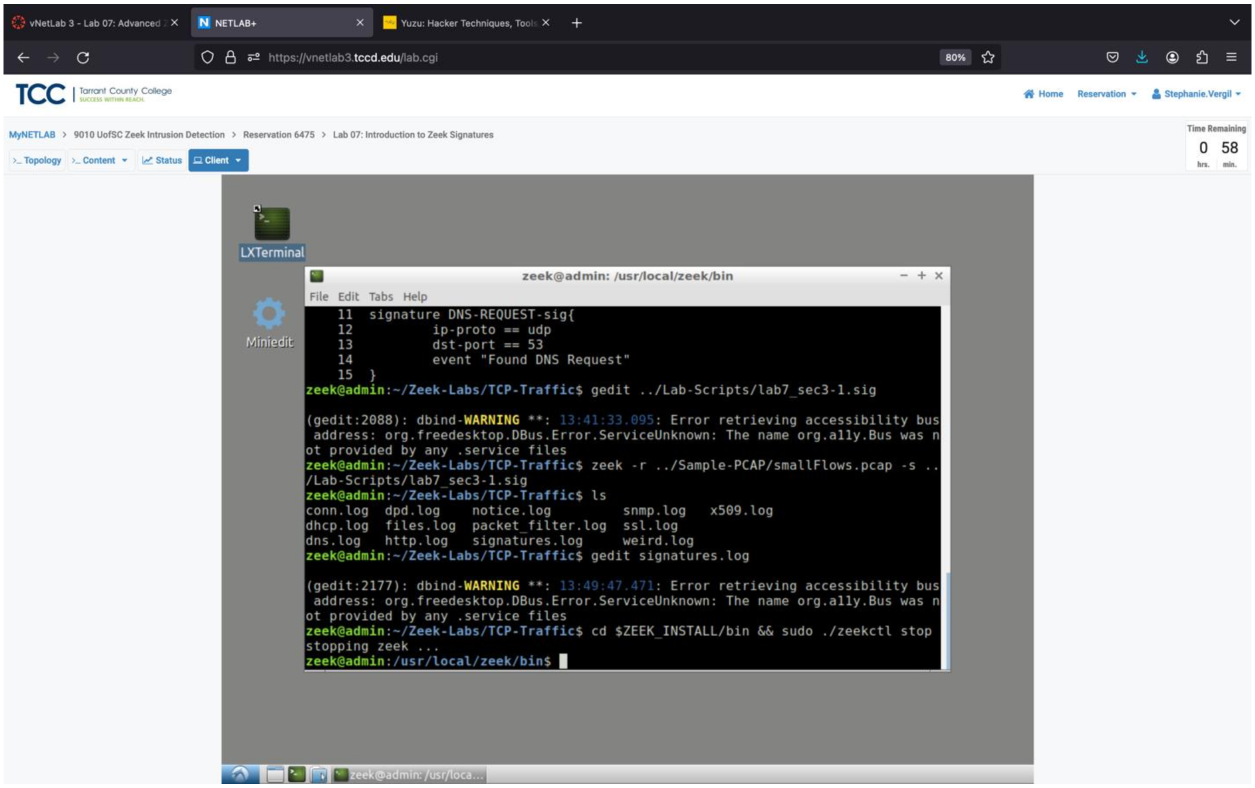
The blue box indicates the SNMP-RESPONSE-sig signature match as well as the triggered IP address and event message.

3.3 Closing the current instance of Zeek.

it is necessary to terminate the currently active instance of Zeek.

Step 1. Enter the following command to stop Zeek by entering the password if prompt:

```
cd $ZEEK_INSTALL/bin && sudo ./zeekctl stop
```


vNetLab 3 - Lab 07: Advanced
NETLAB+
Yuzu: Hacker Techniques, Tools
https://vnetlab3.tccd.edu/lab.cgi
80%
TCC | Tarrant County College
SUCCESS WITHIN REACH.
Home
Reservation
Stephanie.Vergil
MyNETLAB > 9010 UofSC Zeek Intrusion Detection > Reservation 6475 > Lab 07: Introduction to Zeek Signatures
Topology
Content
Status
Client
Time Remaining
0 hrs.
58 min.
LXTerminal
Miniedit
zeek@admin: /usr/local/zeek/bin
File
Edit
Tabs
Help
zeek@admin: /usr/loca...

```
    11  signature DNS-REQUEST-sig{
    12          ip-proto == udp
    13          dst-port == 53
    14          event "Found DNS Request"
    15  }
zeek@admin:~/Zeek-Labs/TCP-Traffic$ gedit ../Lab-Scripts/lab7_sec3-1.sig

(gedit:2088): dbind-WARNING **: 13:41:33.095: Error retrieving accessibility bus
 address: org.freedesktop.DBus.Error.ServiceUnknown: The name org.ally.Bus was n
ot provided by any .service files
zeek@admin:~/Zeek-Labs/TCP-Traffic$ zeek -r ../Sample-PCAP/smallFlows.pcap -s ..
/Lab-Scripts/lab7_sec3-1.sig
zeek@admin:~/Zeek-Labs/TCP-Traffic$ ls
conn.log  dpd.log    notice.log         snmp.log   x509.log
dhcp.log  files.log  packet_filter.log  ssl.log
dns.log   http.log   signatures.log     weird.log
zeek@admin:~/Zeek-Labs/TCP-Traffic$ gedit signatures.log

(gedit:2177): dbind-WARNING **: 13:49:47.471: Error retrieving accessibility bus
 address: org.freedesktop.DBus.Error.ServiceUnknown: The name org.ally.Bus was n
ot provided by any .service files
zeek@admin:~/Zeek-Labs/TCP-Traffic$ cd $ZEEK_INSTALL/bin && sudo ./zeekctl stop
stopping zeek ...
zeek@admin:/usr/local/zeek/bin$ 
```

Leveraging pattern matching, Zeek signatures can be used to quickly discover packets that follow predetermined formats, while employing a low-level framework for generating warnings and notifications.